

Using the Authenticate–Until Property in DHCP

Document ID: 5745

Introduction

Prerequisites

Requirements

Components Used

Conventions

Authentication Expiration of a DHCP Client

Unauthenticated Client Address Reassignment

Related Information

Introduction

DHCP provides a mechanism to allocate IP addresses dynamically and set denial of service for certain DHCP clients. This document provides information on the authentication expiration of a DHCP client and address reassignment of the unauthenticated client.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Authentication Expiration of a DHCP Client

The authenticate–until property provides a mechanism to limit authentication of a client entry. By default, client entries are authenticated forever. Use the authenticate–until property to specify an expiration time. When the client is no longer authenticated, the DHCP server uses the value of the unauthenticated–client–class property for the name of the client–class to respond to the request from the client. If the unauthenticated–client–class property is not set, or if there is no client–class entry in the unauthenticated–client–class property, the server ignores the request and does not provide the client an IP address.

You can set up a test case for the authenticate–until property to drop the packets when the authentication time expires. Client–class processing must be enabled on the DHCP server.

To set up the test case, complete these steps:

1. Create a scope–selection–tag to tie the client to a scope.

```
nrcmd> scope-selection-tag AuthSelectionTag create
```

2. Create the client with an authentication–until expiration time. Tie the client to the scope–selection–tag.

```
nrcmd> client 01:02:03:04:05:06 create authenticate-until=+10m
nrcmd> client 01:02:03:04:05:06 set selection-criteria=AuthSelectionTag
```

3. Create a scope with an address range and tie it to the scope–selection–tag.

```
nrcmd> scope myScope create 192.168.2.0 255.255.255.0
nrcmd> scope myScope addRange 192.168.2.1 192.168.2.50
nrcmd> scope myScope set selection-tags=AuthSelectionTag
```

4. Enable client–class processing for the server.

```
nrcmd> dhcp set client-class=enabled
```

5. Set the destination and receive ports.

```
nrcmd> dhcp-interface default set dhcp-port=5067
nrcmd> dhcp-interface default set client-port=5067
```

6. Save the settings and reload the server.

```
nrcmd> save
nrcmd> server dhcp reload
```

After the authentication expires, the server drops any request the client makes and does not assign the client a new address.

Unauthenticated Client Address Reassignment

Use the authenticate–until property and client–classes to select between two different scopes: authenticated client and unauthenticated client.

To select between the two different scopes, complete these steps:

1. Create two scope–selection–tags to tie the authenticated and unauthenticated client to a scope.

```
nrcmd> scope-selection-tag AuthSelectionTag create
nrcmd> scope-selection-tag UnauthSelectionTag create
```

2. Create an authenticated and an unauthenticated client–class. Set the selection–criteria for each as appropriate.

```
nrcmd> client-class AuthClientClass create
nrcmd> client-class AuthClientClass set selection-criteria=AuthSelectionTag
nrcmd> client-class UnauthClientClass create
nrcmd> client-class UnauthClientClass set selection-criteria=UnauthSelectionTag
```

3. Create the client and include the authenticate–until expiration time. Set the client–class–name and unauthenticated–client–class–name as appropriate.

```
nrcmd> client 01:02:03:04:05:06 create authenticate-until=+10m
nrcmd> client 01:02:03:04:05:06 set client-class-name=AuthClientClass
nrcmd> client 01:02:03:04:05:06 set unauthenticated-client-class-name=UnauthClientClass
```

4. Create the authenticated and unauthenticated scopes and define their address ranges. Tie the scopes to their respective selection–tags.

```
nrcmd> scope AuthScope create 192.168.2.0 255.255.255.0
nrcmd> scope AuthScope addRange 192.168.2.1 192.168.2.50
nrcmd> scope AuthScope set selection-tags=AuthSelectionTag
nrcmd> scope UnauthScope create 192.168.2.0 255.255.255.0
nrcmd> scope UnauthScope addRange 192.168.2.51 192.168.2.100
nrcmd> scope UnauthScope set selection-tags=UnauthSelectionTag
```

5. Enable client–class processing for the server.

```
nrcmd> dhcp set client-class=enabled
```

6. Set the destination and receive ports.

```
nrcmd> dhcp-interface default set dhcp-port=506  
nrcmd> dhcp-interface default set client-port=5067
```

7. Save the settings and reload the server.

```
nrcmd> save  
nrcmd> server dhcp reload
```

After the authentication expires and the client requests another address, the DHCP server assigns the client an address from the range defined in the UnauthScope scope.

Related Information

- [Cisco CNS Network Registrar Tech Notes](#)
 - [Network Registrar CLI Reference Guide Authenticate–Until](#)
 - [Network Registrar User's Guide Figure 10–7 \(Applicable only to CNR 5.5 and earlier.\)](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 26, 2005

Document ID: 5745
