



Configuring the Cisco IOS DHCP Client

Last Updated: June 13, 2012

Cisco IOS Dynamic Host Configuration Protocol (DHCP) client software provides the flexibility to include various configuration options for the DHCP client. A DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address. This module describes the concepts and tasks needed to configure the Cisco IOS DHCP client. It includes information on the Cisco DHCP FORCERENEW feature, which provides entity authentication and message authentication.

- [Finding Feature Information, page 1](#)
- [Restrictions for Configuring the DHCP Client, page 1](#)
- [Information About the DHCP Client, page 2](#)
- [How to Configure the DHCP Client, page 4](#)
- [Configuration Examples for the DHCP Client, page 10](#)
- [Additional References, page 13](#)
- [Feature Information for the DHCP Client, page 14](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring the DHCP Client

The DHCP client can be configured on Ethernet interfaces and on PPP over ATM (PPPoA) and certain ATM interfaces. The DHCP client works with ATM point-to-point interfaces and will accept any encapsulation type. For ATM multipoint interfaces, the DHCP client is supported using only the aal5snap encapsulation type combined with Inverse Address Resolution Protocol (ARP). Inverse ARP, which builds an ATM map entry, is necessary to send unicast packets to the server (or relay agent) on the other end of the connection. Inverse ARP is supported only for the aal5snap encapsulation type.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

For multipoint interfaces, an IP address can be acquired using other encapsulation types because broadcast packets are used. However, unicast packets to the other end will fail because there is no ATM map entry and thus DHCP renewals and releases also fail.

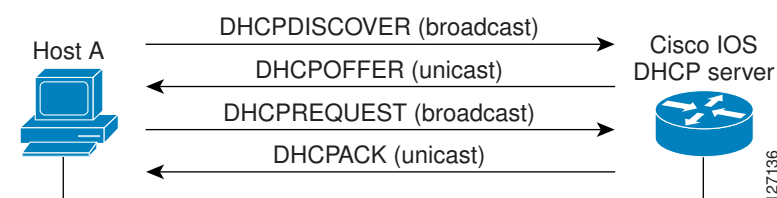
Information About the DHCP Client

- [DHCP Client Operation, page 2](#)
- [DHCP Client Overview, page 2](#)
- [DHCP Client on WAN Interfaces, page 3](#)
- [DHCP FORCERENEW, page 3](#)

DHCP Client Operation

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. A DHCP client is an Internet host using DHCP to obtain configuration parameters such as an IP address. The figure below shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a DHCP server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message. The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

Figure 1 DHCP Request for an IP Address from a DHCP Server



A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address.

The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

DHCP Client Overview

The configurable DHCP client functionality allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server.

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 12--This option specifies the name of the client. The name may or may not be qualified with the local domain.
- Option 33--This option is used to configure a list of static routes in the client.

- Option 51--This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address.
- Option 55--This option allows the DHCP client to request certain options from the DHCP server. The **ip dhcp client request** command allows the system administrator to turn off some of the requested options, thus removing them from the request list.
- Option 60--This option allows the user to configure the vendor class identifier string to use in the DHCP interaction.
- Option 61--This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.
- Option 120--This option is used to specify a 32-bit (binary) IPv4 address to be used by the Session Initiation Protocol (SIP) client to locate a SIP server.
- Option 121--This option is used to configure classless static routes by specifying classless network destinations in these routes: that is, each routing table entry includes a subnet mask.

**Note**

If a request includes both static routes and classless static routes, the client uses only the classless static routes. If the DHCP server returns both a classless static route option and a router option, the DHCP client ignores the router option.

- Option 125--This option is used by DHCP clients and servers to exchange vendor-specific information.

DHCP Client on WAN Interfaces

The DHCP client on WAN interfaces allows a DHCP client to acquire an IP address over PPPoA and certain ATM interfaces. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as Domain Name System (DNS) addresses, the DNS default domain name, and the default route.

The configuration of PPPoA and Classical IP and ARP over ATM already allows for a broadcast capability over the interface (using the **broadcast** keyword on the ATM interface). Most changes in this feature are directed at removing already existing restrictions on what types of interfaces are allowed to send out DHCP packets (previously, dialer interfaces have not been allowed). This feature also ensures that DHCP RELEASE messages are sent out the interface before a connection is allowed to be broken.

DHCP FORCERENEW

The Cisco DHCP FORCERENEW feature provides entity authentication and message authentication, in accordance with RFC 3118, by which DHCP clients and servers authenticate the identity of other DHCP entities and verify that the content of a DHCP message has not been changed during delivery through the network.

The message authentication mechanism allows servers to determine whether a request for DHCP information comes from a client that is authorized to use the network. It also allows clients to verify that a DHCP server can be trusted to provide valid configuration.

The Cisco DHCP FORCERENEW feature requires authentication. All client-server exchanges must be authenticated: The **ip dhcp client authentication mode** and **key chain** commands must be configured.

When the client gets a FORCERENEW message, it does the following:

- Authenticates the message according to the authentication mode specified in the **ip dhcp client authentication mode** command. The Cisco DHCP FORCERENEW feature supports both token-based and Message Digest 5 (MD5)-based authentication.
 - Token-based authentication is useful only for basic protection against inadvertently instantiated DHCP servers. Tokens are transmitted in plain text; they provide weak authentication and do not provide message authentication.
 - MD5-based authentication provides better message and entity authentication because it contains a single-use value generated by the source as a message authentication code.
- Changes its state to RENEW.
- Tries to renew its lease according to normal DHCP procedures.

The client discards any multicast FORCERENEW message or message that fails authentication.

How to Configure the DHCP Client

- [Configuring the DHCP Client, page 4](#)
- [Forcing a Release or Renewal of a DHCP Lease for a DHCP Client, page 7](#)
- [Enabling FORCERENEW-Message Handling, page 9](#)

Configuring the DHCP Client

- [DHCP Client Default Behavior, page 4](#)
- [Troubleshooting Tips, page 6](#)

DHCP Client Default Behavior

Cisco routers running Cisco IOS software include DHCP server and relay agent software, which are enabled by default. Your router can act as both the DHCP client and DHCP server. Use the **ip address dhcp** command to obtain IP address information for the configured interface.

You must configure the **ip dhcp client** commands before entering the **ip address dhcp** command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The **ip dhcp client** commands are checked only when an IP address is acquired from DHCP. If any of the **ip dhcp client** commands are entered after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will take effect only after either the **ip address dhcp** command or the **release dhcp** and **renew dhcpEXEC** commands have been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip dhcp client client-id** { *interface-name* | **ascii string** | **hex string** }
5. **ip dhcp client class-id** { *string* | **hex string** }
6. **ip dhcp client lease** *days* [*hours*][*minutes*]
7. **ip dhcp client hostname** *host-name*
8. [**no**] **ip dhcp client request** *option-name*
9. **ip address dhcp**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 interface <i>type number</i> Example: <pre>Router(config)# interface Ethernet 1</pre>	Configures an interface type and enters interface configuration mode.
Step 4 ip dhcp client client-id { <i>interface-name</i> ascii string hex string } Example: <pre>Router(config-if)# ip dhcp client client-id ascii mytest1</pre>	(Optional) Specifies the client identifier. <ul style="list-style-type: none"> • When you specify the no form of this command, the configuration is removed and the system returns to using the default form. It is not possible to configure the system to not include a client identifier.

Command or Action	Purpose
<p>Step 5 <code>ip dhcp client class-id {string hex string}</code></p> <p>Example:</p> <pre>Router(config-if)# ip dhcp client class-id my-class-id</pre>	(Optional) Specifies the class identifier.
<p>Step 6 <code>ip dhcp client lease days [hours][minutes]</code></p> <p>Example:</p> <pre>Router(config-if)# ip dhcp client lease 2</pre>	(Optional) Configures the duration of the lease for an IP address that is requested from a DHCP client to a DHCP server.
<p>Step 7 <code>ip dhcp client hostname host-name</code></p> <p>Example:</p> <pre>Router(config-if)# ip dhcp client hostname router1</pre>	(Optional) Specifies or modifies the hostname sent in the DHCP message.
<p>Step 8 <code>[no] ip dhcp client request option-name</code></p> <p>Example:</p> <pre>Router(config-if)# no ip dhcp client request tftp-server-address</pre>	<p>(Optional) Configures a DHCP client to request an option from a DHCP server.</p> <ul style="list-style-type: none"> The option name can be tftp-server-address, netbios-nameserver, vendor-specific, static-route, domain-name, dns-nameserver, or router. By default, all these options are requested. The no form of the command instructs the system to not request certain options.
<p>Step 9 <code>ip address dhcp</code></p> <p>Example:</p> <pre>Router(config-if)# ip address dhcp</pre>	Acquires an IP address on an interface from DHCP.

Troubleshooting Tips

To verify the configuration, you can use the **debug dhcp detail** command to display the DHCP packets that were sent and received. To display the server side of the DHCP interaction, use the **debug ip dhcp server packets** command.

The following are troubleshooting tips for DHCP clients on WAN interfaces:

- An ATM primary interface is always multipoint.
- An ATM subinterface can be multipoint or point-to-point.
- If you are using a point-to-point interface, the routing table determines when to send a packet to the interface and ATM map entries are not needed. Consequently, Inverse ARP, which builds ATM map entries, is not needed.

- If you are using a multipoint interface, you must use Inverse ARP to discover the IP address of the other side of the connection.
- You can specify Inverse ARP through the **protocol ip inarp** command. You must use the **aal5snap** encapsulation type when using Inverse ARP because it is the only encapsulation type that supports Inverse ARP.

Forcing a Release or Renewal of a DHCP Lease for a DHCP Client

Perform this task to force a release or renewal of a DHCP lease for a DHCP client.

Forcing a release or renewal of a DHCP lease for a DHCP client provides the ability to perform two independent operations from the command-line interface (CLI) in EXEC mode:

- Immediately release a DHCP lease for a DHCP client.
- Force a DHCP renewal of a lease for a DHCP client.

This functionality provides the following benefits:

- Eliminates the need to go into the configuration mode to reconfigure the router to release or renew a DHCP lease.
- Simplifies the release and renewal of a DHCP lease.
- Reduces the amount of time spent performing DHCP IP release and renewal configuration tasks.

- [DHCP Release and Renew CLI Operation, page 7](#)

DHCP Release and Renew CLI Operation

- [Release a DHCP Lease, page 7](#)
- [Renew a DHCP Lease, page 7](#)

Release a DHCP Lease

The **release dhcp** command starts the process to immediately release a DHCP lease for the specified interface. After the lease is released, the interface address is deconfigured. The **release dhcp** command does not deconfigure the **ip address dhcp** command specified in the configuration file for the interface. During a write memory or show running configuration file action, or if the router is rebooted, the **ip address dhcp** command executes to acquire a DHCP address for the interface.

The original IP address for the interface must be assigned by the DHCP server. If the interface is not assigned an IP address by the DHCP server, the **release dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

Renew a DHCP Lease

The **renew dhcp** command advances the DHCP lease timer to the next stage, at which point one of the following occurs:

- If the lease is currently in a BOUND state, the lease is advanced to the RENEW state and a DHCP RENEW request is sent.
- If the lease is currently in a RENEW state, the timer is advanced to the REBIND state and a DHCP REBIND request is sent.

If there is no response to the RENEW request, the interface remains in the RENEW state. In this case, the lease timer will advance to the REBIND state and subsequently send a REBIND request.

If a NAK response is sent in response to the RENEW request, the interface is deconfigured.

The original IP address for the interface must be assigned by the DHCP server. If the interface is not assigned an IP address by the DHCP server, the **renew dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

**Note**

In Cisco IOS Release 15.0(1)M and later releases Cisco IOS DHCP clients do not accept packets with zero lease time or no lease time option.

The DHCP client must be assigned an IP address by the DHCP server.

**Note**

If the DHCP client is not assigned an IP address by the DHCP server, the DHCP release and renew CLI commands will fail.

```
>
```

SUMMARY STEPS

1. **enable**
2. **release dhcp** *type number*
3. **renew dhcp** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	release dhcp <i>type number</i> Example: Router# release dhcp ethernet 3/1	Performs an immediate release of the DHCP lease for the interface and deconfigures the IP address for the interface.
Step 3	renew dhcp <i>type number</i> Example: Router# renew dhcp ethernet 3/1	Forces the DHCP timer to advance to the next stage, at which point a subsequent action is taken: A DHCP REQUEST packet is sent to renew or rebind the lease.

Enabling FORCERENEW-Message Handling

Perform this task to specify the type of authentication to be used in DHCP messages on the interface, specify the key chain to be used in authenticating a request, and enable FORCERENEW-message handling on the DHCP client when authentication is enabled.

You must configure the same authentication mode, and the same secret ID and secret value that were configured in the **key chain** command, on both the client and the server.

SUMMARY STEPS

1. **interface** *type number*
2. **ip dhcp client authentication key-chain** *name*
3. **ip dhcp client authentication mode** *type*
4. **exit**
5. **key chain** *name-of-chain*
6. **exit**
7. **ip dhcp-client forcerenew**
8. **end**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface Ethernet 1</pre>	Configures an interface type and enters interface-configuration mode.
<p>Step 2 ip dhcp client authentication key-chain <i>name</i></p> <p>Example:</p> <pre>Router(config-if)# ip dhcp client authentication key-chain dhcp1</pre>	Specifies the key chain to be used in authenticating a request.
<p>Step 3 ip dhcp client authentication mode <i>type</i></p> <p>Example:</p> <pre>Router(config-if)# ip dhcp client authentication mode md5</pre>	Specifies the type of authentication to be used in DHCP messages on the interface.
<p>Step 4 exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.

Command or Action	Purpose
<p>Step 5 <code>key chain name-of-chain</code></p> <p>Example:</p> <pre>Router(config-keychain)# key chain dhcpl</pre> <p>Example:</p> <pre>key 1234</pre> <p>Example:</p> <pre>key-string secret</pre>	Enters key-chain configuration mode and identifies the authentication strings to be used in the named key chain.
<p>Step 6 <code>exit</code></p> <p>Example:</p> <pre>Router(config-keychain)# exit</pre>	Exits key-chain configuration mode and enters global configuration mode.
<p>Step 7 <code>ip dhcp-client forcerenew</code></p> <p>Example:</p> <pre>Router(config)# ip dhcp-client forcerenew</pre>	Enables DHCP FORCERENEW-message handling on the DHCP client.
<p>Step 8 <code>end</code></p> <p>Example:</p> <pre>Router(config)# end</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for the DHCP Client

Example Configuring the DHCP Client

The figure below shows a simple network diagram of a DHCP client on an Ethernet LAN.

Figure 2 Topology Showing a DHCP Client with a Ethernet Interface



On the DHCP server, the configuration is as follows:

```
ip dhcp pool 1
network 10.1.1.0 255.255.255.0
lease 1 6
```

On the DHCP client, the configuration is as follows on interface E2:

```
interface Ethernet2
ip address dhcp
```

This configuration allows the DHCP client to acquire an IP address from the DHCP server through an Ethernet interface.

Example Customizing the DHCP Client Configuration

The following example shows how to customize the DHCP client configuration with various options on Ethernet interface 1:

```
interface Ethernet 1
ip dhcp client client-id ascii my-test1
ip dhcp client class-id my-class-id
ip dhcp client lease 0 1 0
ip dhcp client hostname host1
no ip dhcp client request tftp-server-address
ip address dhcp
```

Example Configuring an ATM Primary Interface (Multipoint) Using aal5snap Encapsulation and Inverse ARP

In the following example, the **protocol ip 255.255.255.255 broadcast** configuration is needed because there must be an ATM map entry to recognize the broadcast flag on the permanent virtual circuit (PVC). You can use any ATM map entry. The **protocol ip inarp** configuration is needed so that the ATM Inverse ARP can operate on the interface such that the system can be pinged once an address is assigned by DHCP.

```
interface atm0
ip address dhcp
pvc 1/100
encapsulation aal5snap
broadcast
protocol ip 255.255.255.255 broadcast
protocol ip inarp
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15snap Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15snap encapsulation:

```
interface atm0.1 point-to-point
ip address dhcp
pvc 1/100
encapsulation aal5snap
broadcast
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15nlpid Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15nlpid encapsulation:

```
interface atm0.1 point-to-point
 ip address dhcp
 pvc 1/100
  encapsulation aal5nlpid
  broadcast
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15mux PPP Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15mux PPP encapsulation:

```
interface atm0.1 point-to-point
 pvc 1/100
  encapsulation aal5mux ppp virtual-templatel
  broadcast
!
interface virtual-templatel
 ip address dhcp
```

Example Releasing a DHCP Lease

In the following example, a DHCP release is performed on an interface that was originally assigned an IP address by the DHCP server:

```
Router# release dhcp ethernet 3/1
```

In the following example, an attempt is made to release the DHCP lease on an interface that was not originally assigned an IP address by the DHCP server:

```
Router# release dhcp ethernet 3/1
```

```
Interface does not have a DHCP originated address
```

In the following example, the **release dhcp** command is executed without specifying the *type* and *number* arguments:

```
Router# release dhcp
```

```
Incomplete command.
```

Example Renewing a DHCP Lease

In the following example, the DHCP lease is renewed on an interface that was originally assigned an IP address by the DHCP server:

```
Router# renew dhcp ethernet 3/1
```

In the following example, an attempt is made to renew the DHCP lease on an interface that was not originally assigned an IP address by the DHCP server:

```
Router# renew dhcp ethernet 3/1

Interface does not have a DHCP originated address
```

In the following example, the **renew dhcp** command is executed without specifying the *type* and *number* arguments:

```
Router# renew dhcp

Incomplete command.
```

Additional References

The following sections provide references related to the DHCP client.

Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	<i>Cisco IOS IP Addressing Services Command Reference</i>
DHCP conceptual information	“DHCP Overview” module
DHCP server configuration	“Configuring the Cisco IOS DHCP Server” module
DHCP server on-demand address pools	“Configuring the DHCP Server On-Demand Address Pool Manager” module
DHCP relay agent configuration	“Configuring the Cisco IOS DHCP Relay Agent” module
DHCP advanced features	“Configuring DHCP Services for Accounting and Security” module
DHCP enhancements for edge-session management	“Configuring DHCP Enhancements for Edge-Session Management” module

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2131	<i>Dynamic Host Configuration Protocol</i>
RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>
RFC 3118	<i>Authentication for DHCP Messages</i>
RFC 3203	<i>DHCP reconfigure extension</i>
RFC 3361	<i>DHCP-for-IPv4 Option for SIP Servers</i>
RFC 3442	<i>Classless Static Route Option for DHCPv4</i>
RFC 3925	<i>Vendor-Identifying Vendor Options for DHCPv4</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the DHCP Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for the Cisco IOS DHCP Client

Feature Name	Releases	Feature Information
Configurable DHCP Client	12.2(28)SB 12.3(8)T	<p>The Configurable DHCP Client feature provides the flexibility to include various configuration options for the DHCP client. A DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address.</p> <p>The following commands were introduced: ip dhcp client class-id, ip dhcp client client-id, ip dhcp client hostname, ip dhcp client lease, ip dhcp client request.</p>
DHCP Release and Renew CLI in EXEC Mode	12.2(28)SB 12.2(33)SRC 12.3(4)T	<p>This feature provides the ability to perform two independent operations from the CLI:</p> <ul style="list-style-type: none"> • Immediately release a DHCP lease for a DHCP client • Force a DHCP renewal of a lease for a DHCP client <p>The following commands were introduced: release dhcp and renew dhcp.</p>
DHCP Client on WAN Interfaces	12.2(8)T 12.2(28)SB	<p>The DHCP Client on WAN Interfaces feature extends the DHCP to allow a DHCP client to acquire an IP address over PPP over ATM (PPPoA) and certain ATM interfaces.</p> <p>No commands were introduced or modified by this feature.</p>

Feature Name	Releases	Feature Information
Cisco DHCP FORCERENEW	12.4(22)YB 15.0(1)M	<p>This feature enhances security by providing entity authentication and message authentication.</p> <p>The following commands were introduced or modified: ip dhcp client authentication key-chain, ip dhcp client authentication mode, ip dhcp-client forcerenew, ip dhcp client request.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.