Network Working Group
Request for Comments: 2563
Category: Standards Track

R. Troll
@Home Network

May 1999

DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients

Status of this Memo

Copyright Notice

Abstract

Operating Systems are now attempting to support ad-hoc networks of two or more systems, while keeping user configuration at a minimum. To accommodate this, in the absence of a central configuration mechanism (DHCP), some OS's are automatically choosing a link-local IP address which will allow them to communicate only with other hosts on the same link. This address will not allow the OS to communicate with anything beyond a router. However, some sites depend on the fact that a host with no DHCP response will have no IP address. This document describes a mechanism by which DHCP servers are able to tell clients that they do not have an IP address to offer, and that the client should not generate an IP address it's own.

1. Introduction

With computers becoming a larger part of everyday life, operating systems must be able to support a larger range of operating environments. One aspect of this support is the selection of an IP address. The Dynamic Host Configuration Protocol [DHCP] provides a superb method by which site administrators may supply IP addresses (and other network parameters) to network devices. However, some operating environments are not centrally maintained, and operating systems must now be able to handle this quickly and easily.

IPv6 accounts for this, and allows an IPv6 stack to assign itself a global address in the absence of any other mechanism for configuration [IPv6SAC]. However, Operating System designers can't wait for IPv6 support everywhere. They need to be able to assume

they will have IPv4 addresses, so that they may communicate with one another even in the smallest networks.

This document looks at three types of network nodes, and how IPv4 address auto-configuration may be disabled on a per-subnet (or even per-node) basis. The three types of network nodes are:

* A node for which the site administrator will hand out configuration information,

* A node on a network segment for which there is no site administrator, and

* A node on a network segment that has a central site administrator, and that administrator chooses not to hand out any configuration information to the node.

The difference between the second and third cases is the clients behavior.

In one case, the node may assign itself an IP address, and have full connectivity with other nodes on the local wire. In the last case, the node is not told what to do, and while it may assign itself a network address in the same way as case #2, this may not be what the central administrator wants.

The first scenario is handled by the current DHCP standard. However, the current DHCP specification [DHCP] says servers must silently ignore requests from hosts they do not know. Because of this, DHCP clients are unable to determine whether they are on a subnet with no administration, or with administration that is choosing not to hand out addresses.

This document describes a method by which DHCP clients will be able to determine whether or not the network is being centrally administrated, allowing it to intelligently determine whether or not it should assign itself a "link-local" address.

1.1. Conventions Used in the Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [KEYWORDS].

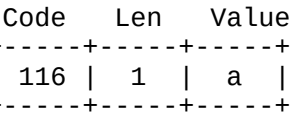
1.2. Terminology

DHCP client — A DHCP client is an Internet host using DHCP to obtain configuration parameters such as a network address.

DHCP server — A DHCP server is an Internet host that returns configuration parameters to DHCP clients.

2. The Auto-Configure Option

This option code is used to ask whether, and be notified if, auto-configuration should be disabled on the local subnet. The auto-configure option is an 8-bit number.



Code	Len	Value
116	1	a

The code for this option is 116, and its length is 1.

This code, along with the IP address assignment, will allow a DHCP client to determine whether or not it should generate a link-local IP address.

2.1. Auto-Configure Values

The auto-configure option uses the following values:

DoNotAutoConfigure	0
AutoConfigure	1

When a server responds with the value "AutoConfigure", the client MAY generate a link-local IP address if appropriate. However, if the server responds with "DoNotAutoConfigure", the client MUST NOT generate a link-local IP address, possibly leaving it with no IP address.

2.2. DHCP Client Behavior

Clients that have auto-configuration capabilities MUST add the Auto-Configure option to the list of options included in its initial DHCPDISCOVER message. ([DHCP] Section 4.4.1) At this time, the option's value should be set to "AutoConfigure".

When a DHCPOFFER is received, it is handled as described in [DHCP], section 4.4.1, with one exception. If the 'yiaddr' field is 0x00000000, the Auto-Configure option must be consulted. If this

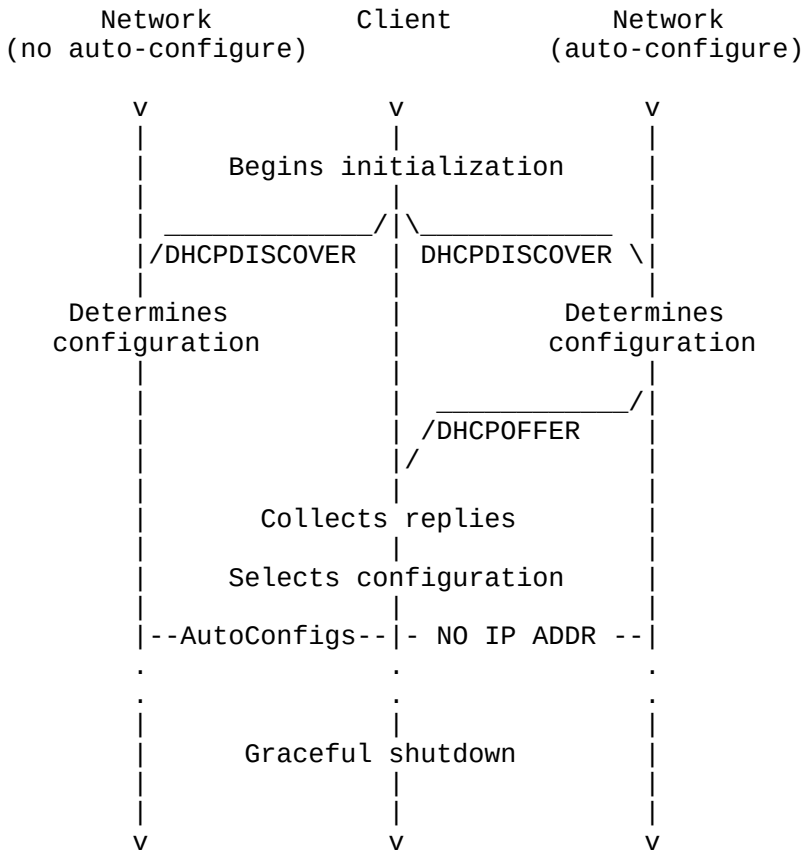
option is set to "AutoConfigure", then the DHCPOFFER MUST be ignored, and the DHCP client MAY generate a link-local IP address. However, if this option is set to "DoNotAutoConfigure", then the DHCPOFFER MUST be ignored, and the client MUST NOT generate a link-local IP address.

If a DHCP client receives any DHCPOFFER which contains a 'yiaddr' of 0x00000000, and the Auto-Configure flag says "DoNotAutoConfigure", in the absence of a DHCPOFFER with a valid 'yiaddr', the DHCP client MUST NOT generate a link-local IP address. The amount of time a DHCP client waits to collect any other DHCPOFFERs is implementation dependant.

DHCPOFFERs with a 'yiaddr' of 0x00000000 will only be sent by DHCP servers supporting the Auto-Configure option when the DHCPDISCOVER contained the Auto-Configure option. Since the DHCPDISCOVER will only contain the Auto-Configure option when a DHCP client knows how to handle it, there will be no inter-operability problems.

If the DHCP server does have an address to offer, the message states are the same as those described in [DHCP], section 3.

The following depicts the difference in responses for non-registered DHCP clients that support the "Auto-Configure" option on networks that have DHCP servers that support auto-configuration and networks with DHCP servers that do not.



2.3. DHCP Server Behavior

When a DHCP server receives a DHCPDISCOVER, it MUST be processed as described in [DHCP], section 4.3.1. However, if no address is chosen for the host, a few additional steps MUST be taken.

If the DHCPDISCOVER does not contain the Auto-Configure option, it is not answered.

If the DHCPDISCOVER contains the Auto-Configure option, and the site administrator has specified that Auto-Configuration should be disabled on the subnet the DHCPDISCOVER is originating from, or for the client originating the request, then a DHCPOFFER MUST be sent to the DHCP client. This offer MUST be for the address 0x00000000, and the Auto-Configure option MUST be set to "DoNotAutoConfigure".

If the site administrator allows auto-configuration on the originating subnet, the DHCPDISCOVER is not answered as before.

2.4. Mixed Environments

Environments containing a mixture of clients and servers that do and do not support the Auto-Configure option will not be a problem. Every DHCP transaction is between a Server and a Client, and the possible mixed scenarios between these two are listed below.

2.4.1. Client Supports, Server Does Not

If a DHCP client sends a request that contains the Auto-Configure tag, a DHCP server that does not know what this tag is will respond normally. According to [DHCP] Section 4.3.1, the server MUST NOT return a value for that parameter.

In this case, the server will either respond with a valid DHCPOFFER, or it will not respond at all. In both cases, a DHCP client that supports this option will never care what the state of the option is, and may auto-configure.

2.4.2. Servers Supports, Client Does Not

If the Auto-Configure option is not present in the DHCPDISCOVER, the server will do nothing about it. The client will auto-configure if it doesn’t receive a response and believes that’s what it should do.

This scenario SHOULD not occur, as any stacks that implement an auto-configuration mechanism MUST implement this option as well.

2.5. Interaction With Other DHCP Messages

As this option only affects the initial IP address selection, it does not apply to subsequent DHCP messages. If the DHCP client received a lease from a DHCP server, future DHCP messages (RENEW, INFORM, ACK, etc.) have no need to fall over into an auto- configuration state.

If the DHCP client’s lease expires, the client falls back into the INIT state, and the initial DHCPDISCOVER is sent as before.

2.5.1. DHCPRELEASE Messages

DHCPRELEASEs occur exactly as described in [DHCP], section 4.4.6. When a DHCP client is done with a lease, it MAY notify the server that it is finished. For this to occur, the DHCP client already received a DHCP lease, and the state of Auto-Configuration on the local wire does not matter.

2.5.2. DHCPDECLINE Messages

A DHCPDECLINE is sent by the DHCP client when it determines the network address it is attempting to use is already in use. As a network address has been tested, it must have been offered by the DHCP Server, and the state of Auto-Configuration on the local wire does not matter.

2.5.3. DHCPINFORM Messages

DHCPINFORMs should be handled as described in [DHCP], section 4.4.3. No changes are necessary.

2.6. Message Option

If the DHCP server would like to tell a client why it is not allowed to auto-configure, it MAY add the Message option to the response. This option is defined in [DHCPOPT], Section 9.9.

If the DHCP client receives a response with the Message option set, it MUST provide this information to the administrator of the DHCP client. How this information is provided is implementation dependant.

3. Security Considerations

DHCP per se currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification [DHCP].

This mechanism does add one other potential attack. Malicious users on a subnet may respond to all DHCP requests with responses telling DHCP clients that they should NOT auto-configure on the local wire. On a network where Auto-Configuration is required, this will cause all DHCP clients to not choose an address.

4. Acknowledgments

This idea started at a joint Common Solutions Group / Microsoft meeting at Microsoft in May, 1998. The IP stacks in Win98 and NT5 assign themselves an IP address (in a specific subnet) in the absence of a responding DHCP server, and this is causing headaches for many sites that actually rely on machines not getting IP addresses when the DHCP servers do not know them.

Walter Wong proposed a solution that would allow the DHCP servers to tell clients not to do this. His initial solution would not work without slight modifications to DHCP itself. This document describes

those modifications.

5. IANA Considerations

The IANA has assigned option number 116 for this option.

6. References

[DHCP] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[DHCPOPT] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extension", RFC 2132, March 1997.

[IPv6SAC] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7. Author's Address

Ryan Troll
@Home Network
425 Broadway
Redwood City, CA 94063

Phone: (650) 556-6031
EMail: rtroll@corp.home.net

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.