

Internet Engineering Task Force (IETF)
Request for Comments: 6911
Category: Standards Track
ISSN: 2070-1721

W. Dec, Ed.
Cisco Systems, Inc.
B. Sarikaya
Huawei USA
G. Zorn, Ed.
Network Zen
D. Miles
Google
B. Lourdelet
Juniper Networks
April 2013

RADIUS Attributes for IPv6 Access Networks

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 an 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.

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/rfc6911>.

Copyright Notice

Copyright (c) 2013 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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
1.1. Requirements Language	3
2. Deployment Scenarios	3
2.1. IPv6 Address Assignment	4
2.2. DNS Servers	5
2.3. IPv6 Route Information	5
2.4. Delegated IPv6 Prefix Pool	6
2.5. Stateful IPv6 Address Pool	6
3. Attributes	6
3.1. Framed-IPv6-Address	6
3.2. DNS-Server-IPv6-Address	8
3.3. Route-IPv6-Information	9
3.4. Delegated-IPv6-Prefix-Pool	10
3.5. Stateful-IPv6-Address-Pool	11
3.6. Table of Attributes	11
4. Diameter Considerations	12
5. Security Considerations	12
6. IANA Considerations	12
7. Acknowledgments	13
8. References	13
8.1. Normative References	13
8.2. Informative References	13

1. Introduction

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

- o The assignment of specific IPv6 addresses to hosts via DHCPv6.
- o The assignment of an IPv6 DNS server address, via DHCPv6 or Router Advertisement [RFC6106].
- o The configuration of more specific routes to be announced to the user via the Route Information Option defined in [RFC4191], Section 2.3.
- o The assignment of a named delegated prefix pool for use with "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6" [RFC3633].
- o The assignment of a named stateful address pool for use with DHCPv6 stateful address assignment [RFC3315].

1.1. 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 RFC 2119 [RFC2119].

2. Deployment Scenarios

The extensions in this document are intended to be applicable across a wide variety of network access scenarios in which RADIUS is involved. One such typical network scenario is illustrated in Figure 1. It is composed of an IP Routing Residential Gateway (RG) or host; a Layer 2 Access Node (AN), e.g., a Digital Subscriber Line Access Multiplexer (DSLAM); an IP Network Access Server (NAS) (incorporating an Authentication, Authorization, and Accounting (AAA) client); and a AAA server.

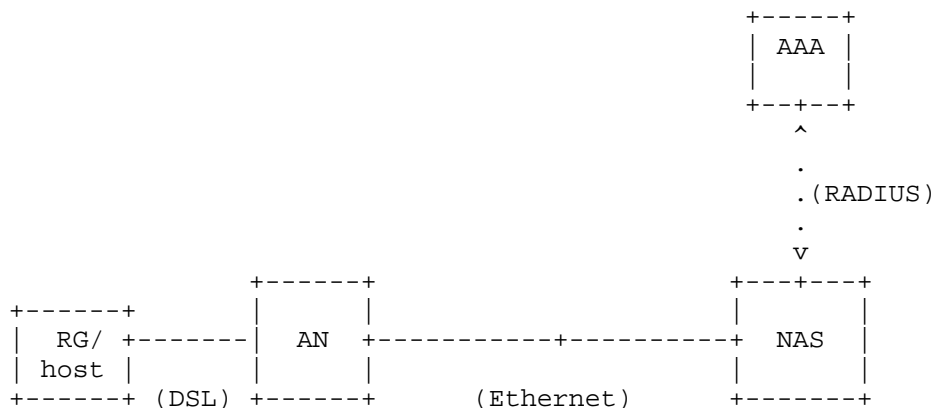


Figure 1

In the depicted scenario, the NAS may utilize an IP address configuration protocol (e.g., DHCPv6) to handle address assignment to RGs/hosts. The RADIUS server authenticates each RG/host and returns the Attributes used for authorization and accounting. These Attributes can include a host's IPv6 address, a DNS server address, and a set of IPv6 routes to be advertised via any suitable protocol, e.g., ICMPv6 (Neighbor Discovery). The name of a prefix pool to be used for DHCPv6 Prefix Delegation or the name of an address pool to be used for DHCPv6 address assignment can also be Attributes provided to the NAS by the RADIUS AAA server.

The following subsections discuss how these Attributes are used in more detail.

2.1. IPv6 Address Assignment

DHCPv6 [RFC3315] provides a mechanism to assign one or more 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 (Section 3.1).

While [RFC3162] permits the specification of an IPv6 address via the combination of the Framed-Interface-Id and Framed-IPv6-Prefix Attributes, this separation is more natural for use with PPP's IPv6 Control Protocol than it is for use with DHCPv6, and the use of a single IPv6 address Attribute makes for easier processing of accounting records.

Because DHCPv6 can be deployed on the same network as ICMPv6 stateless address autoconfiguration (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 in this case, the Framed-IPv6-Address Attribute is intended 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. 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 Recursive DNS Server Option [RFC6106]. To provide the NAS with the IPv6 address of one or more DNS servers, this document specifies the DNS-Server-IPv6-Address Attribute (Section 3.2).

2.3. IPv6 Route Information

The IPv6 Route Information Option [RFC4191], is intended to be used to inform a host connected to the NAS that a specific route is reachable via any given NAS.

This document specifies the Route-IPv6-Information Attribute (Section 3.3) that allows the AAA server 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 RFC 4191 or other equivalent methods. Any other information, such as preference or lifetime values, that is to be present in the actual announcement using a given method is assumed to be determined by the NAS using means not specified by this document (e.g., local configuration on the NAS).

While the Framed-IPv6-Prefix Attribute ([RFC3162], Section 2.3) allows the route to be advertised in an RA, it cannot be used to configure more specific routes. While the Framed-IPv6-Route Attribute ([RFC3162], Section 2.5) causes the route to be configured on the NAS and potentially to be announced via an IP routing protocol, 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 (DHCPv6-PD) [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 (Section 3.4) allows the RADIUS server to convey a prefix pool name to a NAS that is hosting a DHCPv6-PD server and that is acting as a delegating router.

Because DHCPv6 Prefix Delegation can be used with SLAAC on the same network, 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 non-temporary IPv6 addresses to hosts. Section 3.1 introduces the Framed-IPv6-Address Attribute to be used to provide 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 Stateful-IPv6-Address-Pool Attribute (Section 3.5) to allow the RADIUS server to convey a pool name to be used for such stateful DHCPv6-based addressing and for any subsequent accounting.

3. Attributes

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

3.1. Framed-IPv6-Address

The Framed-IPv6-Address 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 RADIUS server that it would prefer this IPv6 address, but the RADIUS server is not required to honor the hint. Because it is assumed that the

NAS will add a route corresponding to the address, it is not necessary for the RADIUS 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. The format of the Address field is identical to that of the corresponding field in the NAS-IPv6-Address Attribute [RFC3162].

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      Address      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|      Address (cont)      |
+-----+-----+-----+-----+-----+-----+

```

Type

168 for Framed-IPv6-Address

Length

18

Address

A 128-bit IPv6 address.

3.2. DNS-Server-IPv6-Address

The DNS-Server-IPv6-Address Attribute contains the IPv6 address of a 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 DNS server address to an RG/host. The Attribute MAY be used in an Access-Request packet as a hint by the NAS to the RADIUS server regarding the DNS IPv6 address, but the RADIUS server is not required to honor the hint.

The content of this Attribute can be copied to an instance of the DHCPv6 DNS Recursive Name Server Option [RFC3646] or to an IPv6 Router Advertisement Recursive DNS Server Option [RFC6106]. If more than one DNS-Server-IPv6-Address Attribute is present in the Access-Accept packet, the addresses from the Attributes SHOULD be copied in the same order as received.

A summary of the DNS-Server-IPv6-Address Attribute format is given below. The format of the Address field is the same as that of the corresponding field in the NAS-IPv6-Address Attribute [RFC3162].

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      Address      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|                                     Address (cont)      |
+-----+-----+-----+-----+-----+-----+-----+
|      Address (cont)      |
+-----+-----+-----+-----+-----+-----+

```

Type

169 for DNS-Server-IPv6-Address

Length

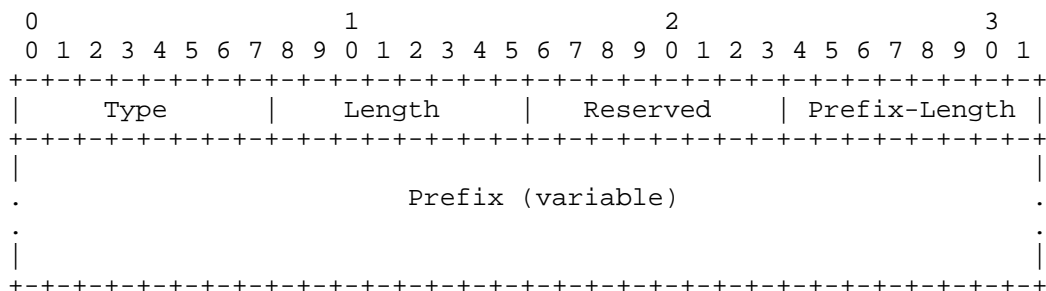
18

Address

The 128-bit IPv6 address of a DNS server.

3.3. Route-IPv6-Information

The Route-IPv6-Information 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 be used in an Access-Request packet as a hint by the NAS to the RADIUS server, but the RADIUS server is not required to honor the hint. The Route-IPv6-Information Attribute format is depicted below. The format of the prefix is as per [RFC3162].



Type

170 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 can range from 0 to 128. The prefix field is 0, 8, or 16 octets depending on Length.

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

The Delegated-IPv6-Prefix-Pool Attribute contains the name of an assigned pool that SHOULD be used to select an IPv6 delegated prefix for the user on the NAS. If a NAS does not support prefix pools, the NAS MUST ignore this Attribute. It MAY be used in an Access-Request packet as a hint by the NAS to the RADIUS server regarding the pool, but the RADIUS server is not required to honor the hint.

A summary of the Delegated-IPv6-Prefix-Pool Attribute format is shown below.

```

      0                               1                               2
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      String...
+-----+-----+-----+-----+-----+-----+-----+

```

Type

171 for Delegated-IPv6-Prefix-Pool

Length

Length, in bytes. At least 3.

String

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

Note: The string data type is as documented in [RFC6158] and carries binary data that is external to the RADIUS protocol, e.g., the name of a pool of prefixes configured on the NAS.

3.5. Stateful-IPv6-Address-Pool

The Stateful-IPv6-Address-Pool Attribute contains the name of an assigned pool that SHOULD be used to select an IPv6 address for the user on the NAS. 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. It MAY be used in an Access-Request packet as a hint by the NAS to the RADIUS server regarding the pool, but the RADIUS server is not required to honor the hint.

```

      0                               1                               2
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-----+-----+-----+-----+-----+-----+-----+-----+
|      Type      |      Length      |      String...
+-----+-----+-----+-----+-----+-----+-----+

```

Type

172 for Stateful-IPv6-Address-Pool

Length

Length, in bytes. At least 3.

String

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

Note: The string data type is as documented in [RFC6158] and carries binary data that is external to the RADIUS protocol, e.g., the name of a pool of addresses configured on the NAS.

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. The optional inclusion of the options in Access Request messages is intended to allow for a NAS to provide the RADIUS server with a hint of the Attributes in advance of user authentication, which may be useful in cases in which a user reconnects or has a static address. The server is under no obligation to honor such hints.

Request	Accept	Reject	Challenge	Accounting	#	Attribute
				Request		
0+	0+	0	0	0+	168	Framed-IPv6-Address
0+	0+	0	0	0+	169	DNS-Server-IPv6-Address
0+	0+	0	0	0+	170	Route-IPv6-Information
0+	0+	0	0	0+	171	Delegated-IPv6-Prefix-Pool
0+	0+	0	0	0+	172	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 specifies additional IPv6 RADIUS Attributes useful in residential broadband network deployments. In such networks, the RADIUS protocol may run either over IPv4 or over IPv6, and known security vulnerabilities of the RADIUS protocol, e.g., [SECI], apply to the Attributes defined in this document. A trust relationship between a NAS and RADIUS server is expected to be in place, with communication optionally secured by IPsec or Transport Layer Security (TLS) [RFC6614].

6. IANA Considerations

IANA has assigned five new RADIUS Attribute types in the "Radius Attribute Types" registry (currently located at <http://www.iana.org/assignments/radius-types>) for the following Attributes:

- o Framed-IPv6-Address
- o DNS-Server-IPv6-Address
- o Route-IPv6-Information
- o Delegated-IPv6-Prefix-Pool
- o Stateful-IPv6-Address-Pool

7. Acknowledgments

The authors would like to thank Bernard Aboba, Benoit Claise, Peter Deacon, Alan DeKok, Ralph Droms, Brian Haberman, Alfred Hines, Stephen Farrell, Jouni Korhonen, Roberta Maglione, Pete Resnick, Mark Smith, and Leaf Yeh 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] 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.
- [RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.
- [RFC6158] DeKok, A. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, March 2011.

- [RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga,
"Transport Layer Security (TLS) Encryption for RADIUS",
RFC 6614, May 2012.
- [SECI] Hill, J., "An Analysis of the RADIUS Authentication
Protocol", November 2001, <[http://regul.uni-mb.si/~meolic/
ptk-seminarske/radius.pdf](http://regul.uni-mb.si/~meolic/ptk-seminarske/radius.pdf)>.

Authors' Addresses

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 Drive, Suite 500
Plano, TX
US

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

Glen Zorn (editor)
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thailand

Phone: +66 (0) 8-1000-4155
EMail: glenzorn@gmail.com

David Miles
Google

EMail: davidmiles@google.com

Benoit Lourdelet
Juniper Networks
France

EMail: blourdel@juniper.net

