Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 20, 2010

B. Lourdelet, Ed.
W. Dec, Ed.
Cisco Systems, Inc.
B. Sarikaya
Huawei USA
G. Zorn
Network Zen
D. Miles
Alcatel-Lucent

December 17, 2009

RADIUS attributes for IPv6 Access Networks
draft-lourdelet-radext-ipv6-access-02.txt

Abstract

IPv6 nodes can have configuration information provided to them using DHCPv6 and/or Router Advertisements. This document specifies RADIUS attributes that complement RFC3162 for use with DHCPv6 and/or Router Advertisements (SLAAC) for use in network access scenarios.

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 June 20, 2010.

Table of Contents

1. Requirements Language

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].

2. Introduction

This document specifies new IPv6 RADIUS attributes used to support IPv6 network access. As IPv6 specifies two configuration mechanisms (DHCP and SLAAC) the attributes defined in this document may apply to DHCPv6, SLAAC or both with the new attributes are targeted at both protocols when it makes sense. The RADIUS attributes defined in [RFC3162]and [RFC4818] do not define methods for assignment of IPv6 addresses to hosts (via DHCPv6) or IPv6 recursive DNS servers (via DHCPv6 or [[RFC5006]), nor the passing of route prefix info (via [RFC4191]. The Radius options to do so are the subject of this draft.

3. Deployment Scenarios

3.1. IPv6 Address Assignment

DHCPv6 [RFC3315] provides a mechanism to assign one or more or non-temporary IPv6 addresses to nodes. In IPv6, both SLAAC and DHCPv6 can be used for address assignment. While SLAAC provides a host with a /64 IPv6 prefix from which to construct its address, the host is free to construct a 64-bit Interface ID that when concatenated with the /64 prefix provides a unique address. By providing a host only a /64 network operators are unaware of the exact IP addresses in use by a device. To contrast SLAAC, DHCPv6 requires a host explicitly request non-temporary addresses from a DHCPv6 server permitting an operator control over address assignment. This document specifies a new RADIUS attribute for the assignment of non-temporary IPv6 addresses to a host via DHCPv6. Other DHCPv6 parameters such as preferred and valid address lifetimes are provided for by the NAS and not through RADIUS attributes. As a DHCPv6 client may request an address at any time, a RADIUS server may be required to service additional RADIUS Access-Requests for a single network access session.

3.2. Recursive DNS Servers

DHCPv6 provides an option for recursive DNS servers to hosts, as does a Router Advertisement supporting the experimental [RFC5006]. Existing DHCPv4 options only convey DNS as 32-bit IPv4 addresses and

cannot support a 128-bit IPv6 address. In the current RADIUS specifications there are no IETF/IANA defined attributes for recursive DNS and many NAS implement vendor specific attributes (e.g.: Ascend-Primary-DNS). In some operator environments a network access session may be configured with a specific set of one or more recursive DNS. This document specifies a new RADIUS attribute to convey a list of IPv6 addresses that can be used for a host for domain name service. Best current practice is to configure hosts with more than one recursive domain name server, this is achieved in the RADIUS environment by returning multiple IPv6-DNS-Server-Address options within an Access-Accept. The NAS shall use the addresses returned in the RADIUS IPv6-DNS-Server-Address attribute for the DHCPv6 DNS-Servers option [RFC3646], the Router Advertisement Recursive DNS Server Option [RFC5006], or both.

3.3. IPv6 Route Information

In scenarios where Stateless Address Autoconfiguration (SLAAC) [RFC4862] is used for address assignment, a Router Advertisement is multicast with one or more Prefix Information Options with the autonomous-bit set to true. A Prefix Information Option, when used for SLAAC, is a /64 prefix to which a host appends its locally-generated Interface Id to create a unique 128-bit IPv6 address. [RFC3162] currently defines a Framed-IPv6-Prefix which can be used by a NAS to advertise on-link prefixes in a Router Advertisement Prefix Information Option [RFC4861]. The IPv6 Route Information attribute is almost the inverse; it is intended to be used to instruct a host connected to the NAS that a specific route is reachable via the NAS/router. [RFC4191] defines an ICMPv6 Route Information Option for this purpose, ie to convey route information from a router to a host. The Route Information Option is used in environments where multiple advertising routers are present. It directs a host to which router each specific route should be the next-hop to. For each IPv6-Prefix-Information attribute, the NAS may advertise a unique [RFC4191] Route Information Option.

4. Attributes

The fields shown in the diagrams below are transmitted from left to right.

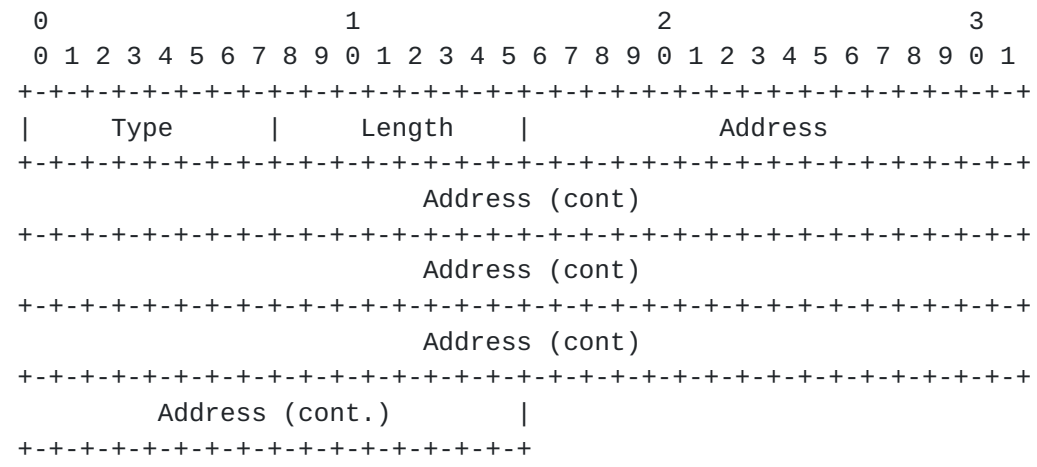
4.1. Framed-IPv6-Address

This Attribute indicates an IPv6 Address that is assigned to the uplink NAS-facing interface of the user equipment. It MAY be used in Access-Accept packets, and can appear multiple times. It MAY be used in an Access-Request packet as a hint by the NAS to the server that

it would prefer these IPv6 address(es), but the server is not required to honor the hint. Since it is assumed that the NAS, when necessary, will add a route corresponding to the address it is not necessary for the server to also send a host Framed-IPv6-Route attribute for the same address.

This Attribute can be used by DHCPv6 to offer a unique IPv6 address or can be used for a-posteriori validation or announcment of an autoconfigured address.

A summary of the Framed-IPv6-Address Attribute format is shown below.



Type

TBA1 for Framed-IPv6-Address

Length

18

Address

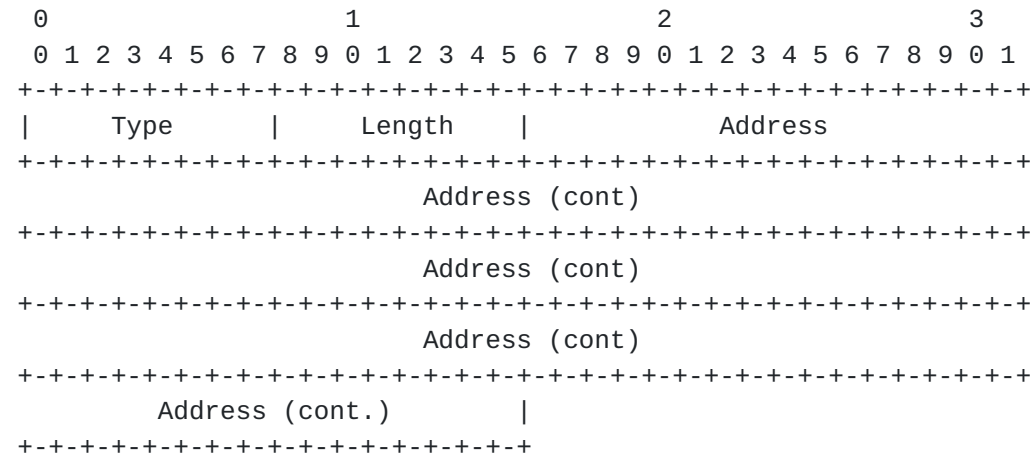
The Address field contains a 128-bit IPv6 address.

4.2. IPv6-DNS-Server-Address

The IPv6-DNS-Server-Address Attribute contains the IPv6 address of a DNS server. This attribute MAY be included multiple times in Access-Accept packets.

The content of this attribute can be inserted in a Router Advertisement as specified in [RFC5006] or mapped to the matching DHCPv6 option.

A summary of the IPv6-DNS-Server-Address Attribute format is given below.



Type

TBA2 for IPv6-DNS-Server-Address

Length

18

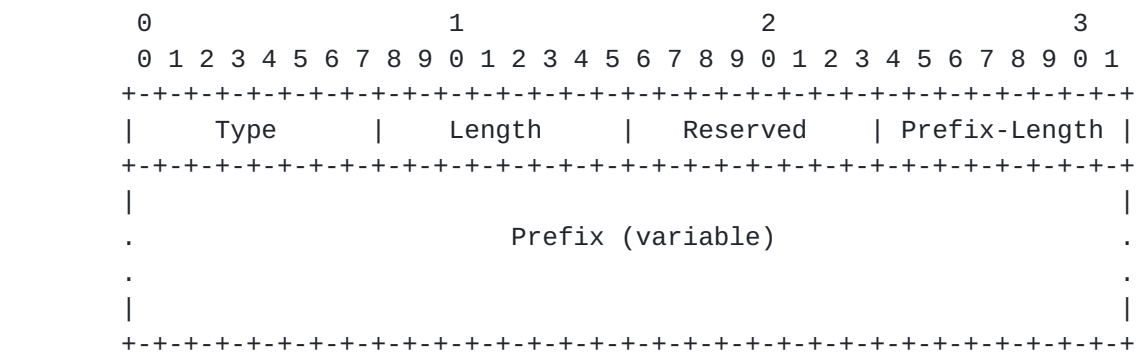
Address

The 128-bit IPv6 address of a DNS server.

4.3. IPv6-Route-Information

This Attribute specifies a prefix (and corresponding route) to be authorized for announcement towards the user by the NAS, with the reachable by means of routing towards the NAS. It is used in the Access-Accept packet and can appear multiple times. It may also be used in the Access-Request packet.

A summary of the IPv6-Route-Information attribute format is shown below. The route information option defined in [RFC4191] is captured in this and following two attributes.



Type

TBA3 for IPv6-Route-Information

Length

Length in bytes. At least 4 and no larger than 20; typically 12 or less.

Prefix Length

The length of the prefix, in bits; at least 0 and no more than 128; typically 64 or less.

Prefix

Variable-length field containing an IP prefix. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length (if any) up to the byte boundary are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

4.4. Table of attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0+	0+	0	0	0+	TBA1	Framed-IPv6-Address
0+	0+	0	0	0+	TBA2	IPv6-DNS-Server-Address
0	0+	0	0	0+	TBA3	IPv6-Route-Information

5. Diameter Considerations

Since the Attributes defined in this document are allocated from the standard RADIUS type space (see Section 7), no special handling is required by Diameter entities.

6. Security Considerations

This document describes the use of RADIUS for the purposes of authentication, authorization and accounting in IPv6-enabled networks. In such networks, the RADIUS protocol may run either over IPv4 or over IPv6. Known security vulnerabilities of the RADIUS protocol apply to the attributes defined in this document. Since IPSEC is natively defined for IPv6, it is expected that running RADIUS implementations supporting IPv6 may want to run over IPSEC. Where RADIUS is run over IPSEC and where certificates are used for authentication, it may be desirable to avoid management of RADIUS shared secrets, so as to leverage the improved scalability of public key infrastructure.

7. IANA Considerations

This document requires the assignment of three new RADIUS Attribute Types in the "Radius Types" registry (currently located at http://www.iana.org/assignments/radius-types for the following attributes:

- Framed-IPv6-Address
- IPv6-DNS-Server-Address
- IPv6-Prefix-Information

IANA should allocate these numbers from the standard RADIUS Attributes space using the "IETF Review" policy [RFC5226].

8. Acknowledgements

The authors would like to thank Alfred Hines for his contributions and comments to this document.

9. References

9.1. Normative References

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

9.2. Informative References

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 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.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RFC4818] Salowey, J. and R. Droms, "RADIUS Delegated-IPv6-Prefix Attribute", RFC 4818, April 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5006] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

Benoit Lourdelet (editor)
Cisco Systems, Inc.
Village ent. GreenSide, Bat T3,
400, Av de Roumanille,
06410 BIOT - Sophia-Antipolis Cedex
France

Phone: +33 4 97 23 26 23
Email: blourdel@cisco.com

Wojciech Dec (editor)
Cisco Systems, Inc.
Haarlerbergweg 13-19
Amsterdam , NOORD-HOLLAND 1101 CH
Netherlands

Email: wdec@cisco.com

Behcet Sarikaya
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX
US

Phone: +1 972-509-5599
Email: sarikaya@ieee.org

Glen Zorn
Network Zen
1310 East Thomas Street
Seattle, WA
US

Email: gwz@net-zen.net

David Miles
Alcatel-Lucent
L3 / 215 Spring St
Melbourne, Victoria 3000,
Australia

Phone:
Fax:
Email: David.Miles@alcatel-lucent.com
URI: