Internet Engineering Task Force (IETF)
Request for Comments: 6930
Category: Standards Track
ISSN: 2070-1721

D. Guo
S. Jiang, Ed.
Huawei Technologies Co., Ltd
R. Despres
RD-IPtech
R. Maglione
Cisco Systems

April 2013

RADIUS Attribute for IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)

Abstract

The IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) provides both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 coexistence period. The Dynamic Host Configuration Protocol (DHCP) 6rd option has been defined to configure the 6rd Customer Edge (CE). However, in many networks, the configuration information may be stored in the Authentication Authorization and Accounting (AAA) servers, while user configuration is mainly acquired from a Broadband Network Gateway (BNG) through the DHCP protocol. This document defines a Remote Authentication Dial-In User Service (RADIUS) attribute that carries 6rd configuration information from the AAA server to BNGs.

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/rfc6930.

Table of Contents

1. Introduction 3
2. Terminology 3
3. IPv6 6rd Configuration with RADIUS 4
4. Attributes 6
4.1. IPv6-6rd-Configuration Attribute 6
4.2. Table of Attributes 9
5. Diameter Considerations 9
6. Security Considerations 9
7. IANA Considerations 10
8. Acknowledgments 10
9. References 10
9.1. Normative References 10
9.2. Informative References 11

1. Introduction

Recently, providers have started to deploy IPv6 and to consider transition to IPv6. The IPv6 Rapid Deployment (6rd) [RFC5969] provides both IPv4 and IPv6 connectivity services simultaneously during the IPv4/IPv6 coexistence period. 6rd is used to provide IPv6 connectivity service through legacy IPv4-only infrastructure. 6rd uses the Dynamic Host Configuration Protocol (DHCP) [RFC2131], and the 6rd Customer Edge (CE) uses the DHCP 6rd option [RFC5969] to discover a 6rd Border Relay and to configure an IPv6 prefix and address.

In many networks, user-configuration information is managed by Authentication, Authorization, and Accounting (AAA) servers. The Remote Authentication Dial-In User Service (RADIUS) protocol [RFC2865] is usually used by AAA servers to communicate with network elements. In a fixed-line broadband network, the Broadband Network Gateways (BNGs) act as the access gateway for users. The BNGs are assumed to embed a DHCP server function that allows them to handle locally any DHCP requests issued by hosts.

Since the 6rd configuration information is stored in AAA servers, and user configuration is mainly through DHCP between BNGs and hosts/CEs, new RADIUS attributes are needed to propagate the information from AAA servers to BNGs.

2. Terminology

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].

The terms 6rd Customer Edge (6rd CE) and 6rd Border Relay (BR) are defined in [RFC5969]. "MAC" stands for Media Access Control.

3. IPv6 6rd Configuration with RADIUS

Figure 1 illustrates how DHCP and the RADIUS protocol cooperate to provide 6rd CE with 6rd configuration information.

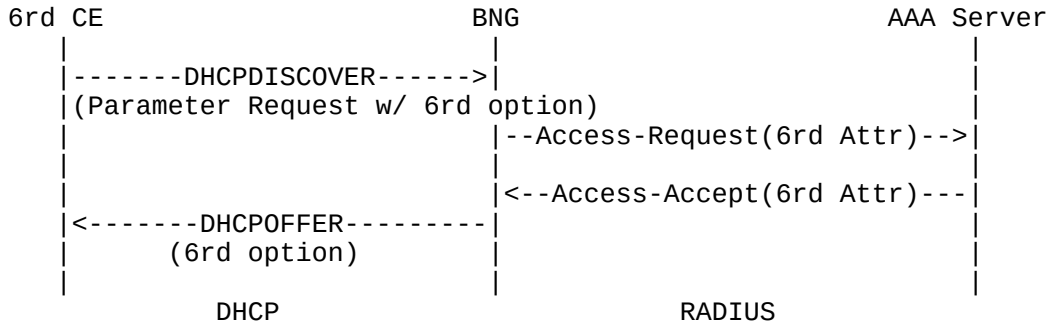


Figure 1: The Cooperation between DHCP and RADIUS When Combined with RADIUS Authentication

The BNG acts as a client of RADIUS and as a DHCP server. First, the 6rd CE MAY initiate a DHCPDISCOVER message that includes a Parameter Request option (55) [RFC2132] with the 6rd option [RFC5969]. When the BNG receives the DHCPDISCOVER, it SHOULD initiate a RADIUS Access- Request message to the RADIUS server. In that message,

- the User-Name attribute (1) SHOULD be filled by the 6rd CE MAC address, and

- the User-Password attribute (2) SHOULD be filled by the shared 6rd password that has been preconfigured on the DHCP server.

The BNG requests authentication, as defined in [RFC2865], with the IPv6-6rd-Configuration attribute (Section 4.1) in the desired attribute list. If the authentication request is approved by the AAA server, an Access-Accept message MUST be acknowledged with the IPv6-6rd-Configuration attribute. Then, the BNG SHOULD respond to the 6rd CE with a DHCPOFFER message, which contains a DHCP 6rd option. The recommended format of the MAC address is as defined in Calling-Station-Id ([RFC3580], Section 3.20) without the SSID (Service Set Identifier) portion.

Figure 2 describes another scenario -- later re-authorization -- in which the authorization operation is not coupled with authentication. Authorization relevant to 6rd is done independently after the authentication process.

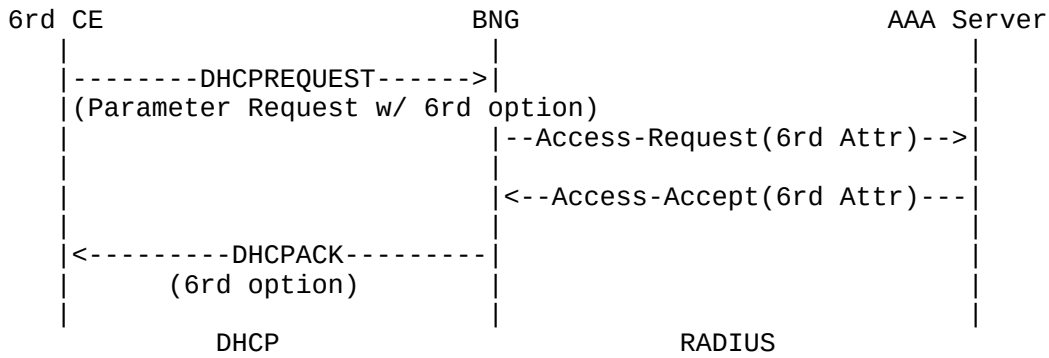


Figure 2: The Cooperation between DHCP and RADIUS
When Decoupled from RADIUS Authentication

In this scenario, the Access-Request packet SHOULD contain a Service-Type attribute (6) with the value Authorize Only (17); thus, according to [RFC5080], the Access-Request packet MUST contain a State attribute that it obtains from the previous authentication process.

In both above-mentioned scenarios, Message-Authenticator (type 80) [RFC2865] SHOULD be used to protect both Access-Request and Access-Accept messages.

After receiving the IPv6-6rd-Configuration attribute in the initial Access-Accept, the BNG SHOULD store the received 6rd configuration parameters locally. When the 6rd CE sends a DHCP Request message to request an extension of the lifetime for the assigned address, the BNG does not have to initiate a new Access-Request towards the AAA server to request the 6rd configuration parameters. The BNG could retrieve the previously stored 6rd configuration parameters and use them in its reply.

If the BNG does not receive the IPv6-6rd-Configuration attribute in the Access-Accept, it MAY fall back to a preconfigured default 6rd configuration, if any. If the BNG does not have any preconfigured default 6rd configuration or if the BNG receives an Access-Reject, the tunnel cannot be established.

As specified in [RFC2131], Section 4.4.5 ("Reacquisition and expiration"), if the DHCP server to which the DHCP Request message was sent at time T1 has not responded by time T2 (typically 0.375*duration_of_lease after T1), the 6rd CE (the DHCP client) SHOULD enter the REBINDING state and attempt to contact any server.

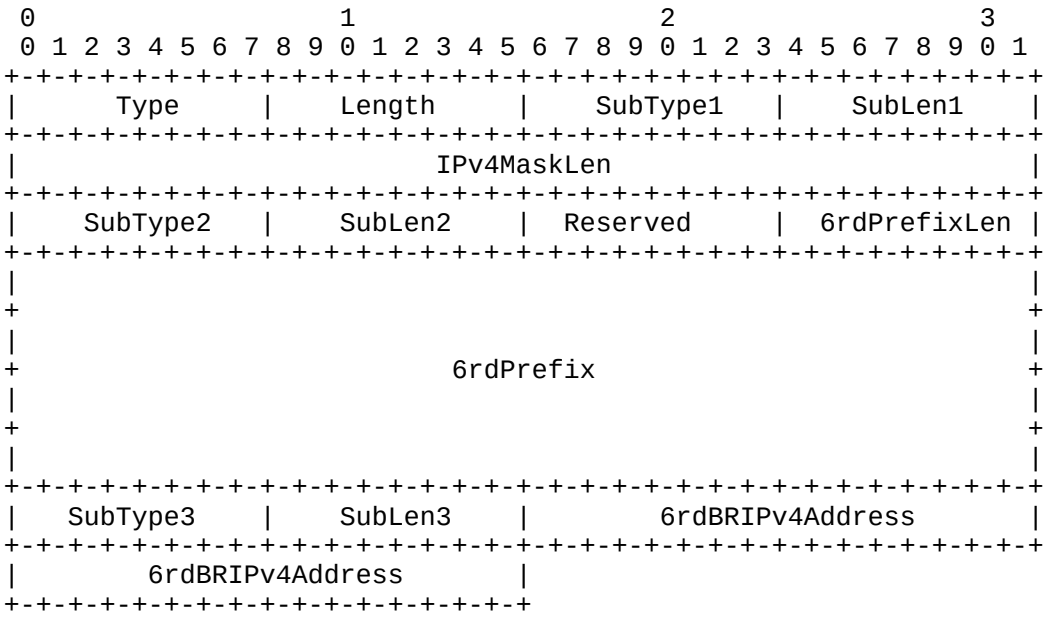
In this situation, the secondary BNG receiving the new DHCP message MUST initiate a new Access-Request towards the AAA server. The secondary BNG MAY include the IPv6-6rd-Configuration attribute in its Access-Request.

4. Attributes

This section defines the IPv6-6rd-Configuration attribute that is used in both above-mentioned scenarios. The attribute design follows [RFC6158] and refers to [RFC6929].

4.1. IPv6-6rd-Configuration Attribute

The specification requires that multiple IPv4 addresses are associated with one IPv6 prefix. Given that RADIUS currently has no recommended way of grouping multiple attributes, the design below appears to be a reasonable compromise. The IPv6-6rd-Configuration attribute is structured as follows:



Type

173

Length

28 + n*6 (the length of the entire attribute in octets, where n is the number of BR IPv4 addresses and minimum n is 1)

SubType1

1 (SubType number, for the IPv4 Mask Length suboption)

SubLen1

6 (the length of the IPv4 Mask Length suboption)

IPv4MaskLen

The number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. This may be any value between 0 and 32. Any value greater than 32 is invalid. Since [RFC6158], Appendix A.2.1, has forbidden 8-bit fields, a 32-bit field is used here.

SubType2

2 (SubType number for the 6rd prefix suboption)

SubLen2

20 (the length of the 6rd prefix suboption)

Reserved

Set to all 0 for now. Reserved for future use. To be compatible with other IPv6 prefix attributes in the RADIUS protocol, the bits MUST be set to zero by the sender and MUST be ignored by the receiver.

6rdPrefixLen

The IPv6 Prefix length of the Service Provider’s 6rd IPv6 prefix in number of bits. The 6rdPrefixLen MUST be less than or equal to 128.

6rdPrefix

The Service Provider’s 6rd IPv6 prefix represented as a 16-octet IPv6 address. The bits after the 6rdPrefixlen number of bits in the prefix SHOULD be set to zero.

SubType3

3 (SubType number, for the 6rd Border Relay IPv4 address suboption)

SubLen3

6 (the length of the 6rd Border Relay IPv4 address suboption)

6rdBRIPv4Address

One or more IPv4 addresses of the 6rd Border Relay(s) for a given 6rd domain. The maximum RADIUS attribute length of 255 octets results in a limit of 37 IPv4 addresses.

Since the subtypes have values, they can appear in any order. If multiple 6rdBRIPv4Address (subtype 3) appear, they are RECOMMENDED to be placed together.

The IPv6-6rd-Configuration attribute is normally used in Access-Accept messages. It MAY be used in Access-Request packets as a hint to the RADIUS server; for example, if the BNG is preconfigured with a default 6rd configuration, these parameters MAY be inserted in the attribute. The RADIUS server MAY ignore the hint sent by the BNG, and it MAY assign different 6rd parameters.

If the BNG includes the IPv6-6rd-Configuration attribute, but the AAA server does not recognize it, this attribute MUST be ignored by the AAA server.

If the BNG does not receive the IPv6-6rd-Configuration attribute in the Access-Accept, it MAY fallback to a preconfigured default 6rd configuration, if any. If the BNG does not have any preconfigured default 6rd configuration, the 6rd tunnel cannot be established.

If the BNG is pre-provisioned with a default 6rd configuration and the 6rd configuration received in Access-Accept is different from the configured default, then the 6rd configuration received in the Access-Accept message MUST be used for the session.

If the BNG cannot support the received 6rd configuration for any reason, the tunnel SHOULD NOT be established.

4.2. Table of Attributes

The following table adds to the one in [RFC2865], Section 5.44, providing a guide to the quantity of IPv6-6rd-Configuration attributes that may be found in each kind of packet.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0-1	0-1	0	0	0-1	173	IPv6-6rd-Configuration
0-1	0-1	0	0	0-1	1	User-Name
0-1	0	0	0	0-1	2	User-Password
0-1	0-1	0	0	0-1	6	Service-Type
0-1	0-1	0-1	0-1	0-1	80	Message-Authenticator

The following key defines the meanings of the above table entries.

0 This attribute MUST NOT be present in packet.
0+ Zero or more instances of this attribute MAY be present in packet.
0-1 Zero or one instance of this attribute MAY be present in packet.
1 Exactly one instance of this attribute MUST be present in packet.

5. Diameter Considerations

This attribute is usable within either RADIUS or Diameter [RFC6733]. Since the attribute defined in this document has been allocated from the standard RADIUS type space, no special handling is required by Diameter entities.

6. Security Considerations

In 6rd scenarios, both CE and BNG are within a provider network, which can be considered as a closed network and a lower-threat environment. A similar consideration can be applied to the RADIUS message exchange between the BNG and the AAA server.

In 6rd scenarios, the RADIUS protocol is run over IPv4. Known security vulnerabilities of the RADIUS protocol are discussed in [RFC2607], [RFC2865], and [RFC2869]. Use of IPsec [RFC4301] for providing security when RADIUS is carried in IPv6 is discussed in [RFC3162].

To get unauthorized 6rd configuration information, a malicious user may use MAC address spoofing and/or a dictionary attack on the shared 6rd password that has been preconfigured on the DHCP server. The relevant security issues have been considered in Section 12 of [RFC5969].

Security issues that may arise specifically between the 6rd CE and BNG are discussed in [RFC5969]. Furthermore, generic DHCP security mechanisms can be applied to DHCP intercommunication between 6rd CE and BNG.

Security considerations for the Diameter protocol are discussed in [RFC6733].

7. IANA Considerations

Per this document, IANA has assigned one new RADIUS Attribute Type in the "Radius Types" registry (currently located at http://www.iana.org/assignments/radius-types) for the following attribute:

IPv6-6rd-Configuration (173)

8. Acknowledgments

The authors would like to thank Alan DeKok, Yong Cui, Leaf Yeh, Sean Turner, Joseph Salowey, Glen Zorn, Dave Nelson, Bernard Aboba, Benoit Claise, Barry Lieba, Stephen Farrell, Adrian Farrel, Ralph Droms, and other members of the SOFTWIRE WG, RADEXT WG, AAA Doctors, and Security Directorate for valuable comments.

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.

[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.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5080] Nelson, D. and A. DeKok, "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes", RFC 5080, December 2007.

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

[RFC6158] DeKok, A., Ed., and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, March 2011.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, October 2012.

9.2. Informative References

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[RFC6929] DeKok, A. and A. Lior, "Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions", RFC 6929, April 2013.

Authors' Addresses

Dayong Guo
Huawei Technologies Co., Ltd
Q14 Huawei Campus, 156 BeiQi Road,
ZhongGuan Cun, Hai-Dian District, Beijing 100095
P.R. China

EMail: guoseu@huawei.com

Sheng Jiang (Editor)
Huawei Technologies Co., Ltd
Q14 Huawei Campus, 156 BeiQi Road,
ZhongGuan Cun, Hai-Dian District, Beijing 100095
P.R. China

EMail: jiangsheng@huawei.com

Remi Despres
RD-IPtech
3 rue du President Wilson
Levallois
France

EMail: despres.remi@laposte.net

Roberta Maglione
Cisco Systems
181 Bay Street
Toronto, ON
M5J 2T3
Canada

EMail: robmgl@cisco.com