Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: September 13, 2012

J. Schoenwaelder
Jacobs University Bremen
T. Tsou
C. Zhou
Huawei Technologies

March 12, 2012

Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for Network Management Protocols
draft-schoenw-opsawg-nm-dhc-03

Abstract

This document defines new Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) options providing lists of IP addresses that can be used to locate network management services.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 13, 2012.

Copyright Notice

Table of Contents

1. Introduction

This document defines new Dynamic Host Configuration Protocol (DHCPv4 [RFC2131] and DHCPv6 [RFC3315]) options providing lists of IP addresses that can be used to locate network management services. The Dynamic Host Configuration (DHC) options defined in this memo address some gaps identified for the automated configuration of large IP networks [I-D.ietf-opsawg-automated-network-configuration].

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].

2. DHC Options for SYSLOG

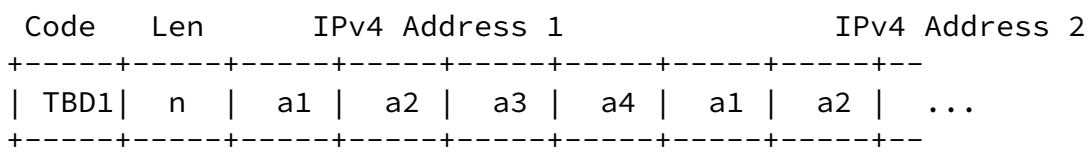
The SYSLOG protocol [RFC5424] supports several transport mappings. According to RFC 5424, implementations MUST support the TLS/TCP-based transport defined in [RFC5425] and they SHOULD also support the UDP-based transport defined in [RFC5426] for compatibility with traditional SYSLOG. An optional transport of SYSLOG messages over DTLS/DCCP and DTLS/UDP is defined in [RFC6012].

The DHC options described below provide a list of IPv4 or IPv6 addresses of SYSLOG collectors in order of preference. The client SHOULD use the addresses sequentially but may be configured to try secure and/or congestion aware transports before falling back to transports that are not congestion aware or insecure. As such, the client may prefer to select an address providing a secure congestion aware transport even if it is listed with lower preference.

2.1. SYSLOG Collector Address Option for DHCPv4

This section describes the SYSLOG IPv4 Address Option for DHCPv4. The SYSLOG IPv4 Address Option begins with an option code followed by a length octet. The value of the length octet does not include

itself or the option code. The option layout is depicted below:



The code for the SYSLOG DHCPv4 option is [IANA: TBD1]. The minimum length of the option is 4 octets, and the length MUST always be a multiple of 4.

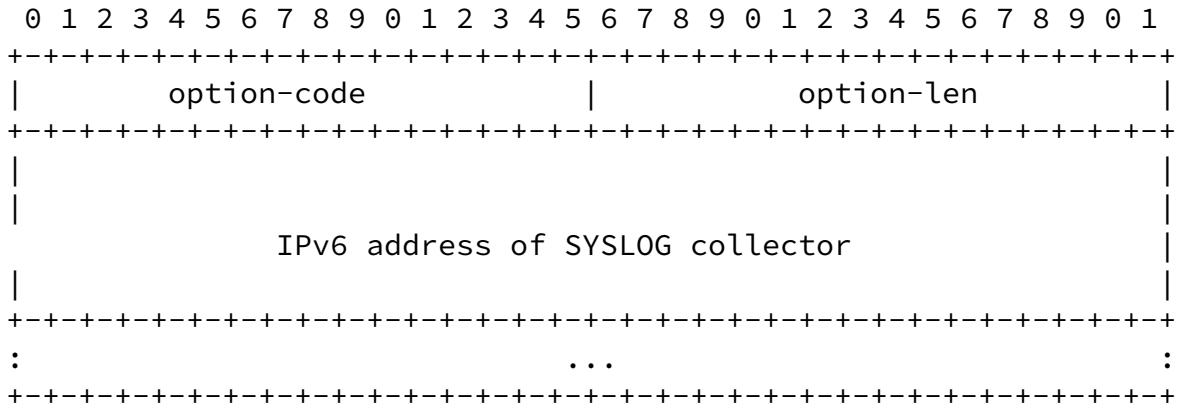
The option MUST NOT be specified by the DHCPv4 client, as it is

intended only to be returned from the DHCPv4 server. If the DHCPv4 client wants to receive this information from the server, it needs to include the number [IANA: TBD1] in the "DHCP Parameter Request 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 in a different order according to some local policy (e.g., the client prefers secure and/or congestion aware transports as described above).

2.2. SYSLOG Collector Address Option for DHCPv6

This section describes the SYSLOG IPv6 Address Option for DHCPv6. The SYSLOG IPv6 Address Option begins with an option-code followed by the option-len. The value of the option-len does not include itself or the option-code. The option layout is depicted below:



The option-code of the SYSLOG DHCPv6 option OPTION_SYSLOG_COLLECTOR is [IANA: TBD2]. The minimum option-len is 16 octets, and the length MUST always be a multiple of 16.

The option MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request and Reply. The option number for these options MAY appear in the Option Request Option (6) in the following messages: Solicit, Request, Renew, Rebind, Information-Request and Reconfigure.

The addresses SHOULD be listed in order of preference, and the client SHOULD use the addresses sequentially but may be configured to use addresses in a different order according to some local policy (e.g., the client prefers secure and/or congestion aware transports as described above).

3. DHC Options for SNMP

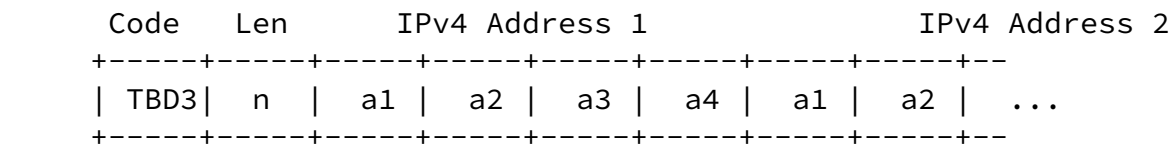
The SNMP protocol [RFC3410] supports several transport mappings. The preferred IP-based transport is SNMP over UDP [RFC3417]. An experimental transport of SNMP over TCP is defined in [RFC3430]. An optional standards-track transport of SNMP over SSH is defined in [RFC5592] while optional standards-track transports over TLS and DTLS are defined in [RFC6353]

The DHC options described below provide a list of IPv4 or IPv6 addresses of SNMP entities hosting Notification Receiver applications in order of preference. The client SHOULD use the addresses sequentially but may be configured to try secure and/or congestion aware transports before falling back to transports that are not congestion aware or insecure. As such, the client may prefer to select an address providing a secure congestion aware transport even if it is listed with lower preference.

3.1. SNMP Notification Receiver Address Option for DHCPv4

This section describes the SNMP IPv4 Address Option for DHCPv4. The SNMP IPv4 Address Option begins with an option code followed by a

length octet. The value of the length octet does not include itself or the option code. The option layout is depicted below:



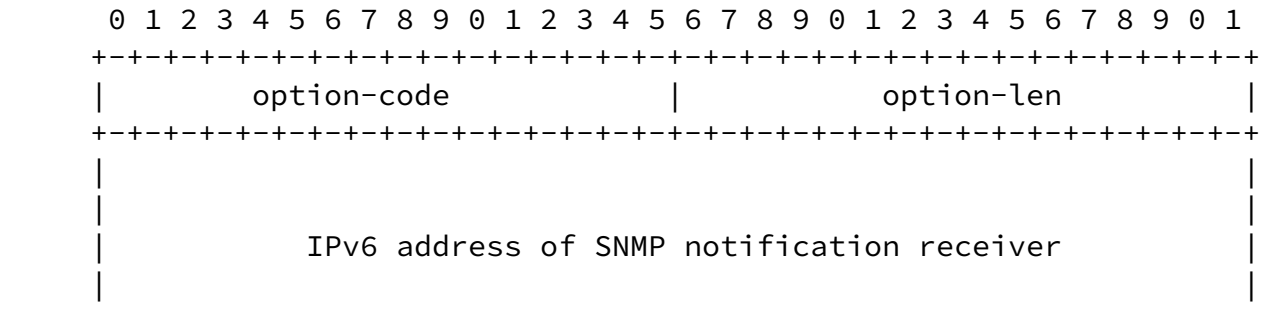
The code for the SNMP notification receiver DHCPv4 option is [IANA: TBD3]. The minimum length of the option is 4 octets, and the length MUST always be a multiple of 4.

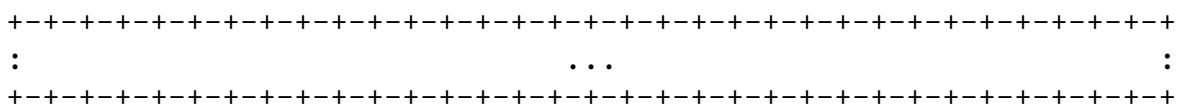
The option MUST NOT be specified by the DHCPv4 client, as it is intended only to be returned from the DHCPv4 server. If the DHCPv4 client wants to receive this information from the server, it needs to include the number [IANA: TBD3] in the "DHCP Parameter Request List" option (55).

The addresses SHOULD be listed in order of preference, and the client SHOULD use the addresses sequentially but may be configured to use addresses in a different order according to some local policy (e.g., the client prefers secure and/or congestion aware transports as described above).

3.2. SNMP Notification Receiver Address Option for DHCPv6

This section describes the SNMP IPv6 Address Option for DHCPv6. The SNMP IPv6 Address Option begins with an option-code followed by the option-len. The value of the option-len does not include itself or the option-code. The option layout is depicted below:





The option-code of the SNMP notification receiver DHCPv6 option OPTION_SNMP_NOT_RECEIVER is [IANA: TBD4]. The minimum option-len is 16 octets, and the length MUST always be a multiple of 16.

The option MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request and Reply. The option number for these options MAY appear in the Option Request Option (6) in the following messages: Solicit, Request, Renew, Rebind, Information-Request and Reconfigure.

Server addresses SHOULD be listed in order of preference, and the client SHOULD use the addresses sequentially but may be configured to use addresses in a different order according to some local policy (e.g., the client prefers secure and/or congestion aware transports as described above).

4. Security Considerations

The security considerations in [RFC2131] and [RFC3315]) apply. If an adversary manages to modify the response from a DHCPv4 or DHCPv6 server or insert its own response, a node could be led to contact a rogue network management server.

It is recommended to use the DHCPv4 authentication option described in [RFC3118] where available. This will also protect against denial-of-service attacks to DHCP servers. [RFC3118] provides mechanisms for both entity authentication and message authentication.

In IPv6 networks using DHCPv6, it is recommended that clients use authentication of DHCPv6 messages as described in Section 21 of [RFC3315].

In deployments where DHCPv4 or DHCPv6 authentication is not available, lower-layer security services may be sufficient to protect DHCPv4 and DHCPv6 messages.

5. IANA Considerations

IANA is requested to assign [IANA: TBD1] as an option code from the "DHCP Option Codes" registry.

IANA is requested to assign [IANA: TBD2] as an option code from the "DHCPv6 Options Codes" registry for OPTION_SYSLOG_COLLECTOR.

IANA is requested to assign [IANA: TBD3] as an option code from the "DHCP Option Codes" registry.

IANA is requested to assign [IANA: TBD4] as an option code from the "DHCPv6 Options Codes" registry for OPTION_SNMP_NOT_RECEIVER.

6. Acknowledgements

The authors like to thank Ralf Droms, Ted Lemon and Bernie Volz for their helpful comments.

7. References

7.1. 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.

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

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62,

RFC 3413, December 2002.

[RFC3417] Presuhn, R., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, December 2002.

[RFC3430] Schoenwaelder, J., "Simple Network Management Protocol Over Transmission Control Protocol Transport Mapping", RFC 3430, December 2002.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

[RFC5425] Miao, F., Ma, Y., and J. Salowey, "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, March 2009.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, June 2009.

[RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, October 2010.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", RFC 6353, July 2011.

7.2. Informational References

[I-D.ietf-opsawg-automated-network-configuration] Tsou, T., Schoenwaelder, J., Shi, Y., and T. Taylor, "Problem Statement for the Automated Configuration of Large IP Networks", draft-ietf-opsawg-automated-network-configuration-02 (work in progress), October 2011.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

Appendix A. Relationship to the SNMP Configuration MIB Modules

The SNMP notification receiver address DHCPv4 and DHCPv6 options defined in Section 3.1 and Section 3.2 provide the basic information to setup a target in the SNMP-TARGET-MIB and the SNMP-NOTIFICATION-MIB [RFC3413]. After selecting the transport (e.g., by probing the availability of possible SNMP transport endpoints according to some local policy, a volatile entry in the snmpTargetTable can be created as follows (assuming xyz is some suitable unique handle for the received DHCP option):

```
snmpTargetAddrName             = "dhcp-xyz"          (INDEX)
snmpTargetAddrTDomain          = snmpUDPDomain
snmpTargetAddrTAddress         = "a.b.c.d"
snmpTargetAddrTimeout          = 1500                (DEFVAL)
snmpTargetAddrRetryCount       = 3                   (DEFVAL)
snmpTargetAddrTagList          = "dhcp-xyz-tag"
snmpTargetAddrParams           = "dhcp-xyz-param"
snmpTargetAddrStorageType      = volatile(2)
snmpTargetAddrRowStatus        = active(1)
```

A matching volatile entry in the snmpNotifyTable can also be easily created:

```
snmpNotifyName                 = "dhcp-xyz"          (INDEX)
snmpNotifyTag                  = "dhcp-xyz-tag"
snmpNotifyType                 = trap(1)             (DEFVAL)
snmpNotifyStorageType          = volatile(2)
snmpNotifyRowStatus            = active(1)
```

In addition, an entry in the snmpTargetParamsTable is needed. Its structure for SNMPv3/USM user "joe" is as follows:

```
snmpTargetParamsName           = "dhcp-xyz-param"    (INDEX)
snmpTargetParamsMPModel        = 3                   (SNMPv3)
snmpTargetParamsSecurityModel  = 3                   (USM)
snmpTargetParamsSecurityName   = "joe"
snmpTargetParamsSecurityLevel  = authNoPriv(2)
snmpTargetParamsStorageType    = volatile(2)
snmpTargetParamsRowStatus      = active(1)
```

Creating of a suitable entry in the snmpTargetParamsTable requires local information. Depending on the security model, additional information will be necessary.

The creation of a suitable snmpTargetParamsTable entry may either be

dynamic (i.e., the entry is created upon receipt of a DHC lease using some local policy information and deleted when the DHC lease expires)

or suitable snmpTargetParamsTable entries may be pre-provisioned based on the expected naming of the target entries that are created dynamically. Implementations may also pre-provision snmpTargetAddrTable entries and only dynamically create suitable snmpNotifyTable entries.

Authors' Addresses

Juergen Schoenwaelder
Jacobs University Bremen
Campus Ring 1
Bremen 28759
Germany

Email: j.schoenwaelder@jacobs-university.de

Tina Tsou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: tena@huawei.com

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathyzhou@huawei.com