DHCP and Dynamic DNS

Ebenezer Schubert
Ebenezer_schubert@hp.com
Anand S. Medikeri
Anandsm@india.hp.com
Hewlett-Packard company

Abstract

The Domain Name System (DNS) was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made as manual edits to a zone's master file. Enhancements to the protocol (RFC2136) have made dynamic updates possible.

DHCP server provides a powerful mechanism for IP host configuration. However, the configuration capability provided by DHCP does not include updating DNS and, specifically, updating the name-to-address and address-to-name mappings maintained in the DNS.

This paper specifies how HP's DHCP servers will use the Dynamic DNS Updates mechanism in RFC2136 to update the DNS name-to-address and address-to-name mappings so that the mappings for DHCP clients will be consistent with the IP addresses that the clients acquire via DHCP. This paper will go into detail about how the DNS server and the DHCP server need to be configured to use this feature.

1. Introduction

The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts. DHCP is based on bootstrap protocol (BOOTP). It consists of two components:

- a protocol for delivering host-specific configuration parameters from a DHCP server to a host
- a mechanism for automatic allocation of reusable network addresses.

This paper provides an overview of the new features provided in the version of DHCP shipped with HP-UX 11i. This includes the dynamic DNS update capability and also performance enhancements.

2. DHCP- Dynamic DNS

2.1 Dynamic DNS – Overview

DNS (RFC1034[1], RFC1035[2]) maintains (among other things) the information about mapping between hosts' Fully Qualified Domain Names (FQDNs) RFC1594[4] and IP addresses assigned to the hosts. The information is maintained in two types of Resource Records (RRs): A and PTR. The A RR contains mapping from a FQDN to an IP address; the PTR RR contains mapping from an IP address to a FQDN.

The Domain Name System was originally designed to support queries from a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made as external edits to a zone's Master File. However in the latest version of DNS implementations (BIND-8.1.2 and upwards), it is possible to update the DNS database dynamically. Using the UPDATE opcode introduced in the Dynamic DNS specification (RFC 2136), it is possible to dynamically add or

delete resource records (RRs) or sets of resource records (RRsets) from a specified zone. The following is a sample entry in the configuration file enabling dynamic updates for the zone isc.org. By default dynamic updates are disabled.

```
zone "isc.org" in {
        type master;
       file "master/isc.org";
        allow_updates {15.10.13.124};
  };
```

2.2 DDNS updates by DHCP.

The DHCP available on HP-UX 11I is capable of updating dynamic DNS server (DDNS). This new feature in DHCP updates the DDNS with name and IP address of the client. This means for every client to which it assigns a name and IP address, it also adds an "A" and "PTR" resource records (RR's) of that client to the DDNS.

In order to assign a name for every IP address, a new tag "pcsn" has been introduced. This tag is a boolean tag. If set the dhcp server gives priority to the name (if any) provided by the client. Names should be fully qualified domain name (FQDN). If the name provided by the client is not an FQDN, then the dhcp server will reject the name provided by the client and assign one of its choice.

If the "pcsn" tag is unset, then the dhcp server will try to assign a name of it's choice for every IP address.

The dynamic dns server has a couple of pre-requisites for accepting an update from the DHCP server. The pre-requisites that the DHCP server uses are:

* The RR (Resource Record) should not exist for an add operation.
* The RR must exist for a delete operation.

By default these pre-requisites are used for an update (add/delete) operation by the DHCP server. These pre-requisites can be suppressed by including the tag "sp" in the /etc/dhcptab configuration file.

To enable the DHCP server to perform updates to DDNS, a new tag "ddns-address" which specfies the address of the DDNS server has to be added in the "dhcp_pool_group" or "dhcp_device_group" keywords. The "pcsn" tag is also added within the same entry.

A sample DHCP_DEVICE_GROUP entry with the"ddns-address" tag and the "pcsn" tag is as shown:

```
# DEVICE group with prerequisite enabled.

    DHCP_DEVICE_GROUP:\
      ba:\
      pcsn:\
      class-name=SUBNET_128_XTERMINAL_GROUP:\
      class-id="xterminal:"\
      subnet-mask=255.255.255.0 :\
      addr-pool-start-address=  1.14.128.1 :\
      addr-pool-last-address=   1.14.128.254 :\
      ddns-address=1.2.3.4:\
      lease-time=604800 :\
      lease-grace-period=5 :\

# DEVICE group with prerequisite disabled.

    DHCP_DEVICE_GROUP:\
      ba:\
```

```
pcsn:\
class-name=SUBNET_128_PRINTER_GROUP:\
class-id="printers:"\
subnet-mask=255.255.255.0 :\
addr-pool-start-address=  2.15.122.2 :\
addr-pool-last-address=   2.15.122.22 :\
sp:\
ddns-address=1.2.3.4:\
lease-time=604800 :\
lease-grace-period=5 :\
```

2.3 Security.

DHCP is built directly on UDP and IP which are as yet inherently insecure. Furthermore, DHCP is generally intended to make maintenance of remote and/or diskless hosts easier. While perhaps not impossible, configuring such hosts with passwords or keys may be difficult and inconvenient. Therefore, DHCP in its current form is quite insecure. In the current implementation of DHCP and DNS, the interactions between DHCP and DNS is not secure. Hence the users of this feature are strongly recommended to use it with some security measures such as IPSec, etc.

3. dhcpdeny feature

A new configuration file /etc/dhcpdeny is available where you can list the hardware addresses of the clients for which you want to deny IP address allocation. The syntax of this configuration file is:

```
hardware-address1
hardware-address2
```

An example configuration file:

```
0x000aabbbcccd
0x0060B02088B4
6a123400ffed
```

By default DHCP assumes all the addresses are hexadecimal addresses. Hence if you do not have to prefix the addresses with 0x, they will be treated as a hexadecimal address.

4. Performance enhancements

The new implementation of DHCP for 11i has major performance enhancements. The performance tuning is achieved by altering the method DHCP writes to the internal database file /etc/dhcpdb and by altering the PING feature.

4.1 Asynchronous write to dhcpdb file

DHCP maintains the binding information(IP address and configuration parameters) for all the clients in a file by name /etc/dhcpdb. Whenever the server commits the binding for a client, the binding information is written immediately to this file. This write operation was synchronous in previous releases. For 11i asynchronous write operation is used to write the bindings to the dhcpdb file. The asynchronous write operation spawns a child process to do this operation while the server carries on with further processing as if it has completed the write operation to the file.

4.2 Asynchronous PING.

Before an IP address is offered to a client in a DHCPOFFER the IP address is probed by pinging to that IP address if PING featured is enabled. The server in previous releases used to send a ping request and immediately wait for a fixed period of 1 second for the PING reply (synchronous). In 11i wait period for the ping is configurable in milliseconds and the PING reply is handled asynchronously. Instead of waiting for a PING reply the server goes back and tries to serve other clients if there are any outstanding requests.

5.0 Conclusion.

The performance enhancements that have been done to the DHCP server, would make HPs DHCP offering one of the best in the industry and also the ability to do dynamic updates to DNS will help in the automation of IP address management to a great extent.

7.0 References

DROMS, R., "Dynamic Host Configuration Protocol", RFC 1531, Bucknell university, October 1993.

Alexander, S, Droms, R. “DHCP options and BOOTP vendor extentsions”, RFC 2132, SGI, Bucknell University, March 1997

RFC2136 Dynamic Updates in Domain Name System (DNS UPDATE)