Network Working Group	B.L. Lourdelet
Internet-Draft	W.D. Dec, Ed.
Intended status: Standards Track	Cisco Systems, Inc.
Expires: May 17, 2012	B.S. Sarikaya
	Huawei USA
	G.Z. Zorn
	Network Zen
	D.M. Miles
	Alcatel-Lucent
	November 14, 2011

RADIUS attributes for IPv6 Access Networks
draft-ietf-radext-ipv6-access-06.txt

Abstract

This document specifies additional IPv6 RADIUS attributes useful in residential broadband network deployments. The attributes, which are used for authorization and accounting, enable assignment of a host IPv6 address and IPv6 DNS server address via DHCPv6; assignment of an IPv6 route announced via router advertisement; assignment of a named IPv6 delegated prefix pool; and assignment of a named IPv6 pool for host DHCPv6 addressing.

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 RFC 2119 *[RFC2119]*.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies additional RADIUS attributes used to support configuration of DHCPv6 and/or ICMPv6 parameters on a per-user basis. The attributes, which complement those defined in [RFC3162] and [RFC4818], support the following:

*Assignment of specific IPv6 addresses to hosts via DHCPv6.

*Assignment of an IPv6 DNS server address, via DHCPv6 or [RFC5006].

*Configuration of more specific routes to be announced to the user via the Route Information Option defined in [RFC4191] Section 2.3.

*The assignment of a named delegated prefix pool for use with "IPv6 Prefix Options for DHCPv6" [RFC3633].

*The assignment of a named stateful address pool for use with DHCPv6 stateful address assignment [RFC3315]

2. Deployment Scenarios

A common broadband network scenario is illustrated in Figure 1. It is composed of a IP Routing Residential Gateway (RG) or host, a Layer 2 Access-Node (e.g. a DSLAM), one or more IP Network Access Servers (NASes), and an AAA server. The RG or host are expected to be multi homed to both NASes. Layer 2 Connectivity between the host and NAS can be either via PPPoE or IP over Ethernet, and established dynamically.

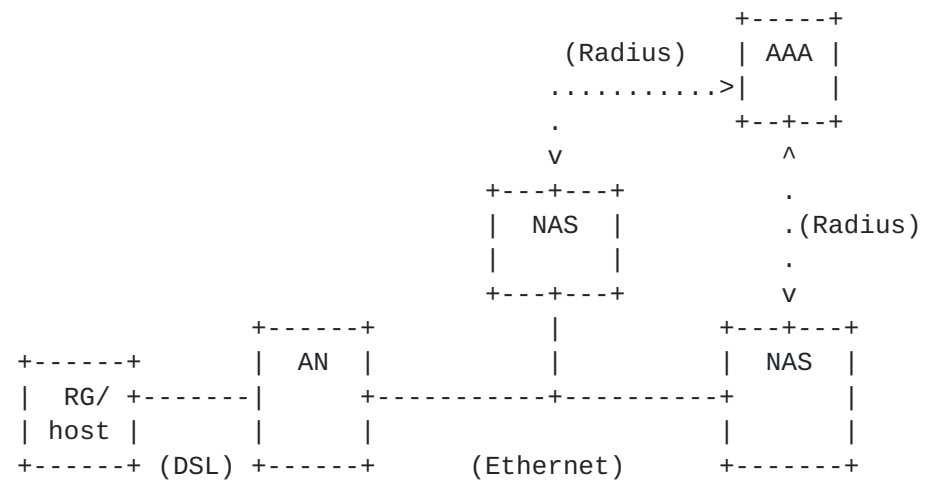


Figure 1

In this scenario the NASes may embed a DHCPv6 server to handle DHCPv6 requests issued by RGs/hosts, as well as acting as a router providing

Router Advertisements. The RADIUS server authenticates each RG/host and returns to the NAS attributes used for authorization and accounting. These attributes can include a host IPv6 address to be configured via DHCPv6; the IPv6 address of a DNS server to configured via DHCPv6 or router advertisement; the name of a prefix pool to be used for DHCPv6 Prefix Delegation; or IPv6 routes to be announced to the host.
The following sub-sections discuss how these uses in more detail.

2.1. IPv6 Address Assignment

DHCPv6 [RFC3315] provides a mechanism to assign one or more or non-temporary IPv6 addresses to hosts. To provide a DHCPv6 server residing on a NAS with one or more IPv6 addresses to be assigned, this document specifies the Framed-IPv6-Address Attribute.
While [RFC3162] permits an IPv6 address to be specified via the combination of the Framed-Interface-Id and Framed-IPv6-Prefix attributes, this separation is more natural for use with IPv6CP than it is for use with DHCPv6, and the use of a single IPv6 address attribute makes for easier processing of accounting records.
Since DHCPv6 can be deployed on the same network as ICMPv6 stateless (SLAAC) [RFC4862], it is possible that the NAS will require both stateful and stateless configuration information. Therefore it is possible for the Framed-IPv6-Address, Framed-IPv6-Prefix and Framed-Interface-Id attributes [RFC3162] to be included within the same packet. To avoid ambiguity, the Framed-IPv6-Address attribute is only used for authorization and accounting of DHCPv6-assigned addresses and the Framed-IPv6-Prefix and Framed-Interface-Id attributes are used for authorization and accounting of addresses assigned via SLAAC.

2.2. Recursive DNS Servers

DHCPv6 provides an option for configuring a host with the IPv6 address of a DNS server. The IPv6 address of a DNS server can also be conveyed to the host using ICMPv6 with Router Advertisements, via the experimental [RFC5006] option. To provide the NAS with the IPv6 address of a DNS server, this document specifies the DNS-Server-IPv6-Address Attribute.

2.3. IPv6 Route Information

An IPv6 Route Information option, defined in [RFC4191] is intended to be used to inform a host connected to the NAS that a specific route is reachable via the NAS. This is particularly desirable in cases where the RG or host are multi-homed to different NASes as shown in Figure 1. This document specifies the RADIUS attribute that allows the AAA system to provision the announcement by the NAS of a specific Route Information Option to an accessing host. The NAS may advertise this route using the method defined in [RFC4191] or using other equivalent methods.
While the Framed-IPv6-Prefix Attribute defined in [RFC3162] Section 2.3 causes the route to be advertised in an RA, it cannot be used to configure more specific routes. While the Framed-IPv6-Route Attribute defined in [RFC3162] Section 2.5 causes the route to be configured on

the NAS, and potentially announced via an IGP, depending on the value of Framed-Routing, it does not result in the route being announced in an RA.

2.4. Delegated IPv6 Prefix Pool

DHCPv6 Prefix Delegation [RFC3633] involves a delegating router selecting a prefix and delegating it on a temporary basis to a requesting router. The delegating router may implement a number of strategies as to how it chooses what prefix is to be delegated to a requesting router, one of them being the use of a local named prefix pool. The Delegated-IPv6-Prefix-Pool Attribute allows the RADIUS server to convey a prefix pool name to a NAS hosting a DHCPv6-PD server and acting as a delegated router.
Since DHCPv6 Prefix Delegation can conceivably be used on the same network as SLAAC, it is possible for the Delegated-IPv6-Prefix-Pool and Framed-IPv6-Pool attributes to be included within the same packet. To avoid ambiguity in this scenario, use of the Delegated-IPv6-Prefix-Pool attribute should be restricted to authorization and accounting of prefix pools used in DHCPv6 Prefix Delegation and the Framed-IPv6-Pool attribute should be used for authorization and accounting of prefix pools used in SLAAC.

2.5. Stateful IPv6 address pool

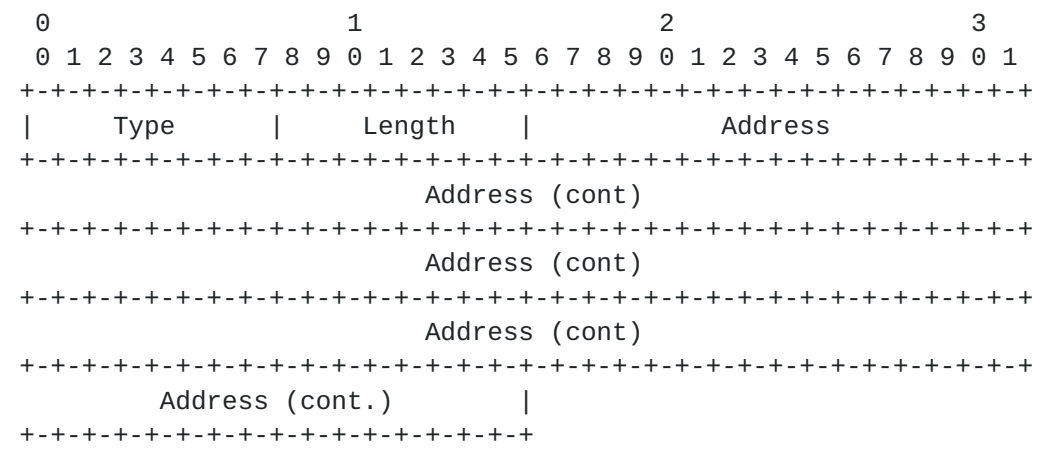
DHCPv6 [RFC3315] provides a mechanism to assign one or more or non-temporary IPv6 addresses to hosts. Section 2.1 introduces the Framed-IPv6-Address Attribute to be used for providing a DHCPv6 server residing on a NAS with one or more IPv6 addresses to be assigned to the clients. An alternative way to achieve a similar result is for the NAS to select the IPv6 address to be assigned from an address pool configured for this purpose on the NAS. This document specifies the DHCPv6-IPv6-Address-Pool attribute to allow the RADIUS server to convey a pool name to be used for such stateful DHCPv6 based addressing, and any subsequent accounting.

3. Attributes

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

3.1. Framed-IPv6-Address

This Attribute indicates an IPv6 Address that is assigned to the NAS-facing interface of the RG/host. It MAY be used in Access-Accept packets, and MAY 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 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 a DHCPv6 process on the NAS to assign a unique IPv6 address to the RG/host.



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

Type

TBA1 for Framed-IPv6-Address

Length

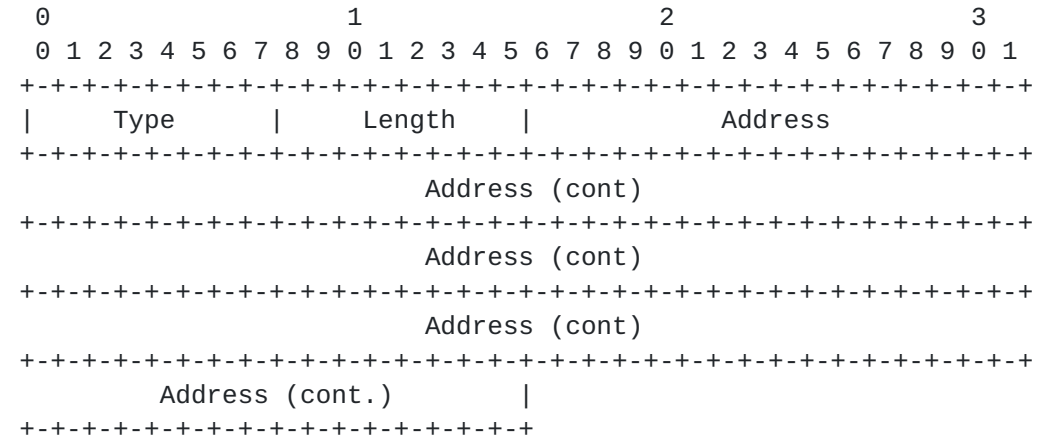
18

Address

The IPv6 address field contains a 128-bit IPv6 address.

3.2. DNS-Server-IPv6-Address

The DNS-Server-IPv6-Address Attribute contains the IPv6 address of a recursive DNS server. This attribute MAY be included multiple times in Access-Accept packets, when the intention is for a NAS to announce more than one recursive DNS address to an RG/host. The same order of the attributes is expected to be followed in the announcements to the client.
The content of this attribute can be inserted in a DHCPv6 option as specified in [RFC3646] or mapped option.



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

Type

TBA2 for DNS-Server-IPv6-Address

Length

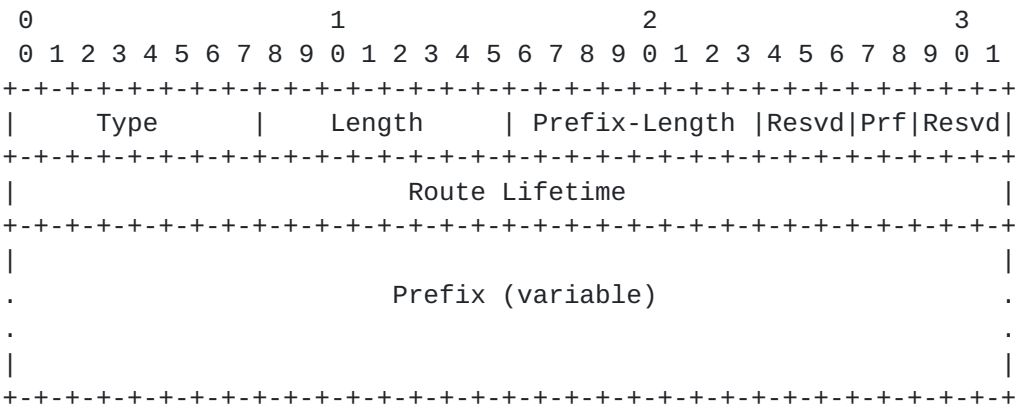
18

Address

The 128-bit IPv6 address of a DNS server.

3.3. Route-IPv6-Information

This Attribute specifies a prefix (and corresponding route) for the user on the NAS, which is to be announced using the Route Information Option defined in "Default Router Preferences and More Specific Routes" [RFC4191] Section 2.3. It is used in the Access-Accept packet and can appear multiple times. It may also be used in the Access-Request packet as hint to the server. A summary of the Route-IPv6-Information attribute format is shown below.



Type

TBA3 for Route-IPv6-Information

Length

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

Prefix Length

8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 1. The prefix field is 0, 8 or 16 octets depending on Length.

Prf (Route Preference) 2-bit signed integer. The Route Preference indicates whether to prefer the router associated with this prefix

over others, when multiple identical prefixes (for different routers) have been received.

Resvd (Reserved) Two 3-bit unused fields. They MUST be initialized to zero.

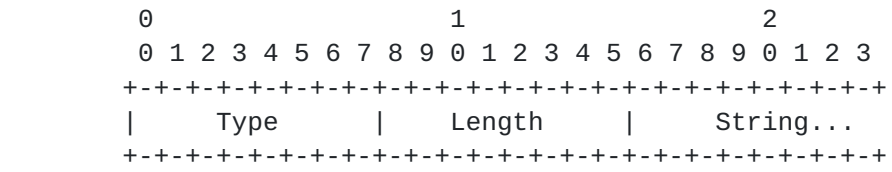
Route Lifetime 32-bit unsigned integer. The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for route determination. A value of all one bits (0xffffffff) represents infinity.

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) are reserved and MUST be initialized to zero.

3.4. Delegated-IPv6-Prefix-Pool

This Attribute contains the name of an assigned pool that SHOULD be used to select an IPv6 delegated prefix for the user. If a NAS does not support multiple prefix pools, the NAS MUST ignore this Attribute.
A summary of the Delegated-IPv6-Prefix-Pool Attribute format is shown below. The fields are transmitted from left to right.



Type

TBA4 for Delegated-IPv6-Prefix-Pool

Length

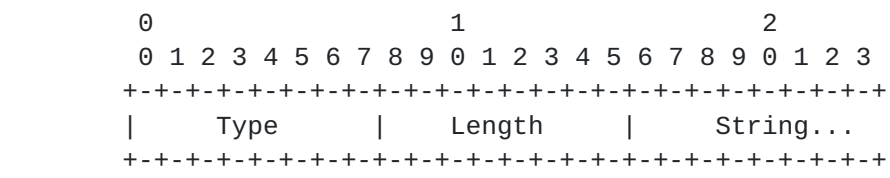
Length in bytes. At least 4.

String

The string field contains the name of an assigned IPv6 prefix pool configured on the NAS. The field is not NULL (hex 00) terminated.

3.5. Stateful-IPv6-Address-Pool

This Attribute contains the name of an assigned pool that SHOULD be used to select an IPv6 address for the user. If a NAS does not support address pools, the NAS MUST ignore this Attribute. A summary of the Stateful-IPv6-Address-Pool Attribute format is shown below. The fields are transmitted from left to right.



Type

TBA5 for Stateful-IPv6-Address-Pool

Length

Length in bytes. At least 4.

String

The string field contains the name of an assigned IPv6 stateful address pool configured on the NAS. The field is not NULL (hex 00) terminated.

3.6. 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	DNS-Server-IPv6-Address
0	0+	0	0	0+	TBA3	Route-IPv6-Information
0	0-1	0	0	0-1	TBA4	Delegated-IPv6-Prefix-Pool
0	0-1	0	0	0-1	TBA5	Stateful-IPv6-Address-Pool

4. Diameter Considerations

Given that the Attributes defined in this document are allocated from the standard RADIUS type space (see Section 6), no special handling is required by Diameter entities.

5. 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.

6. 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

*DNS-Server-IPv6-Address

*Route-IPv6-Information

*Delegated-IPv6-Prefix-Pool

*Stateful-IPv6-Address-Pool

7. Acknowledgements

The authors would like to thank Bernard Aboba, Roberta Maglione, Alfred Hines, Alan DeKok, Peter Deacon, and Mark Smith for their help and comments in reviewing this document.

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

8.2. Informative References

, "

[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.
[RFC3633]	Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
[RFC3646]	", .
[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.

Authors' Addresses

Benoit Lourdelet Lourdelet 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 Dec Cisco Systems, Inc. Haarlerbergweg 13-19 Amsterdam , NOORD-HOLLAND 1101 CH, Netherlands EMail: wdec@cisco.com

Behcet Sarikaya Sarikaya Huawei USA 1700 Alma Dr. Suite 500 Plano, TX US Phone: +1 972-509-5599 EMail: sarikaya@ieee.org

Glen Zorn Zorn Network Zen 1310 East Thomas Street Seattle, WA US EMail: gwz@net-zen.net

David Miles Miles Alcatel-Lucent L3 / 215 Spring St Melbourne, Victoria 3000, Australia EMail: David.Miles@alcatel-lucent.com