Internet Engineering Task Force (IETF)
Request for Comments: 5859
Category: Informational
ISSN: 2070-1721

R. Johnson
Cisco Systems, Inc.

June 2010

TFTP Server Address Option for DHCPv4

Abstract

This memo documents existing usage for the "TFTP Server Address" option. The option number currently in use is 150. This memo documents the current usage of the option in agreement with RFC 3942, which declares that any pre-existing usages of option numbers in the range 128-223 should be documented, and the Dynamic Host Configuration working group will try to officially assign those numbers to those options. The option is defined for DHCPv4 and works only with IPv4 addresses.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5859.

Table of Contents

1. Introduction

Voice over IP (VoIP) devices, such as IP phones, have a need to download their configuration from a configuration server on the network. There are two commonly accepted methods to discover this server via DHCP; the "sname" field in the DHCP header [RFC2131] and the "TFTP Server Name" option (66) [RFC2132]. Both of these sources of information, however, contain the TFTP server's hostname. That hostname must then be translated to an IP address. The usual method to accomplish this would be DNS [RFC1034]. This means the firmware in a VoIP device (with possibly limited flash, memory, and/or processing resources) would need to implement the DNS protocol in order to perform this translation. This would also introduce an additional unnecessary point of failure whereby the device is dependent on the DNS server infrastructure in order to boot up and communicate with its call agent.

In order to eliminate DNS as a point of failure and to keep the firmware in such a VoIP device to a minimum, the "VoIP Configuration Server Address" option (150) was introduced. This option allows the DHCP server to pass one or more IP addresses of the VoIP configuration server(s) instead of the hostname, thus making the information directly usable by the VoIP device.

Other reasons for this option are (1) the "siaddr" field is not configurable on some DHCP servers; (2) the "siaddr" field only allows for one IPv4 address, and it is desirable to have the ability to configure multiple IP addresses for redundancy; (3) some DHCP servers have been found to fill in their own IPv4 address as siaddr; (4) some customers were already using the "siaddr" field for other purposes; and finally (5) the configuration server may use a protocol other than TFTP to serve configuration files, making the use of the "TFTP Server Name" option (66) inappropriate.

In cases where other download server address information also appears in the response packet, such as "sname" and "TFTP Server Name", it is left to the device to decide which piece of information to use.

2. Conventions

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 RFC 2119 [RFC2119].

3. TFTP Server Address Option Definition

The TFTP Server Address option is a DHCP option [RFC2132]. The option contains one or more IPv4 addresses that the client MAY use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.

The format of the option is:

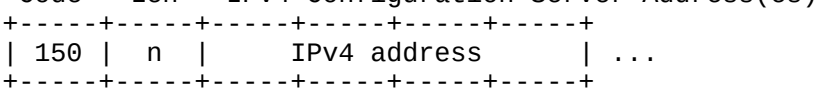

Figure 1

The option minimum length (n) is 4.

The "Len" field must specify a length that is an integral multiple of 4 octets (4, 8, 12, etc.). If an option is received where this is not the case, the option information MUST be ignored, but further option processing may continue. Dividing this "Len" value by 4 will give the number of IPv4 VoIP configuration server addresses that are specified in the option.

The option MUST NOT be specified by the DHCP client, as it is intended only to be returned from the DHCP server. If the DHCP client wants to receive this information from the server, it needs to include the number 150 in the "DHCP Parameter List" option (55).

Server addresses SHOULD be listed in order of preference, and the client SHOULD use the addresses sequentially but may be configured to use addresses randomly. The client may use as many or as few of the addresses provided as it likes. For example, if the client is only capable of accepting two configuration server addresses, it may ignore any other addresses provided after the second address.

Each TFTP server address that is being used by the client should be tried a total of four times with a 4-second wait time before proceeding to the next address.

When this option appears along with the TFTP Server Name option (66) [RFC2132], this option SHOULD have priority over option 66.

There is currently no defined IPv6 DHCP equivalent for this option.

4. Security Considerations

A rogue DHCP server could use this option in order to coerce a client into downloading configuration data from an alternate configuration server, and thus gain control of the device's configuration. This, however, is no more of a security threat than similar attacks using other DHCP options that specify server names or addresses, of which there are many. If this is a concern, then DHCP authentication may be used, but even secure delivery of an address over DHCP does not protect the subsequent insecure download over TFTP. TFTP itself provides no authentication or access control mechanisms, so even if DHCP messages were authenticated, downloading the configuration would still be insecure, unless some object-level security mechanisms were used.

Where security concerns are an issue, it is suggested that configuration files should be signed by a trusted agent. Configuration files may also be encrypted based on a configuration parameter on the DHCP client device. In other words, there are various methods to ensure the integrity of configuration data independent from ensuring the integrity of this DHCP option or even DHCP itself. The full extent of such options is far too broad to be addressed in this document.

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [RFC3118]. Potential exposures to attack are discussed in Section 7 of the DHCP protocol specification [RFC2131].

5. IANA Considerations

IANA has assigned DHCP option number 150, in accordance with [RFC3942].

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3942] Volz, B., "Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options", RFC 3942, November 2004.

6.2. Informative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

Author’s Address

Richard A. Johnson
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
USA

Phone: +1 408 526 4000
EMail: raj@cisco.com