Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 11, 2018

M. Boucadair
C. Jacquenet
Orange

October 8, 2017

RADIUS Extensions for Network-Assisted Multipath TCP (MPTCP)
draft-boucadair-mptcp-radius-05

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 MPTCP Conversion Point (MCP). 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. MCPs 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 MCPs.

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].

Table of Contents

1. Introduction

One of the promising deployment scenarios for Multipath TCP (MPTCP, [RFC6824]) is to enable a Customer Premises Equipment (CPE) that is connected to multiple networks (e.g., DSL, LTE, WLAN) to optimize the usage of such resources, see for example [RFC4908].

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. This deployment scenario relies on MPTCP proxies located on both the CPE and network sides (Figure 1).

MPTCP proxies are responsible for establishing multi-path communications on behalf of endpoints, thereby taking advantage of MPTCP capabilities to optimize resource usage to achieve different goals that include (but are not limited to) bandwidth aggregation, primary/backup communication paths, and traffic offload management.

```
  +------------+        _--------_    +----------------+
  |            |       (    LTE   )   |                |
  |   CPE      +=======+          +====+ Backbone      |
  |  (MCP)     |       (_         _)   |   Network      |
  |            |         (_______)    |+--------------+|
  |            |       IP Network #1  || Concentrator ||------> Internet
  |            |                      ||    (MCP)     ||
  |            |                      |+--------------+|
  |            |       IP Network #2  |                |
  |            |        _--------_    |                |
  |            |       (    DSL    )  |                |
  |            +=======+           +==+                |
  |            |       (_         _)   |                |
  +-----+------+        (_______)     +----------------+
        |
  ---- LAN ----
        |
    end-nodes
```

Figure 1: Network-Assisted MPTCP: Reference Architecture

Within this document, an MPTCP Conversion Point (MCP) refers to a functional element that is responsible for aggregating the traffic originated by a group of CPEs. This element is located in the network. One or multiple MCPs can be deployed in the network to assist MPTCP-enabled CPEs to establish MPTCP connections via their available network attachments. On the uplink path, the MCP terminates the MPTCP connections received from its customer-facing interfaces and transforms these connections into legacy TCP connections [RFC0793] towards upstream servers. On the downlink path, the MCP turns the legacy server's TCP connection into MPTCP connections towards its customer-facing interfaces.

This document specifies two new Remote Authentication Dial-In User Service (RADIUS, [RFC2865]) attributes that carry the MCP IP address list (Section 2). In order to accommodate both IPv4 and IPv6 deployment contexts, and given the constraints in Section 3.4 of [RFC6158], 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 Section 3.

This document assumes that the MCP(s) reachability information can be stored in Authentication, Authorization, and Accounting (AAA) servers while the CPE configuration is usually provided by means of DHCP ([RFC2131][RFC3315]). Further Network-Assisted MPTCP deployment and operational considerations are discussed in [I-D.nam-mptcp-deployment-considerations].

This specification assumes an MCP 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 CPE are managed by the same administrative entity.

This document adheres to [RFC8044] for defining the new attributes.

2. MPTCP RADIUS Attributes

2.1. MPTCP-MCP-IPv4

Description

The RADIUS MPTCP-MCP-IPv4 attribute contains the IPv4 address of an MCP that is assigned to a CPE.

Because multiple MCP IP addresses may be provisioned to an authorised CPE (that is a CPE entitled to solicit the resources of an MCP to establish MPTCP connections), multiple instances of the MPTCP-MCP-IPv4 attribute MAY be included; each instance of the attribute carries a distinct IP address.

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

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

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

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

Type

TBA (see Section 6).

Length

6

Data Type

The attribute MPTCP-MCP-IPv4 is of type ip4addr (Section 3.3 of [RFC8044]).

Value

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

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

2.2. MPTCP-MCP-IPv6

Description

The RADIUS MPTCP-MCP-IPv6 attribute contains the IPv6 address of an MCP that is assigned to a CPE.

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

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

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

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

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

Type

TBA (see Section 6).

Length

18

Data Type

The attribute MPTCP-MCP-IPv6 is of type ip6addr (Section 3.9 of [RFC8044]).

Value

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

The MPTCP-MCP-IPv6 attribute MUST NOT include multicast and host loopback addresses [RFC6890]. Anycast addresses are allowed to be included in an MPTCP-MCP-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 MPTCP-MCP-IPv6 and MPTCP-MCP-IPv4 attributes can be helpful. Typical deployment scenarios are described, for instance, in [RFC6911].

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

```
        CPE                             NAS                        AAA
   DHCPv6 client                   DHCPv6 server                 server
         |                               |                          |
         |---------DHCPv6 Solicit-------->|                          |
         |                               |----Access-Request ---->|
         |                               |                          |
         |                               |<----Access-Accept------|
         |                               |    MPTCP-MCP-IPv6       |
         |<-------DHCPv6 Advertisement----|                          |
         |        (OPTION_V6_MPTCP)       |                          |
         |                               |                          |
         |---------DHCPv6 Request-------->|                          |
         |                               |                          |
         |<---------DHCPv6 Reply----------|                          |
         |       (OPTION_V6_MPTCP)        |                          |

                     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 MCP reachability information (namely a list of IP addresses).

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

Upon change of the MCP assigned to a CPE, the RADIUS server sends a RADIUS CoA message [RFC5176] that carries the RADIUS MPTCP-MCP-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 MCP with the new one.

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

```
        CPE                                  NAS                    AAA
    DHCPv4 client                       DHCPv4 server              server
          |                                   |                         |
          |-----------DHCPDISCOVER---------->|                         |
          |                                   |----Access-Request ---->|
          |                                   |                         |
          |                                   |<----Access-Accept------|
          |                                   |    MPTCP-MCP-IPv4       |
          |<------------DHCPOFFER------------|                         |
          |          (OPTION_V4_MPTCP)        |                         |
          |                                   |                         |
          |------------DHCPREQUEST---------->|                         |
          |          (OPTION_V4_MPTCP)        |                         |
          |                                   |                         |
          |<-----------DHCPACK---------------|                         |
          |         (OPTION_V4_MPTCP)         |                         |

                        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].

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

Traffic theft is a risk if an illegitimate MCP is inserted in the path. Indeed, inserting an illegitimate MCP 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 an MCP 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.

Access-Request	Access-Accept	Access-Reject	Challenge	Acct. Request	#	Attribute
0+	0+	0	0	0+	TBA	MPTCP-MCP-IPv4
0+	0+	0	0	0+	TBA	MPTCP-MCP-IPv6

CoA-Request	CoA-ACK	CoA-NACK	#	Attribute
0+	0	0	TBA	MPTCP-MCP-IPv4
0+	0	0	TBA	MPTCP-MCP-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:

MPTCP-MCP-IPv4 (TBA)

MPTCP-MCP-IPv6 (TBA)

7. Acknowledgements

Thanks to Alan DeKok for the comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <https://www.rfc-editor.org/info/rfc6158>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC8044] DeKok, A., "Data Types in RADIUS", RFC 8044, DOI 10.17487/RFC8044, January 2017, <https://www.rfc-editor.org/info/rfc8044>.

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", draft-nam-mptcp-deployment-considerations-01 (work in progress), December 2016.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[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", RFC 4014, DOI 10.17487/RFC4014, February 2005, <https://www.rfc-editor.org/info/rfc4014>.

[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", RFC 4908, DOI 10.17487/RFC4908, June 2007, <https://www.rfc-editor.org/info/rfc4908>.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, 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", RFC 6181, DOI 10.17487/RFC6181, March 2011, <https://www.rfc-editor.org/info/rfc6181>.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, 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", RFC 6911, DOI 10.17487/RFC6911, April 2013, <https://www.rfc-editor.org/info/rfc6911>.

[RFC7037] Yeh, L. and M. Boucadair, "RADIUS Option for the DHCPv6 Relay Agent", RFC 7037, DOI 10.17487/RFC7037, October 2013, <https://www.rfc-editor.org/info/rfc7037>.

Authors' Addresses

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Christian Jacquenet
Orange
Rennes
France

Email: christian.jacquenet@orange.com