Internet Engineering Task Force (IETF)
Request for Comments: 6153
Category: Standards Track
ISSN: 2070-1721

S. Das
Telcordia Technologies
G. Bajko
Nokia

February 2011

DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery

Abstract

This document defines new Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) options to enable a mobile node to discover Access Network Discovery and Selection Function (ANDSF) entities in an IP network. ANDSF is being developed in the Third Generation Partnership Project (3GPP) and provides inter-system mobility policies and access-network-specific information to the mobile nodes (MNs).

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in 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/rfc6153.

Table of Contents

1. Introduction

Access Network Discovery and Selection Function (ANDSF) is being defined in 3GPP [3GPPTS23.402] to provide necessary network discovery and selection assistance data to the mobile nodes for multi-access network scenarios where 3GPP access-network level solutions are not sufficient for the mobile nodes to perform network discovery and selection of non-3GPP networks.

The information provided by ANDSF contains inter-system mobility policies and access-network-specific data to assist the mobile node with performing the inter-system handover. This set of information can either be provisioned in the mobile node by the home operator or provided to the mobile node (MN) dynamically by the ANDSF over the S14 reference point as defined in [3GPPTS23.402] and [3GPPTS24.302].

In 3GPP, the ANDSF is located either in the subscriber’s home operator or visited network and needs to be known to the MN or discovered by the MN. According to [3GPPTS23.402] and [3GPPTS24.302], the ANDSF is discovered through interaction with the Domain Name Service function or the DHCP server function.

This document defines new DHCPv4 and DHCPv6 options called the ANDSF IP Address Options, which allow the MN to locate an ANDSF server.

1.1. Conventions Used in This 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 [RFC2119].

1.2. Terminology and Abbreviations Used in This Document

ANDSF (Access Network Discovery and Selection Function): An entity that provides network discovery and selection assistance data to the user entity (UE) as per operator policy [3GPPTS23.402].

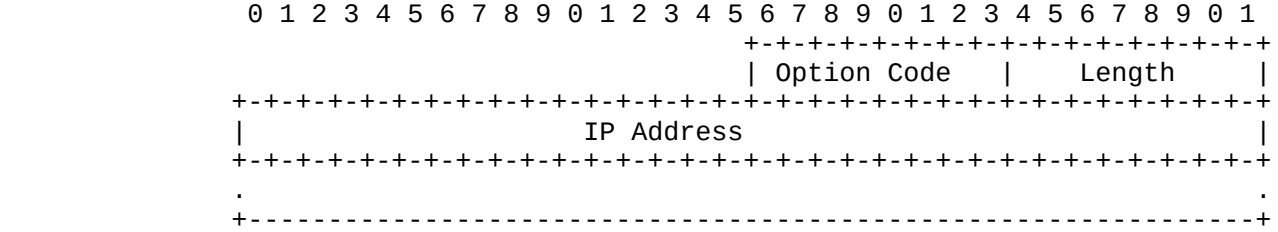
Access Network: A network that is accessed by the UE.

3GPP Network: A radio access network specified by Third Generation Partnership Project

Non-3GPP Network: A radio access network specified outside 3GPP by other projects or standards organizations

2. ANDSF IPv4 Address Option for DHCPv4

This section describes the ANDSF IPv4 Address Option for DHCPv4. The option layout is depicted below:



Option Code
OPTION-IPv4_Address-ANDSF (142)

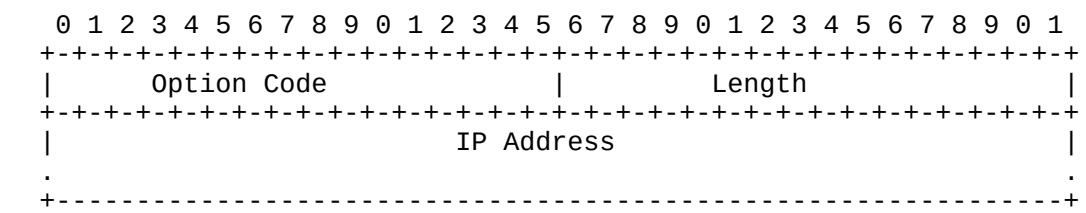
Length
Length (in bytes) of the option excluding the 'Option Code' and the 'Length' fields; 'Length' field is set to 4N, where N is the number of IPv4 addresses carried in the option

IP Address
IPv4 address(es) of ANDSF server(s)

ANDSF servers MUST be listed in order of preference, and the client SHOULD process them in decreasing order of preference.

3. ANDSF IPv6 Address Option for DHCPv6

This section describes the ANDSF IPv6 Address Option for DHCPv6. All values in the option are represented in network byte order. The option layout is depicted below:



Option Code
OPTION-IPv6_Address-ANDSF (143)

Length
Length (in bytes) of the option excluding the 'Option Code' and the 'Length' fields; 'Length' field is set to 16N, where N is the number of IPv6 addresses carried in the option

IP Address
IPv6 address(es) of ANDSF server(s)

ANDSF servers MUST be listed in order of preference, and the client SHOULD process them in decreasing order of preference.

4. Option Usage

4.1. Usage of ANDSF Options for DHCPv4

The requesting and sending of the proposed DHCPv4 options follow the rules for DHCP options in [RFC2131].

4.1.1. Mobile Node Behavior

The mobile node MAY request the IP address of an ANDSF server either during initial association with a network or when the policy and access network information is required from ANDSF. It MAY also request the IP address of an ANDSF server when the network information is outdated or the mobile node does not have any ANDSF information.

In order to request an address of a ANDSF server, the mobile node (DHCP client) MUST include an ANDSF IPv4 Address Option in the Parameter Request List (PRL) in the respective DHCP messages as

defined in [RFC2131] and [RFC2132]. The DHCP client MAY initiate a new DHCP exchange or piggyback on other DHCP message exchanges. DHCP client-handling PRL options are specified in [RFC2131], Section 4.4.

4.2. Usage of ANDSF Options for DHCPv6

The requesting and sending of the proposed DHCPv6 options follow the rules for DHCP options in [RFC3315].

4.2.1. Mobile Node Behavior

The mobile node MAY request the IP address of an ANDSF server according to the scenarios described in Section 4.1.1.

In order to discover the address of an ANDSF server, the mobile node (DHCP client) MUST include an ANDSF IPv6 Address Option in the Option Request Option (ORO) in the respective DHCP messages as defined in [RFC3315]. The DHCP client MAY initiate a new DHCP exchange or piggyback on other DHCP message exchanges. DHCP client-handling ORO options are specified in [RFC3315], Sections 17.1 and 18.1.

5. Security Considerations

If an adversary manages to modify the response from a DHCP server or insert its own response, an MN could be led to contact a rogue ANDSF server. A modified response could also be used to mount an amplification attack.

The DHCP authentication option described in [RFC3118] and [RFC3315] MAY be used to mitigate the above attacks. In deployments where DHCP authentication is not available, 3GPP-specific lower-layer security services can be used to protect DHCP messages [3GPPTS33.402]. The 3GPP ANDSF framework also provides additional mechanisms that can be used to mitigate the above attacks and to protect message exchanges between an ANDSF client and server at the higher layer [3GPPTS33.402].

6. IANA Considerations

This document defines two new DHCP options as described in Sections 2 and 3:

ANDSF IPv4 Address Option for DHCPv4 (OPTION-IPv4_Address-ANDSF) 142

ANDSF IPv6 Address Option for DHCPv6 (OPTION-IPv6_Address-ANDSF) 143

7. Acknowledgments

The authors would like to acknowledge the following individuals for their valuable comments: Patrick Stuper, Vijay Devarapalli, Jouni Korhonen, Jari Arkko, Ted Lemon, and Ralph Droms.

8. References

8.1. 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.

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

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

8.2. Informative References

[3GPPTS23.402] 3GPP TS 23.402, v8.8.0 (2009-12): Architecture enhancements for non-3GPP accesses, http://www.3gpp.org/ftp/Specs/html-info/23402.htm.

[3GPPTS24.302] 3GPP TS 24.302, v8.4.1 (2009-12): Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3, http://www.3gpp.org/ftp/Specs/html-info/24302.htm.

[3GPPTS33.402] 3GPP TS 33.402, v8.6.0 (2009-12): 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses, http://www.3gpp.org/ftp/Specs/html-info/33402.htm.

Authors' Addresses

Subir Das
Telcordia Technologies Inc.
EMail: subir@research.telcordia.com

Gabor Bajko
Nokia
EMail: gabor@bajko.nokia.com