# DHCP Protocol

bintec Dm730-I

## Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

# I Related Documents

bintec Dm702-I TCP-IP

bintec Dm723-I DNS

bintecDm754-I NSLA

bintec Dm775-I VRF-Lite Facility

# Chapter 1 Introduction

## 1.1 Introduction to the DHCP Protocol

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism to assign configuration information to clients on a TCP/IP network. DHCP has two main components: a protocol to deliver configuration data to the various clients from a DHCP server and a mechanism to store all the network addresses for the clients.

DHCP is built over a client-server model, whereby a designated DHCP server allocates network addresses and delivers the configuration parameters to the clients that are going to be dynamically configured. The DHCP server in **bintec Router**s has two mechanisms by which it can assign IP addresses. The first consists of dynamically providing IP addresses to DHCP clients for a limited period of time or until the client releases them (dynamic allocation). The second is where the network administrator predefines the IP addresses that must be assigned to the devices and the DHCP server transmits this information to the client (manual allocation).

Out of these, only the dynamic allocation mechanism allows IP addresses that are no longer needed by clients to be automatically reused. This is particularly useful when it comes to assigning addresses to clients that only connect to the network for a limited period of time, or when sharing a limited number of IP addresses among a group of clients that do not require permanent addresses. It can also be an excellent option for assigning addresses to a new client that is permanently connected to a network where the IP addresses are limited, in order to reclaim them when old clients resign.

The **bintec Router** can operate as a DHCP client, DHCP server and DHCP relay agent.

- A DHCP client dynamically obtains configuration parameters that allow it to initialize correctly in the network. When acting as a DHCP client, the **bintec Router** can get its IP address and default router (or *gateway*) from a DHCP server through the DHCP protocol. The offered address will only be accepted if it is on a different subnet to the IP addresses configured on the remaining interfaces.
- The relay agent forwards incoming messages from DHCP clients on the same network to one or more known DHCP servers.
- The DHCP server assigns IP addresses and other configuration parameters to clients that request them.

The DHCP protocol is designed to provide DHCP clients with the configuration parameters defined in the Host Specifications RFCs. Once the configuration parameters have been obtained through DHCP, the clients should be able to exchange packets with other intranet or Internet devices, provided those addresses remain available. A client and a server can *negotiate* the concession of client-specific parameters or subnet-specific parameters.

While not required, DHCP can also be used to transfer other configuration parameters such as DNS ( *Domain Name System*) addresses.

## 1.2 Protocol

The DHCP protocol is built over a client/server architecture. The interaction between client and server is described below. Some of the steps are omitted when the client already knows its address.

The first step for the client is to send a DHCPDISCOVER broadcast message on its physical subnet. This message may suggest values for the lease time and network address (but will be empty if it comes from a **bintec Router** acting as client). If the server is on a different subnet, the DHCPDISCOVER message reaches it via a relay agent (this is a device that forwards requests between clients and servers on different subnets).

Each server can respond with a DHCPOFFER message that includes a valid network address and other configuration parameters.

The following table details the different types of DHCP messages:

| **Message** | **Use** |
|---|---|
| DHCPDISCOVER | Client broadcast to locate available servers. |
| DHCPOFFER | From server to client, in response to a DHCPDISCOVER message. These messages contain configuration parameters. |
| DHCPREQUEST | Client broadcast to servers:<br>a) requesting some parameters offered by one of the servers,<br>b) confirming the stored address correction after rebooting the system, or<br>c) extending the lease for the assigned address. |
| DHCPACK | From server to client, these messages contain configuration parameters including |

| | |
|---|---|
| | the assigned network address. |
| DHCPNAK | From server to client, these messages indicate that the client network address is incorrect or its lease has expired. |
| DHCPDECLINE | From client to server, these messages indicate the address is in use. |
| DHCPRELEASE | From client to server, these messages release the assigned network address and cancel the lease granted. |
| DHCPINFORM | From client to server, these messages request local configuration parameters. The client has already received the address externally. |

The DHCP client receives one or more DHCPOFFER messages from one or more servers. The client can expect multiple responses. The client chooses a server from whom to request the configuration parameters, basing this choice on the configuration parameters that the server offered in the DHCPOFFER messages. The client broadcasts the DHCPREQUEST message indicating the identity of the selected server in it. The value for the received address should be in the *yiaddr* field of the server's DHCPOFFER message. The DHCPREQUEST message should be sent to all the servers who received the DHCPDISCOVER message so they can reuse the originally offered address.

The selected server permanently stores the information on the lease and responds with a DHCPACK containing the configuration parameters. If it cannot do this for any reason, the server responds with a DHCPNAK.

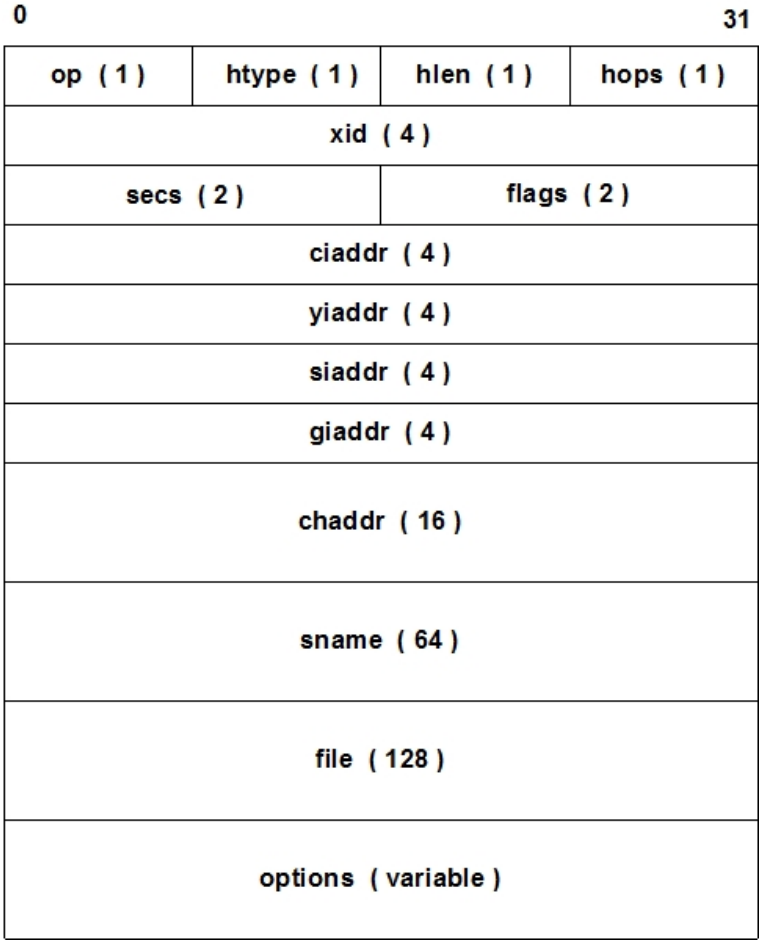
The client receives the DHCPACK confirmation message and configures once he has validated the assigned address. If he cannot validate the address, he sends a DHCPDECLINE message informing the server. If he receives a DHCPNAK message, the process begins anew.

The client can release the address lease provided by the server by simply sending a DHCPRELEASE message to the server containing the information on the assigned address.

All the messages mentioned above are UDP packets. The format for these packets is explained below.

### 1.2.1 Message Format

The DHCP protocol exchanges messages with the following format:




The meaning of each of the fields is as follows:

#### 1.2.1.1 OP (TYPE OF MESSAGE)

1 octet. Type of DHCP message being sent.

#### 1.2.1.2 HTYPE (TYPE OF HARDWARE ADDRESS)

1 octet. Indicates the type of hardware address (Ethernet, Token Ring etc.).

#### 1.2.1.3 HLEN (LENGTH OF HARDWARE ADDRESS)

1 octet. Length of hardware address (6 in the cases of Ethernet and Token Ring).

#### 1.2.1.4 HOPS

1 octet. The client is set to zero. This value can sometimes change, however, when a message is sent via a relay agent.

#### 1.2.1.5 XID (TRANSACTION IDENTIFIER)

4 octets. Random identifier to associate the messages and responses between a client and a server.

#### 1.2.1.6 SECS (SECONDS)

2 octets. Filled out by the client, this indicates the seconds from the moment the client initiates the petition process or configuration renewal.

#### 1.2.1.7 FLAGS

2 octets.

#### 1.2.1.8 CIADDR (CLIENT ADDRESS)

4 octets. Client IP address. This is only filled out if the client is in renewal procedure and can respond to ARP petitions.

#### 1.2.1.9 YIADDR (ASSIGNED IP ADDRESS)

4 octets. IP address assigned to the client. This is filled out in the server responses.

#### 1.2.1.10 SIADDR (NEXT SERVER IP ADDRESS)

4 octets. IP address for the next server used in the starting process (when the client is told to download certain files from a specific server).

#### 1.2.1.11 GIADDR (RELAY AGENT IP ADDRESS)

4 octets. IP address for the relay agent when addresses are being assigned through a relay.

#### 1.2.1.12 CHADDR (CLIENT HARDWARE ADDRESS)

16 octets. Client hardware address.

#### 1.2.1.13 SNAME (SERVER NAME)

64 octets. Optional parameter: DHCP server name.

#### 1.2.1.14 FILE (FILE NAME)

128 octets. Boot file name. This is only filled out in DHCPOFFER.

#### 1.2.1.15 OPTIONS

Variable length field where the configuration options are specified. The minimum length should be 312 octets so the packet is equal to a minimum IP packet size.

# Chapter 2 Configuration

## 2.1 DHCP protocol configuration

The **bintec Router** can be configured as a DHCP client, a DHCP server or a DHCP relay agent.

The DHCP client requests IP addresses and other configuration parameters that enable it to initialize in the network. To do this, the client sends broadcast messages to the servers or agents on the same physical subnet, beginning with the exchange of DHCP messages leading to an address being given to the client by a server. The **bintec Router** is capable of dynamically acquiring the IP address (and the associated mask) and the default *gateway* or route. To enable this behavior, simply indicate this has been dynamically obtained using the DHCP protocol when configuring an IP address in an Ethernet interface or subinterface.

A **bintec Router** acting as a DHCP client can also act as a DHCP server and relay agent. The basic configuration (necessary or minimum) for a DHCP client is executed outside of the menu corresponding to the DHCP protocol and does not interfere with the device's other two behavior modes.

A DHCP relay is designed to capture DHCP messages in a LAN generated by potential clients connected to it, and to send them to one or more known DHCP servers located outside the LAN. The relay is needed as the messages generated by the clients are sent through a broadcast within the LAN when clients have not yet been configured (they are going to be configured through DHCP) and do not know their IP address or the server address. As a result, if there is no server in the LAN itself, a relay is needed to convert the messages sent through broadcast to unicast, which can then be rerouted to a known server outside the LAN. Consequently, for the **bintec Router** to function as relay, all it needs to know is the list containing one or more DHCP servers. Optionally, the source IP address used to transmit the DHCP messages from the relay to the server and the relay agent IP address are configurable i.e., the address sent in the *giaddr* field. Additionally, it's possible to indicate, where the scenario needs it, the VRF through which the DHCP server is accessed when the latter and the DHCP client are not on the same VPN (please see manual bintec Dm775-I VRF-Lite Facility).

For a router to behave as a DHCP server, the configuration is more complex. On the one hand, it must be able to present the *subnets* topology to those who are going to provide DHCP service bearing in mind that some of the *subnets* may not be directly connected (those that are accessed through a relay); on the other hand, a policy for assigning addresses must be set.

To represent the subnets topology to those who are going to provide DHCP service, concepts for *Shared Network, Subnet Host* and *Class* are available. Normally each router interface supporting DHCP has to create a *shared network*. For example, if the device has a Token Ring interface and another one has Ethernet, (or 2 Ethernet interfaces connected to physically separated subnets), two *shared networks* are created. Additionally, you can create as many *shared networks* as physical segments have access to through relays. As you can see, this concept is intimately tied to each physical segment over which the DHCP is going to act.

Once you have created as many *shared networks* as necessary, you can associate each one to distinct *subnets*, *hosts* (devices) and *classes* (special devices). Normally there is one single *subnet* in each *shared network*, but one physical segment may also support various subnets and classes so diverse *subnet*s and *classes* can be configured. The *hosts* identify the possible DHCP clients present in a physical segment (*shared network*). Identifying each and every potential client that is going to send petitions in the server is not necessary. Whether to identify them or not is part of the address assignment policy that must be set. On the other hand, a *host* can be configured for several *shared networks*. This is very useful when the same *host* can connect to various distinct physical segments.

Once the server is operating, it responds to the client's petitions and provides an IP address for a specified time. This is known as a *lease*. Depending on the physical interface where the client petition enters, the server assigns a *shared network* address or a different one. The server has a wide range of addresses in each *shared network* that it can distribute. Additionally, the concept of *class* lets you define one or more reserved IP address ranges to a determined type of client, which are identified through the DHCP protocol option 60 (vendor-class-identifier option). It is also possible to set a specific address for a determined client (this can be configured at the same time as creating the *host*). In this case, the address is not reused for other clients when the owner is not connected as it is permanently assigned to the latter.

When a client receives a *lease* from a server, he not only receives an IP address but also other configuration parameters. These parameters are known as options and are encoded in DHCP packets. You can configure various options at a global level and at a *subnet*, *host*, and *class* level in the **bintec Router**. Naturally, if the *host* has a particular option configured, this value prevails over those configured at a *class* and *subnet* level. Options configured at *class* level prevail over those configured at *subnet* level. Similarly, options configured at a *subnet* level prevail over those configured at a global level. For example, an option value configured at a global level is only sent if there is no value configured for this option in the *subnet*, or in the *class*, or in the *host*.

There are other parameters that are not options and which can also be configured. These parameters let you set, for example, the maximum time an address *lease* can last, the possibility of distributing addresses to unknown clients or not (i.e., clients who are not declared in the configuration as *hosts*), etc. These parameters are important for protocol

operation as, for example, the *lease* duration time determines who often clients try to renew it. Another parameter (configurable at the *subnet* level) is the *Server Identifier*; this is the DHCP server IP address. This address is used by the client to communicate with the server from the moment the client receives an address (e.g., to renew it when the *lease* time has expired). The server by default sets an address from the interface as a *server identifier*. This address is from the same *subnet* where the *lease* is assigned. However, there are times when this parameter must be manually configured (e.g., to configure a client through a relay). In this case, you normally configure the address pertaining to the relay in the client's LAN as the *server identifier*.

## 2.2 Backup DHCP Server for a Relay Agent

The **bintec Router** allows you to activate or deactivate a DHCP server *shared network* depending on the results of an *advisor* belonging to the bintec NSLA feature. In turn, the DHCP relay feature can be monitored to detect drops in the DHCP servers configured in the relay and update a *level indicator* for the NSLA feature if the connection drops. Thus, it's possible to configure the *shared network* for the router's DHCP server so they activate as backup on detecting drops in the servers the DHCP packets are being forwarded to. For further information on the configuration of the NSLA feature, please see manual bintec Dm754-I – NSLA.

The Relay agent is assigned a previously configured level indicator using NSLA. This level indicator increases when it detects all the servers configured in the Relay agent are inaccessible. Depending on the indicator level, an *advisor,* also configured through NSLA, activates or deactivates. On the router's DHCP server side, configure a *shared network* to specify that this state is controlled by said *advisor*. When the *advisor* activates, the *shared network* enables and begins to provide service for the DHCP petitions being received.

The level indicator updates when the Relay Agent makes a transition from the following states:

- UP: when at least one of the DHCP servers configured in the agent responds to the DHCPDISCOVER packets.
- DOWN: when none of the configured DHCP servers respond to DHCPDISCOVER packets.

The state of the Relay agent depends on the availability of the servers it has configured. To determine availability for a specific server, the number of DHCPDISCOVER packets that have been forwarded to said server without receiving a response is monitored. When the number of packets reach the threshold value, the Relay Agent assumes said server is no longer available and establishes the server state as down. If, at some point, the agent receives a packet from this server, the counter goes back to zero and the agent assumes the server is available once again.

Once the Relay agent has moved from UP to DOWN, a monitoring process begins to see if one of the servers that was down is now up. DHCPDISCOVER packets are periodically sent to force a client to request a new IP address. The **bintec Router** offers the option of configuring this monitoring process so that it is continuous, thus providing early detection should a server go down.

Server monitoring depends on three parameters:

- Packet threshold: this is the number of DHCPDISCOVER packets consecutively transmitted to a server without receiving any response. At this point, the server is considered down or inaccessible.
- Monitoring interval: when monitoring for a server state is activated, this is the time interval between two DHCPDISCOVER packets generated by the Relay Agent itself.
- Monitoring mode: there are two operating modes. In the default mode, the monitoring only activates when a Relay Agent passes to a DOWN state and deactivates when the agent switches back to UP. In the second mode, the monitoring process is continuous regardless of the state of the Relay Agent.

A server can be configured in various Relay Agents. In this case, when a change in the state of a server is detected by a Relay Agent, it affects all agents monitoring the server.

In order for a **bintec Router**'s DHCP server to offer backup for a Relay Agent, a *shared network* is configured so that it is controlled by an *advisor*. This *shared network* remains disabled until said *advisor* activates because an indicator has been updated. Once the backup server has activated, on enabling the *shared network*, its function is exactly the same as any other DHCP server located in this network segment.

If a backup server's *shared network* has been deactivated by an *advisor*, a DHCPNACK answer is sent to a received DHCPREQUEST packet asking to extend the concession of an IP address previously assigned by said server. Consequently, the process in the client to obtain a new IP is relaunched and, this time, assigned by another server.

**Note**

To prevent conflicts, it is very important that the address ranges assigned by the DHCP servers in the Relay Agent and the backup server do not overlap.

## 2.3 DHCP protocol configuration commands

As already explained, a DHCP client dynamically acquires its configuration from the network using the DHCP protocol. It's possible to enable this behavior in the Ethernet interfaces and subinterfaces in the **bintec Router**: to do this, simply add a *dhcp-negotiated* IP address, which implies initiating the message exchange process that leads a DHCP server to loan a given configuration to the client (*lease*) for a certain amount of time. To disable the DHCP client in an interface, simply delete the previously configured *dhcp-negotiated* IP address.

In the **bintec Router**, there is a menu associated with the configuration for the DHCP client where you can configure, among other things, the administrative distance for the routes acquired by the client and the DHCP 60 option (vendor-class-identifier option).

### 2.3.1 Enabling DHCP client in an interface

To enable the DHCP client in an Ethernet interface or subinterface, enter the **ip address dhcp-negotiated** command from the configuration menu of the interface itself.

*Example:*

```
*config
Config>network ethernet0/0
-- Ethernet Interface User Configuration --
ethernet0/0 config>ip address dhcp-negotiated
ethernet0/0 config>
```

When this command is entered from the dynamic configuration process (P5 or running-config), the device immediately begins to behave as a DHCP client, initiating message exchange with the servers or relay agents in the network (which connect through this particular interface). If, however, the behavior is enabled as DHCP client from the static configuration process (P4 or config), save the configuration and restart the device to activate this functionality. In either case, the process ends with the DHCP server loaning an IP address with its associated mask and a default *gateway*. On receiving these parameters, the device associates the received IP address and its mask to the interface involved in the process, and adds the a default route to the static route tables whose next hop is the indicated *gateway*.

To disable the DHCP client functionality, delete the IP address by entering **no ip address dhcp-negotiated**.

*Example:*

```
ethernet0/0 config>no ip address dhcp-negotiated
ethernet0/0 config>
```

## 2.4 Accessing the DHCP client, DHCP Server and DHCP relay configuration

This section explains all the steps required to configure the DHCP protocol in the **bintec Router** when it acts as a DHCP client, DHCP server or relay agent. If you configure the DHCP protocol in the static configuration menu (***config**, ***process 4**), you need to save the setting and restart the device for it to take effect. If said configuration is carried out in the dynamic configuration menu (***running-config**, ***process 5**), you do not need to restart the device as the changes are dynamically applied. However, if you wish to maintain this configuration for the next device boot, you will need to save it.

To access the DHCP protocol static configuration environment, enter the following commands:

```
*config
Config>protocol dhcp
-- DHCP Configuration --
DHCP config>
```

To access the DHCP protocol dynamic configuration environment, enter the following commands:

```
*running-config
Config$protocol dhcp
-- DHCP Configuration --
DHCP config$
```

The following commands are available within the DHCP protocol configuration environment:

| Command | Function |
|---|---|
| *? (HELP)* | Lists the available commands or their options. |

| | |
|---|---|
| *CLIENT* | Accesses the configuration of specific parameters for the DHCP client. |
| *LIST* | Lists the information for the router operation mode (relay or server). |
| *RELAY* | Enters the configuration of the relay configuration parameters. |
| *SERVER* | Enters the configuration of the server configuration parameters. |
| *EXIT* | Exits the DHCP configuration prompt. |

### 2.4.1 ? (HELP)

Lists the valid commands at the level the router is programmed. You can also use it after a specific command to list the available options.

*Syntax:*

```
DHCP config>?
```

*Example:*

```
DHCP config>?
  client     Access the DHCP Client configuration menu
  list       List configuration
  relay      Access the DHCP Relay configuration menu
  server     Access the DHCP Server configuration menu
  exit
DHCP config>
```

### 2.4.2 CLIENT

Lets you access the DHCP client configuration menu where you can configure the DHCP client parameters.

*Syntax:*

```
DHCP config>CLIENT
```

*Example:*

```
DHCP config>client
-- DHCP Client Configuration --
DHCP-Client config>
```

### 2.4.3 LIST

Displays the **bintec Router**s DHCP operating mode: DHCP relay agent, DHCP server, both or neither. The relay agent is enabled through VRF, in which case enabled VRFs will appear.

*Syntax:*

```
DHCP config>LIST
```

*Example:*

```
DHCP config>list
DHCP-Relay enabled in "main" VRF
DHCP-Server enabled

DHCP config>
```

### 2.4.4 RELAY

Lets you access the DHCP Relay configuration menu, where you can configure proprietary DHCP Relay parameters.

Syntax:

```
DHCP config>RELAY
```

Example:

```
DHCP config>relay
-- DHCP Relay Configuration --
DHCP-Relay config>
```

### 2.4.5 SERVER

Accesses the DHCP Server configuration menu.

*Syntax:*

```
DHCP config>SERVER
```

*Example:*

```
DHCP config>server
-- DHCP Server Configuration --
DHCP-Server config>
```

### 2.4.6 EXIT

Exits the DHCP protocol configuration environment. Returns to the general configuration prompt.

*Syntax:*

```
DHCP config>EXIT
```

*Syntax:*

```
DHCP config>exit
Config>
```

## 2.5 DHCP Client Configuration Commands

A specific configuration for the DHCP client can be executed for each VRF configured in a **bintec Router**. Parameters configured from the main DHCP client menu apply to the global VRF. To configure DHCP client parameters associated with a given VRF, access the DHCP client VRF configuration menu using the **VRF** command.

Any interface capable of acting as a DHCP client belongs to a given VRF. Where this exists, a DHCP client uses the parameters defined for the VRF associated with said interface.

### 2.5.1 Configuration Commands for Client mode

Once in the configuration menu for the *DHCP client* operating mode, the following options are presented:

| Command | Function |
|---|---|
| *? (HELP)* | Lists the commands or the available options. |
| *CLIENT-ID* | Configures a value for the DHCP option 61 to be sent by the client. |
| *DISTANCE* | Modifies the administrative distance for the routes learned through the DHCP client. |
| *HOSTNAME* | Configures a value for the DHCP 12 option to be sent by the client. |
| *LIST* | Lists the information on the client operating mode. |
| *NO* | Eliminates or resets the default value. |
| SKIP-IP-CHECKING | Avoids checking IPs on configured interfaces. |
| *VENDOR-CLASS-IDENTIFIER* | Configures a value for the DHCP 60 option to be sent by the client. |
| *VENDOR-OPTION-KEYWORD* | Allows you to configure a key word to distinguish between the DHCP offers from the servers: this is found in option 43. |
| *VRF* | Specific configuration for the DHCP client in a VRF. |
| *EXIT* | Command to exit the DHCP client mode configuration menu. |

### 2.5.2 ? (HELP)

Displays the configuration commands available for the DHCP client mode.

*Syntax:*

```
DHCP-Client config>?
```

*Example:*

```
DHCP-Client config>?
  client-id                Client identifier
  distance                 Administrative distance for routes learnt through dhcp
  hostname                 Hostname (option 12)
  list                     List DHCP client configuration
  no                       Negate a command or set its defaults
  vendor-class-identifier  Vendor-class identifier
  vendor-option-keyword    Keyword in vendor option to accept lease
  vrf                      VRF specific configuration
  exit
```

### 2.5.3 [NO] CLIENT-ID <format><value>

Configures a value for the DHCP option 61 (client-identifier). This value allows you to identify the client in the servers so the latter can select a specific address in their allocation tables. We recommend using a value that uniquely identifies the device and doesn't coincide with identifications configured for other devices. There are two formats: *ascii* (string of ASCII characters) and *hex* (string of hexadecimal characters). The ASCII character string cannot contain spaces or inverted commas.

*Syntax:*

```
DHCP-Client config>client-id <format> <value>
```

*Example:*

```
DHCP-Client config>client-id ascii router_bintec
DHCP-Client config>
```

### 2.5.4 [NO] DISTANCE

Sets the administrative distance for routes learned through the DHCP client.

For further information on administrative distance, please see the **administrative-distance** command found in manual bintec Dm702-I TCP-IP. The default value is 254.

*Syntax:*

```
DHCP-Client config>distance ?
  <10..255>    Value in the specified range
```

*Example:*

```
DHCP-Client config>distance 30
DHCP-Client config>
```

### 2.5.5 [NO] HOSTNAME {GLOBAL | specific <string>}

Configures the option 12 value that the DHCP client sends in its messages. The *global* option causes the DHCP client to send, where available, the hostname value configured in the device. The *specific* value causes the DHCP client to send the indicated string (without any blank spaces or quotation marks).

*Syntax:*

```
DHCP-Client config>hostname {global | specific <string>}
```

*Example:*

```
DHCP-Client config>hostname specific bintec-ISP
```

### 2.5.6 LIST

Lists the information associated with the DHCP client in each of the configured VRFs.

*Syntax:*

```
DHCP-Client config>list
```

*Example:*

```
DHCP-Client config>list
 ============================
 =       DHCP client        =
 ============================
        Global configuration

                Administrative distance: 34
                Vendor-class-identifier: sample super
                Hostname (option 12):    sample-ISP (specific)

        Specific configuration of VRF "vrf-51"

                Administrative distance: 51
                Vendor-class-identifier: sample-vrf-51
                Hostname (option 12):    [not enabled] (default)

        Specific configuration of VRF "vrf-52"

                Administrative distance: 52
                Vendor-class-identifier: 0x00112233445566778899aabbccddeeff
                Hostname (option 12):    [no global hostname configured]

        Specific configuration of VRF "vrf-53"

                Administrative distance: 53
                Vendor-class-identifier: router-sample-vrf-53
                Hostname (option 12):    MYROUTER (global)

DHCP-Client config>
```

### 2.5.7 [NO] SKIP-IP-CHECKING

Avoids checking if the IP offered has already been assigned, or if it is in the same subnet as any other IP configured in an interface belonging to the same VRF.

*Syntax:*

```
DHCP-Client config>skip-ip-checking
```

*Example:*

```
DHCP-Client config>skip-ip-checking
DHCP-Client config>
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*[no]skip-ip-checking*" command has been added as of version 11.01.09. |

### 2.5.8 VENDOR-CLASS-IDENTIFIER <format><value>

Configures a value for DHCP option 60 (vendor-class-identifier). This value overwrites the default value sent by a **bintec Router** when it acts as a DHCP client. There are two types of format: *ascii* (ADCII character string) and *hex* (hexadecimal character string).

*Syntax:*

```
DHCP-Client config>vendor-class-identifier <format> <value>
```

*Example:*

```
DHCP-Client config>vendor-class-identifier ascii router_bintec
DHCP-Client config>
```

### 2.5.9 [NO] VENDOR-OPTION-KEYWORD <value>

Configures a value to distinguish between server offers. This value allows you to identify the servers' offers through option 43. If a received offer doesn't contain the *vendor-option-keyword* value (configured at the beginning of option 43), it is rejected. This value must be a string of ASCII characters. It cannot contain spaces or inverted commas, and must have a maximum length of 64 characters.

*Syntax:*

```
DHCP-Client config>vendor-option-keyword <value>
```

*Example:*

```
DHCP-Client config>vendor-option-keyword antenna
DHCP-Client config>
```

### 2.5.10 VRF <vrf_name>

Accesses, from the command line, the configuration menu for the DHCP client parameters belonging to the VRF specified.

*Syntax:*

```
DHCP-Client config>vrf <vrf_name>
```

*Example:*

```
DHCP-Client config>vrf vrf-52
DHCP-Client vrf config>
```

### 2.5.11 EXIT

Exits the DHCP client configuration menu.

*Syntax:*

```
DHCP-Client config>exit
```

*Example:*

```
DHCP-Client config>exit
DHCP config>
```

## 2.6 DHCP Relay Configuration Commands

Relay configuration can be carried out in two ways. The first is done from the DHCP protocol configuration menu and involves a global configuration applied to all of the router's physical interfaces where the relay agent can operate. By default, the configuration defined in the DHCP-Relay main menu is applied to the router's global VRF. To carry out a relay configuration in a specific VRF, access the relay parameters configuration menu for VRF.

Additionally, you can enable the agent in just some of the router interfaces, optionally specifying the typical configuration parameters for the relay agent for this interface. This is carried out in the interface configuration menu. The second way to do this takes precedence over the first. For further details on the second configuration mode, please see manual bintec Dm702-I TCP-IP Configuration.

### 2.6.1 RELAY mode configuration commands

Once in the configuration menu for the Relay functionality mode, the following options are presented:

| Command | Function |
|---|---|
| *? (HELP)* | Lists the commands or their available options. |
| *AGENT-INFORMATION* | Inserts information on the relay agent (DHCP option 82) in the packets destined to the DHCP server. |
| *ENABLE* | Enables DHCP relay in all the interfaces. |
| *GIADDR* | Configures the relay agent IP address. |
| *MONITOR-OPTIONS* | Configures the monitoring options for servers. |
| *NO* | Deletes a previously added DHCP server or restores the source address the pack- |

| | |
|---|---|
| | ets sent by the relay must exit with, or the relay agent IP address (giaddr) to its default value (automatic choice). |
| *SERVER* | Adds or modifies a DHCP server. |
| *SOURCE-ADDRESS* | Configures the source IP address for the Relay agent packets. |
| *UPDATE* | Configures the updating for an NSLA level indicator. |
| *VRF* | Specifies parameters for a VRF instance. |
| *EXIT* | Command to exit the Relay agent configuration menu. |

### 2.6.2 ? (HELP)

Displays all the available configuration commands for the server mode.

*Syntax:*

```
DHCP-Relay config>?
```

*Example:*

```
DHCP-Relay config>?
  agent-information    Insert relay agent information in forwarded packets
  enable               Enable the DHCP Relay agent
  giaddr               Relay agent IP address (giaddr)
  monitor-options      Configure options for relay monitoring
  no                   Negate a command or set its defaults
  server               Add a new DHCP server or change an existing one
  source-address       Source IP address for DHCP relay packets
  update               Update a level indicator
  vrf                  Specify parameters for a VPN Routing/Forwarding instance
  exit
```

### 2.6.3 AGENT-INFORMATION

Through this command, you can enable the feature by which the relay agent inserts information associated with the interface/VPN from which packets from DHCP clients arrive. This information is used in DHCP servers that support this feature to select configuration parameters to send to a client.

*Syntax:*

```
DHCP-Relay config>AGENT-INFORMATION <option> [<value>]
```

#### 2.6.3.1 AGENT-INFORMATION HEX <VALUE>

Configures the option 82 data field in hexadecimal, which the relay agent inserts in the packets received by the interfaces pertaining to the main VRF, before being forwarded to the DHCP server.

*Example:*

```
DHCP-Relay vrf config>agent-information hex 0207636c6173735f61
```

Hexadecimal sequence configuration is not limited to any specific format regarding the order, value or length of the data (up to a maximum of 200 characters). This gives the user the freedom to personalize the content depending on the configuration of his DHCP server.

### 2.6.4 ENABLE-ALL-INTERFACES

Globally enables the DHCP relay, i.e., in all the interfaces pertaining to the VRF instance being configured where the DHCP protocol can operate.

*Syntax:*

```
DHCP-Relay config>ENABLE ALL-INTERFACES
```

*Example:*

```
DHCP-Relay config>enable all-interfaces
```

To globally disable the relay agent, enter **no enable all-interfaces.**

### 2.6.5 GIADDR

Configures the relay agent IP address. This is the address the relay DHCP sends in the giaddr field in the DHCP messages addressed to the servers.

By default, when the **giaddr** command is not configured, the device automatically selects the relay agent IP address, choosing the first of the IP addresses for the interface through which the client petition was received, or uses the router's global address if there isn't another address configured in this interface.

The server uses the relay agent IP address to identify the network the client pertains to and, based on that, select the parameters it must assign. The address the relay has in the client LAN must be, therefore, configured.

*Syntax:*

```
DHCP-Relay config>GIADDR <IP address>
```

*Example:*

```
DHCP-Relay config>giaddr 10.10.0.1
DHCP-Relay config>
```

To configure automatic selection of the relay agent IP address (giaddr), enter **no giaddr**.

### 2.6.6 MONITOR-OPTIONS

Configures the parameters that regulate server monitoring in a Relay Agent. This monitoring process only activates if, through the **update** command, the Relay Agent has been configured to update an NSLA level indicator when it changes its state. To configure an indicator through the NSLA feature, please see manual bintec Dm754-I – NSLA.

*Syntax:*

```
DHCP-Relay config>monitor-options ?
  packets-threshold    Number of sent packets without response
  interval             Time interval between servers monitoring
  always-on            Set servers monitoring always enable
```

#### 2.6.6.1 monitor-options packet-threshold

Establishes the threshold for DHCPDISCOVER packets transmitted by the Relay Agent to a server without receiving a response from it. Once this threshold has been reached, the server is considered down.

*Syntax:*

```
DHCP-Relay config>monitor-options packets-threshold <1..255>
```

Default is 10 packets.

#### 2.6.6.2 monitor-options interval

Configures a time interval between the consecutive sending of two DHCPDISCOVER packets, internally generated by the Relay Agent due to the monitoring process of the servers.

*Syntax:*

```
DHCP-Relay config>monitor-options interval <1s..1h>
```

Default is 1 minute.

#### 2.6.6.3 monitor-options always-on

Forces the periodic monitoring of servers to be continuously operating in the Relay agent, instead of waiting until all of its servers are inaccessible.

*Syntax:*

```
DHCP-Relay config>monitor-options always-on
```

By default, this monitoring mode is deactivated.

**Note**

If you do not configure this monitoring process option, it will only initiate when all the servers for a Relay agent are considered down.

### 2.6.7 SERVER

Adds a DHCP server to which the Relay Agent transmits the DHCP messages that listen in the network segment it is in. The server is specified through the IP address and, optionally, through an additional identification name (as this is dispensable, it has no effect on the relay operation). By default, when this is not explicitly specified, the defined DHCP server is found in the same VRF over which the relay is being configured. Where a multi-VRF configuration is required (e.g., when one or more clients are located in a VRF/VPN different to the server), the VRF instance for the latter must be specified.

*Syntax:*

```
DHCP-Relay config>SERVER [global-vrf | vrf <VRF_Name>] <IP address> [<identifier name>]
```

*Example:*

```
DHCP-Relay config>server global-vrf 192.168.155.43
DHCP-Relay config>
```

In the above example, we have included a *global-vrf* token indicating that the subsequently specified server is accessed through the global routing table (main VRF).

*Example:*

```
DHCP-Relay config>server vrf server-1 192.168.138.133
DHCP-Relay config>
```

In the above example, we have included the *vrf server-1* option indicating that the subsequently specified server is accessed through the VRF server-1 configured in the **bintec Router**.

To eliminate a DHCP server, enter **no dhcp-server <IP address>**.

*Example:*

```
DHCP-Relay config>no server 192.168.156.3
DHCP-Relay config>
```

### 2.6.8 SOURCE-ADDRESS

Configures the source IP address the DHCP Relay Agent uses in the packets sent towards the DHCP servers.

By default, the device automatically selects the source address from the output interface through which the IP packet is sent, or it uses the router's global address.

*Syntax:*

```
DHCP-Relay config>SOURCE-ADDRESS <IP address>
```

*Example:*

```
DHCP-Relay config>source-address 10.10.0.1
DHCP-Relay config>
```

To configure automatic selection of the source IP address in DHCP Relay packets, enter **no source-address**.

### 2.6.9 UPDATE

Configures a level indicator to update by a certain value when a change of state is produced in the Relay Agent. The indicator increases by said value when the agent detects that none of its DHCP servers is accessible (when a change in state to DOWN is produced). The indicator decreases by this same value when the opposite change of state is produced i.e., when the agent returns to UP.

*Syntax:*

```
DHCP-Relay config>update level-indicator <1..255> value <1..255> when-down
```

*Example:*

```
DHCP-Relay config>update level-indicator 1 value 10 when-down
DHCP-Relay config>
```

### 2.6.10 VRF

Accesses the specific parameter configuration menu for the DHCP-Relay VRF instance specified through the command line. After executing this command, the DHCP-Relay vrf config> prompt appears in order to indicate that you have accessed the previously described menu.

*Syntax:*

```
DHCP-Relay config>VRF <VRF_Name>
```

*Example:*

```
DHCP-Relay config>vrf cliente-1
DHCP-Relay vrf config>
```

### 2.6.11 EXIT

Lets you exit the DHCP Relay agent configuration menu.

Syntax:

```
DHCP-Relay config>EXIT
```

Example:

```
DHCP-Relay config>exit
DHCP config>
```

### 2.6.12 Specific commands for a relay VRF instance

Once in the parameter configuration menu for a DHCP-Relay VRF instance, you will find the following possibilities:

| **Command** | **Function** |
|---|---|
| *? (HELP)* | Lists all the commands or their available options. |
| *AGENT-INFORMATION* | Inserts the relay agent information (DHCP option 82) in packets addressed to the DHCP server. |
| *ENABLE* | Enables DHCP relay in all the interfaces. |
| *GIADDR* | Configures the relay agent IP address. |
| *MONITOR-OPTIONS* | Configures the monitoring options for servers. |
| *NO* | Deletes a previously added DHCP server or restores the source address that the packets, sent by the relay, must exit with or the relay agent IP address (giaddr) to its default address (automatic selection). |
| *SERVER* | Adds or modifies a DHCP server. |
| *SOURCE-ADDRESS* | Configures the source IP address for the packets from the Relay agent. |
| UPDATE | Configures the updating for an NSLA level indicator. |
| *EXIT* | Command used to exit the Relay agent configuration menu. |

Out of all the above commands, the only one that offers different options in the main relay agent configuration menu is the one shown below. For all the other commands, please see the information given in the previous section.

### 2.6.13 AGENT-INFORMATION

Through this command, you can enable the functionality allowing the relay agent to insert information associated with the interface/VPN from which packets coming from the DHCP clients have arrived. This information is used in DHCP servers that support this functionality to select configuration parameters to be sent to a client.

*Syntax:*

```
DHCP-Relay vrf config>agent-information ?
  vpn    Add VRF name suboption into forwarded DHCP packet
  hex    Hexadecimal string inserted in option 82 data field
```

#### 2.6.13.1 AGENT-INFORMATION VPN

Where this is enabled, the relay agent inserts information over the VRF name (through which the client petitions arrived), the main relay IP address in the interface through which the petition arrived and the network address for the latter. The three fields travel in the DHCP packet as sub-options in the protocol's option 82.

*Example:*

```
DHCP-Relay vrf config>agent-information vpn
```

#### 2.6.13.2 AGENT-INFORMATION-HEX <VALUE>

Configures the option 82 data field in hexadecimal. The Relay agent inserts this value in the packets received by the interfaces pertaining to the main VRF before they are forwarded to the DHCP server.

*Example:*

```
DHCP-Relay vrf config>agent-information hex 0207636c6173735f62
```

Hexadecimal sequence configuration is not limited to any specific format regarding the order, value or length of the data (up to a maximum of 200 characters). This gives the user the freedom to personalize the content depending on the configuration of his DHCP server.

## 2.7 DHCP Server Configuration Commands

### 2.7.1 SERVER mode configuration commands

Once in the configuration menu for the *DHCP Server* functionality mode, the following options are presented:

| Command | Function |
|---|---|
| *? (HELP)* | Lists the available commands or their options. |
| *CLASS* | Configures the *Classes* parameters. |
| *ENABLE* | Enables the DHCP server. |
| *GLOBAL* | Configures the DHCP server global parameters. |
| *HOST* | Configures the parameters for the *Hosts*. |
| *LIST* | Lists the DHCP server information. |
| *NO* | Deletes a DHCP server parameter configuration. |
| *OPTION* | Configures miscellaneous DHCP Server options. |
| *SHARED* | Creates a *Shared Network*. |
| *SUBNET* | Configures the parameters for the *Subnets*. |
| *EXIT* | Command to exit the DHCP server configuration menu. |

### 2.7.2 ? (HELP)

Displays the available commands or their options.

*Syntax:*

```
DHCP-Server config>?
```

*Example:*

```
DHCP-Server config>?
  class     Create a class
  global    Configure the dhcp server global parameters
  enable    Enable the DHCP server in all interfaces
  host      Configure the parameters of a host
  list      List configuration
  no        Negates a command or sets its defaults
  option    Configure miscellaneous DHCP Server options
  shared    Create a shared network
  subnet    Configure a subnet
  exit
DHCP-Server config>
```

### 2.7.3 CLASS

Lets you define a class to identify a particular group of clients to which you can assign specific configuration options. It's also possible to reserve one or more address ranges for class members. There is a configuration option within the *class* menu to identify class members. A DHCP client can send option 60 (vendor-class-identifier) in its petition with a value that normally depends on the manufacturer of the device the DHCP petition is sent from. This value is used in the client identification process. If it is a class member, then the server replies with the options that were previously configured for the members of said class.

The following parameters must be defined:

- *Class* name.
- *Shared network* number.

The minimum configuration parameters specifically necessary for a class are as follows:

#### 2.7.3.1 Vendor-class-id

Provides the DHCP server with the vendor-class-identifier field value sent by those DHCP clients who are members of the class. Describing the full field simply to configure a subfield (which uniquely identifies class members) is not necessary.

This can be entered in hexadecimal (by introducing a text string with hexadecimal characters) or in ASCII (entering a text string).

#### 2.7.3.2 default-lease-time <time>

Establishes a default time in which an address is assigned. Time, in seconds, during which an address is assigned to a client if the client making the petition does not request a specific timeout period.

*Syntax:*

```
DHCP-Server config>class <class_name> <shared_id> default-lease-time <time>
```

*Example:*

```
DHCP-Server config>class class_A 1 default-lease-time 2h30m
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*default-lease-time <time>*" command has been introduced as of version 11.01.09. |

#### 2.7.3.3 max-lease-time <time>

Maximum amount of time (in seconds) that an address is assigned if the client making the petition requests a specific expiry period.

*Syntax:*

```
DHCP-Server config>class <class_name> <shared_id> max-lease-time <time>
```

*Example:*

```
DHCP-Server config>class class_A 1 max-lease-time 1d2h
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*max-lease-time <time>*" command has been introduced as of version 11.01.09. |

#### 2.7.3.4 subnet-name

Associates class members to a configured *subset*. This parameter is required to reserve one or various IP address ranges for class members. The ranges, which are defined below, must be compatible with the address and mask of the associated *subnet*.

When no range of IP addresses in the class has been configured, the clients pertaining to this class are offered addresses from some of the ranges configured in the subnet associated with said class. However, those DHCP options defined in the class are delivered to the client as they carry preference over the subnet options.

**Important**

For the class to operate correctly, the **vendor-class-id** parameter must be defined. If you also want to assign specific address ranges for the DHCP clients who are class members, configure one or more IP address ranges within the class options.

*Example:*

```
DHCP-Server config$class clase 1 vendor-class-id asc bintec-vendor-class
DHCP-Server config$class clase 1 subnet-name relay
DHCP-Server config$class clase 1 option 43 hex 0x001122
DHCP-Server config$class clase 1 range 10.0.0.30 10.0.0.35
DHCP-Server config$list class
 ============================
 =     CLASS List    1     =
 ============================
 CLASS: clase
   Class identifier: bintec-vendor-class
   Associated subnet: relay
   Range: 10.0.0.30       --> 10.0.0.35
   - DHCP Option 43: 0x001122

DHCP-Server config$
```

#### 2.7.3.5 source-address <ip address>

Configures the source address for IP packets sent by the DHCP server.

*Syntax:*

```
DHCP-Server config>class <clase_name> <shared_id> source-address {<ip_address> | <interface>}
```

*Example:*

```
DHCP-Server config>class class_A 1 source-address 192.168.7.2
```

**Command history:**

| Release | Modification |
|---|---|
| 10.09.27, 11.00.06, 11.01.02 | New command added. |

### 2.7.4 GLOBAL

Lets you configure the proprietary DHCP server parameters at a global level, as well as the options that are sent to the DHCP clients.

This section explains how to configure the DHCP server's specific parameters at a global level. The *Options* configuration will be explained in later sections.

*Syntax:*

```
DHCP-Server config>GLOBAL <parameter, value>
```

The DHCP server's specific parameters at a global level are as follows:

#### 2.7.4.1 boot-unknown-clients

Indicates whether the server should assign addresses to unknown clients (i.e., those who have not specifically been configured).

Default is yes and allows the server to assign addresses to unknown clients. To disable this option, enter **no global no boot-unknown-clients**.

This parameter can only be configured at a global level (global parameters).

#### 2.7.4.2 bootfile <filename>

Specifies (at global level) the boot filename, which has to be downloaded by the client.

This parameter is usually configured at the same time as the *next-server* is configured.

You can configure this at any level or scope: global, subnet or host.

#### 2.7.4.3 conflict-lease-time <time>

Configures the time that a server waits to resolve an IP address conflict detected in the network. Once this time has timed out, the IP address in the conflict will be available once again and can be offered to a new client.

If you do not configure this parameter, the default value of 1 hour is taken. To reestablish the default value, use the **no global conflict-lease-time** command.

#### 2.7.4.4 ddns allow-client-updates

On enabling this parameter, DHCP clients can execute dynamic updating for the A register in the corresponding DNS server when they request option 81 (FQDN) in the DHCPREQUEST.

By default, this option is disabled (i.e., DHCP clients cannot execute DNS dynamic updating of any type).

To activate this parameter, the *ddns-updates* option must be enabled.

#### 2.7.4.5 ddns-domain <domain name>

Establishes the domain name used in the DDNS updates. This domain name is linked to the client hostname to construct the *fully-qualified domain-name* (FQDN), which will update in the DNS server.

This parameter is exclusively configured at a global level.

To activate this parameter, the *ddns-updates* option must be enabled.

#### 2.7.4.6 ddns-hostname mac-address

Specifies the type of hostname to be used in the DDNS updates. By default, the hostname provided by the DHCP client is used. This command lets you enable the **mac-address** option, which indicates a string of ascii characters constructed from the client MAC is used as the hostname. For example, the hostname associated with MAC address 00-02-44-53-9d-e6 is 0-2-44-53-9d-e6.

This parameter is exclusively configured at a global level.

To activate this parameter, the DDNS updates must be enabled *(ddns-updates)*.

#### 2.7.4.7 ddns-revdomain <inverse domain name>

Domain name linked to the DHCP client inverse IP address (which is made up of inverted digits) to construct the name to be used in the DDNS updates for the PTR registers (used for name inverse resolution).

The default value for this parameter is **in-addr.arpa.**

This parameter is exclusively configured at a global level.

To activate this parameter, the DDNS updates must be enabled *(ddns-updates)*.

#### 2.7.4.8 ddns-updates [on-demand]

Through this command, the DNS dynamic updates are enabled (DDNS updates) for the DHCP client's "fully-qualified domain-name" (FQDN).

The DHCP protocol has an option known as the *Client FQDN* option (option number 81), which is used to exchange information on the FQDN between a client and a DHCP server and to execute DDNS updates for the A and PTR registers in a DNS server. This means a DNS server is capable of executing direct/inverse resolution for a device name that receives its configuration through DHCP.

DDNS updates are disabled by default. If they are enabled with the optional **on-demand** flag, then these updates are only carried out if the DHCP client has this option included in its DHCPREQUEST.

If the *ddns-allow-client-updates* parameter is enabled, the DHCP server will execute updating for both the A and the PTR registers.

**Important**

To execute DDNS updates, the router must have at least ONE DNS server configured in the DNS Client facility. If there are various DNS servers configured, the first of these is selected as the main server. For further information on the DNS Client faculty, please see associated manual bintec Dm723-I.

#### 2.7.4.9 default-lease-time <time>

Establishes a default time in which an address is assigned. Time, in seconds, during which an address is assigned to a client if the client making the petition does not request a specific timeout period.

You can configure this at any level or scope: global, subnet, class or host.

Default is 43200 seconds.

#### 2.7.4.10 max-lease-time <time>

Maximum amount of time (in seconds) that an address is assigned if the client making the petition requests a specific expiry period.

You can configure this at any level or scope: global, subnet, class or host.

Default is 86400 seconds.

#### 2.7.4.11 next-server <ip address>

Indicates (at a global level) the server's IP address from which you should load the initial booting file indicated by the *filename* parameter. If no *next-server* is indicated, the clients download the file from the DHCP server itself.

You can configure this at any level or scope: global, subnet or host.

#### 2.7.4.12 one-lease-per-client

Establishes that each client is going to be assigned a maximum of one address. Should this be activated, only one address per client will be assigned.

This parameter is enabled by default. To disable it, enter **global no one-lease-per-client**.

This parameter can only be configured at a global level (global parameters).

#### 2.7.4.13 server-name <identifier>

Supplies the DHCP server name to the client.

This parameter can only be configured at a global level (global parameters).

*Example:*

```
DHCP-Server config>global no boot-unknown-clients
DHCP-Server config>global default-lease-time 36000
DHCP-Server config>global max-lease-time 72000
DHCP-Server config>global server-name my.dhcp.server
DHCP-Server config>global bootfile defaultfile.cfg
DHCP-Server config>global next-server 192.168.1.1
DHCP-Server config>list global
 ============================
 =    GLOBAL Parameters     =
 ============================
   Server Name: my.dhcp.server
   Next Server: 192.168.1.1
   Lease time: Default 36000, Maximum 72000
   Boot Unknown clients: No
   One Lease Per client: Yes
   Dynamic DNS Updates (FQDN): Disabled (deny client updates)
   DDNS Update Hostname: client hostname
   Bootfile: defaultfile.cfg

DHCP-Server config>
```

### 2.7.5 ENABLE

Globally enables the DHCP server, i.e., in all interfaces, so that the DHCP protocol can operate.

*Syntax:*

```
DHCP-Server config>ENABLE
```

*Example:*

```
DHCP-Server config>enable
```

To disable the DHCP server, use the **no enable** command.

### 2.7.6 HOST

Lets you configure the parameters for a given *host* to which an IP address will be assigned. A host must be explicitly declared when you always wish to assign the same IP address to it, or when you only wish to assign addresses to known hosts (or clients). This prevents the DHCP server from assigning addresses to other non-specified clients. The following parameters must always be indicated for this:

- *host* Identifier.
- *shared network* Number.

The same host can be defined on different *Shared Networks* (depending on where it is connected, it receives one configuration or another). Consequently, you must correctly identify which one is being configured.

*Syntax:*

```
DHCP-Server config>HOST <identifier, shared network> <parameter, value>
```

To eliminate a host and all associated configuration parameters, use **no host <identifier, shared-network>**.

The specific configuration parameters for the Hosts are as follows:

#### 2.7.6.1 bootfile <filename>

Specifies the boot filename for the specified host.

This parameter is usually configured at the same time as the *next-server* is configured.

You can configure this at any level or scope: global, subnet or host.

#### 2.7.6.2 client-id <format><identifier>

Specifies the DHCP *client-identifier* option (option 61), which identifies the DHCP client those DHCP options, defined in the host configuration, should be assigned to. This has preference over other ways to identify a host ( *Ethernet*, described below).

This can be entered in hexadecimal (introducing a hexadecimal character string) or in ASCII.

#### 2.7.6.3 default-lease-time <time>

Establishes a default time in which an address is assigned. Time, in seconds, during which an address is assigned to a client if the client making the petition does not request a specific timeout period.

You can configure this at any level or scope: global, subnet, class or host.

*Syntax:*

```
DHCP-Server config>host <host_name> <shared_id> default-lease-time <time>
```

*Example:*

```
DHCP-Server config>host host_A 1 default-lease-time 2h30m
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*default-lease-time <time>*" command has been introduced as of version 11.01.09. |

#### 2.7.6.4 ethernet <mac>

Specifies the host MAC address and also indicates this is Ethernet.

#### 2.7.6.5 fixed-ip <ip address>

Configures a fixed IP address to be assigned to the host.

Where this parameter isn't configured, the DHCP options configured in the host are assigned to the client, identified through the **client-id** or **Ethernet** command. The IP address will be one available in the pool associated with one of the subnets associated with the host *shared network*.

**Important**

When you assign a fixed IP address to a Host, check said address is not from within one of the ranges used by the server to assign addresses. Otherwise, this address could be assigned to any DHCP client.

#### 2.7.6.6 max-lease-time <time>

Maximum amount of time (in seconds) during which an address is assigned if the client making the petition requests a specific expiry period.

You can configure this at any level or scope: global, subnet, class or host.

*Syntax:*

```
DHCP-Server config>host <host_name> <shared_id> max-lease-time <time>
```

*Example:*

```
DHCP-Server config>host host_A 1 max-lease-time 1d2h
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*max-lease-time <time>*" command has been introduced as of version 11.01.09. |

#### 2.7.6.7 next-server <ip address>

Indicates (for the specified host) the server's IP address from which you should load the initial booting file indicated by the *bootfile* parameter. If there is no *next-server* indicated, the clients download the file from the DHCP server itself.

You can configure this at any level or scope: global, subnet or host.

#### 2.7.6.8 token-ring <mac>

Specifies the host MAC address and also indicates this is Token-Ring.

*Example:*

```
DHCP-Server config>host eth-host 0 ethernet 00aa11bb22cc
DHCP-Server config>host eth-host 0 fixed-ip 192.168.1.7
DHCP-Server config>host eth-host 0 bootfile ethfile.cfg
DHCP-Server config>host eth-host 0 next-server 192.168.1.3
DHCP-Server config>host tkr-host 1 token-ring 33dd44ee55ff
DHCP-Server config>host tkr-host 1 bootfile tkrfile.cfg
DHCP-Server config>list host
 ============================
 =      HOST List    0     =
 ============================
 HOST: eth-host
   Ethernet hw: 00AA11BB22CC, Fixed Address: 192.168.1.7
   Next Server: 192.168.1.3
   Bootfile: ethfile.cfg
 ============================
 =      HOST List    1     =
 ============================
```

```
 HOST: tkr-host
   Token Ring hw: 33DD44EE55FF, No Fixed IP Address
   Bootfile: tkrfile.cfg

DHCP-Server config>
```

### 2.7.7 LIST

Displays the DHCP Server configuration.

*Syntax:*

```
DHCP-Server config>LIST <option>
```

The <option> field indicates the type of information you want to list.

*Example:*

```
DHCP-Server config>LIST ?
  all       List all the dhcp server configuration
  global    List global dhcp server parameters
  host      List parameters of all configured hosts
  shared    List the configured shared networks
  subnet    List the configuration of all the subnets
DHCP-Server config>
```

#### 2.7.7.1 LIST ALL

Displays *all* the *DHCP Server* configuration information.

*Example:*

```
DHCP-Server config>LIST ALL
 ============================
 =    GLOBAL Parameters     =
============================
   Server Name: dhcp.server
   Next Server: 0.0.0.0
   Lease time: Default 43200, Maximum 86400
   Boot Unknown clients: Yes
   One Lease Per client: Yes
   Dynamic DNS Updates (FQDN): Disabled (deny client updates)
   DDNS Update Hostname: client hostname
 ============================
 =   SHARED NETWORK List    =
 ============================
   Shared Network: 2
============================
 =     SUBNET List    0     =
 ============================
 SUBNET: sevilla
   Address: 172.27.0.0, Mask: 255.255.0.0
   Utilization (low/high): 0/100
   Range: 172.27.15.10    --> 172.27.15.250
   - Router: 172.27.0.2
 SUBNET: sevilla-2
   Address: 172.35.156.0, Mask: 255.255.255.0
   Utilization (low/high): 0/100
   Range: 172.35.156.77   --> 172.35.156.80
   - Router: 172.35.156.3
   - Static Route to 192.157.252.0   via 172.35.156.111
 ============================
 =     SUBNET List    2     =
 ============================
SUBNET: lugo
   Address: 168.252.57.0, Mask: 255.255.255.0
   Utilization (low/high): 0/100
   Range: 168.252.57.25   --> 168.252.57.30
   Next Server: 168.252.57.6
```

```
   Server Identifier: 168.252.57.6
   Bootfile: lugofile.conf
 ============================
 =      HOST List    0     =
 ============================
   No Host defined
 ============================
 =      HOST List    2     =
 ============================
 HOST: myhost
   Ethernet hw: 0020AF4452EE, No Fixed IP Address
   - Router: 168.252.57.6

DHCP-Server config>
```

#### 2.7.7.2 LIST CLASS

Displays information relating to parameters and options for classes configured in the DHCP server.

*Example:*

```
DHCP-Server config$list class
 ============================
 =     CLASS List    0     =
 ============================
CLASS: clase
   Identifier: 0x61616161
   Associated subnet: mired
   Utilization (low/high): 0/100
   Range: 172.24.252.42   --> 172.24.252.42
   - DHCP Option 43: 0x22

DHCP-Server config$
```

#### 2.7.7.3 LIST GLOBAL

Displays information on the DHCP Server's *global* parameters and options.

*Example:*

```
DHCP-Server config>LIST GLOBAL
 ============================
 =    GLOBAL Parameters    =
 ============================
   Server Name: dhcp.server
   Next Server: 0.0.0.0
   Lease time: Default 43200, Maximum 86400
   Boot Unknown clients: Yes
   One Lease Per client: Yes
   Dynamic DNS Updates (FQDN): Disabled (deny client updates)
   DDNS Update Hostname: client hostname
   - IP Forwarding: Disabled

DHCP-Server config>
```

#### 2.7.7.4 LIST HOST

Displays information relevant to all configured *hosts* (including all hosts in the *shared networks*, the corresponding *shared network* number is indicated in the header).

*Example:*

```
DHCP-Server config>LIST HOST
 ============================
 =      HOST List    0     =
 ============================
 HOST: hredondo
   Ethernet hw: 00105A2F0B02, Fixed Address: 192.136.21.64
 HOST: jlperez
```

```
   Ethernet hw: 00500433DDAF, Fixed Address: 192.136.21.134
   - Router: 192.136.21.198
 HOST: fuentes
   Ethernet hw: 0000383D3148, No Fixed IP Address
   - Router: 192.136.21.198
 HOST: lgomez
   Ethernet hw: 0060973E4EF5, No Fixed IP Address
 ============================
 =      HOST List    2     =
 ============================
 HOST: probe-server
   Token Ring hw: 0000C91EED5C, No Fixed IP Address
DHCP-Server config>
```

#### 2.7.7.5 LIST SHARED

Displays the configured *shared networks*. Apart from the configured *shared networks*, there always exists the default *shared network* (0).

*Example:*

```
DHCP-Server config>LIST SHARED

 ============================
 =   SHARED NETWORK List    =
 ============================
   Shared Network: 2

DHCP-Server config>
```

#### 2.7.7.6 LIST SUBNET

Displays the information on all subnets configured in the device. Those for each *shared network* are also listed (the associated *shared network* number is indicated in the header).

*Example:*

```
DHCP-Server config>LIST SUBNET
 ============================
 =     SUBNET List    0     =
 ============================
 SUBNET: 192.16
   Address: 192.16.1.0, Mask: 255.255.255.0
   Utilization (low/high): 20/90
   Range: 192.16.1.162     --> 192.16.1.163
   - Router: 192.16.1.57
   - NetBios Node Type: P-node
   - Static Route to 172.27.0.0      via 192.16.1.133
   - Static Route to 202.5.0.0       via 192.16.1.176
 SUBNET: 192.19
   Address: 192.19.75.0, Mask: 255.255.255.0
   Utilization (low/high): 0/100
   Range: 192.19.75.250   --> 192.19.75.254
 ============================
 =     SUBNET List    2     =
 ============================
 SUBNET: 172.27
   Address: 172.27.0.0, Mask: 255.255.0.0
   Utilization (low/high): 0/80
   Range: 172.27.0.10     --> 172.27.0.100

DHCP-Server config>
```

### 2.7.8 OPTION

Configures miscellaneous options in the DHCP Server. The available options are as follows:

#### 2.7.8.1 ping packets <number-of-packets>

By default, the DHCP server sends two ICMP echo packets to the IP for a lease before being offered to a client. Through this command you can change the number of ICMP echo packets sent by the client (provided that a response has not been received to a previously sent packet) before considering the lease is available.

Where the number of packets is set to 0, the server will not check the dynamic leases before offering them to clients.

#### 2.7.8.2 ping timeout <time.ms>

By default, the DHCP server waits for 500 ms to receive a response to the ICMP echo packet sent from one of the devices in the network. You can change the wait time via this command.

#### 2.7.8.3 strict-client-identifier

By default, the DHCP server ignores the DHCP client-identifier option when the MAC address for the client is encoded. This behavior is disabled through this command.

*Example:*

```
DHCP-Server config$option strict-client-identifier
DHCP-Server config$option ping packets 1
DHCP-Server config$option ping timeout 1000
DHCP-Server config$list options
 ============================
 =   DHCP-Server Options    =
 ============================
   Number of ping packets: 1
   Ping timeout: 1000 (ms)
   Strict "client-identifier"

DHCP-Server config$
```

#### 2.7.8.4 update-leases-time

The device periodically saves the active leases list in its memory with the aim of recovering them if a RESET is produced. On start up, if the DHCP server is enabled, these leases continue to be available so the clients can renew the IP addresses they have assigned. Use the **update-leases-time** option to configure the period in which the list of active leases stored in memory is updated.

After start up, a lease remains active for the time that remained until expiry when the list was last updated before the RESET occurred. By default, the update period is 5 minutes.

*Example:*

```
DHCP-Server config> option update-leases-time <1s..3550w5d3h14m7s>
```

To reconfigure the default value, use the command **no option update-leases-time**.

### 2.7.9 SHARED

Creates a *shared network* with the specified identifier. A *shared network* can be configured specifying the VRF instance where the address assignment service is offered. Thus, the addresses are assigned using the *shared networks* configured for the same VRF instance in the interface the client accesses the router through. If the DHCP server doesn't have a *shared network* for said interface in this VRF, it uses the *shared networks* that have been configured without specifying the VRF. If you want one *shared network* to be exclusively used for the main VRF, specify the GLOBAL-VRF option. The *shared network* can be configured so it is controlled by an *advisor* configured through the bintec NSLA feature. For further information on the NSLA feature, please see manual bintec Dm754-I NSLA. A *shared network* controlled by an *advisor* remains disabled, i.e., that server cannot use it to assign addresses until said *advisor* notifies it.

*Syntax:*

```
DHCP-Server config>SHARED <identifier> [{GLOBAL-VRF | VRF <vrf_tag>}] [TRACK NSLA-ADVISOR
<advisor_id>]
```

- *<vrf_tag>*: name of the VRF instance.
- *<advisor_id>*: *advisor* identifier for the *advisor* configured through the NSLA features.

To eliminate a *shared network* and all the associated configuration parameters (*subnets*, *host*, etc.), use **no shared**

**<identifier>**.

*Example:*

```
DHCP-Server config>SHARED 3
DHCP-Server config>SHARED 4 TRACK NSLA-ADVISOR 1
DHCP-Server config>SHARED 5 vrf vrf2
DHCP-Server config>SHARED 6 GLOBAL-VRF TRACK NSLA-ADVISOR 1
DHCP-Server config>SHARED 6 vrf vrf2 TRACK NSLA-ADVISOR 1
DHCP-Server config>
```

## 2.7.10 SUBNET

Lets you configure the various subnet options and parameters. To do this, indicate the following parameters:

- *subnet* Identifier.
- *shared network* Number.

The maximum length admitted by the subnet identifier is 15 characters.

The same subnet identifier can be defined in different *shared networks* so you must correctly identify which one you are configuring.

*Syntax:*

```
DHCP-Server config>SUBNET <identifier, shared network> <parameter, value>
```

To eliminate a *subnet* and all associated configuration parameters, use **no subnet <identifier, shared-network>** .

The specific configuration parameters for the SUBNETS are as follows:

### 2.7.10.1 bootfile <filename>

Specifies the boot filename for the specified subnet.

This parameter is usually configured at the same time as the *next-server* is configured.

You can configure this at any level or scope: global, subnet or host.

### 2.7.10.2 default-lease-time <time>

Establishes a default time during which an address is assigned. Time, in seconds, during which an address is assigned to a client if the client making the petition does not request a specific timeout period.

You can configure this at any level or scope: global, subnet, class or host.

*Syntax:*

```
DHCP-Server config>subnet <subnet_name> <shared_id> default-lease-time <time>
```

*Example:*

```
DHCP-Server config>subnet s1 1 default-lease-time 2h30m
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*default-lease-time <time>*" command was introduced as of version 11.01.09. |

### 2.7.10.3 max-lease-time <time>

Maximum amount of time (in seconds) during which an address is assigned if the client making the petition requests a specific expiry period.

You can configure this at any level or scope: global, subnet, class or host.

*Syntax:*

```
DHCP-Server config>subnet <subnet_name> <shared_id> max-lease-time <time>
```

*Example:*

```
DHCP-Server config>subnet s1 1 max-lease-time 1d2h
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.09 | The "*max-lease-time <time>*" command has been introduced as of version 11.01.09. |

### 2.7.10.4 network <network address, network mask>

Defines the subnet through its address and mask.

### 2.7.10.5 next-server <ip address>

Indicates (for the specified subnet) the server's IP address from which you should load the initial booting file indicated by the *bootfile* parameter. If there is no *next-server* indicated, the clients download the file from the DHCP server itself.

You can configure this at any level or scope: global, subnet or host.

### 2.7.10.6 range <initial ip address, final ip address>

Defines a range of IP addresses, which will be assigned to DHCP clients.

For each subnet in which IP addresses are dynamically assigned through a DHCP server, there must be at least one specified range of addresses. If none is specified, only those hosts who have been explicitly configured with a fixed address from this subnet are attended to.

The range of addresses must pertain to the subnet where it has been defined.

The range is specified through an initial IP address and a final IP address. You can define various ranges in the same subnet as well as specified individual addresses.

**Note**

Verify that the range of IP addresses to assign DOES NOT contain IP addresses for devices, which are statically configured in the network (not configured dynamically with DHCP) or addresses for devices to which the DHCP server assigns fixed IP.

### 2.7.10.7 server-identifier <ip address>

Defines the value sent in the DHCP Server Identifier option for a specific subnet. The DHCP server identifier is specified through the IP address and must be reachable for all the clients in this subnet.

We recommend that you do not configure this parameter (the router by default will set the appropriate value) unless it's use is absolutely necessary to ensure correct performance:

- Assignment of addresses to subnets that arrive through a DHCP relay. In this case, the LAN address of the DHCP relay agent must be specified as SERVER-IDENTIFIER.
- When the DHCP server has two subnets defined in a LAN interface and only has one IP address configured in this interface, specify the address possessed by the server configured in the LAN as *SERVER-IDENTIFIER*. However, if the server has an IP address belonging to each subnet defined, specifying the *SERVER-IDENTIFIER* is NOT necessary (as the router, by default, configures the appropriate value for each).

This parameter can only be configured at the subnet layer.

*Example:*

```
DHCP-Server config>subnet mynet 0 network 192.168.7.0 255.255.255.0
DHCP-Server config>subnet mynet 0 range 192.168.7.50 192.168.7.200
DHCP-Server config>subnet mynet 0 server-identifier 192.168.7.1
DHCP-Server config>list subnet
 ============================
 =     SUBNET List    0    =
 ============================
 SUBNET: mynet
   Address: 192.168.7.0, Mask: 255.255.255.0
   Range: 192.168.7.50    --> 192.168.7.200
   Server Identifier: 192.168.7.1

DHCP-Server config>
```

#### 2.7.10.8 source-address <ip address>

Configures the source address of the IP packets sent by the DHCP server.

*Syntax:*

```
DHCP-Server config>subnet <subnet_name> <shared_id> source-address {<ip_address> | <interface>}
```

*Example:*

```
DHCP-Server config>subnet mynet 0 source-address 192.168.7.2
```

**Command history:**

| Release | Modification |
|---|---|
| 10.09.27, 11.00.06, 11.01.02 | New command added. |

### 2.7.11 Configuring OPTIONS

Options can be configured in any scope, inheriting those from a superior scope, i.e., the *shared networks* and the *hosts* have the options globally configured by default, while the *subnets* and *classes* have their *shared network* options by default.

The configured options determine the client behavior and functionality.

To configure an option at the global level:

```
DHCP-Server config>GLOBAL <option, value>
```

To configure an option in a subnet:

```
DHCP-Server config>SUBNET <identifier, shared network> <option, value>
```

To configure an option in a host:

```
DHCP-Server config>HOST <identifier, shared network> <option, value>
```

The available options (at all levels) are as follows:

#### 2.7.11.1 BROADCAST-ADDRESS <ip address>

Specifies the broadcast address in the client's subnet. The legal values for broadcast addresses are specified in RFC 1122.

*Example:*

```
DHCP-Server config>GLOBAL BROADCAST-ADDRESS 255.255.255.255
DHCP-Server config>
```

#### 2.7.11.2 DEFAULT-IP-TTL <ttl>

Specifies the default TTL (*time-to-live*) that the client must use when sending datagrams.

*Example:*

```
DHCP-Server config>subnet localsubnet 0 default-ip-ttl 250
DHCP-Server config>
```

#### 2.7.11.3 DNS-DOMAIN <name of domain>

Specifies the domain name that must be used by the client when resolving host names via DNS.

In certain scopes, only one domain name can be specified.

*Example:*

```
DHCP-Server config>subnet develop 0 dns-domain development.bintec.es
DHCP-Server config>
```

#### 2.7.11.4 DNS-SERVER <ip address>

Lets you specify a list of available DNS servers for the client. The servers must be specified in order of preference.

*Example:*

```
DHCP-Server config>global dns-server 200.200.200.200
DHCP-Server config>
```

#### 2.7.11.5 INTERFACE-MTU <mtu>

Specifies the MTU (*maximum-transfer-unit*) to be used in this interface. The minimum permitted value is 68 bytes.

*Example:*

```
DHCP-Server config>global interface-mtu 2048
DHCP-Server config>
```

#### 2.7.11.6 IP-FORWARDING <enabled/disabled>

Specifies whether the client is going to carry out IP packet routing.

*Example:*

```
DHCP-Server config>host myhost 1 ip-forwarding enabled
DHCP-Server config>
```

#### 2.7.11.7 MAX-DGRAM-REASSEMBLY <size>

Specifies the maximum datagram size the client must be prepared to reassemble. The minimum value permitted is 576 bytes.

*Example:*

```
DHCP-Server config>global max-dgram-reassembly 16000
DHCP-Server config>
```

#### 2.7.11.8 NETBIOS-NAME-SERVER <ip address>

Configures a list of NetBIOS server names (NBNS), specified in order of preference.

*Example:*

```
DHCP-Server config>subnet localsubnet 3 netbios-name-server 172.24.0.1
DHCP-Server config>
```

#### 2.7.11.9 NETBIOS-NODE-TYPE <type>

The NetBIOS node type option lets you configure the NetBIOS clients over TCP/IP as described in RFC 1001 and RFC 1002. The value is specified as one octet that identifies the type of node.

Permitted values are:

- **b-node: Broadcast**.
- **p-node: Point-to-point**.
- **m-node: Mixed**.
- **h-node: Hybrid**.

*Example:*

```
DHCP-Server config>subnet localsubnet 3 netbios-node-type m-node
DHCP-Server config>subnet othersubnet 3 netbios-node-type b-node
DHCP-Server config>
```

#### 2.7.11.10 NETBIOS-SCOPE <scope>

Specifies the client NetBIOS scope parameter as specified in RFC 1001 and RFC 1002.

*Example:*

```
DHCP-Server config>subnet localsubnet 3 netbios-scope netbios.com
DHCP-Server config>
```

#### 2.7.11.11 NTP-SERVER <ip address>

Specifies the NTP IP addresses list (RFC 1035) available to the client. These servers are indicated in order of preference.

*Example:*

```
DHCP-Server config>host myhost 1 ntp-server 192.168.99.23
DHCP-Server config>
```

#### 2.7.11.12 OPTION <option number> <option format> <option value>

Lets you generically configure any DHCP option (excluding those DHCP options that are unnecessary for the user to configure such as option 53, which defines the type of DHCP message, etc.). The first field indicates the DHCP option number, the second the format the option value is specified in (ASCII string or hexadecimal string) and the last field is the option value.

If the value of an option is too long to configure on one line, enter it on various lines by simply repeating the option number. In this case, the maximum total length of the value is 384 hexadecimals characters or 191 ASCIL characters.

*Example:*

```
DHCP-Server config>class class 1 option 43 hex 0xa30045f033
DHCP-Server config>class class 1 option 190 asc bintec
DHCP-Server config>
```

In the case of option 43, please use the configuration set forth in the first example when configuring only one option. If, however, there is more than one option 43 available, please include a code for each value.The first field will indicate the DHCP option number, the second one will refer to the option code, the third one to the format in which you specify the option value (ASCII string or hexadecimal string), and the last one will be the value of the option.

*Example:*

```
DHCP-Server config>global option 43 code 1 asc teldat
```

**Command history:**

| Release | Modification |
|---|---|
| 11.01.05 | Option 43 can now be configured to add a code to each value that makes up the Vendor Specific Information. |

#### 2.7.11.13 ROUTER <ip address>

Specifies a list of router IP addresses in the client's subnet. The client's default gateway is determined through this option.

Routers should be configured in order of priority or preference.

*Example:*

```
DHCP-Server config>host myhost 1 router 192.168.0.254
DHCP-Server config>
```

#### 2.7.11.14 STATIC-ROUTE <destination ip, next hop>

Establishes a series of static routes that the client must install in his routing cache. If you specify various routes to the same destination, these are configured in a decreasing order of priority.

When configuring a route, first indicate the destination address and subsequently the router used to reach this destination.

You cannot configure a default route through a static router. To specify a default route, use the **ROUTER** option.

*Example:*

```
DHCP-Server config>global static-route 200.0.0.0 192.168.0.252
```

```
DHCP-Server config
```

#### 2.7.11.15 SUBNET-MASK <mask>

Configures the client subnet mask (in compliance with RFC 950). If you do not configure the subnet mask option in any scope, the subnet mask appearing in the subnet definition is used as a last resort.

*Example:*

```
DHCP-Server config>host myhost 1 subnet-mask 255.255.255.0
DHCP-Server config>
```

#### 2.7.11.16 UTILIZATION MARK

Sets two thresholds that determine whether the state of use of a pool of IP addresses in a class or subnet is "high" or "low". A pool is in "high" use when the number of IP addresses leased is equal to, or greater than, the "high" threshold. On the other hand, a pool is in "low" use if the number of leased IP addresses is lower than the "low" threshold.

If configured, an ELS event, Syslog message or SNMP trap is generated when the state of use of the pool switches to "high". Likewise, an ELS event, Syslog message or SNMP trap is generated when the state of use of the pool switches to "low".

This parameter is configured as a percentage. By default, values are 100% for the "high" threshold and 0% for the "low" threshold.

*Syntax:*

```
DHCP-Server config>subnet <subnet_name> <shared_id> utilization mark {high | low} <percentage>
DHCP-Server config>class <class_name> <shared_id> utilization mark {high | low} <percentage>
```

*Example:*

```
DHCP-Server config>subnet lan1 1 utilization mark high 85
DHCP-Server config>subnet lan1 1 utilization mark low 20
```

In this example, the configured values determine that the address pool that belongs to the "lan1" subnet will be in "high" use when 85% of the addresses get leased. On the other hand, the state of use of the pool will be "low" when the percentage of leased addresses falls under 20%.

**Command history:**

| Release | Modification |
|---|---|
| 11.00.06, 11.01.02 | New command added. |

### 2.7.12 EXIT

Allows you to exit the DHCP Server configuration menu and return to the DHCP general configuration prompt.

*Syntax:*

```
DHCP-Server Config>EXIT
```

*Example:*

```
DHCP-Server config>EXIT
DHCP config>
```

# Chapter 3 Monitoring

## 3.1 DHCP protocol monitoring

The DHCP protocol monitoring displays information related to the router function as either Relay or DHCP Server.

If IP parameters dynamic acquisition has been configured in a **bintec Router** interface, i.e., if the DHCP client has been enabled in the monitoring menu corresponding to this operating mode, the parameters received and accepted by the client are displayed together with the DHCP server who sent the ceded address (*lease*) and the timers that control address renewal or *lease* expiry.

When the **bintec Router** is in DHCP Relay mode, the relay configuration is shown on each interface that is enabled. This configuration includes the configured DHCP servers, the source IP address that the packets sent by the relay to the server exit with and the IP address of the relay agent, which is the one transmitted in the giaddr field of the messages transmitted by the relay to the server.

Finally, if the router acts as a DHCP Server, the corresponding monitoring menu displays the non-volatile storing of the addresses assigned by the server and for the duration of the lease these cannot be reused.

To access the DHCP protocol monitoring menu, enter the following commands at the general monitoring prompt:

```
*MONITOR
Console Operator
+PROTOCOL DHCP

DHCP Protocol monitor
DHCP+
```

## 3.2 DHCP protocol monitoring commands

Within the DHCP protocol monitoring prompt, the following options appear:

```
DHCP+?
  client          Access the DHCP client monitoring menu
  memory-usage    Display the amount of RAM memory used by the DHCP protocol
  relay           Access the DHCP relay monitoring menu
  server          Access the DHCP server monitoring menu
  exit
DHCP+
```

### 3.2.1 MEMORY-USAGE

Displays the amount of RAM memory used by the DHCP protocol.

*Syntax:*

```
DHCP+memory-usage
```

*Example:*

```
DHCP+memory-usage
DHCP memory usage: 172864 bytes
DHCP+
```

### 3.2.2 CLIENT

Accesses the specific monitoring menu for the DHCP client.

*Syntax:*

```
DHCP+client
```

*Example:*

```
DHCP+client
DHCP-Client+
```

The following commands are available in this menu:

```
DHCP-Client+?
  list       Display information on the interfaces with DHCP-Client enabled
  release    Release the lease assigned on the interface specified
  renew      Update the lease timer to the next stage on the interface
             specified
  exit
DHCP-Client+
```

#### 3.2.2.1 LIST

Displays information on the interfaces where dynamic acquisition has been enabled through the DHCP protocol (i.e., DHCP client). The following is shown for each of these: the assigned IP address and mask, the state the DHCP client is in (according to the machine status described in RFC 2131), the transactions identification corresponding to the exchange of frames to acquire the IP address, the DHCP server from which the address has been sent (*lease*), the timers that control address renewal or *lease* expiry and the rest of the options received from the server and accepted by the DHCP client (currently, only the router is acquired by default).

*Example:*

```
DHCP-Client+list

DHCP client enabled on interface ethernet0/0
  Temp IP addr: 192.168.1.22
  Temp subnet mask: 255.255.255.0
    State: BOUND
    DHCP transaction id: 0X100B2AF5
    DHCP Lease server: 192.168.1.1
    Timers:        Lease   =      86400 secs, fires after 23h59m27s
                   Renewal =      43200 secs, fires after 11h59m27s
                   Rebind  =      75600 secs, fires after 20h59m27s
    Other options:
                   Temp default-gateway addr: 192.168.1.1

DHCP-Client+
```

#### 3.2.2.2 RELEASE

Provokes the release of the assigned *lease* for the DHCP client associated with the indicated interface (introduced from the command line).

*Example:*

```
DHCP-Client+release ethernet0/0
DHCP-Client+
```

#### 3.2.2.3 RENEW

Forces the *lease* timer corresponding to the DHCP client associated with the indicated interface (entered from the command line) to advance to its next stage as follows:

- If this is in a BOUND state, it passes to RENEWING.
- If this is in a RENEWING, it passes to REBINDING.
- If the machine status is STOPPED, it starts up and initiates the process.
- In any other state, it does nothing.

*Example:*

```
DHCP-Client+renew ethernet0/0
DHCP-Client+
```

#### 3.2.2.4 EXIT

Exits the DHCP Client monitoring menu.

*Example:*

```
DHCP-Client+exit
```

```
DHCP+
```

### 3.2.3 RELAY

Accesses the DHCP Relay monitoring menu.

*Syntax:*

```
DHCP+relay
```

*Example:*

```
DHCP+relay
DHCP-Relay+
```

The following commands are available in the DHCP Relay monitoring menu:

```
DHCP-Relay+?
  list    List DHCP relay configuration
  exit
DHCP-Relay+
```

#### 3.2.3.1 LIST <mode>

Displays the DHCP relay configuration in the interfaces that are enabled and have at least one server configured. There are two list modes. The first one shows the relay configuration in all interfaces that are enabled. The second mode displays the configuration in the interface specified as a command option.

*Syntax:*

```
DHCP-Relay+list <mode>
```

*Example:*

```
DHCP-Relay+list ?
  all    List current configuration in all interfaces with DHCP-Relay enabled
  ifc    List current DHCP-Relay configuration in interface specified (if enabled)
DHCP-Relay+list all
DHCP Relay configuration
 Interface:    ethernet0/0
   DHCP server address:    192.168.2.25
   Relay agent address:    192.168.1.40
   Source IP address:      192.168.1.40
DHCP-Relay+list ifc ethernet0/0
DHCP Relay configuration
 Interface:    ethernet0/0
   DHCP server address:    192.168.2.25
   Relay agent address:    192.168.1.40
   Source IP address:      192.168.1.40
   Relay-agent-information hexadecimal option: 0207636C6173735F61
DHCP-Relay+
```

#### 3.2.3.2 EXIT

Exits the DHCP Relay monitoring menu.

*Syntax:*

```
DHCP-Relay+exit
```

*Example:*

```
DHCP-Relay+exit
DHCP+
```

### 3.2.4 SERVER

Accesses the DHCP Server monitoring menu.

*Syntax:*

```
DHCP+server
```

*Example:*

```
DHCP+server
DHCP-Server+
```

The following commands are available in the DHCP Server monitoring menu:

```
DHCP-Server+?
  clear-conflict-lease    Clear the conflict flag of a lease
  conflict-leases         Display conflict leases
  leases     Display information of currently active leases
  release    Release an address concession or lease
  release                 Release an address concession or lease
  shared                  Monitoring of shared networks
  exit
DHCP-Server+
```

#### 3.2.4.1 CLEAR-CONFLICT-LEASE IP <ip address>

Returns the specified lease to the pool of available leases. Here, it is classified as *in conflict* by the DHCP server.

*Syntax:*

```
DHCP-Server+clear-conflict-lease ip <ip address> [vrf <vrf name>]
```

#### 3.2.4.2 CONFLICT-LEASES

Through this command, the leases classified by the DHCP server as in conflict are shown. (These are IP addresses the DHCP server received an ICMP response for).

#### 3.2.4.3 LEASES

Displays the information on the currently active *leases*. This includes data such as the assigned IP address, MAC address and type of client hardware, date when the lease was granted and when it ends, etc.

*Syntax:*

```
DHCP-Server+leases
```

*Example:*

```
DHCP-Server+leases
========================================
..:: Currently assigned DHCP Leases ::..
========================================
172.24.254.12   hardware ethernet 00:01:02:f9:cd:f9
                start Fri Oct 07 2005 12:40:56  end Fri Oct 07 2005 13:00:56
                uid '\001\000\001\002\371\315\371'

172.24.254.11   hardware ethernet 00:50:73:77:41:78
                start Fri Oct 07 2005 12:37:29  end Fri Oct 07 2005 12:57:29
                uid '\000router-0050.7377.4178-Et0'

172.24.254.254  hardware ethernet 00:02:44:53:9d:e6
                start Fri Oct 07 2005 12:35:39  end Fri Oct 07 2005 12:55:39
                uid '\001\000\002DS\235\346'

172.24.254.10   hardware ethernet 00:a0:26:70:90:b0
                start Fri Oct 07 2005 12:35:15  end Fri Oct 07 2005 12:55:15
                uid '\000bintec-router'

DHCP-Server+
```

#### 3.2.4.4 OFFERED-LEASES

Returns a list of leases that have been offered to DHCP clients over the last two minutes.

*Syntax:*

```
DHCP-Server+offered-leases
```

*Example:*

```
DHCP-Server+offered-leases
========================================
..:: Currently offered DHCP Leases ::..
========================================
172.24.250.253  hardware ethernet 00:d0:e9:40:33:19
                start Tue Feb 05 2008 16:13:05  end Tue Feb 05 2008 16:15:05
                uid '\001\000\320\351@3\031'

DHCP-Server+
```

#### 3.2.4.5 RELEASE IP <ip / all address>

Lets you release an address concession or *lease*, or all the concessions made using the *all* option. It is equivalent to receiving a DHCPRELEASE message from a DHCP client.

*Syntax:*

```
DHCP-Server+release ip <ip | all address> [vrf <name vrf>]
```

*Example:*

```
DHCP-Server+release ip 172.24.254.254
Lease 172.24.254.254  hardware ethernet 00:02:44:53:9d:e6  released
DHCP-Server+
```

#### 3.2.4.6 SHARED

Displays information on the *shared networks* configured in the DHCP server. This information is presented in a table format where the meaning of each of the columns is as follows:

- *Id*: *shared network* identifier.
- *VRF*: *shared network* VRF instance. The global tag is displayed when the *shared network* has been configured to be exclusively used over the device's main VRF. If a VRF has not been specified in the configuration, this column displays a "-".
- *A-leases*: number of non-static *leases* active on this *shared network*.
- *O-leases*: number of non-static *leases* offered in this *shared network*.
- *C-leases*: number of non-static *leases* in conflict on this *shared network*.
- *Advisor*: identifier for the *advisor* controlling the state of the *shared network*. Where an *advisor* has not been configured, the "-" tag is printed.
- *State*: *shared network* state.

*Example:*

```
DHCP-Server+shared
========================================
..:: Shared networks monitoring ::..
========================================
A-leases: active leases; O-leases: offered leases; C-leases: conflicted leases

Id    VRF         A-leases  O-leases  C-leases    Advisor   State
-----------------------------------------------------------------
2     vrf-aux     0         0         0           3         disabled
1     vpn-office  17        0         1           -         enabled
0     -           5         1         0           -         enabled

DHCP-Server+
```

#### 3.2.4.7 EXIT

Exits the DHCP Server monitoring menu.

*Syntax:*

```
DHCP-Server+exit
```

*Example:*

```
DHCP-Server+exit
DHCP+
```

### 3.2.5 EXIT

Exits the DHCP protocol monitoring menu and returns to the general monitoring prompt (+).

*Syntax:*

```
DHCP+exit
```

*Example:*

```
DHCP+exit
+
```

# Chapter 4 DHCP Configuration Example

## 4.1 Scenario 1

The scenario given as an example is as follows:

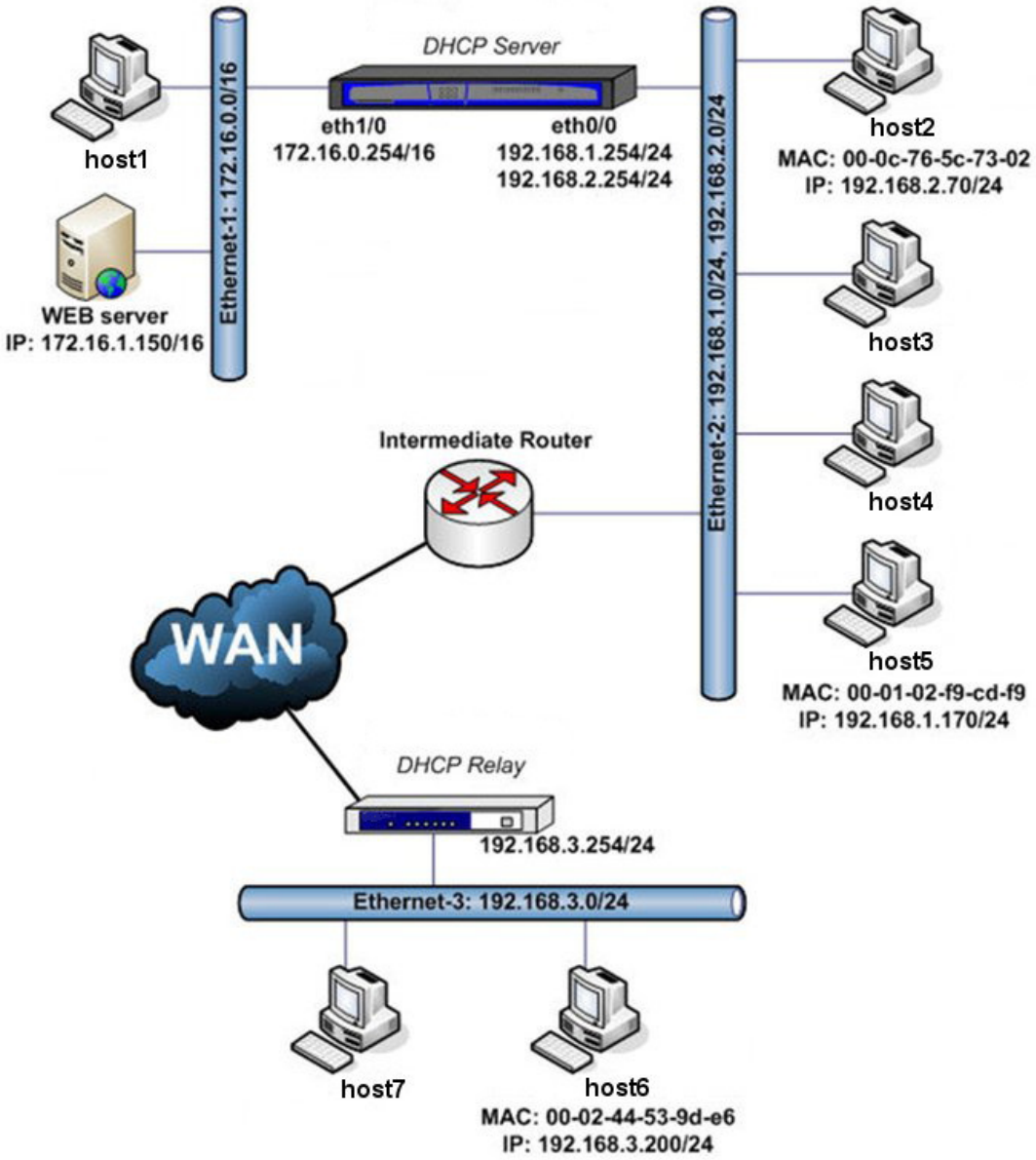



*Fig. 1:* **DHCP configuration example**

A *DHCP Server* assigns addresses (together with other configuration elements) to the devices connected in subnets 172.16.0.0/16, 196.168.1.0/24, 192.168.2.0/24 and 192.168.3.0/24.

There is also a *DHCP Relay*, which sends DHCP messages originating from the DHCP clients found in subnet 192.168.3.0/24 to the DHCP server that assigns addresses to devices.

Physically, you can distinguish 3 different local networks in this scenario: *ethernet-1*, *ethernet-2* (which supports 2 subnets), both directly connected to the DHCP server, and *ethernet-3* connected to the DHCP Relay. A given number of devices (those that provide their MAC address together with an IP address) are specifically configured so they are assigned a specific IP address.

### 4.1.1 DHCP Relay Configuration

We assume that the configuration that is not related to DHCP protocol operation has been correctly carried out and that the *DHCP Relay* LAN interface has IP address 192.168.3.254/24.

To configure the router so that it behaves as a *DHCP Relay*, carry out the steps described below.

#### 4.1.1.1 Enable DHCP Relay and access the Relay menu

To access the DHCP relay configuration prompt and to globally enable it (in all the interfaces):

```
*config
Config>protocol dhcp
-- DHCP Configuration --
DHCP config>relay
-- DHCP Relay Configuration --
DHCP-Relay config>enable all-interfaces
DHCP-Relay config>
```

#### 4.1.1.2 Aggregate the DHCP Server

The DHCP server is added at the DHCP Relay configuration prompt. The DHCP messages originating from subnet 192.168.1.254/24 will be sent to this server:

```
DHCP-Relay config>server 192.168.1.254 dhcp-server
DHCP-Relay config>
```

DHCP protocol configuration in the DHCP Relay is as follows:

```
DHCP config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; Super Router * * Version 10.7.3TM
      relay
; -- DHCP Relay Configuration --
         enable all-interfaces
         server 192.168.1.254 dhcp-server
      exit
;
```

Save the configuration and restart the *DHCP Relay* router.

### 4.1.2 DHCP Server Configuration

We assume that the configuration that is not related to DHCP protocol operation has been correctly carried out and that the *DHCP Server* has 192.168.1.254/24 and 192.168.2.254/24 IP addresses for the ethernet0/0 interface and 172.16.0.254/16 for the ethernet1/0 interface.

To configure the router so it behaves as a *DHCP Server*, carry out the steps described below.

#### 4.1.2.1 Enabling the DHCP Server and accessing the Server menu

To access the DHCP configuration prompt and enable the *DHCP Server*:

```
*config
Config>protocol dhcp

-- DHCP Configuration --
DHCP config>server

-- DHCP Server Configuration --
DHCP-Server config>enable
DHCP-Server config>
```

#### 4.1.2.2 Configure the parameters and global options

Configure the *DHCP Server* name:

```
DHCP-Server config>global server-name dhcp-server
DHCP-Server config>
```

This sets the default lease time for addresses at 8 hours (28800 seconds), while the maximum time is one day (24 hours, 86400 seconds):

```
DHCP-Server config>global default-lease-time 8h
DHCP-Server config>global max-lease-time 24h
```

```
DHCP-Server config>
```

Check the global parameter configuration:

```
DHCP-Server config>list global
 ============================
 =    GLOBAL Parameters     =
 ============================
   Server Name: dhcp-server
   Next Server: 0.0.0.0
   Lease time: Default 28800, Maximum 86400
   Boot Unknown clients: Yes
   One Lease Per client: Yes
   Dynamic DNS Updates (FQDN): Disabled (deny client updates)
   DDNS Update Hostname: client hostname

DHCP-Server config>
```

#### 4.1.2.3 Aggregate Shared Networks

To assign addresses to all the segments of the sample scenario, 3 *shared networks* need to be available. The default *shared network,* with identifier "", is always available and cannot be eliminated. Since you need 2 additional *shared networks*, these must be added.

```
DHCP-Server config>shared 1
DHCP-Server config>shared 2
DHCP-Server config>
```

Now you have 3 *shared networks* available, 0, 1 and 2. The network segment corresponding to the ethernet0/0 interface (which contains subnets 192.168.1.0/24 and 192.168.2.0/24) is configured in *shared network* 0. The part corresponding to the ethernet1/0 interface network segment is configured in *shared network* 1 and the segment reaching the server through the DHCP Relay is configured in *shared network* 2.

#### 4.1.2.4 Configuration of Subnets and Hosts

##### 4.1.2.4.1 Shared Network Subnets and Hosts

This *shared network* contains two subnets: 192.168.1.0/24 and 192.168.2.0/24 and wishes to assign addresses in each one. Since the server has an address for each of the subnets in its LAN (through which it assigns addresses), specifying a *SERVER-IDENTIFIER* is not necessary.

Creating the *subnets*.

```
DHCP-Server config>subnet 192.168.1 0 network 192.168.1.0 255.255.255.0
DHCP-Server config>subnet 192.168.2 0 network 192.168.2.0 255.255.255.0
DHCP-Server config>
```

A range of addresses, which the server will assign to clients according to the petitions received (from 192.168.1.125 to 192.168.1.150) is configured in subnet 192.168.1.0/24. The default router in this subnet is 192.168.1.1 (for example), which will also be the DNS server. It is further established that PC **host5** exclusively and permanently has address 192.168.1.170.

```
DHCP-Server config>subnet 192.168.1 0 range 192.168.1.125 192.168.1.150
DHCP-Server config>subnet 192.168.1 0 router 192.168.1.1
DHCP-Server config>subnet 192.168.1 0 dns-server 192.168.1.1
DHCP-Server config>
```

Now configure PC **host5**.

```
DHCP-Server config>host host5 0 ethernet 000102f9cdf9
DHCP-Server config>host host5 0 fixed-ip 192.168.1.170
DHCP-Server config>
```

A range of addresses (from 192.168.2.55 to 192.168.2.75) is configured in subnet 192.168.2.0/24 and PC **host2** with IP address 192.168.2.70. In this case, the default router is 192.168.2.254 (the DHCP server) while the DNS server is 192.168.2.80. As the PC *host2* IP address is within the range of addresses the server assigns, it is necessary to separate the initial range into two separate ranges to avoid assigning the *host2* IP address.

```
DHCP-Server config>subnet 192.168.2 0 range 192.168.2.55 192.168.2.69
DHCP-Server config>subnet 192.168.2 0 range 192.168.2.71 192.168.2.75
DHCP-Server config>subnet 192.168.2 0 router 192.168.2.254
```

```
DHCP-Server config>subnet 192.168.2 0 dns-server 192.168.2.80
DHCP-Server config>host host2 0 ethernet 000c765c7302
DHCP-Server config>host host2 0 fixed-ip 192.168.2.70
DHCP-Server config>
```

#### 4.1.2.4.2 Shared Network 1 Subnets and Host

In this *shared network*, there is a single subnet. A range of addresses is defined, a default router and a DNS server (which will be the DHCP server itself) and there is no need to configure a host with a fixed IP address.

However, given that a WEB server configured with a static IP (172.16.1.150/16) exists in the subnet, avoid this address in the range of addresses to be assigned.

```
DHCP-Server config>subnet 172.16 1 network 172.16.0.0 255.255.0.0
DHCP-Server config>subnet 172.16 1 range 172.16.1.100 172.16.2.149
DHCP-Server config>subnet 172.16 1 range 172.16.1.151 172.16.2.200
DHCP-Server config>subnet 172.16 1 router 172.16.0.254
DHCP-Server config>subnet 172.16 1 dns-server 172.16.0.254
DHCP-Server config>
```

#### 4.1.2.4.3 Shared Network 2 Subnets and Host

This *shared network* corresponds to the physical segment accessing the DHCP server through the DHCP Relay. A range of addresses and a host with a specific IP address (**host6**) is defined in this *shared network*.

In this case, indicate the DHCP Relay LAN interface address as the *SERVER-IDENTIFIER* so the client's successive DHCP messages reach the server.

You also need to establish that the default router and the DNS server is the DHCP Relay itself.

```
DHCP-Server config>subnet 192.168.3 2 network 192.168.3.0 255.255.255.0
DHCP-Server config>subnet 192.168.3 2 server-identifier 192.168.3.254
DHCP-Server config>subnet 192.168.3 2 range 192.168.3.50 192.168.3.100
DHCP-Server config>subnet 192.168.3 2 router 192.168.3.254
DHCP-Server config>subnet 192.168.3 2 dns-server 192.168.3.254
DHCP-Server config>host host6 2 ethernet 000244539de6
DHCP-Server config>host host6 2 fixed-ip 192.168.3.200
DHCP-Server config>
```

### 4.1.2.5 Complete Configuration List

Verify the configuration through a complete configuration list.

```
DHCP-Server config>LIST ALL
 ============================
 =    GLOBAL Parameters    =
 ============================
   Server Name: dhcp-server
   Next Server: 0.0.0.0
   Lease time: Default 28800, Maximum 86400
   Boot Unknown clients: Yes
   One Lease Per client: Yes
   Dynamic DNS Updates (FQDN): Disabled (deny client updates)
   DDNS Update Hostname: client hostname
============================
 =   SHARED NETWORK List   =
 ============================
   Shared Network: 1
   Shared Network: 2
 ============================
 =     SUBNET List    0    =
 ============================
 SUBNET: 192.168.1
   Address: 192.168.1.0, Mask: 255.255.255.0
   Range: 192.168.1.125   --> 192.168.1.150
   - DNS Server: 192.168.1.1
   - Router: 192.168.1.1
 SUBNET: 192.168.2
   Address: 192.168.2.0, Mask: 255.255.255.0
```

```
   Range: 192.168.2.55    --> 192.168.2.69
   Range: 192.168.2.71    --> 192.168.2.75
   - DNS Server: 192.168.2.80
   - Router: 192.168.2.254
 ============================
 =     SUBNET List    1    =
 ============================
 SUBNET: 172.16
   Address: 172.16.0.0, Mask: 255.255.0.0
   Range: 172.16.1.100    --> 172.16.2.149
   Range: 172.16.1.151    --> 172.16.2.200
   - DNS Server: 172.16.0.254
   - Router: 172.16.0.254
 ============================
 =     SUBNET List    2    =
 ============================
 SUBNET: 192.168.3
   Address: 192.168.3.0, Mask: 255.255.255.0
   Range: 192.168.3.50    --> 192.168.3.100
   Server Identifier: 192.168.3.254
   - DNS Server: 192.168.3.254
   - Router: 192.168.3.254
 ============================
 =      HOST List    0     =
 ============================
HOST: host5
   Ethernet hw: 000102F9CDF9, Fixed Address: 192.168.1.170

 HOST: host6
   Ethernet hw: 000C765C7302, Fixed Address: 192.168.2.70
 ============================
 =      HOST List    1     =
 ============================
   No Host defined
 ============================
 =      HOST List    2     =
 ============================
 HOST: host6
   Ethernet hw: 000244539DE6, Fixed Address: 192.168.3.200
```

The DHCP protocol configuration in the DHCP Server is as follows:

```
; Showing System Configuration ...
;
protocol dhcp
; -- DHCP Configuration --
   enable server
   server
; -- DHCP Server Configuration --
      global default-lease-time 8h
      global server-name dhcp-server
      shared 1
      shared 2
;
      subnet 192.168.1 0 address 192.168.1.0
      subnet 192.168.1 0 mask 255.255.255.0
      subnet 192.168.1 0 range 192.168.1.125 192.168.1.150
      subnet 192.168.1 0 dns-server 192.168.1.1
      subnet 192.168.1 0 router 192.168.1.1
;
      subnet 192.168.2 0 address 192.168.2.0
      subnet 192.168.2 0 mask 255.255.255.0
      subnet 192.168.2 0 range 192.168.2.55 192.168.2.69
      subnet 192.168.2 0 range 192.168.2.71 192.168.2.75
      subnet 192.168.2 0 dns-server 192.168.2.80
      subnet 192.168.2 0 router 192.168.2.254
;
      subnet 172.16 1 address 172.16.0.0
```

```
      subnet 172.16 1 mask 255.255.0.0
      subnet 172.16 1 range 172.16.1.100 172.16.2.149
      subnet 172.16 1 range 172.16.1.151 172.16.2.200
      subnet 172.16 1 dns-server 172.16.0.254
      subnet 172.16 1 router 172.16.0.254
;
      subnet ken-192.168.3 2 address 192.168.3.0
      subnet ken-192.168.3 2 mask 255.255.255.0
      subnet ken-192.168.3 2 range 192.168.3.50 192.168.3.100
      subnet ken-192.168.3 2 server-identifier 192.168.3.254
      subnet ken-192.168.3 2 dns-server 192.168.3.254
      subnet ken-192.168.3 2 router 192.168.3.254
;
      host host5 0 ethernet 00-01-02-f9-cd-f9
      host host5 0 fixed-ip 192.168.1.170
;
      host host2 0 ethernet 00-0c-76-5c-73-02
      host host2 0 fixed-ip 192.168.2.70
;
      host host6 2 ethernet 00-02-44-53-9d-e6
      host host6 2 fixed-ip 192.168.3.200
;
   exit
;
exit
;
```

Now save the configuration and restart the *DHCP Server* router.

## 4.2 Scenario 2: DHCP-Relay Multi-VRF

We will now include an example of how to configure a relay agent in a **bintec Router** that is part of a multi-VRF scenario.

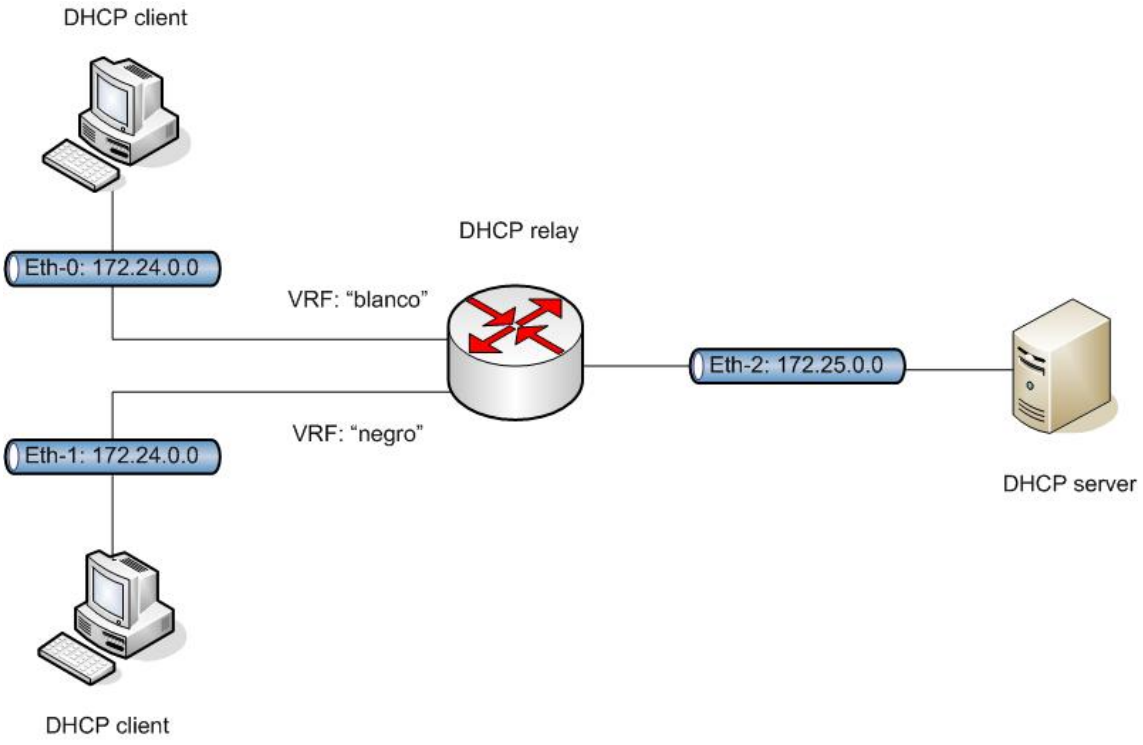



*Fig. 2:* **Relay agent configuration example**

Apart from the main one, there are two VRFs configured in the **bintec Router**: blanco and negro. Two of the router’s Ethernet interfaces respectively pertain to the two indicated VRFs. The DHCP clients’ petitions arrive through both interfaces. Through a third Ethernet interface, in this case pertaining to the global routing table, we can access a DHCP server that is going to respond to the DHCP petitions from the relay.

The following sections detail the configuration corresponding to the relay agent. We will also restrict ourselves to the

specific configuration for the relay agent, assuming that the VRF and associated interfaces are already configured. To do this, let's assume the interface associated with VRF *blanco* is ethernet0/0.1, the one associated with VRF *negro* is ethernet0/0.2 and the interface through which you access the DHCP sever is ethernet0/0.3.

### 4.2.1 Enabling the "relay-agent-information" option

First, configure the relay agent so that, in the packets addressed to the server, it inserts the necessary information associated with the VRF through which clients are connected. The goal is for the DHCP server to know what options it can offer when responding to clients.

```
*config
Config>protocol dhcp
-- DHCP Configuration --
DHCP config>relay
-- DHCP Relay Configuration --
DHCP-Relay config>vrf blanco

DHCP-Relay vrf config>agent-information vpn
DHCP-Relay vrf config>exit
DHCP-Relay config>vrf negro

DHCP-Relay vrf config>agent-information vpn
DHCP-Relay vrf config>
```

### 4.2.2 Configuring the DHCP server IP address

Finally, to complete the minimum configuration, configure the DHCP server IP address in the interface configuration over which we want to carry out relay.

In this case, the server IP address is 172.25.0.150, accessible through the global routing table (main VRF).

```
*config
Config>network ethernet0/0.1
-- Ethernet Subinterface Configuration --
ethernet0/0.1 config>ip dhcp-relay server global-vrf 172.25.0.150
ethernet0/0.1 config>exit
Config>network ethernet0/0.2
-- Ethernet Subinterface Configuration --
ethernet0/0.2 config>ip dhcp-relay server global-vrf 172.25.0.150
ethernet0/0.2 config>
```

### 4.2.3 Listing the complete configuration for the router

Below, the complete configuration for the router to act as the DHCP relay agent in this example is provided.

```
*config
Config>show config
; Showing Menu and Submenus Configuration for access-level 15 ...
; Super Router * * Version 10.7.4-Alfa TM

   log-command-errors
   no configuration
   add device eth-subinterface ethernet0/0 1
   add device eth-subinterface ethernet0/0 2
   add device eth-subinterface ethernet0/0 3
   feature vrf
; -- VRF user configuration -
      vrf blanco
      vrf negro
   exit
;
;
;
;
   network ethernet0/0.1
; -- Ethernet Subinterface Configuration --
      ip vrf forwarding blanco
```

```
;
      ip address 172.24.0.1 255.255.0.0
;
;
;
      ip dhcp-relay server global-vrf 172.25.0.150
;
;
;
;
   exit
;
   network ethernet0/0.2
; -- Ethernet Subinterface Configuration --
      ip vrf forwarding negro
;
      ip address 172.24.0.1 255.255.0.0
;
;
;
      ip dhcp-relay server global-vrf 172.25.0.150
;
;
;
;
   exit
;
;
   network ethernet0/0.3
; -- Ethernet Subinterface Configuration --
      ip address 172.25.0.1 255.255.0.0
;
;
;
;
;
;
;
   exit
;
;
;
;
   protocol dhcp
; -- DHCP Configuration --
      relay
; -- DHCP Relay Configuration --
         vrf blanco
            agent-information vpn
         exit
;
         vrf negro
            agent-information vpn
         exit
;
      exit
;
;
;
   exit
;
   dump-command-errors
   end
Config>
```

## 4.3 Scenario 3: DHCP Server with classes

This example aims to show the minimum configuration for a bintec DHCP server using the ‘class’ concept. The latter includes a group of DHCP clients to whom we want to give a specific configuration (in this case, a range of specific addresses).

This group of clients will be clearly identified by means of a special DHCP protocol option included in their DHCP request. This shall be DHCP option 60 (vendor-class identifier):

The server’s minimum configuration includes the definition of a class using the identifier associated with the clients to which services are going to be provided. Given that we want to assign a pool of dedicated IP addresses, we need to associate said class with a previously created subnet and complete the configuration by specifying the range to be reserved for this group of clients.

We are only going to show the DHCP server configuration, as we are assuming that the server IP addresses have been correctly configured.

```
*config
Config>protocol dhcp
-- DHCP Configuration --
DHCP config>server
-- DHCP Server Configuration --
DHCP-Server config>enable
DHCP-Server config>subnet datos 0 network 172.24.0.0 255.255.0.0
DHCP-Server config>subnet voz 0 network 172.25.0.0 255.255.0.0
DHCP-Server config>subnet datos 0 range 172.24.252.10 172.24.252.90
DHCP-Server config>class voz 0 id hex 0x0123456789abcdef
DHCP-Server config>class voz 0 subnet-name voz
DHCP-Server config>class voz 0 range 172.25.252.110 172.25.252.190
DHCP-Server config>
```

As you can see, we have defined two subnets: datos and voz. In turn, we have defined a class with a fictitious identifier (theoretically the hexadecimal string sent to the clients in this class). We have associated this class with the voice subnet and finally defined a range of IP addresses to assign to the members of this class.

Below, you can see the resulting configuration list for the DHCP server.

```
DHCP-Server config>list subnet
 ============================
 =     SUBNET List    0     =
 ============================
 SUBNET: datos
   Address: 172.24.0.0, Mask: 255.255.0.0
   Range: 172.24.252.10   --> 172.24.252.90
 SUBNET: voz
   Address: 172.25.0.0, Mask: 255.255.0.0
DHCP-Server config>list class
 ============================
 =     CLASS List    0      =
 ============================
 CLASS: voz
   Identifier: 0x0123456789abcdef
   Associated subnet: voz
   Range: 172.25.252.110  --> 172.25.252.190
DHCP-Server config>
```

## 4.4 Scenario4: Multi-VRF DHCP Server

The following schema shows a simple multi-VRF DHCP server configuration scenario:

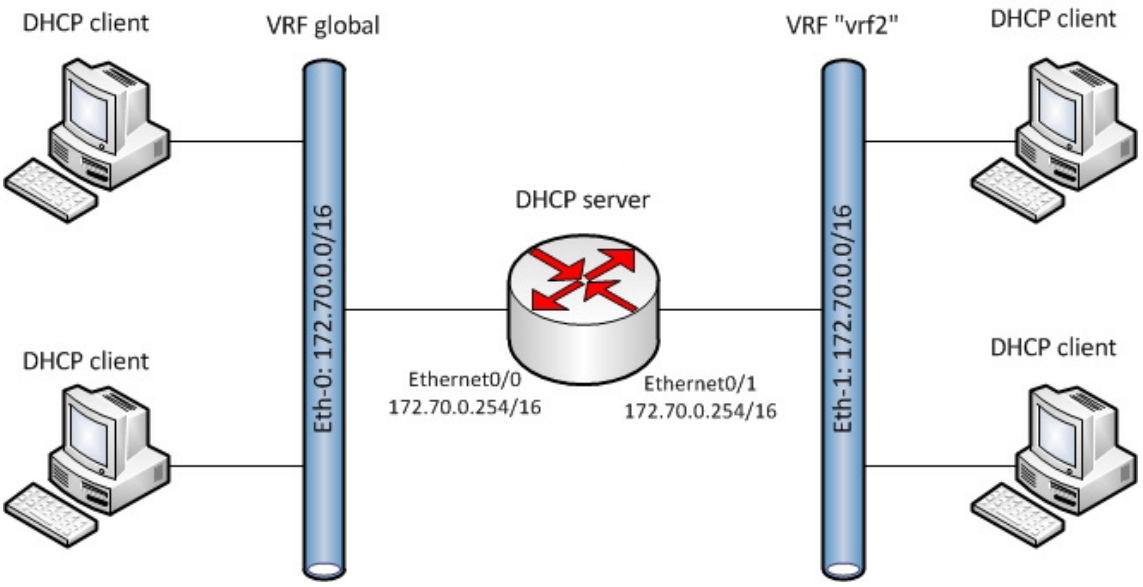



*Fig. 3:* **Simple multi-VRF DHCP server configuration scenario**

In this scenario, a server configured in a **bintec Router** is providing DHCP services to two networks: Eth-0 and Eth-1. The router accesses each network through a different VRF instance so the IP addresses in both networks can overlap.

To communicate with the devices located in the first network, the router uses the ethernet0/0 interface configured in the main VRF, whose IP address is 172.70.0.254/16. A secondary VRF instance is defined as *vrf2*. It is configured in the ethernet0/1 interface to access the devices in the second network. Both networks are defined by the same network address (i.e., 172.70.0.0/16). The ethernet0/1 interface is configured with IP address 172.70.0.254/16.

Two *shared networks* are configured in the DHCP server, one per interface. Through them, IP addresses are assigned to the DHCP clients in both networks.

### 4.4.1 Configuring the DHCP server

Define the *net-70 subnet* in *shared network* 1, which is used by the server to handle the client packets that arrive through the ethernet0/0 interface. The addresses assigned by the *net-70 subnet* range from 172.70.2.1 to 172.70.2.20.

Below, a *shared network* with identifier 1 has been configured for VRF instance *vrf2* so that only the interfaces in this VRF can use it. *Subnet net2-70* has been defined for this *shared network* 1, with addresses ranging from 172.70.2.1 to 172.70.2.20.

```
      server
; -- DHCP Server Configuration --
         enable
;
         shared 1 global-vrf
         shared 2 vrf vrf2
;
         subnet net-70 1 network 172.70.0.0 255.255.0.0
         subnet net-70 1 range 172.70.2.1 172.80.2.20
         subnet net-70 1 router 172.70.0.1
;
         subnet net2-70 2 network 172.70.0.0 255.255.0.0
         subnet net2-70 2 range 172.70.2.1 172.70.2.20
         subnet net2-70 2 router 172.70.0.1
;
      exit
```

## 4.5 Scenario 5: Relay agent with backup DHCP server

This example shows a basic scenario where the **bintec Router**'s DHCP server is configured to offer backup to the Relay Agent should the remote DHCP servers go down. The scenario is as follows:

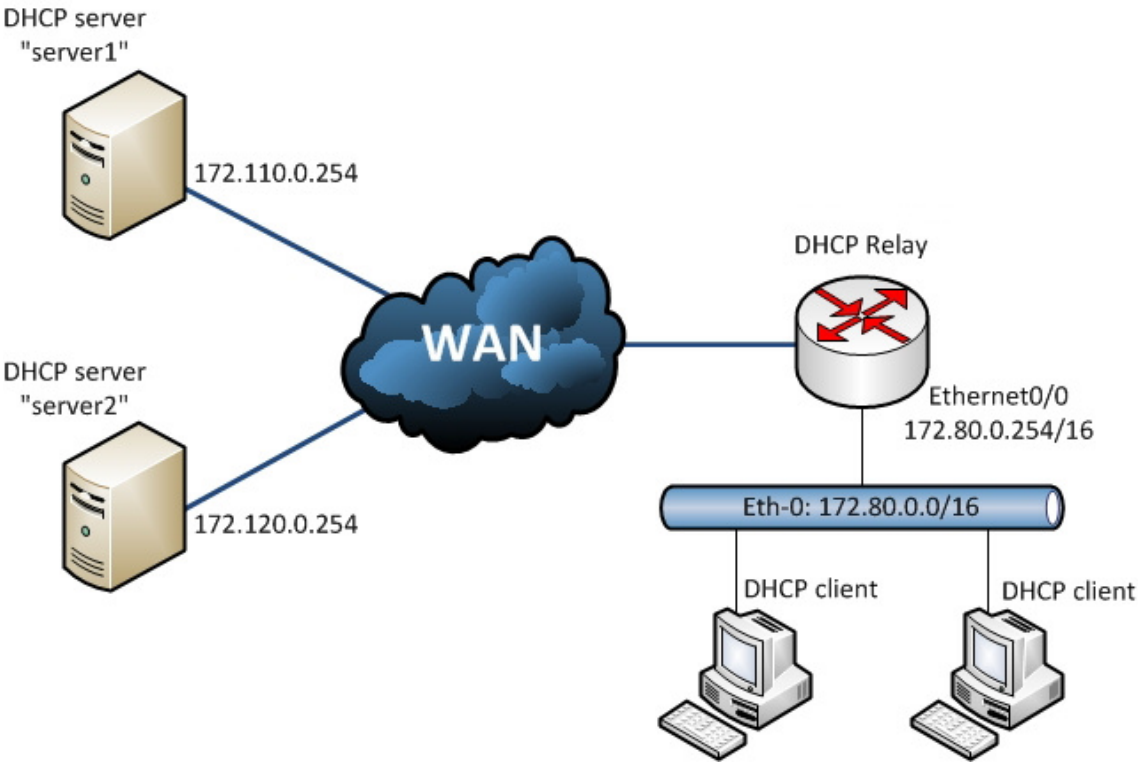



*Fig. 4:* **Relay agent with backup DHCP server**

The Relay Agent is enabled in the **bintec Router** through the ethernet0/0 interface that provides services to DHCP clients in network 172.80.0.0/16. The packets received by the Relay are forwarded to the two *server1* and *server2* DHCP servers with IP addresses 172.110.0.254 and 172.120.0.254 respectively.

A level indicator is configured so that the Relay Agent can detect when remote servers are down. This updates each time the agent changes state.

In order to ensure continuity in the service if agent servers stop responding, a *shared network* is configured in the **bintec Router**'s DHCP server. It remains disabled until needed. This *shared network* is configured to be controlled by an *advisor*. This *advisor* notifies the *shared network* whenever the Relay agent's level indicator exceeds a certain threshold (at which point the *shared network* activates).

### 4.5.1 Configuring the NSLA feature

Configure a filter with identifier 1 using the NSLA feature. This filter is configured so that it activates when the indicator level exceeds threshold value 5 and deactivates when it falls below 5. Alarm 1 is configured so that it is triggered by filter 1 and notifies advisor 1. The NSLA feature configuration is as follows:

```
   feature nsla
; -- Feature Network Service Level Advisor --
      enable
;
      filter 1 level-indicator 1
      filter 1 activation threshold 5
      filter 1 deactivation threshold 5
;
      alarm 1 filter-id 1
;
      advisor 1 alarm-id 1
;
   exit
```

For further information on the configuration of this feature, please see manual bintec Dm704-I – NSLA.

### 4.5.2 Configuring the Relay Agent

The Relay Agent is enabled to listen to DHCP clients in all of the router's interfaces. Two DHCP servers are configured in the main VRF, with IP addresses 172.110.0.254 and 172.120.0.254.

Subsequently, using the **update level-indicator** command, configure this so indicator level 1 increases by a value of

10 when the Relay Agent passes to DOWN. This happens when both servers stop responding. Through the **monitor-options packets-threshold** command, indicate that a server that does not respond after 5 DHCPDISCOVER packets are sent is to be considered down. While the agent is DOWN, DHCPDISCOVER packets are generated every 30 seconds and transmitted to both servers to check they are still not responding. This 30-second period is configured through the **monitor-options interval** command. The configuration for the Relay agent is shown below:

```
      relay
; -- DHCP Relay Configuration --
         enable all-interfaces
         server 172.120.0.254
         server 172.110.0.254
         update level-indicator 1 value 10 when-down
         monitor-options packets-threshold 5
         monitor-options interval 30s
;
      exit
```

### 4.5.3 Configuring the DHCP Server

In the router's DHCP server, configure *shared network* 1 and indicate that it's going to be controlled by *advisor* 1 through the **track nsla-adivsor** option. In this *shared network*, define subnet *net-80* using the range of IP addresses that can be assigned to clients in network 172.80.0.0/16. The server configuration is as follows:

```
      server
; -- DHCP Relay Configuration --
         enable
;
         global default-lease-time 4m
         global max-lease-time 5m
;
         shared 1 track nsla-advisor 1
;
         subnet net-80 1 network 172.80.0.0 255.255.0.0
         subnet net-80 1 range 172.80.2.1 172.80.2.20
         subnet net-80 1 router 172.80.0.1
;
      exit
```