Extending DHCP Features in Cisco Prime Network Registrar

What You Will Learn

Dynamic Host Configuration Protocol (DHCP) is a core network access technology. Every device must be assigned a unique address when connected to the network, a nearly impossible task to undertake manually due to the increasing number of devices that access network services. Because of the increasing number of connected users and connected devices, along with the growth in demand for network services driven by rich-media applications, automating the tracking and controlling of users and devices with a high capacity DHCP server is a priority among network operators. Additionally, as a result of the new and sometimes complex network services being designed and deployed, network administrators may have needs that go beyond the features provided by standard DHCP offerings. Cisco Prime™ Network Registrar, a high-performance, scalable, integrated Domain Name System (DNS), DHCP, and IP address management (IPAM) (DDI) solution that supports IPv4 and IPv6 deployments on a single server, meets this need for customization or “extensibility” with two unique features.

One is **expressions**, which can be written in a simple language similar to LISt Processing (LISP) to set values for packets used for decision making within the DHCP server. Another is **DHCP extensions**, which are written in Tool Command Language (Tcl) or C/C++ and which allow administrators to alter and customize the operation of the DHCP server by modifying request or response packets or through environment variables stored in the environment dictionary. This white paper provides an overview of these two extensibility capabilities of Cisco Prime Network Registrar and includes two use-case examples based on these capabilities.

Challenge: The Need for DHCP Extensibility in a DDI Product

Standard DHCP products allow administrators to designate on a subnet a set of IP addresses that use the DHCP service (a scope) along with the configuration parameters and server information related to the addresses (for example, which address is leasable and whether to ping clients before offering a lease) for dynamic addressing. Once this information is input, an embedded policy is created that contains client confirmation data such as the lease duration and the address of the local DNS server. The policy has no associated properties or DHCP options until the administrator adds them.

With the wide array of applications and devices on the Internet and private networks today, administrators are finding that their needs sometimes go beyond the above features of standard DHCP products.

Cisco has therefore provided an API with which administrators can create custom extensions to Cisco Prime Network Registrar using pseudo code that enhances the capabilities of the product. Extensions easily create new solutions such as billing, security, and lawful interception. This extensibility allows for packet intercept and the extraction or addition of information from or into packets. DCHP requests or responses can be modified based on default, predefined, or situation-specific policies.

Solution: Cisco Prime Network Registrar

Cisco Prime Network Registrar is an integrated, high-performance, standards-based, and highly scalable DHCP, DNS, and IPAM solution for enterprises and service providers running both IPv4 and IPv6 networks. The solution is composed of four application components, including:

- **A DHCP server** that supports both IPv4 and IPv6 for device network access, service delivery, and internal and external client reservations
- **A DNS server** that supports both IPv4 and IPv6 for IP address translation
- **An IP address management system** integrated with DNS and DHCP for configuration, reporting, and management of IPv4 and IPv6
- **A Caching DNS server** with that supports DNS Security Extensions (DNSSEC)

The DHCP server is fast and scalable, capable of handling up to 47,000 returning client requests per second. A single customer deployment can support tens of millions of IP addresses. Cisco's patent-pending Discriminating Rate Limiter identifies and prioritizes returning clients so that their services are restored prior to new client requests in the event of a service disruption, reducing downtime. Cisco Prime Network Registrar also supports DHCP IPv4 failover. A Chatty Client Filter extension is available that can cut misbehaving DHCP traffic by more than50 percent.

Extensible Features

Cisco Prime Network Registrar has powerful, industry-leading extension support for both IPv4 and IPv6 to allow for DHCP server processing customization, improving network security, network performance, and third-party application integration. The two options for extending features include DHCP extensions and expressions.

Expressions

Expressions are a mechanism within Cisco Prime Network Registrar that enables the use of data from an input packet to set certain values used with the DHCP server for processing the packet. Written in a simple language similar to LISP, expressions are read-only and do not modify any content of the packet but set values that can be used in decision making within the DHCP server. An expression is interpreted so that it cannot crash the server. If an expression fails, it will typically drop the packet and log an error message and may only generate a warning message if constructed properly.

An example of an expression is to use the values in the DHCP Option 82 to choose a specific IP address from a scope. This could be used to make sure that a port on a switch always gets the same IP address.

DHCP Extensions

DHCP extensions allow administrators to alter and customize the operation of the DHCP server using programs written in Tcl or C/C++. Tcl is a fast, easier method of writing an extension. C/C++ provides the maximum possible performance and flexibility and includes communication with external processes.

Extension points are places in the packet processing path where an extension can be inserted. These points include three types of dictionaries: request, response, and environment. Extensions interact with the server by modifying request or response packets and through environment variables stored in the environment dictionary. They can be used to classify client types; add, remove, or modify options in packets; query or update an external database; and much more.

DHCP extensions can be written to alter how Cisco Prime Network Registrar handles and responds to DHCP requests and to change the behavior of a DHCP server in ways that cannot be done through the user interfaces. Extensions are flexible enough to be written in the service provider or enterprise development environment with no coding or custom software builds required. All operating platforms and devices are supported.

Typically clients go through a relay, a router that converts a broadcast to a unicast and forwards to helper addresses (DHCP servers). The Cisco Prime Network Registrar DHCP server examines certain elements of the DHCP packet and makes decisions based on its configuration, such as:

- Whether or not to give out an address to a certain client
- What scope to choose an address from
- What options to include in its offer

DHCP extensions in Cisco Prime Network Registrar allow the DHCP server to:

- Modify the request
- Interrupt the packet flow and do a database lookup based on an combination of concatenated fields extracted from the request packet
- Modify the response based on client ID, DHCP Option 82 suboptions, and device manufacturer (based on the first half of the MAC address)
- Create custom options

Use Case: Chatty Client Filter Extension

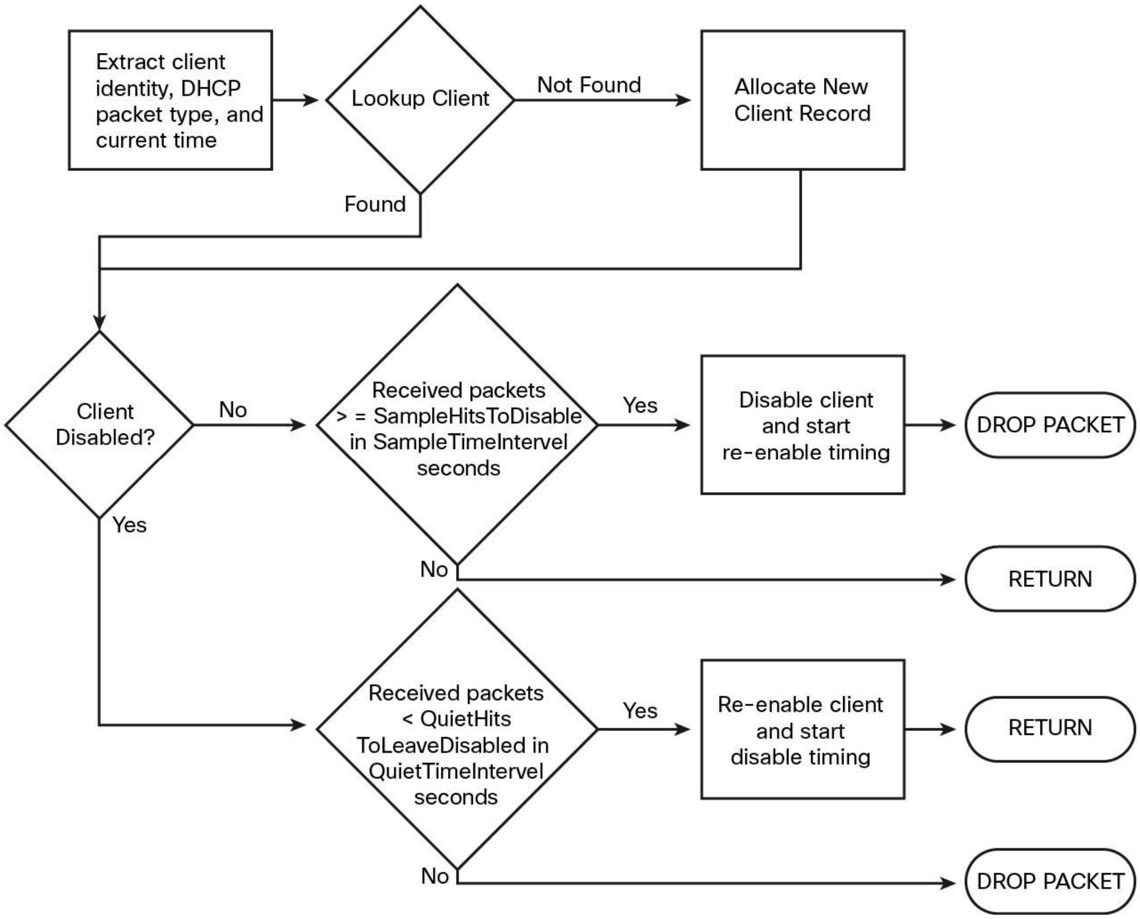
One example of an effective use of a DHCP extension is to protect against clients flooding the server with unnecessary traffic. The Chatty Client Filter extension can be used to offload the processing of chatty client packets from the server. “Chatty” clients may, for example, repeatedly generate a sequence of DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, and after 30 seconds, DHCPRELEASE messages. The devices repeat this cycle and cause a significant, unproductive load on the DHCP server and DNS updates.

The Chatty Client Filter extension has been shown to cut DHCP traffic by more than50 percent, and it is included with the Cisco Prime Network Registrar DHCP product. In a network with large numbers of DHCP clients, this extension will be very useful, and it is tunable by network operators for variations in traffic patterns and actions.

- Monitors DHCP traffic and drops traffic from clients that send too many requests or have broken behavior
- Uses the Cisco Network Registrar DHCP server **extension** interface
- Is included with the product and with downloadable updates

The Chatty Client Filter extension is available in the /examples/dhcp/dex directory of the Cisco Prime Network Registrar installation. It is compiled and ready to use in /extensions/dhcp/dex/dexextension.so or /extensions/dhcp/dex/dexextension.dll. The extension monitors client requests, based on the MAC address, and disables the client if it generates more than a certain number of packets in a time interval, as shown in Figure 1. Disabling a client means that the server discards packets received from it. However, the server does not ignore the client entirely because it continues to monitor its traffic. If the server detects that the client is starting to generate less than a certain number of packets in a certain time interval, it re-enables the client and begins to allow receipt of packets again.

Figure 1. The Chatty Client Filter Extension Workflow in Cisco Prime Network Registrar

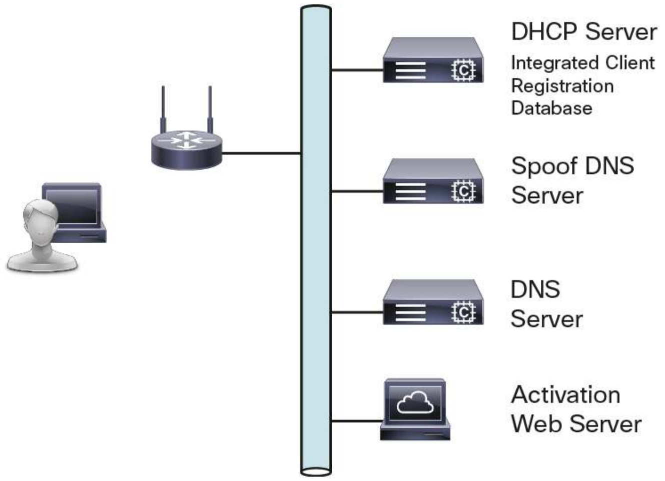

Extract client identity, DHCP packet type, and current time
Lookup Client
Not Found
Allocate New Client Record
Found
Client Disabled?
No
Received packets > = SampleHitsToDisable in SampleTimeInterval seconds
Yes
Disable client and start re-enable timing
DROP PACKET
Yes
No
RETURN
Received packets < QuietHits ToLeaveDisabled in QuietTimeInterval seconds
Yes
Re-enable client and start disable timing
RETURN
No
DROP PACKET

The criteria for disabling and re-enabling a client are set through arguments to the Chatty Client Filter extension. By default, the server disables a client when it receives more than 15 packets within 30 seconds. The server re-enables the client when it sends fewer than five packets within 10 seconds. Note: these defaults are conservative and do not protect against all situations. For example, the server does not disable a client that sends packets every three seconds. Even allowing for a few retransmissions, a client should never need to send more than a half dozen packets in a short interval.

Use Case: Student Registration Extension

Each fall, 10,000 students show up for registration at a university needing access to the university’s network. Without DHCP extensions, a manual process would be required to gather MAC addresses and populate a database in this “bring your own device” (BYOD) environment. The concept here is to allow the student onto the network with limited access, force the user to register, and then give the user full access to the network, as shown in Figure 2.Cisco Prime Network Registrar allows you to write extensions to affect handling and response to DHCP requests and to change the behavior of the DHCP server to meet this use case requirement easily.

Figure 2. The Student Registration Extension Setup



Initial DHCP request:

1. The client boots onto the network and issues a DHCP DISCOVER. The DISCOVER packet contains the client's MAC address.
2. The DHCP server, configured for client-class processing, looks up the client's MAC address to see if there is a client associated with it.
3. Because this is a device that is not yet activated, there is no client entry for the MAC address. Therefore, the DHCP server uses the default client rule set.
4. Using this default rule set, the DHCP server builds and sends a DHCP OFFER packet to the client. The DHCP OFFER contains a temporary IP address, with option 6, the DNS address of the spoof DNS server.
5. The client issues a DHCP REQUEST for a lease on the IP address in the OFFER.
6. The DHCP server performs steps 2 and 3 again (it does this for all inbound packets) and then builds the DHCP Acknowledgement (ACK) packet, containing lease information and the default (inactivated) set of DHCP options.

The activation server is contacted:

1. The user opens a web browser.
2. The browser issues an HTTP request for its configured home page (can be any webpage).
3. The client DNS resolver attempts to resolve the hostname in this URL, sending a DNS query to the Cisco Prime Network Registrar spoof DNS server.
4. The Cisco Prime Network Registrar spoof DNS server resolves all hostnames to the IP address of the activation web server.
5. The HTTP query now goes to the activation web server instead of to the configured homepage.
6. The browser sends its request to the activation web server.
7. The activation web server answers with an activation form.

The client then activates a user account:

1. The user enters a username and registration code and submits the activation form.
2. The activation server captures the temporary IP address of the client.
3. Using the Cisco Prime Network Registrar software development kit (SDK), the activation server inquires about the IP address of the student.
4. The DHCP server responds with the MAC address associated with the temporary IP address of the client.
5. The activation server sends the next screen of information, asking for additional information, such as computer type, location, department, and so on.
6. The user completes the required fields and submits the form.

The DHCP server is updated using the SDK:

- The activation server issues a command through the SDK to the Cisco Prime Network Registrar DHCP server, telling it to create a client entry for this MAC address.
- The Common Gateway Interface (CGI) script sends the next screen of information, informing the user that the computer has been activated and to reboot his or her computer.

In summary, Cisco Prime Network Registrar DHCP provides powerful extension and expression support to allow for DHCP server processing customization to meet unique network operator requirements.

For More Information

For more information on Cisco Prime Network Registrar, visit http://www.cisco.com/go/networkregistrar, contact your local account representative, or send an email to ask-networkregistrar@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-728807-00 07/13