Dynamic Host Configuration Protocol

From Wikipedia, the free encyclopedia

The **Dynamic Host Configuration Protocol** (**DHCP**) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Contents

Overview

Computers use the Dynamic Host Configuration Protocol to request Internet Protocol parameters, such as an IP address, from a network server. The protocol operates based on the client–server model. As of 2011, modern networks ranging in size from home networks to large campus networks and regional Internet service provider networks commonly use DHCP.[1] Most residential network routers receive a globally unique IP address within the provider network. Within a local network, DHCP assigns a local IP address to devices connected to the local network.

When a computer or other networked device connects to a network, the DHCP client software sends a broadcast query requesting necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers. On receiving a request, the server may respond with specific information for each client, as previously configured by an administrator, or with a specific address and any other information valid for the entire network and for the time period for which the allocation (*lease*) is valid. A client typically queries for this information immediately after booting, and periodically thereafter before the expiration of the information. When a

DHCP client refreshes an assignment, it initially requests the same parameter values, but the DHCP server may assign a new address based on the assignment policies set by administrators.

On large networks that consist of multiple links, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. Such agents relay messages between DHCP clients and DHCP servers located on different subnets.

Depending on implementation, the DHCP server may have three methods of allocating IP addresses:

- *Dynamic allocation*: a network administrator reserves a range of IP addresses for DHCP, and each DHCP client on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.
- *Automatic allocation*: the DHCP server permanently assigns an IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- *Manual allocation*: commonly called *Static allocation*, the DHCP server allocates an IP address based on a preconfigured mapping to each client's MAC address. This feature is variously called *static DHCP assignment* by DD-WRT, *fixed-address* by the dhcpd documentation, *address reservation* by Netgear, *DHCP reservation* or *static DHCP* by Cisco and Linksys, and *IP address reservation* or *MAC/IP address binding* by various other router manufacturers.

DHCP is used for Internet Protocol version 4 (IPv4), as well as for IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 differ sufficiently that they may be considered separate protocols.[2] For the IPv6 operation, devices may alternatively use stateless address autoconfiguration. IPv6 hosts may also use link-local addressing to achieve operations restricted to the local network link.

History

In 1984, the Reverse Address Resolution Protocol (RARP), defined in RFC 903, was introduced to allow simple devices such as diskless workstations to dynamically obtain a suitable IP address. However, because it acted at the data link layer it made implementation difficult on many server platforms, and also required that a server be present on each individual network link. Soon afterwards it was superseded by the "Bootstrap Protocol" (BOOTP) defined in RFC 951. This introduced the concept of a *relay agent*, which allowed the forwarding of BOOTP packets across networks, allowing one central BOOTP server to serve hosts on many IP subnets.[3]

DHCP is based on BOOTP but can dynamically allocate IP addresses from a pool and reclaim them when they are no longer in use. It can also be used to deliver a wide range of extra configuration parameters to IP clients, including platform-specific parameters.[4] It was first defined in RFC 1531 in October 1993; but due to errors in the editorial process was almost immediately reissued as RFC 1541.

Four years later the DHCPINFORM message type[5] and other small changes were added by RFC 2131; which as of 2014 remains the standard for IPv4 networks.

DHCPv6 was initially described by RFC 3315 in 2003, but this has been updated by many subsequent RFCs.[6] RFC 3633 added a DHCPv6 mechanism for prefix delegation, and stateless address autoconfiguration was added by RFC 3736.

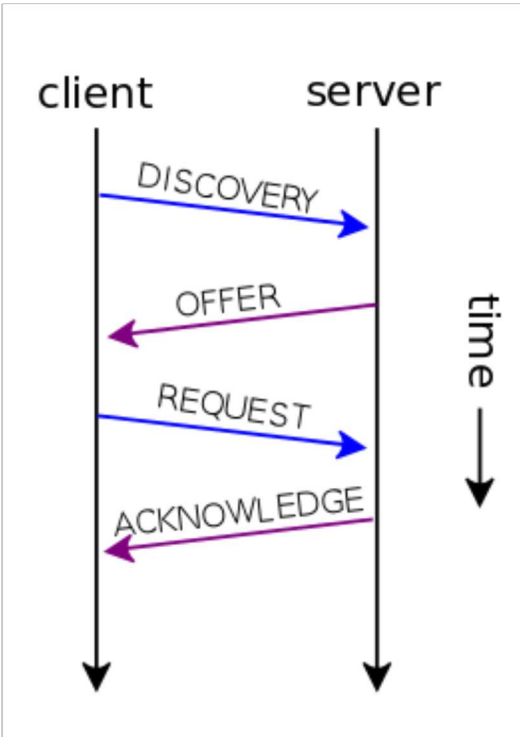
Operation

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is

implemented with two UDP port numbers for its operations which are the same as for the BOOTP protocol. UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client.

DHCP operations fall into four phases: server discovery, IP lease offer, IP request, and IP lease acknowledgement. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgement.

The DHCP operation begins with clients broadcasting a request. If the client and server are on different subnets, a DHCP Helper or DHCP Relay Agent may be used. Clients requesting renewal of an existing lease may communicate directly via UDP unicast, since the client already has an established IP address at that point. Additionally, there is a BOOTP flag the client can use to indicate in which way (broadcast or unicast) it can receive the DHCPOFFER: 0x8000 for broadcast, 0x0000 for unicast.[8] Only hosts with preconfigured IP address can receive unicast packets so in the usual use case clients in discovery phase should set BOOTP flag to 0x8000 (broadcast).



An illustration of a typical non-renewing DHCP session; each message may be either a broadcast or a unicast, depending on the DHCP client capabilities.[7]

DHCP discovery

The client broadcasts messages on the network subnet using the destination address 255.255.255.255 or the specific subnet broadcast address. A DHCP client may also request its last-known IP address. If the client remains connected to the same network, the server may grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An authoritative server denies the request, causing the client to issue a new request. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to expire the request and ask for a new IP address.

DHCPDISCOVER message

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67			
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x8000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0x00000000			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s, or overflow space for additional options. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP Discover			
DHCP option 50: 192.168.1.100 requested			
DHCP option 55: Parameter Request List: Request Subnet Mask (1), Router (3), Domain Name (15), Domain Name Server (6)			

DHCP offer

When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

The server determines the configuration based on the client's hardware address as specified in the CHADDR (client hardware address) field. Here the server, 192.168.1.1, specifies the client's IP address in the YIADDR (your IP address) field.

DHCPOFFER message

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 | dPort=68			
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164 (This translates to 192.168.1.100)			
SIADDR (Server IP address)			
0xC0A80101 (This translates to 192.168.1.1)			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP Offer			
DHCP option 1: 255.255.255.0 subnet mask			
DHCP option 3: 192.168.1.1 router			
DHCP option 51: 86400s (1 day) IP address lease time			
DHCP option 54: 192.168.1.1 DHCP server			
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18			

DHCP request

In response to the DHCP offer, the client replies with a DHCP request, broadcast to the server,[a] requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on required *server identification* option in the request and broadcast messaging, servers are informed whose offer the client has accepted.[10]:Section 3.1, Item 3 When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

DHCPREQUEST message

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255[a] dPort=67			
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0xC0A80101			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP Request			
DHCP option 50: 192.168.1.100 requested			
DHCP option 54: 192.168.1.1 DHCP server.			

DHCP acknowledgement

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.

The protocol expects the DHCP client to configure its network interface with the negotiated parameters.

After the client obtains an IP address, it should probe the newly received address[11] (e.g. with ARP Address Resolution Protocol) to prevent address conflicts caused by overlapping address pools of DHCP servers.

DHCPACK message

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68			
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0xC0A80164			
SIADDR (Server IP address)			
0xC0A80101			
GIADDR (Gateway IP address switched by relay)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic cookie			
0x63825363			
DHCP Options			
DHCP option 53: DHCP ACK (value=5) or DHCP NAK (value=6)			
DHCP option 1: 255.255.255.0 subnet mask			
DHCP option 3: 192.168.1.1 router			
DHCP option 51: 86400s (1 day) IP address lease time			
DHCP option 54: 192.168.1.1 DHCP server			
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18			

DHCP information

A DHCP client may request more information than the server sent with the original DHCPOFFER. The client may also request repeat data for a particular application. For example, browsers use *DHCP Inform* to obtain web proxy settings via WPAD.

DHCP releasing

The client sends a request to the DHCP server to release the DHCP information and the client deactivates its IP address. As client devices usually do not know when users may unplug them from the network, the

protocol does not mandate the sending of *DHCP Release*.

Client configuration parameters

A DHCP server can provide optional configuration parameters to the client. RFC 2132 describes the available DHCP options defined by Internet Assigned Numbers Authority (IANA) - DHCP and BOOTP PARAMETERS.[12]

A DHCP client can select, manipulate and overwrite parameters provided by a DHCP server.[13]

DHCP options

Options are variable length octet strings. The first octet is the option code, the second octet is the number of following octets and the remaining octets are code dependent. For example, the DHCP Message type option for an Offer would appear as 0x35,0x01,0x02, where 0x35 is code 53 for "DHCP Message Type", 0x01 means one octet follows and 0x02 is the value of "Offer".

The following tables list the available DHCP options, as stated in RFC2132.[14]

RFC1497 vendor extensions[14]:Section 3

Code	Name	Length	Notes
0	Pad[14]:Section 3.1	0 octets	Can be used to pad other options so that they are aligned to the word boundary; is not followed by length byte
1	Subnet Mask[14]:Section 3.3	4 octets	Must be sent after the router option (option 3) if both are included
2	Time Offset[14]:Section 3.4	4 octets	
3	Router	multiples of 4 octets	Available routers, should be listed in order of preference
4	Time Server	multiples of 4 octets	Available time servers to synchronise with, should be listed in order of preference
5	Name Server	multiples of 4 octets	Available IEN 116 name servers, should be listed in order of preference
6	Domain Name Server	multiples of 4 octets	Available DNS servers, should be listed in order of preference
7	Log Server	multiples of 4 octets	Available log servers, should be listed in order of preference.
8	Cookie Server	multiples of 4 octets	"Cookie" in this case means "fortune cookie" or "quote of the day," a pithy or humorous anecdote often sent as part of a logon process on large computers; it has nothing to do with cookies sent by websites.
9	LPR Server	multiples of 4 octets	
10	Impress Server	multiples of 4 octets	
11	Resource Location Server	multiples of 4 octets	
12	Host Name	minimum of 1 octet	
13	Boot File Size	2 octets	Length of the boot image in 4KiB blocks
14	Merit Dump File	minimum of 1 octet	Path where crash dumps should be stored
15	Domain Name	minimum of 1 octet	
16	Swap Server	4 octets	
17	Root Path	minimum of 1 octet	
18	Extensions Path	minimum of 1 octet	
255	End	0 octets	Used to mark the end of the vendor option field

IP Layer Parameters per Host[14]:Section 4

Code	Name	Length	Notes
19	IP Forwarding Enable/Disable	1 octet	
20	Non-Local Source Routing Enable/Disable	1 octet	
21	Policy Filter	multiples of 8 octets	
22	Maximum Datagram Reassembly Size	2 octets	
23	Default IP Time-to-live	1 octet	
24	Path MTU Aging Timeout	4 octets	
25	Path MTU Plateau Table	multiples of 2 octets	

IP Layer Parameters per Interface[14]:Section 5

Code	Name	Length	Notes
26	Interface MTU	2 octets	
27	All Subnets are Local	1 octet	
28	Broadcast Address	4 octets	
29	Perform Mask Discovery	1 octet	
30	Mask Supplier	1 octet	
31	Perform Router Discovery	1 octet	
32	Router Solicitation Address	4 octets	
33	Static Route	multiples of 8 octets	A list of destination/router pairs

Link Layer Parameters per Interface[14]:Section 6

Code	Name	Length	Notes
34	Trailer Encapsulation Option	1 octet	
35	ARP Cache Timeout	4 octets	
36	Ethernet Encapsulation	1 octet	

TCP Parameters[14]:Section 7

Code	Name	Length	Notes
37	TCP Default TTL	1 octet	
38	TCP Keepalive Interval	4 octets	
39	TCP Keepalive Garbage	1 octet	

Application and Service Parameters[14]:Section 8

Code	Name	Length	Notes
40	Network Information Service Domain	minimum of 1 octet	
41	Network Information Servers	multiples of 4 octets	
42	Network Time Protocol Servers	multiples of 4 octets	
43	Vendor Specific Information	minimum of 1 octets	
44	NetBIOS over TCP/IP Name Server	multiples of 4 octets	
45	NetBIOS over TCP/IP Datagram Distribution Server	multiples of 4 octets	
46	NetBIOS over TCP/IP Node Type	1 octet	
47	NetBIOS over TCP/IP Scope	minimum of 1 octet	
48	X Window System Font Server	multiples of 4 octets	
49	X Window System Display Manager	multiples of 4 octets	
64	Network Information Service+ Domain	minimum of 1 octet	
65	Network Information Service+ Servers	multiples of 4 octets	
68	Mobile IP Home Agent	multiples of 4 octets	
69	Simple Mail Transport Protocol (SMTP) Server	multiples of 4 octets	
70	Post Office Protocol (POP3) Server	multiples of 4 octets	
71	Network News Transport Protocol (NNTP) Server	multiples of 4 octets	
72	Default World Wide Web (WWW) Server	multiples of 4 octets	
73	Default Finger Server	multiples of 4 octets	
74	Default Internet Relay Chat (IRC) Server	multiples of 4 octets	
75	StreetTalk Server	multiples of 4 octets	
76	StreetTalk Directory Assistance (STDA) Server	multiples of 4 octets	

DHCP Extensions[14]:Section 9

Code	Name	Length	Notes
50	Requested IP address	4 octets	
51	IP address Lease Time	4 octets	
52	Option Overload	1 octet	
53	DHCP Message Type	1 octet	
54	Server Identifier	4 octets	
55	Parameter Request List	minimum of 1 octet	
56	Message	minimum of 1 octet	
57	Maximum DHCP Message Size	2 octets	
58	Renewal (T1) Time Value	4 octets	
59	Rebinding (T2) Time Value	4 octets	
60	Vendor class identifier	minimum of 1 octet	
61	Client-identifier	minimum of 2 octets	
66	TFTP server name	minimum of 1 octet	
67	Bootfile name	minimum of 1 octet	

Vendor identification

An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters or octets which has a meaning specified by the vendor of the DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is to set a value in its DHCP requests called the Vendor Class Identifier (VCI) (Option 60).

This method allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately. Some types of set-top boxes also set the VCI (Option 60) to inform the DHCP server about the hardware type and functionality of the device. The value this option is set to gives the DHCP server a hint about any required extra information that this client needs in a DHCP response.

DHCP relaying

In small networks, where only one IP subnet is being managed, DHCP clients communicate directly with DHCP servers. However, DHCP servers can also provide IP addresses for multiple subnets. In this case, a DHCP client that has not yet acquired an IP address cannot communicate directly with the DHCP server using IP routing, because it does not have a routable IP address, nor does it know the IP address of a router.

In order to allow DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. The DHCP client broadcasts on the local link; the relay agent receives the broadcast and transmits it to one or more DHCP servers using unicast. The relay agent stores its own IP address in the GIADDR field of the DHCP packet. The DHCP server uses the GIADDR to determine the subnet on which the relay agent received the broadcast, and allocates an IP address on that subnet. When the DHCP server replies to the client, it sends the reply to the GIADDR address, again using unicast. The relay agent then retransmits the response on the local network.

Reliability

The DHCP protocol ensures reliability in several ways: periodic renewal, rebinding,[10]:Section 4.4.5 and failover. DHCP clients are allocated leases that last for some period of time. Clients begin to attempt to renew their leases once half the lease interval has expired.[10]:Section 4.4.5 Paragraph 3 They do this by sending a unicast DHCPREQUEST message to the DHCP server that granted the original lease. If that server is down or unreachable, it will fail to respond to the DHCPREQUEST. However, in that case the client repeats the DHCPREQUEST from time to time,[10]:Section 4.4.5 Paragraph 8[b] so if the DHCP server comes back up or becomes reachable again, the DHCP client will succeed in contacting it and renew the lease.

If the DHCP server is unreachable for an extended period of time,[10]:Section 4.4.5 Paragraph 5 the DHCP client will attempt to rebind, by broadcasting its DHCPREQUEST rather than unicasting it. Because it is broadcast, the DHCPREQUEST message will reach all available DHCP servers. If some other DHCP server is able to renew the lease, it will do so at this time.

In order for rebinding to work, when the client successfully contacts a backup DHCP server, that server must have accurate information about the client's binding. Maintaining accurate binding information between two servers is a complicated problem; if both servers are able to update the same lease database, there must be a mechanism to avoid conflicts between updates on the independent servers. A proposal for implementing fault-tolerant DHCP servers was submitted to the Internet Engineering Task Force, but never formalized[15][c]

If rebinding fails, the lease will eventually expire. When the lease expires, the client must stop using the IP address granted to it in its lease.[10]:Section 4.4.5 Paragraph 9 At that time it will restart the DHCP process from the beginning by broadcasting a DHCPDISCOVER message. Since its lease has expired, it will accept any IP

address offered to it. Once it has a new IP address (presumably from a different DHCP server) it will once again be able to use the network. However, since its IP address has changed, any ongoing connections will be broken.

Security

The base DHCP protocol does not include any mechanism for authentication.[16] Because of this, it is vulnerable to a variety of attacks. These attacks fall into three main categories:

- Unauthorized DHCP servers providing false information to clients.[17]
- Unauthorized clients gaining access to resources.[17]
- Resource exhaustion attacks from malicious DHCP clients.[17]

Because the client has no way to validate the identity of a DHCP server, unauthorized DHCP servers (commonly called "rogue DHCP") can be operated on networks, providing incorrect information to DHCP clients.[18] This can serve either as a denial-of-service attack, preventing the client from gaining access to network connectivity,[19] or as a man-in-the-middle attack.[20] Because the DHCP server provides the DHCP client with server IP addresses, such as the IP address of one or more DNS servers,[17] an attacker can convince a DHCP client to do its DNS lookups through its own DNS server, and can therefore provide its own answers to DNS queries from the client.[21][22] This in turn allows the attacker to redirect network traffic through itself, allowing it to eavesdrop on connections between the client and network servers it contacts, or to simply replace those network servers with its own.[21]

Because the DHCP server has no secure mechanism for authenticating the client, clients can gain unauthorized access to IP addresses by presenting credentials, such as client identifiers, that belong to other DHCP clients.[18] This also allows DHCP clients to exhaust the DHCP server's store of IP addresses—by presenting new credentials each time it asks for an address, the client can consume all the available IP addresses on a particular network link, preventing other DHCP clients from getting service.[18]

DHCP does provide some mechanisms for mitigating these problems. The Relay Agent Information Option protocol extension (RFC 3046, usually referred to in the industry by its actual number as Option 82[23][24]) allows network operators to attach tags to DHCP messages as these messages arrive on the network operator's trusted network. This tag is then used as an authorization token to control the client's access to network resources. Because the client has no access to the network upstream of the relay agent, the lack of authentication does not prevent the DHCP server operator from relying on the authorization token.[16]

Another extension, Authentication for DHCP Messages (RFC 3118), provides a mechanism for authenticating DHCP messages. Unfortunately RFC 3118 has not seen (as of 2002) widespread adoption because of the problems of managing keys for large numbers of DHCP clients.[25] A 2007 book about DSL technologies remarked that "there were numerous security vulnerabilities identified against the security measures proposed by RFC 3118. This fact, combined with the introduction of 802.1x, slowed the deployment and take-rate of authenticated DHCP, and it has never been widely deployed."[26] A 2010 book notes that "[t]here have been very few implementations of DHCP Authentication. The challenges of key management and processing delays due to hash computation have been deemed too heavy a price to pay for the perceived benefits."[27]

More recent (2008) architectural proposals involve authenticating DHCP requests using 802.1x or PANA (both of which transport EAP).[28] An IETF proposal was made for including EAP in DHCP itself, the so-called EAPoDHCP;[29] this does not appear to have progressed beyond IETF draft level, the last of which dates to 2010.[30]

IETF standards documents

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC 3046, DHCP Relay Agent Information Option
- RFC 3942, Reclassifying Dynamic Host Configuration Protocol Version Four (DHCPv4) Options
- RFC 4242, Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6
- RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
- RFC 4436, Detecting Network Attachment in IPv4 (DNAv4)

See also

- Boot Service Discovery Protocol (BSDP) – a DHCP extension used by Apple's NetBoot
- Comparison of DHCP server software
- Peg DHCP (RFC 2322)
- Preboot Execution Environment (PXE)
- Reverse Address Resolution Protocol (RARP)
- Rogue DHCP
- UDP Helper Address – a tool for routing DHCP requests across subnet boundaries
- Zeroconf – Zero Configuration Networking

Notes

a. As an optional client behavior, some broadcasts, such as those carrying DHCP discovery and request messages, may be replaced with unicasts in case the DHCP client already knows the DHCP server's IP address.[9]
b. The RFC calls for the client to wait one half of the remaining time until T2 before it retransmits the DHCPREQUEST packet
c. The proposal provided a mechanism whereby two servers could remain loosely in sync with each other in such a way that even in the event of a total failure of one server, the other server could recover the lease database and continue operating. Due to the length and complexity of the specification, it was never published as a standard; however, the techniques described in the specification are in wide use, with one open-source implementation in the ISC DHCP server, as well as several commercial implementations.

References

1. Peterson LL, Davie BS. (2011). Computer Networks: A Systems Approach (http://books.google.com/books?id=BvaFreun1W8C&pg=PA372&lpg=PA372).
2. Ralph Droms; Ted Lemon (2003). *The DHCP Handbook*. SAMS Publishing. p. 436. ISBN 0-672-32327-3.
3. Bill Croft; John Gilmore (September 1985). "RFC 951 - Bootstrap Protocol". *Network Working Group*.
4. Network+ Certification 2006 Published By Microsoft Press.
5. used for the Web Proxy Autodiscovery Protocol WPAD
6. RFC 4361, RFC 5494, RFC 6221, RFC 6422, RFC 6644, RFC 7083, RFC 7227, RFC 7283
7. RFC 2131, Section 4.1 Constructing and sending DHCP messages (https://tools.ietf.org/html/rfc2131#section-4.1)
8. Droms, Ralph. "Dynamic Host Configuration Protocol". *tools.ietf.org*. Retrieved 2015-12-26.
9. RFC 2131, Section 4.4.4: Use of broadcast and unicast (https://tools.ietf.org/html/rfc2131#section-4.4.4)
10. Droms, Ralph (March 1997). *DHCP Options and BOOTP Vendor Extensions* (https://tools.ietf.org/html/rfc2131). IETF. RFC 2131. https://tools.ietf.org/html/rfc2131. Retrieved September 9, 2014.
11. RFC2131 Dynamic Host Configuration Protocol: Dynamic allocation of network addresses http://tools.ietf.org/html/rfc2131#section-2.2
12. "Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters". Iana.org. Retrieved 2013-11-28.

13. In Unix-like systems this client-level refinement typically takes place according to the values in a `/etc/dhclient.conf` configuration file.
14. Alexander, Steve; Droms, Ralph (March 1997). *DHCP Options and BOOTP Vendor Extensions* (https://tools.ietf.org/html/rfc2132). IETF. RFC 2132. https://tools.ietf.org/html/rfc2132. Retrieved June 10, 2012.
15. Droms, Ralph; Kinnear, Kim; Stapp, Mark; Volz, Bernie; Gonczi, Steve; Rabil, Greg; Dooley, Michael; Kapur, Arun (March 2003). *DHCP Failover Protocol* (https://tools.ietf.org/html/draft-ietf-dhc-failover-12). IETF. I-D draft-ietf-dhc-failover-12. https://tools.ietf.org/html/draft-ietf-dhc-failover-12. Retrieved May 09, 2010.
16. Michael Patrick (January 2001). "RFC 3046 - DHCP Relay Agent Information Option". *Network Working Group*.
17. Ralph Droms (March 1997). "RFC 2131 - Dynamic Host Configuration Protocol". *Network Working Group*.
18. Timothy Stapko (2011). *Practical Embedded Security: Building Secure Resource-Constrained Systems*. Newnes. p. 39. ISBN 978-0-08-055131-9.
19. Derrick Rountree (2013). *Windows 2012 Server Network Security: Securing Your Windows Network Systems and Infrastructure*. Newnes. p. 22. ISBN 978-1-59749-965-1.
20. Timothy Rooney (2010). *Introduction to IP Address Management*. John Wiley & Sons. p. 180. ISBN 978-1-118-07380-3.
21. Sergey Golovanov (Kaspersky Labs) (June 2011). "TDSS loader now got "legs" ".
22. Akash K Sunny (October 2015). "dhcp protocol and its vulnerabilities".
23. Francisco J. Hens; José M. Caballero (2008). *Triple Play: Building the converged network for IP, VoIP and IPTV*. John Wiley & Sons. p. 239. ISBN 978-0-470-75439-9.
24. David H. Ramirez (2008). *IPTV Security: Protecting High-Value Digital Contents*. John Wiley & Sons. p. 55. ISBN 978-0-470-72719-5.
25. Ted Lemon (April 2002). "Implementation of RFC 3118".
26. Philip Golden; Hervé Dedieu; Krista S. Jacobsen (2007). *Implementation and Applications of DSL Technology*. Taylor & Francis. p. 484. ISBN 978-1-4200-1307-8.
27. Timothy Rooney (2010). *Introduction to IP Address Management*. John Wiley & Sons. pp. 181–182. ISBN 978-1-118-07380-3.
28. Rebecca Copeland (2008). *Converging NGN Wireline and Mobile 3G Networks with IMS*. Taylor & Francis. pp. 142–143. ISBN 978-1-4200-1378-8.
29. Ramjee Prasad; Albena Mihovska (2009). *New Horizons in Mobile and Wireless Communications: Networks, services, and applications* **2**. Artech House. p. 339. ISBN 978-1-60783-970-5.
30. http://tools.ietf.org/search/draft-pruss-dhcp-auth-dsl-07

External links

Wikimedia Commons has media related to ***Dynamic Host Configuration Protocol (DHCP)***.

Categories: Internet Standards | Application layer protocols | Network service