Network Working Group
Request for Comments: 3162
Category: Standards Track

B. Aboba
Microsoft
G. Zorn
Cisco Systems
D. Mitton
Circular Logic UnLtd.

August 2001

# RADIUS and IPv6

## Status of this Memo



## Copyright Notice



## Abstract

This document specifies the operation of RADIUS (Remote Authentication Dial In User Service) when run over IPv6 as well as the RADIUS attributes used to support IPv6 network access.

## 1. Introduction

This document specifies the operation of RADIUS [4]-[8] over IPv6 [13] as well as the RADIUS attributes used to support IPv6 network access.

Note that a NAS sending a RADIUS Access-Request may not know a-priori whether the host will be using IPv4, IPv6, or both. For example, within PPP, IPv6CP [11] occurs after LCP, so that address assignment will not occur until after RADIUS authentication and authorization has completed.

Therefore it is presumed that the IPv6 attributes described in this document MAY be sent along with IPv4-related attributes within the same RADIUS message and that the NAS will decide which attributes to use. The NAS SHOULD only allocate addresses and prefixes that the client can actually use, however. For example, there is no need for

the NAS to reserve use of an IPv4 address for a host that only supports IPv6; similarly, a host only using IPv4 or 6to4 [12] does not require allocation of an IPv6 prefix.

The NAS can provide IPv6 access natively, or alternatively, via other methods such as IPv6 within IPv4 tunnels [15] or 6over4 [14]. The choice of method for providing IPv6 access has no effect on RADIUS usage per se, although if it is desired that an IPv6 within IPv4 tunnel be opened to a particular location, then tunnel attributes should be utilized, as described in [6], [7].

## 1.1. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

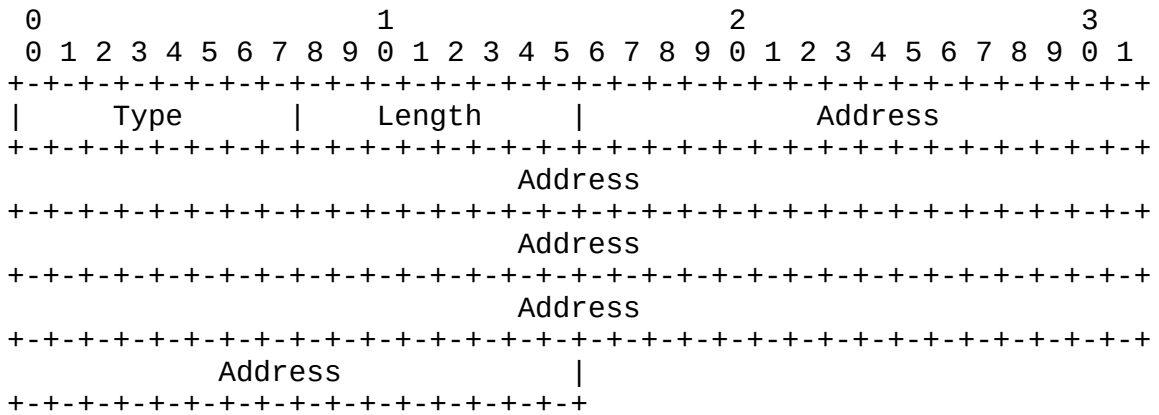
# 2. Attributes

## 2.1. NAS-IPv6-Address

Description

This Attribute indicates the identifying IPv6 Address of the NAS which is requesting authentication of the user, and SHOULD be unique to the NAS within the scope of the RADIUS server. NAS-IPv6-Address is only used in Access-Request packets. NAS-IPv6-Address and/or NAS-IP-Address MAY be present in an Access-Request packet; however, if neither attribute is present then NAS-Identifier MUST be present.

A summary of the NAS-IPv6-Address Attribute format is shown below. The fields are transmitted from left to right.



Type

95 for NAS-IPv6-Address

Length

18

Address

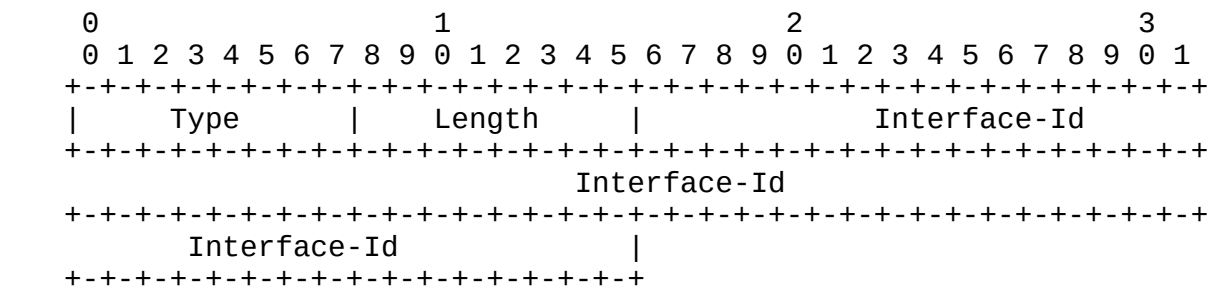
The Address field is 16 octets.

## 3.2. Framed-Interface-Id

Description

This Attribute indicates the IPv6 interface identifier to be configured for the user. It MAY be used in Access-Accept packets. If the Interface-Identifier IPv6CP option [11] has been successfully negotiated, this Attribute MUST be included in an Access-Request packet as a hint by the NAS to the server that it would prefer that value. It is recommended, but not required, that the server honor the hint.

A summary of the Framed-Interface-Id Attribute format is shown below. The fields are transmitted from left to right.




Type

96 for Framed-Interface-Id

Length

10

Interface-Id

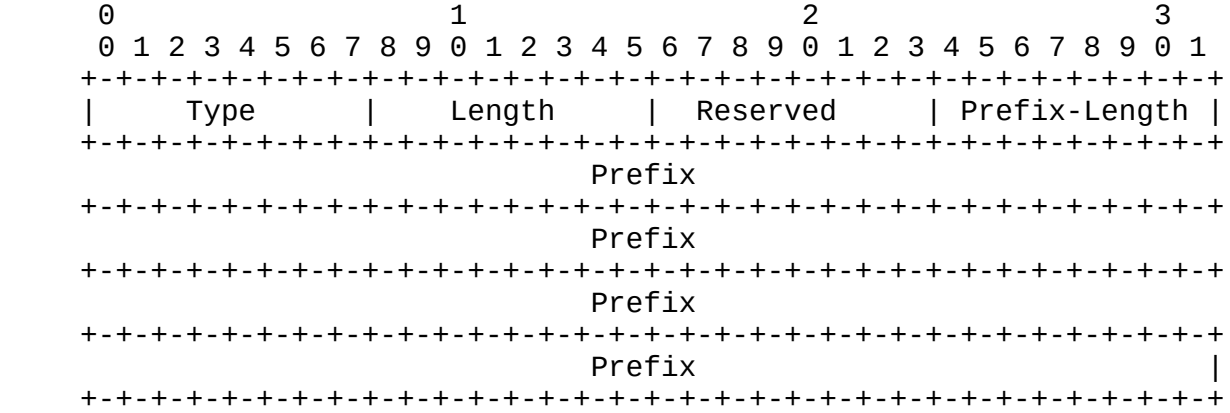
The Interface-Id field is 8 octets.

## 2.3. Framed-IPv6-Prefix

Description

This Attribute indicates an IPv6 prefix (and corresponding route) to be configured for the user. 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 prefix(es), but the server is not required to honor the hint. Since it is assumed that the NAS will plumb a route corresponding to the prefix, it is not necessary for the server to also send a Framed-IPv6-Route attribute for the same prefix.

A summary of the Framed-IPv6-Prefix Attribute format is shown below. The fields are transmitted from left to right.




Type

97 for Framed-IPv6-Prefix

Length

At least 4 and no larger than 20.

Reserved

This field, which is reserved and MUST be present, is always set to zero.

Prefix-Length

The length of the prefix, in bits. At least 0 and no larger than 128.

Prefix

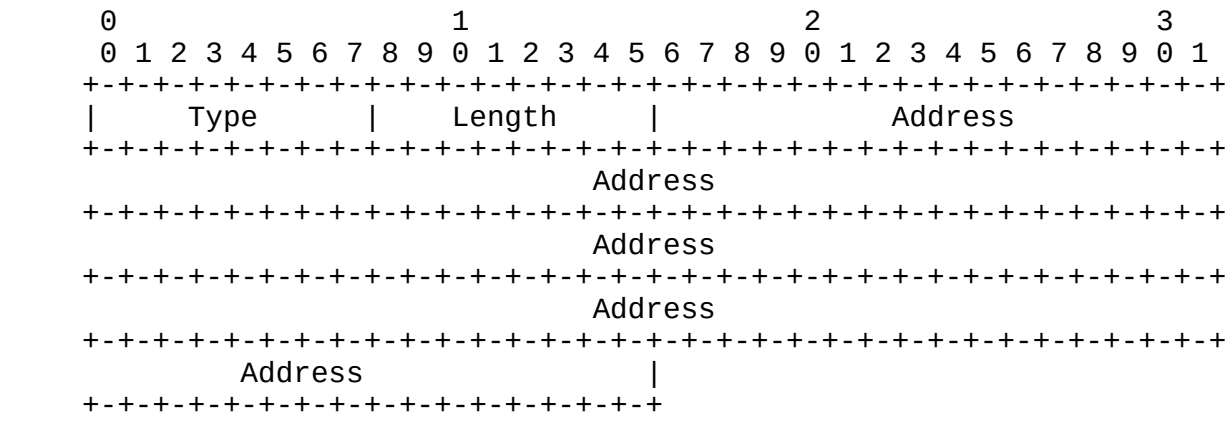
The Prefix field is up to 16 octets in length. Bits outside of the Prefix-Length, if included, must be zero.

## 2.4. Login-IPv6-Host

Description

This Attribute indicates the system with which to connect the user, when the Login-Service Attribute is included. It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint to the server that the NAS would prefer to use that host, but the server is not required to honor the hint.

A summary of the Login-IPv6-Host Attribute format is shown below. The fields are transmitted from left to right.




Type

98 for Login-IPv6-Host

Length

18

Address

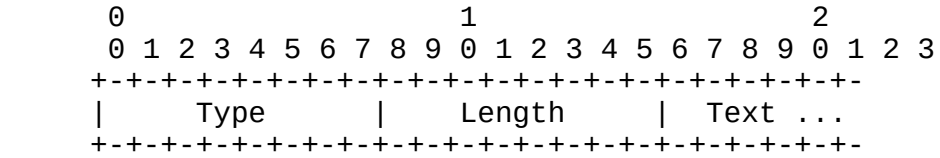
The Address field is 16 octets in length. The value 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF indicates that the NAS SHOULD allow the user to select an address or name to be connected to. The value 0 indicates that the NAS SHOULD select a host to connect the user to. Other values indicate the address the NAS SHOULD connect the user to.

## 2.5. Framed-IPv6-Route

Description

This Attribute provides routing information to be configured for the user on the NAS. It is used in the Access-Accept packet and can appear multiple times.

A summary of the Framed-IPv6-Route Attribute format is shown below. The fields are transmitted from left to right.




Type

99 for Framed-IPv6-Route

Length

>=3

Text

The Text field is one or more octets, and its contents are implementation dependent. The field is not NUL (hex 00) terminated. It is intended to be human readable and MUST NOT affect operation of the protocol.

For IPv6 routes, it SHOULD contain a destination prefix optionally followed by a slash and a decimal length specifier stating how many high order bits of the prefix to use. That is followed by a space, a gateway address, a space, and one or more metrics (encoded in decimal) separated by spaces. Prefixes and addresses are formatted as described in [16]. For example, "2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1".

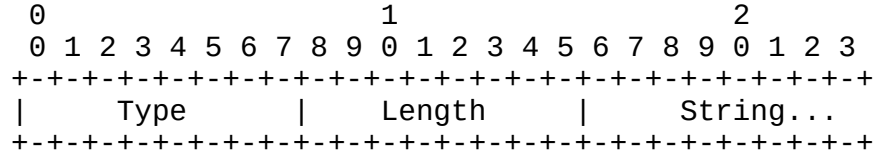
Whenever the gateway address is the IPv6 unspecified address the IP address of the user SHOULD be used as the gateway address. The unspecified address can be expressed in any of the acceptable formats described in [16]. For example, "2000:0:0:106::/64 :: 1".

## 2.6. Framed-IPv6-Pool

Description

This Attribute contains the name of an assigned pool that SHOULD be used to assign an IPv6 prefix for the user. If a NAS does not support multiple prefix pools, the NAS MUST ignore this Attribute.

A summary of the Framed-IPv6-Pool Attribute format is shown below. The fields are transmitted from left to right.




Type

100 for Framed-IPv6-Pool

Length

>= 3

String

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

# 3. 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 |
|---|---|---|---|---|---|---|
| 0-1 | 0 | 0 | 0 | 0-1 | 95 | NAS-IPv6-Address |
| 0-1 | 0-1 | 0 | 0 | 0-1 | 96 | Framed-Interface-Id |
| 0+ | 0+ | 0 | 0 | 0+ | 97 | Framed-IPv6-Prefix |
| 0+ | 0+ | 0 | 0 | 0+ | 98 | Login-IPv6-Host |
| 0 | 0+ | 0 | 0 | 0+ | 99 | Framed-IPv6-Route |
| 0 | 0-1 | 0 | 0 | 0-1 | 100 | Framed-IPv6-Pool |

## 4. References

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

[2] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", RFC 2044, October 1996.

[3] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[4] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[5] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[6] Zorn, G., Mitton, D. and B. Aboba, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

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

[8] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[9] Kent S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[10] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[11] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.

[12] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[13] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[14] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529, March 1999.

[15] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.

[16] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

## 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 are described in [3], [4] and [8].

Since IPSEC [9] is mandatory to implement for IPv6, it is expected that running RADIUS implementations supporting IPv6 will typically 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.

Within RADIUS, a shared secret is used for hiding of attributes such as User-Password [4] and Tunnel-Password [7]. In addition, the shared secret is used in computation of the Response Authenticator [4], as well as the Message-Authenticator attribute [8]. Therefore, in RADIUS a shared secret is used to provide confidentiality as well as integrity protection and authentication. As a result, only use of IPSEC ESP with a non-null transform can provide security services sufficient to substitute for RADIUS application-layer security. Therefore, where IPSEC AH or ESP null is used, it will typically still be necessary to configure a RADIUS shared secret.

However, where RADIUS is run over IPSEC ESP with a non-null transform, the secret shared between the NAS and the RADIUS server MAY NOT be configured. In this case, a shared secret of zero length MUST be assumed.

## 6. IANA Considerations

This document requires the assignment of six new RADIUS attribute numbers for the following attributes:

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool

See section 3 for the registered list of numbers.

## 7. Acknowledgments

The authors would like to acknowledge Jun-ichiro itojun Hagino of IIJ Research Laboratory, Darran Potter of Cisco and Carl Rigney of Lucent for contributions to this document.

## 8. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 936 6605
Fax: +1 425 936 7329
EMail: bernarda@microsoft.com

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004

Phone: +1 425 471 4861
EMail: gwz@cisco.com

Dave Mitton
Circular Logic UnLtd.
733 Turnpike Street #154
North Andover, MA 01845

Phone: 978 683-1814
Email: david@mitton.com

## Full Copyright Statement



## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.