Network Working Group Internet-Draft Intended status: Standards Track Expires: October 17, 2019

RADIUS Extensions for 0-RTT TCP Converters draft-boucadair-radext-tcpm-converter-02

Abstract

Because of the lack of Multipath TCP (MPTCP) support at the server side, some service providers now consider a network-assisted model that relies upon the activation of a dedicated function called Converters. Network-assisted MPTCP deployment models are designed to facilitate the adoption of MPTCP for the establishment of multi-path communications without making any assumption about the support of MPTCP by the communicating peers. Converters located in the network are responsible for establishing multi-path communications on behalf of endpoints, thereby taking advantage of MPTCP capabilities to achieve different goals that include (but are not limited to) optimization of resource usage (e.g., bandwidth aggregation), of resiliency (e.g., primary/backup communication paths), and traffic offload management.

This document specifies a new Remote Authentication Dial-In User Service (RADIUS) attributes that carry the IP addresses that will be returned to authorized users to reach one or multiple Converters.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in <u>BCP</u> <u>14</u> [<u>RFC2119</u>][RFC8174] when, and only when, they appear in all capitals, as shown here.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of <u>BCP 78</u> and <u>BCP 79</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/. 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."

This Internet-Draft will expire on October 17, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents (<u>https://trustee.ietf.org/license-info</u>) 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

$\underline{1}$. Introduction			•	•		•		•				2
2. CONVERT RADIUS Attributes												<u>4</u>
<u>2.1</u> . CONVERT-IPv4												<u>4</u>
2.2. CONVERT-IPv6												<u>5</u>
<u>3</u> . Sample Use Case												<u>6</u>
$\underline{4}$. Security Considerations .												<u>8</u>
5. Table of Attributes												<u>8</u>
6. IANA Considerations												<u>9</u>
<u>7</u> . Acknowledgements	•						•					<u>9</u>
<u>8</u> . References												<u>9</u>
<u>8.1</u> . Normative References												
<u>8.2</u> . Informative Reference	S						•					<u>10</u>
Authors' Addresses												11

1. Introduction

One of the promising deployment scenarios for Multipath TCP (MPTCP, [<u>RFC6824</u>]) is to enable a host or a Customer Premises Equipment (CPE) connected to multiple networks (e.g., DSL, LTE, WLAN) to optimize the usage of such resources. A deployment scenario relies on MPTCP Conversion Points (Converters). A Converter terminates the MPTCP sessions established from a host/CPE, before redirecting traffic into a legacy TCP session [<u>RFC0793</u>].

Figure 1 shows a deployment example of the Converters to assist establishing MPTCP connections.

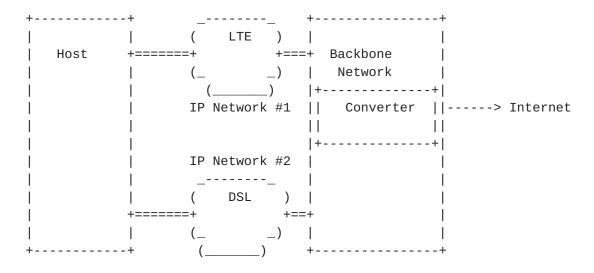


Figure 1: "Network-Assisted" MPTCP Design

[I-D.ietf-tcpm-converters] specifies the Converter as a function that is installed by a network operator to aid the deployment of TCP extensions and to provide the benefits of such extensions to clients. A Transport Converter supports one or more TCP extensions.

Within this document, a Converter refers to a function that terminates a transport flow and relays all data received over it over another transport flow. This element is located upstream in the network. One or multiple Converters can be deployed in the network side. The Converter achieves the following:

- o Listen for client sessions;
- o Receive from a client the address of the final target server;
- o Setup a session to the final server;
- o Relay control messages and data between the client and the server;
- o Perform access controls according to local policies.

The Converter element is located in the network. One or multiple Converters can be deployed.

This document specifies two new Remote Authentication Dial-In User Service (RADIUS, [RFC2865]) attributes that carry the Converter IP address list (Section 2). In order to accommodate both IPv4 and IPv6

Internet-Draft

deployment contexts, and given the constraints in <u>Section 3.4 of</u> [<u>RFC6158</u>], two attributes are specified. Note that one or multiple IPv4 and/or IPv6 addresses may be returned to a requesting CPE. A sample use case is described in <u>Section 3</u>.

This document assumes that the Converter(s) reachability information can be stored in Authentication, Authorization, and Accounting (AAA) servers while the CPE configuration is usually provided by means of DHCP ([<u>RFC2131</u>][RFC8415]). Further Network-Assisted MPTCP deployment and operational considerations are discussed in [<u>I-D.nam-mptcp-deployment-considerations</u>].

This specification assumes a Converter is reachable through one or multiple IP addresses. As such, a list of IP addresses can be communicated via RADIUS. Also, it assumes the various network attachments provided to an MPTCP-enabled host are managed by the same administrative entity.

This document adheres to [<u>RFC8044</u>] for defining the new attributes.

2. CONVERT RADIUS Attributes

2.1. CONVERT-IPv4

Description

The RADIUS CONVERT-IPv4 attribute contains the IPv4 address of a Converter that is assigned to a host.

Because multiple Converters IP addresses may be provisioned to an authorised host (that is a host entitled to solicit the resources of a Converter), multiple instances of the CONVERT-IPv4 attribute MAY be included; each instance of the attribute carries a distinct IP address.

Both CONVERT-IPv4 and CONVERT-IPv6 attributes MAY be present in a RADIUS message.

The CONVERT-IPv4 Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference, although the server is not required to honor such a hint.

The CONVERT-IPv4 Attribute MAY appear in a CoA-Request packet.

The CONVERT-IPv4 Attribute MAY appear in a RADIUS Accounting-Request packet.

The CONVERT-IPv4 Attribute MUST NOT appear in any other RADIUS packet.

Туре

TBA (see <u>Section 6</u>).

Length

6

Data Type

The attribute CONVERT-IPv4 is of type ip4addr (<u>Section 3.3 of</u> [RFC8044]).

Value

This field includes an IPv4 address (32 bits) of the Converter.

The CONVERT-IPv4 attribute MUST NOT include multicast and host loopback addresses [RFC6890]. Anycast addresses are allowed to be included in a CONVERT-IPv4 attribute.

2.2. CONVERT-IPv6

Description

The RADIUS CONVERT-IPv6 attribute contains the IPv6 address of a Converter that is assigned to a host.

Because multiple Converter IP addresses may be provisioned to an authorised CPE (that is a host entitled to solicit the resources of a Converter), multiple instances of the CONVERT-IPv6 attribute MAY be included; each instance of the attribute carries a distinct IP address.

Both CONVERT-IPv4 and CONVERT-IPv6 attributes MAY be present in a RADIUS message.

The CONVERT-IPv6 Attribute MAY appear in a RADIUS Access-Accept packet. It MAY also appear in a RADIUS Access-Request packet as a hint to the RADIUS server to indicate a preference, although the server is not required to honor such a hint.

The CONVERT-IPv6 Attribute MAY appear in a CoA-Request packet.

The CONVERT-IPv6 Attribute MAY appear in a RADIUS Accounting-Request packet.

The CONVERT-IPv6 Attribute MUST NOT appear in any other RADIUS packet.

Туре

TBA (see <u>Section 6</u>).

Length

18

Data Type

The attribute CONVERT-IPv6 is of type ip6addr (<u>Section 3.9 of</u> [RFC8044]).

Value

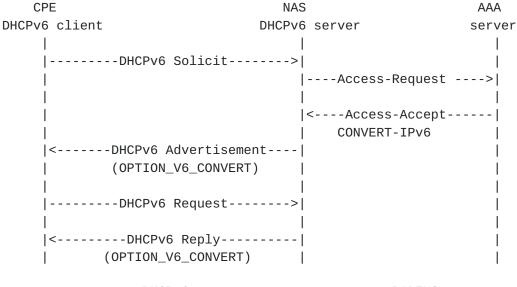
This field includes an IPv6 address (128 bits) of the Converter.

The CONVERT-IPv6 attribute MUST NOT include multicast and host loopback addresses [RFC6890]. Anycast addresses are allowed to be included in an CONVERT-IPv6 attribute.

3. Sample Use Case

This section does not aim to provide an exhaustive list of deployment scenarios where the use of the RADIUS CONVERT-IPv6 and CONVERT-IPv4 attributes can be helpful. Typical deployment scenarios are described, for instance, in [RFC6911].

Figure 2 shows an example where a CPE is assigned a Converter. This example assumes that the Network Access Server (NAS) embeds both RADIUS client and DHCPv6 server capabilities.



DHCPv6

RADIUS

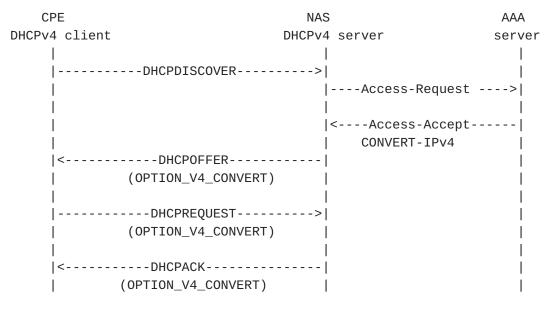
Figure 2: Sample Flow Example (1)

Upon receipt of the DHCPv6 Solicit message from a CPE, the NAS sends a RADIUS Access-Request message to the AAA server. Once the AAA server receives the request, it replies with an Access-Accept message (possibly after having sent a RADIUS Access-Challenge message and assuming the CPE is entitled to connect to the network) that carries a list of parameters to be used for this session, and which include Converter reachability information (namely a list of IP addresses).

The content of the CONVERT-IPv6 attribute is then used by the NAS to complete the DHCPv6 procedure that the CPE initiated to retrieve information about the Converter it has been assigned.

Upon change of the Converter assigned to a CPE, the RADIUS server sends a RADIUS COA message [RFC5176] that carries the RADIUS CONVERT-IPv6 attribute to the NAS. Once that message is accepted by the NAS, it replies with a RADIUS COA ACK message. The NAS replaces the old Converter with the new one.

Figure 3 shows another example where a CPE is assigned a Converter, but the CPE uses DHCPv6 to retrieve a list of IP addresses of a Converter.



DHCPv4

RADIUS

Figure 3: Sample Flow Example (2)

Some deployments may rely on the mechanisms defined in [RFC4014] or [RFC7037], which allows a NAS to pass attributes obtained from a RADIUS server to a DHCP server.

4. Security Considerations

RADIUS-related security considerations are discussed in [RFC2865].

Generic Convert security considerations are discussed in [I-D.ietf-tcpm-converters].

MPTCP-related security considerations are discussed in [RFC6824] and [RFC6181].

Traffic theft is a risk if an illegitimate Converter is inserted in the path. Indeed, inserting an illegitimate Converter in the forwarding path allows to intercept traffic and can therefore provide access to sensitive data issued by or destined to a host. To mitigate this threat, secure means to discover a Converter should be enabled.

5. Table of Attributes

The following table provides a guide as what type of RADIUS packets that may contain these attributes, and in what quantity.

[Page 8]

Access-	Access-	Access-	Chall	enge Acct. #	Attri	bute	
Request	Accept	Reject		Request			
0+	0+	Θ	Θ	0+	TBA	CONVERT-IPv4	
0+	0+	Θ	Θ	0+	TBA	CONVERT-IPv6	
CoA-Req	uest CoA	-ACK CoA	-NACK #	Attribute			
0+	Θ	C)	TBA CONVERT	-IPv4		
0+	Θ	O)	TBA CONVERT	-IPv6		

The following table defines the meaning 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.

6. IANA Considerations

IANA is requested to assign two new RADIUS attribute types from the IANA registry "Radius Attribute Types" located at http://www.iana.org/assignments/radius-types:

CONVERT-IPv4 (TBA)

CONVERT-IPv6 (TBA)

7. Acknowledgements

Thanks to Alan DeKok for the comments.

8. References

8.1. Normative References

- [I-D.ietf-tcpm-converters] Bonaventure, O., Boucadair, M., Gundavelli, S., Seo, S., and B. Hesmans, "0-RTT TCP Convert Protocol", <u>draft-ietf-</u> tcpm-converters-06 (work in progress), March 2019.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", <u>BCP 14</u>, <u>RFC 2119</u>, DOI 10.17487/RFC2119, March 1997, <<u>https://www.rfc-editor.org/info/rfc2119</u>>.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", <u>RFC 2865</u>, DOI 10.17487/RFC2865, June 2000, <<u>https://www.rfc-editor.org/info/rfc2865</u>>.

- [RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <<u>https://www.rfc-editor.org/info/rfc6158</u>>.
- [RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", <u>BCP 153</u>, <u>RFC 6890</u>, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.
- [RFC8044] DeKok, A., "Data Types in RADIUS", <u>RFC 8044</u>, DOI 10.17487/RFC8044, January 2017, <<u>https://www.rfc-editor.org/info/rfc8044</u>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in <u>RFC</u> 2119 Key Words", <u>BCP 14</u>, <u>RFC 8174</u>, DOI 10.17487/RFC8174, May 2017, <<u>https://www.rfc-editor.org/info/rfc8174</u>>.

8.2. Informative References

- [I-D.nam-mptcp-deployment-considerations] Boucadair, M., Jacquenet, C., Bonaventure, O., Henderickx, W., and R. Skog, "Network-Assisted MPTCP: Use Cases, Deployment Scenarios and Operational Considerations", <u>draft-nam-mptcp-deployment-considerations-01</u> (work in progress), December 2016.
- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, <u>RFC 793</u>, DOI 10.17487/RFC0793, September 1981, <<u>https://www.rfc-editor.org/info/rfc793</u>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", <u>RFC 2131</u>, DOI 10.17487/RFC2131, March 1997, <<u>https://www.rfc-editor.org/info/rfc2131</u>>.
- [RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option", <u>RFC 4014</u>, DOI 10.17487/RFC4014, February 2005, <<u>https://www.rfc-editor.org/info/rfc4014</u>>.
- [RFC4908] Nagami, K., Uda, S., Ogashiwa, N., Esaki, H., Wakikawa, R., and H. Ohnishi, "Multi-homing for small scale fixed network Using Mobile IP and NEMO", <u>RFC 4908</u>, DOI 10.17487/RFC4908, June 2007, <<u>https://www.rfc-editor.org/info/rfc4908</u>>.

Internet-Draft RADIUS for 0-RTT TCP Converters

- [RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", <u>RFC 5176</u>, DOI 10.17487/RFC5176, January 2008, <https://www.rfc-editor.org/info/rfc5176>.
- [RFC6181] Bagnulo, M., "Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses", <u>RFC 6181</u>, DOI 10.17487/RFC6181, March 2011, <<u>https://www.rfc-editor.org/info/rfc6181</u>>.
- [RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", <u>RFC 6824</u>, DOI 10.17487/RFC6824, January 2013, <https://www.rfc-editor.org/info/rfc6824>.
- [RFC6911] Dec, W., Ed., Sarikaya, B., Zorn, G., Ed., Miles, D., and B. Lourdelet, "RADIUS Attributes for IPv6 Access Networks", <u>RFC 6911</u>, DOI 10.17487/RFC6911, April 2013, <<u>https://www.rfc-editor.org/info/rfc6911</u>>.
- [RFC7037] Yeh, L. and M. Boucadair, "RADIUS Option for the DHCPv6 Relay Agent", <u>RFC 7037</u>, DOI 10.17487/RFC7037, October 2013, <<u>https://www.rfc-editor.org/info/rfc7037</u>>.
- [RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", <u>RFC 8415</u>, DOI 10.17487/RFC8415, November 2018, <<u>https://www.rfc-editor.org/info/rfc8415</u>>.

Authors' Addresses

Mohamed Boucadair Orange Rennes 35000 France

Email: mohamed.boucadair@orange.com

Christian Jacquenet Orange Rennes France

Email: christian.jacquenet@orange.com