VoIP Configuration Server Address Option
draft-raj-dhc-tftp-addr-option-05.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 10, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This memo documents existing usage for the "VoIP Configuration Server Address Option" (previously known as the "TFTP Server IP Address Option"). The option number currently in use is 150. This memo documents the current usage of the option in agreement with RFC 3942 [RFC3942], which declares that any pre-existing usages of option numbers in the range 128 - 223 should be documented and the working group will try to officially assign those numbers to those options.

Table of Contents

1. Introduction .................................................. 3
2. Conventions .................................................. 4
3. VoIP Configuration Server Address Option Definition .......... 5
4. Security Considerations ...................................... 6
5. IANA Considerations .......................................... 7
6. References .................................................... 8
   6.1. Normative References ..................................... 8
   6.2. Informative References ................................... 8
Author’s Address ................................................. 9
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 commonly accepted methods to discover this server via DHCP; the "sname" field in the DHCP header [RFC2131], 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 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 that, (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) in 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. VoIP Configuration Server Address Option Definition

The VoIP Configuration Server Address option is a DHCP option [RFC2132]. The option contains one or more IPv4 addresses of the VoIP Configuration Server which the client MAY use.

The format of the option is:

```
| Code  | Len   | IPv4 Configuration Server Address(es) |
+-------+-------+--------------------------------------+
| 150   | n     | IPv4 address                         |
|       |       |                                      |
+-------+-------+--------------------------------------+
```

Figure 1

The option minimum length (n) is 4.

The "Len" field must specify a length which 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 SHOULD be ignored. Dividing this "Len" value by 4 will give number of IPv4 VoIP Configuration Server addresses which are specified in the option.

The option SHOULD 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 SHOULD include the number 150 in the DHCP "Parameter List" option (55).

Server addresses SHOULD be listed in order of preference.

The client may use as many or as few of the addresses provided. For example, if client is only capable of accepting 2 configuration server addresses, it may ignore any other addresses provided after the second address. A client SHOULD accept an offer that contains more addresses than it is capable of utilizing and ignore those that it is not capable of using.
4. Security Considerations

A rogue DHCP Server could use this option in order to coerce a Client into downloading configuration 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 which specify server names or addresses, of which there are many. If this is a concern, then DHCP Authentication may be used. Another method of addressing this security threat would be the use of encryption, authentication keys, or even certificates, as part of the configuration data itself and which are tied to the device which is downloading the configuration. In other words, there are various methods to ensure the integrity of configuration data independent from insuring the integrity of this DHCP option or even DHCP itself.

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 in [RFC2131].

Other out-of-band methods of verifying the validity of the VoIP Configuration Server Address, such as certificates of trust, could be used to mitigate some security concerns.
5. IANA Considerations

IANA is requested to assign DHCP option number 150 for this option, in accordance with [RFC3942].
6. References

6.1. Normative References


6.2. Informative References


Author’s Address

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

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