DYNAMIC HOST CONFIGURATION PROTOCOL

DEFINITION

Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP's purpose is to enable individual computers to extract their configurations from a DHCP server, which allows them to participate on an IP network. The most significant piece of information distributed in this manner is the IP address. DHCP allows for automatic management of assigning IP addresses in an organization's network. DHCP allows devices to connect to a network and be automatically assigned an IP address. The overall purpose of this is to reduce the work necessary to administer a large IP network.

DEVELOPMENT

DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force. It appeared as a standard protocol in October 1993. RFC 2131 provides the latest (March 1997) DHCP definition.

IMPLEMENTATIONS

Microsoft introduced DHCP on their NT server with Windows NT version 3.5 in late 1994.

The Internet Software Consortium published DHCP software distributions for Unix variants with version 1.0.0 of the ISC DHCP Server released on December 6, 1997 and a more RFC-compliant version 2.0 on June 22, 1999.

Novell has included a DHCP server in their NetWare operating system since version 5, released in 1998. It integrates with Novell's directory service - Novell eDirectory.

Sun added DHCP support in the July 2001 release of Solaris 8.

Cisco made a DHCP server available in Cisco IOS 12.0 in February 1999. Cisco Systems offers DHCP servers in routers and switches with their IOS software, like Cisco Network Registrar (CNR).

USAGE

DHCP is used by most cable internet providers in the U.S. to allocate IP addresses. DSL providers in the US rarely use DHCP, using PPPoE instead. In addition, many routers and other gateway devices provide DHCP support for networks of up to 255 computers, for assigning private IP addresses. In the U.K. DHCP is used by many broad-band ISP networks, but for XDSL extensive use is made of "infinite lease" which amounts to semi-static IPs. DHCP is also used in office networks, in particular where there is extensive use of laptops that are only occasionally present.

PROTOCOL ANATOMY

Protocol Suite: IP

Protocol Suite Layer: Application Layer.

Related protocols: BOOTP, Bootstrap Protocol.

Ports: 67/UDP server; 68/UDP host.

Working groups: dhc, ip1394

Figure 1: Format of a DHCP message

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| **op** (1) | **htype** (1) | **hlen** (1) | **hops** (1) |

+---------------+---------------+---------------+---------------+

| **xid** (4) |

+-------------------------------+-------------------------------+

| **secs** (2) | **flags** (2) |

+-------------------------------+-------------------------------+

| **ciaddr** (4) |

+---------------------------------------------------------------+

| **yiaddr** (4) |

+---------------------------------------------------------------+

| **siaddr** (4) |

+---------------------------------------------------------------+

| **giaddr** (4) |

+---------------------------------------------------------------+

| |

| **chaddr** (16) |

| |

| |

+---------------------------------------------------------------+

| |

| **sname** (64) |

+---------------------------------------------------------------+

| |

| **file** (128) |

+---------------------------------------------------------------+

| |

| **options** (variable) |

+---------------------------------------------------------------+

Table 1: Description of fields in a DHCP message

FIELD OCTETS DESCRIPTION

----- ------ -----------

**op** 1 Message op code / message type.

1 = BOOTREQUEST, 2 = BOOTREPLY

**htype** 1 Hardware address type, see ARP section in "Assigned

Numbers" RFC; e.g., '1' = 10mb ethernet.

**hlen** 1 Hardware address length (e.g. '6' for 10mb

ethernet).

**hops** 1 Client sets to zero, optionally used by relay agents

when booting via a relay agent.

**xid** 4 Transaction ID, a random number chosen by the

client, used by the client and server to associate

messages and responses between a client and a

server.

**secs** 2 Filled in by client, seconds elapsed since client

began address acquisition or renewal process.

**flags** 2 Flags.

**ciaddr** 4 Client IP address; only filled in if client is in

BOUND, RENEW or REBINDING state and can respond

to ARP requests.

**yiaddr** 4 'your' (client) IP address.

**siaddr** 4 IP address of next server to use in bootstrap;

returned in DHCPOFFER, DHCPACK by server.

**giaddr** 4 Relay agent IP address, used in booting via a

relay agent.

**chaddr** 16 Client hardware address. May contain another type of

identifier, such as a DNS name.

**sname** 64 Optional server host name, null terminated string.

**file** 128 Boot file name, null terminated string; "generic"

name or null in DHCPDISCOVER, fully qualified

directory-path name in DHCPOFFER.

**options** var Optional parameters field.

PACKET BREAKDOWN

Ethernet II Header = **Indigo**

IP Header = **Aqua**

UDP Header = **Yellow**

DHCP Discover

0x0000: **ffff ffff ffff 000b 8201 fc42 0800 4500** ...........B..E.

0x0010: **012c a836 0000 fa11 178b 0000 0000 ffff** .,.6............

0x0020: **ffff 0044 0043 0118 591f 0101 0600 0000** ...D.C..Y.......

0x0030: **3d1d 0000 0000 0000 0000 0000 0000 0000** =...............

0x0040: **0000 0000 0000 000b 8201 fc42 0000 0000** ...........B....

0x0050: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x0060: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x0070: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x0080: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x0090: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x00a0: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x00b0: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x00c0: **0000** **0000 0000 0000 0000 0000 0000 0000** ................

0x00d0: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x00e0: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x00f0: **0000** **0000 0000 0000 0000 0000 0000 0000** ................

0x0100: **0000 0000 0000 0000 0000 0000 0000 0000** ................

0x0110: **0000 0000 0000 6382 5363 3501 013d 0701** ......c.Sc5..=..

0x0120: **000b 8201 fc42 3204 0000 0000 3704 0103** .....B2.....7...

0x0130: **062a ff00 0000 0000 0000** .\*........

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| op: 0x**01** | htype: 0x**01** | hlen: 0x**06** | hops: 0x**00** |

+---------------+---------------+---------------+---------------+

| xid: 0x**0000** 0x**3d1d** |

+-------------------------------+-------------------------------+

| secs: 0x**0000** | flags: 0x**0000** |

+-------------------------------+-------------------------------+

| ciaddr: 0x**0000** 0x**0000** |

+---------------------------------------------------------------+

| yiaddr: 0x**0000** 0x**0000** |

+---------------------------------------------------------------+

| siaddr: 0x**0000** 0x**0000** |

+---------------------------------------------------------------+

| giaddr: 0x**0000** 0x**0000** |

+---------------------------------------------------------------+

| |

| chaddr: 0x**000b** 0x**8201** 0x**fc42** 0x**0000** |

| 0x**0000** 0x**0000** 0x**0000** 0x**0000** |

| |

+---------------------------------------------------------------+

| |

| sname: 64 Octets of 0's |

+---------------------------------------------------------------+

| |

| file: 128 Octets of 0's |

+---------------------------------------------------------------+

| options: 0x**6382** 0x**5363** 0x**3501** 0x**013d** |

| 0x**0701** 0x**000b** 0x**8201** 0x**fc42** |

| 0x**3204** 0x**0000** 0x**0000** 0x**3704** |

| 0x**0103** 0x**062a** 0x**ff00** 0x**0000** |

| 0x**0000** 0x**0000** |

+---------------------------------------------------------------+

Ethereal Analysis

Frame 1 (314 bytes on wire, 314 bytes captured)

Arrival Time: Dec 5, 2004 14:16:24.317453000

Time delta from previous packet: 0.000000000 seconds

Time since reference or first frame: 0.000000000 seconds

Frame Number: 1

Packet Length: 314 bytes

Capture Length: 314 bytes

Protocols in frame: eth:ip:udp:bootp

**Ethernet II**, Src: 00:0b:82:01:fc:42, Dst: ff:ff:ff:ff:ff:ff

Destination: ff:ff:ff:ff:ff:ff (Broadcast)

Source: 00:0b:82:01:fc:42 (Grandstr\_01:fc:42)

Type: IP (0x0800)

**Internet Protocol**, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)

Version: 4

Header length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

0000 00.. = Differentiated Services Codepoint: Default (0x00)

.... ..0. = ECN-Capable Transport (ECT): 0

.... ...0 = ECN-CE: 0

Total Length: 300

Identification: 0xa836 (43062)

Flags: 0x00

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

Time to live: 250

Protocol: UDP (0x11)

Header checksum: 0x178b (correct)

Source: 0.0.0.0 (0.0.0.0)

Destination: 255.255.255.255 (255.255.255.255)

**User Datagram Protocol**, Src Port: bootpc (68), Dst Port: bootps (67)

Source port: bootpc (68)

Destination port: bootps (67)

Length: 280

Checksum: 0x591f (correct)

**Bootstrap Protocol**

**Message type**: Boot Request (1)

**Hardware type**: Ethernet

**Hardware address length**: 6

**Hops**: 0

**Transaction ID**: 0x00003d1d

**Seconds elapsed**: 0

**Bootp flags**: 0x0000 (Unicast)

0... .... .... .... = Broadcast flag: Unicast

.000 0000 0000 0000 = Reserved flags: 0x0000

**Client IP address**: 0.0.0.0 (0.0.0.0)

**Your (client) IP address**: 0.0.0.0 (0.0.0.0)

**Next server IP address**: 0.0.0.0 (0.0.0.0)

**Relay agent IP address**: 0.0.0.0 (0.0.0.0)

**Client MAC address**: 00:0b:82:01:fc:42 (Grandstr\_01:fc:42)

**Server host name not given**

**Boot file name not given**

**Magic cookie**: (OK)

**Option 53**: DHCP Message Type = DHCP Discover

**Option 61**: Client identifier

Hardware type: Ethernet

Client MAC address: 00:0b:82:01:fc:42 (Grandstr\_01:fc:42)

**Option 50**: Requested IP Address = 0.0.0.0

**Option 55**: Parameter Request List

1 = Subnet Mask

3 = Router

6 = Domain Name Server

42 = Network Time Protocol Servers

**End Option**

**Padding**

PROTOCOL TRACE

tcpdump -s 0 -ennXXr DHCP.pcap

14:16:24.317453 00:0b:82:01:fc:42 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 314: IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:0b:82:01:fc:42, length: 272

0x0000: ffff ffff ffff 000b 8201 fc42 0800 4500 ...........B..E.

0x0010: 012c a836 0000 fa11 178b 0000 0000 ffff .,.6............

0x0020: ffff 0044 0043 0118 591f 0101 0600 0000 ...D.C..Y.......

0x0030: 3d1d 0000 0000 0000 0000 0000 0000 0000 =...............

0x0040: 0000 0000 0000 000b 8201 fc42 0000 0000 ...........B....

0x0050: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0080: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0090: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00a0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00b0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00c0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00d0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00e0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00f0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0100: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0110: 0000 0000 0000 6382 5363 3501 013d 0701 ......c.Sc5..=..

0x0120: 000b 8201 fc42 3204 0000 0000 3704 0103 .....B2.....7...

0x0130: 062a ff00 0000 0000 0000 .\*........

14:16:24.317748 00:08:74:ad:f1:9b > 00:0b:82:01:fc:42, ethertype IPv4 (0x0800), length 342: IP 192.168.0.1.67 > 192.168.0.10.68: BOOTP/DHCP, Reply, length: 300

0x0000: 000b 8201 fc42 0008 74ad f19b 0800 4500 .....B..t.....E.

0x0010: 0148 0445 0000 8011 0000 c0a8 0001 c0a8 .H.E............

0x0020: 000a 0043 0044 0134 2233 0201 0600 0000 ...C.D.4"3......

0x0030: 3d1d 0000 0000 0000 0000 c0a8 000a c0a8 =...............

0x0040: 0001 0000 0000 000b 8201 fc42 0000 0000 ...........B....

0x0050: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0080: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0090: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00a0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00b0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00c0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00d0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00e0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00f0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0100: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0110: 0000 0000 0000 6382 5363 3501 0201 04ff ......c.Sc5.....

0x0120: ffff 003a 0400 0007 083b 0400 000c 4e33 ...:.....;....N3

0x0130: 0400 000e 1036 04c0 a800 01ff 0000 0000 .....6..........

0x0140: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0150: 0000 0000 0000 ......

14:16:24.387484 00:0b:82:01:fc:42 > ff:ff:ff:ff:ff:ff, ethertype IPv4 (0x0800), length 314: IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 00:0b:82:01:fc:42, length: 272

0x0000: ffff ffff ffff 000b 8201 fc42 0800 4500 ...........B..E.

0x0010: 012c a837 0000 fa11 178a 0000 0000 ffff .,.7............

0x0020: ffff 0044 0043 0118 9fbd 0101 0600 0000 ...D.C..........

0x0030: 3d1e 0000 0000 0000 0000 0000 0000 0000 =...............

0x0040: 0000 0000 0000 000b 8201 fc42 0000 0000 ...........B....

0x0050: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0080: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0090: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00a0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00b0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00c0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00d0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00e0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00f0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0100: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0110: 0000 0000 0000 6382 5363 3501 033d 0701 ......c.Sc5..=..

0x0120: 000b 8201 fc42 3204 c0a8 000a 3604 c0a8 .....B2.....6...

0x0130: 0001 3704 0103 062a ff00 ..7....\*..

14:16:24.387798 00:08:74:ad:f1:9b > 00:0b:82:01:fc:42, ethertype IPv4 (0x0800), length 342: IP 192.168.0.1.67 > 192.168.0.10.68: BOOTP/DHCP, Reply, length: 300

0x0000: 000b 8201 fc42 0008 74ad f19b 0800 4500 .....B..t.....E.

0x0010: 0148 0446 0000 8011 0000 c0a8 0001 c0a8 .H.F............

0x0020: 000a 0043 0044 0134 dfdb 0201 0600 0000 ...C.D.4........

0x0030: 3d1e 0000 0000 0000 0000 c0a8 000a 0000 =...............

0x0040: 0000 0000 0000 000b 8201 fc42 0000 0000 ...........B....

0x0050: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0060: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0070: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0080: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0090: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00a0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00b0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00c0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00d0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00e0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x00f0: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0100: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0110: 0000 0000 0000 6382 5363 3501 053a 0400 ......c.Sc5..:..

0x0120: 0007 083b 0400 000c 4e33 0400 000e 1036 ...;....N3.....6

0x0130: 04c0 a800 0101 04ff ffff 00ff 0000 0000 ................

0x0140: 0000 0000 0000 0000 0000 0000 0000 0000 ................

0x0150: 0000 0000 0000 ......

REFERENCES

http://en.wikipedia.org/wiki/Dynamic\_Host\_Configuration\_Protocol

http://www.faqs.org/rfcs/rfc2131.html

http://www.networksorcery.com/enp/protocol/dhcp.htm

http://www.dhcp-handbook.com/dhcp\_faq.html

http://wiki.ethereal.com/SampleCaptures

http://www.tubgirl.com

http://www.lemonparty.org

http://www.google.com

CREDITS

Akshat Pradhan