           RADIUS Extensions for Network-Assisted Multipath TCP (MPTCP)
                     draft-boucadair-mptcp-radius-01

Abstract

   One of the promising deployment scenarios for Multipath TCP (MPTCP)
   is to enable a Customer Premises Equipment (CPE) that is connected to
   multiple networks (e.g., DSL, LTE, WLAN) to optimize the usage of its
   network attachments. Because of the lack of MPTCP support at the
   server side, some service providers consider a network-assisted model
   that relies upon the activation of a dedicated function called: MPTCP
   Concentrator.

   This document specifies a new Remote Authentication Dial-In User
   Service (RADIUS) attributes that carry the IP addresses that allow
   CPE devices to reach one or multiple MPTCP Concentrators.

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].

Copyright Notice

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]. This deployment
   scenario relies on MPTCP proxies located on both the CPE and network
   sides (Figure 1). MPTCP Proxies deployed in the network play the
   role of traffic concentrator.

```
                         IP Network #1
  +-----------+         _--------_        +-----------+
  |           |        (e.g., LTE )       |           |
  |   CPE     +=====================+     |           |
  | (MPTCP    |        (_       _)  |Concentrator|
  |  Proxy)   |         (_____)  | (MPTCP     |
  |           |                     |   Proxy)   |------> Internet
  |           |                     |           |
  |           |        IP Network #2 |           |
  |           |         _--------_   |           |
  |           |        ( e.g., DSL ) |           |
  |           +=====================+ |           |
  |           |        (_       _)   |           |
  +-----+-----+         (_____)    +-----------+
        |
   ----CPE network----
        |
     end-nodes
```
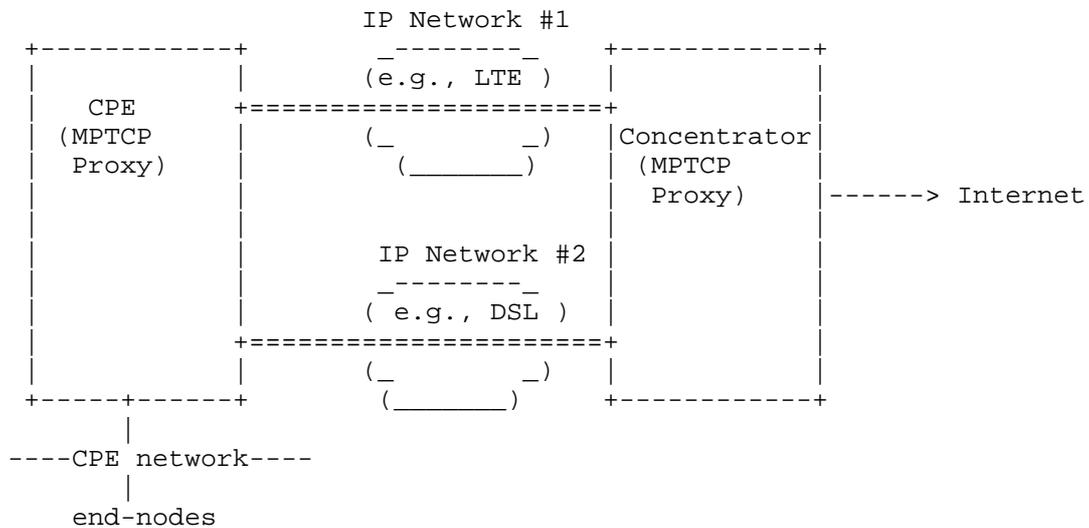
              Figure 1: "Network-Assisted" MPTCP Design

   Within this document, an MPTCP Concentrator (or concentrator) 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 concentrators 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
   concentrator terminates the MPTCP connections [RFC6824] received from
   its customer-facing interfaces and transforms these connections into
   legacy TCP connections [RFC0793] towards upstream servers. On the
   downlink path, the concentrator turns the legacy server's TCP
   connection into MPTCP connections towards its customer-facing
   interfaces.

   Both implicit (where a CPE has no specific knowledge of any
   concentrator deployed in the network) and explicit modes are
   considered to steer traffic towards an MPTCP Concentrator. This
   document focuses on the explicit mode that consists in explicitly
   configuring a CPE with the reachability information of a MPTCP
   concentrator.

   This document specifies two new Remote Authentication Dial-In User
   Service (RADIUS, [RFC2865]) attributes that carry the MPTCP
   Concentrator 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 MPTCP concentrator(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]).

This specification assumes an MPTCP Concentrator 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 [I-D.ietf-radext-datatypes] for defining the
new attributes.

2. MPTCP RADIUS Attributes

2.1. MPTCP-IPv4-Concentrator

Description

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

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

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

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

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

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

Type

   TBA (see Section 6).

Length

   6

Data Type

   The attribute MPTCP-Concentrator-IPv4 is of type ip4addr
   (Section 3.3 of [I-D.ietf-radext-datatypes]).

Value

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

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

2.2. MPTCP-IPv6-Concentrator

Description

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

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

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

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

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

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

Type

TBA (see Section 6).

Length

18

Data Type

The attribute MPTCP-Concentrator-IPv6 is of type ip6addr
(Section 3.9 of [I-D.ietf-radext-datatypes]).

Value

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

The MPTCP-Concentrator-IPv6 attribute MUST NOT include multicast
and host loopback addresses [RFC6890]. Anycast addresses are
allowed to be included in an MPTCP-Concentrator-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-Concentrator-IPv6 and
MPTCP-Concentrator-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 MPTCP
Concentrator. This example assumes that the Network Access Server
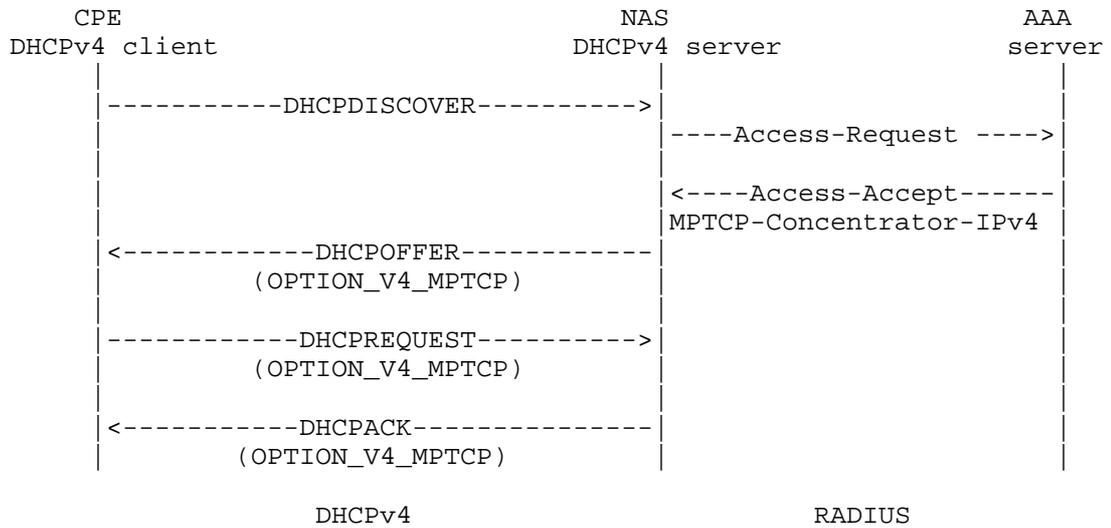(NAS) embeds both RADIUS client and DHCPv6 server capabilities.

```
        CPE                          NAS                     AAA
     DHCPv6 client               DHCPv6 server              server
        |                          |                          |
        |---------DHCPv6 Solicit-------->|                    |
        |                          |----Access-Request ---->|
        |                          |                          |
        |                          |<----Access-Accept------|
        |                          | MPTCP-Concentrator-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
   MPTCP Concentrator reachability information (namely a list of IP
   addresses).

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

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

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

```
          CPE                             NAS                      AAA
       DHCPv4 client                  DHCPv4 server               server
          |                             |                          |
          |----------DHCPDISCOVER---------->|                      |
          |                             |----Access-Request ---->|
          |                             |                          |
          |                             |<----Access-Accept------|
          |                             | MPTCP-Concentrator-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 concentrator is inserted
   in the path. Indeed, inserting an illegitimate concentrator 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 concentrator 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-Concentrator-IPv4
0+	0+	0	0	0+	TBA	MPTCP-Concentrator-IPv6

CoA-Request	CoA-ACK	CoA-NACK	#	Attribute
0+	0	0	TBA	MPTCP-Concentrator-IPv4
0+	0	0	TBA	MPTCP-Concentrator-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-Concentrator-IPv4 (TBA)

    MPTCP-Concentrator-IPv6 (TBA)

7. Acknowledgements

Thanks to Alan DeKok for the comments.

8. References

8.1. Normative References

[I-D.ietf-radext-datatypes]
          DeKok, A., "Data Types in the Remote Authentication Dial-
          In User Service Protocol (RADIUS)", draft-ietf-radext-
          datatypes-02 (work in progress), November 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119,
          DOI 10.17487/RFC2119, March 1997,
          <http://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,
          <http://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,
              <http://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,
              <http://www.rfc-editor.org/info/rfc6890>.

8.2. Informative References

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

   [RFC2131] Droms, R., "Dynamic Host Configuration Protocol",
              RFC 2131, DOI 10.17487/RFC2131, March 1997,
              <http://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, <http://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, <http://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,
              <http://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,
              <http://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,
              <http://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,
              <http://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,
              <http://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, <http://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

                    Dynamic Authorization Proxying in
         Remote Authorization Dial-In User Service Protocol (RADIUS)
                    draft-ietf-radext-coa-proxy-00.txt

   Abstract

   RFC 5176 defines Change of Authorization (CoA) and Disconnect Message
   (DM) behavior for RADIUS. Section 3.1 of that document suggests that
   proxying these messages is possible, but gives no guidance as to how
   that is done. This specification corrects that omission.

Status of this Memo

   This Internet-Draft is submitted to IETF in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   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."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on June 11, 2016.

Table of Contents

1. Introduction

   RFC 5176 [RFC5176] defines Change of Authorization (CoA) and
   Disconnect Message (DM) behavior for RADIUS. Section 3.1 of that
   document suggests that proxying these messages is possible, but gives
   no guidance as to how that is done. This ommission means that
   proxying of CoA packets is, in practice, impossible.

   We correct that ommission here by explaining how an existing RADIUS
   attribute, Operator-Name (Section 4.1 of [RFC5580]), can be used to
   record the visited network for a particular session. We then explain
   how that attribute can be used by CoA proxies to route packets
   "backwards" through a RADIUS proxy chain. We introduce a new
   attribute; Operator-NAS-Identifier, and show how this attribute can
   increase privacy about the internal implementation of the visited
   netowkr.

   We conclude with a discussion of the security implications of the
   design, and show how they are acceptable.

1.1. Terminology

   This document frequently uses the following terms:

   CoA

      Change of Authorization, e.g. CoA-Request, or CoA-ACK, or CoA-NAK,
      as defined in [RFC5176]. That specification also defines
      Disconnect-Request, Disconnect-ACK, and Disconnect-NAK. For
      simplicity here, where we use "CoA", we mean a generic "CoA-
      Request or Disconnect-Request" packet. We use "CoA-Request" or
      "Disconnect-Request" to refer to the specific packet types.

   Network Access Identifier

      The Network Access Identifier (NAI) is the user identity submitted
      by the client during network access authentication. The purpose
      of the NAI is to identify the user as well as to assist in the
      routing of the authentication request. Please note that the NAI
      may not necessarily be the same as the user's email address or the
      user identity submitted in an application layer authentication.

   Network Access Server

      The Network Access Server (NAS) is the device that clients connect
      to in order to get access to the network. In PPTP terminology,
      this is referred to as the PPTP Access Concentrator (PAC), and in
      L2TP terminology, it is referred to as the L2TP Access

Concentrator (LAC). In IEEE 802.11, it is referred to as an
Access Point.

Home Network

The network which holds the authentication credentials for a user.

Visited Network

A network other than the home network, where the user attempts to
gain network access. The Visited Network typically has a
relationship with the Home Network, and can ask the Home Network
is the user is authentic (or not).

1.2. 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 [RFC2119].

2. Problem Statement

   This section describes how RADIUS proxying works, how CoA packets
   work, and why CoA proxying does not work in the current system.

2.1. Typical RADIUS Proxying

   When a RADIUS server proxies an Access-Request packet, it typically
   does so based on the contents of the User-Name attribute, which
   contains Network Access Identifier [RFC7542]. Other methods are
   possible, but we restrict ourselves to this usage, as it is the most
   common one.

   The proxy server looks up the "Realm" portion of the NAI in a logical
   AAA routing table, as described in Section 3 of [RFC7542]. The entry
   in that table is the "next hop" to which the packet is sent. This
   "next hop" may be another proxy, or it may be the home server for
   that realm.

   If the "next hop" is a proxy, it will perform the same Realm lookup,
   and then proxy the packet. Alternatively, if the "next hop" is the
   Home Server for that realm, it will try to authenticate the user, and
   respond with an Access-Accept, Access-Reject, or Access-Challenge.

   The RADIUS client will match the response packet to an outstanding
   request. If the client is part of a proxy, it will then proxy that
   response packet in turn to the system which originated the Access-
   Request. This process occurs until the response packet arrives at
   the NAS.

   The proxies are typically stateful with respect to ongoing request /
   response packets, but stateless with respect to user sessions. Once
   a reply has been recieved by the proxy, it can discard all
   information about the user.

   The same proxy method is used for Accounting-Request packets. The
   combination of the two methods allows proxies to connect Visited
   Networks to Home Networks for all AAA purposes.

2.2. CoA Processing

   [RFC5176] describes how CoA clients send packets to CoA servers. We
   note that system comprising the CoA client is typically co-located
   with, or the same as, the RADIUS server. Similarly, the CoA server
   is a system that is either co-located with, or the same as, the
   RADIUS client.

   In the case of packets sent inside of one network, the source and

destination of CoA packets is locally determined. There is thus no
need for standardization of that process, as networks are free to
send CoA packets whenever they want, for whatever reason they want.

2.3. Failure of CoA Proxying

The situation is more complicated when multiple networks are
involved. [RFC5176] suggests that CoA proxying is permitted, but
makes no suggestions for how it should be done.

If proxies tracked user sessions, it might be possible for a proxy to
match an incoming CoA-Request to a user session, and then to proxy
that packet to the RADIUS client which originated the Access-Request
for that sessions.

There are many problems with such a scenario. The CoA server may, in
fact, not be co-located with the RADIUS client. The RADIUS client
may be down, but there may be a different CoA server which could
accept the packet. User session tracking can be expensive and
complicated for a proxy, and many proxies do not record user
sessions. Finally, [RFC5176] is silent on the topic of "session
identification attributes", which makes it impossible for a proxy to
determine if a CoA packet matches a particular user session.

The result is that CoA proxying cannot be performed when using the
behavior defined in [RFC5176].

3. How to Perform CoA Proxying

The solution to the above problem is to use the Operator-Name
attribute defined in [RFC5580], Section 4.1. We repeat portions of
that definition here for clarity:

    This attribute carries the operator namespace identifier and the
    operator name. The operator name is combined with the namespace
    identifier to uniquely identify the owner of an access network.

Followed by a description of the REALM namespace:

    REALM ('1' (0x31)):

    The REALM operator namespace can be used to indicate operator
    names based on any registered domain name. Such names are
    required to be unique, and the rights to use a given realm name
    are obtained coincident with acquiring the rights to use a
    particular Fully Qualified Domain Name (FQDN). ...

In short, the Operator-Name attribute contains the an ASCII "1",

followed by the Realm of the Visited Network. e.g. for the
"example.com" realm, the Operator-Name attribute contains the text
"1example.com". This information is precisely what we need to
perform CoA proxying.

3.1. Operator-Name in Access-Request and Accounting-Request packets

When a Visited Network proxies an Access-Request or Accounting-
Request packet outside of its network, it SHOULD include an Operator-
Name attribute in the packet, as discussed in Section 4.1 of
[RFC5580]. The contents of the Operator-Name should be "1", followed
by the realm name of the Visited Network. Where the Visited Network
has more than one realm name, one should be chosen, and used for all
packets.

Visited Networks MUST use a consistent value for Operator-Name for
one user session. That is, sending "1example.com" in an Access-
Request packet, and "1example.org" in an Accounting-Request packet
for that same session is forbidden.

Proxies which record user session information SHOULD also record
Operator-Name. Proxies which do not record user session information
SHOULD NOT record Operator-Name.

Home Networks SHOULD record Operator-Name along with other
information about user sessions. Home Networks which expect to send
CoA packets to Visited Networks MUST record Operator-Name for each
user session which originates from a Visited Network.

Networks which contain both the RADIUS client and RADIUS server do
not need to record or track Operator-Name.

3.2. Operator-Name in CoA-Request and Disconnect-Request packets

When a Home Network wishes to send a CoA-Request or Disconnect-
Request packet to a Visited Network, it MUST include an Operator-Name
attribute in the packet. The value of the Operator-Name MUST be the
value which was recorded earlier for that user session.

The Home Network MUST lookup the realm from the Operator-Name in a
logical "realm routing table", as discussed in [RFC7542] Section 3.
In this case, the destination of the packet is not a RADIUS server,
but a CoA server.

In practice, this means that CoA proxying works exactly like "normal"
RADIUS proxying, except that the proxy decision is based on the realm
from the Operator-Name attribute, instead of on the realm from the
User-Name attribute.

Proxies which receive the CoA packet MUST look up the realm from the
Operator-Name in a logical "realm routing table", as with Home
Servers, above. This process continues with any additional proxies
until the packet reaches the Visited Network.

The Visited Network can then send the CoA packet to the NAS, and
return any response packet back up the proxy chain to the Home
Server.

Networks which contain both the CoA client and CoA server do not need
to record or track Operator-Name.

3.3. Operator-NAS-Identifier

The process described in the previous section allows for CoA
proxying, but it does not support privacy for Visited Networks. That
is, all "internal" information about the Visited Network is public.
This information includes NAS-Identifier, NAS-IP-Address, NAS-
IPv6-Address, etc. We belive that the internals of the Visited
Network should be opaque to third parties.

In addition, we will see that privacy provisions can have a positive
impact on the security of the system.

The Operator-NAS-Identifier attribute contains opaque information
identifying a NAS. It MAY appear in the following packets: Access-
Request, Accounting-Request, CoA-Request, Disconnect-Request.
Operator-NAS-Identifier MUST NOT appear in any other packet.

Operator-NAS-Identifier MAY occur in a packet if the packet also
contains an Operator-Name attribute. Operator-NAS-Identifier MUST
NOT appear in a packet if there is no Operator-Name in the packet.
Operator-NAS-Identifier MUST NOT occur more than once in a packet.

An Operator-NAS-Identifer attribute SHOULD be added to an Access-
Request or Accounting-Request packet by a Visited Network just before
proxying a packet to an external RADIUS server. When the Operator-
NAS-Identifer attribute is added to a packet, the following
attributes MUST be deleted: NAS-IP-Address, NAS-IPv6-Address, NAS-
Identifier. The proxy MUST then add a NAS-Identifier attribute, in
order satisfy the requirements of Section 4.1 of [RFC2865], and of
[RFC2866].

We suggest that the contents of the NAS-Identifier be the Realm name
of the Visited Network. That is, for everyone outside of the Visited
Network, the identity NAS is the Visited Network. For the Visited
Network, the identity of the NAS is private information, which is
opaque to everyone else.

Description

An opaque token describing the NAS a user has logged into.

Type

TBD. To be assigned by IANA

Length

TBD. Depends on IANA allocation.

Implementations supporting this attribute MUST be able to handle between one (1) and twenty (20) octets of data. Implementations creating an Operator-NAS-Identifier SHOULD NOT create attributes with more than twenty octets of data. A twenty octet string is more than sufficient to individually address all of the NASes on the planet.

Data Type

string. See [DATA] Section 2.6 for a definition.

Value

The contents of this attribute are an opaque token interpretable only by the Visited Network. The attribute MUST NOT contain any secret or private information.

4. Requirements

4.1. Requirements on Home Servers

A Home Server MUST NOT send CoA packets for users who are not part of its realm. The provisions of the next few sections describe how other participants in the RADIUS ecosystem can enforce this requirement.

The Operator-NAS-Identifier attribute MUST be stored by a Home Server along with any user session identification attributes. When sending a CoA packet for a user session, the Home Server MUST include any Operator-NAS-Identifier it has recorded for that session.

4.2. Requirements on Proxies

   Section 6.1 of [RFC5176] says:

      ... a proxy MAY perform a "reverse
      path forwarding" (RPF) check to verify that a Disconnect-Request
   or
      CoA-Request originates from an authorized Dynamic Authorization
      Client.

   We change that requirement to a proxy MUST perform a "reverse path
   forwarding" (RPF) check to verify that a Disconnect-Request or CoA-
   Request originates from an authorized Dynamic Authorization Client.
   Without this change, a proxy may forward forged packets, and thus
   contribute to the forgery problem instead of preventing it.

   Proxies which record user session information MAY verify the contents
   of the CoA packet against any recorded user session data. If the
   proxy determines that the information in the packet does not match
   the recorded user session, it SHOULD return a CoA-NAK or Disconnect-
   NAK packet, which contains an Error-Cause attribute having value 503
   ("Session Context Not Found").

   Section 2.3 of [RFC5176] makes the following requirement for CoA
   servers:

         In CoA-Request and Disconnect-Request packets, all attributes
   MUST
         be treated as mandatory.

   These requirements are too stringent for a CoA proxy. Instead, we
   say that for a CoA proxy, all attributes MUST NOT be treated as
   mandatory. Proxies SHOULD perform proxying based on Operator-Name,
   but other schemes are possible (though not discussed here). Proxies
   SHOULD forward all packets as-is, with minimal changes. Only the
   final CoA server (i.e RADIUS NAS) is definitive on which attributes
   are mandatory, and which are not.

   Proxies MUST pass any Operator-Realm and Operator-NAS-Identifier
   attributes through unchanged.

   In short, proxies SHOULD behave much like a CoA server, and where
   possible, perform many of the same validations done by a CoA server.

   We recognize that because a proxy will see Access-Request and
   Accounting-Request packets, that it will have sufficient information
   to forge CoA packets. It will thus have the ability to subsequently
   disconnect any user who was authenticated via the proxy.

We suggest that the real-world effect of this security problem is minimal. Proxies can already return Access-Accept or Access-Reject for Access-Request packets, and can change authorization attributes contained in an Access-Accept. Allowing a proxy to change (or disconnect) a user session post-authentication is not substantiall different from changing (or refusing to connect) a user session during the initial process of authentiction.

There are no provisions in RADIUS for "end to end" security. That is, the Visited Network and Home Network cannot communicate privately in the presence of proxies. This limitation originates from the design of RADIUS for Access-Request and Accounting-Request packets. That limitation is then carried over to CoA-Request and Disconnect-Request packets.

We cannot therefore prevent proxies or Home Servers from forging CoA packets. We can only create scenarios where that forgery is hard to perform, and/or is likely to be detected.

4.3. Requirements on Visited Networks

A Visited Network which receives a proxied CoA packet MUST perform all of the checks discussed above for proxies. This requirement is because we assume that the Visited Network has a proxy in between the NAS and any external (i.e. third-party) proxy. Situations where a NAS sends packets directly to a third-party RADIUS server are outside of the scope of this specification.

Due to the requirements of Section 2.3 of [RFC5176], a Visited Netowkr MUST remove Operator-Name and Operator-NAS-Identifier from any CoA-Request or Disconnect-Request packet prior to proxying that packet to a CoA server.

That is, all attributes added to outbound packets by the Visited Network MUST be removed from inbound packets before sending those packets to the NAS.

We note that the above requirement applies not only to Operator-Name and Operator-NAS-Identifier, but also to any future attributes which are added by the Visited Network.

When a Visited Network may create an Operator-Name via many methods. The value SHOULD be cryptographically strong. It SHOULD be verifiable by the Visited Network, without tracking every single user session.

5. Functionality

   This section describes how the two attributes work together to permit
   CoA proxying.

5.1. User Login

   In this scenario, we follow a roaming user attempting authenticastion
   in a visited network. The login attempt is done via a visited NAS.
   That NAS will send an Access-Request packet to the visited RADIUS
   server. The visited RADIUS server will see that the user is roaming,
   and proxy the authentication request to an upstream server. That
   server may be the home server for the user, or it may be another
   proxy.

   The visited RADIUS server should add an Operator-Name attribute, with
   value "1" followed by it's own realm name. e.g. "1example.com".
   Where the visited network has multiple realms, it MUST choose a realm
   name which permits packets to be routed back to itself. The visited
   RADIUS server MAY also add an Operator-NAS-Identifier as discussed
   below.

   The upstream proxy or proxies will then forward the packet to the
   home server. Intermediate proxies MUST NOT modify the contents of,
   or delete the Operator-Name or Operator-NAS-Identifier attributes.

   The Home Server SHOULD record both Operator-Name and Operator-NAS-
   Identfier along with other information about the users session.

5.2. CoA Proxing

   When the Home Server decides to disconnect a user, it looks up the
   Operator-Name and Operator-NAS-Identifer, along with other user
   session identifiers as described in [RFC5176]. It then looks up the
   Operator-Name in the logical AAA routing table to find the CoA server
   for that realm (which may be a proxy). The CoA-Request is then sent
   to that server.

   The CoA server receives the request, and if it is a proxy, performs a
   similar lookup as done by the Home Server. The packet is then
   proxied repeatedly until it reaches the Visited Network.

   If the proxy cannot find a destination for the request, or if no
   Operator-Name attribute exists in the request, the proxy returns a
   CoA-NAK with Error-Cause 502 (Request Not Routable).

   The Visited Network recieves the CoA-Request packet, and uses the
   Operator-NAS-Identifier attribute to determine which local CoA server

(i.e. NAS) the packet should be sent to.

If no CoA server can be found, the Visited Network return a CoA-NAK with Error-Cause 403 (NAS Identification Mismatch).

Any response from the CoA server (NAS) is returned to the Home Network.

6. Security Considerations

This specification incorporates by reference the [RFC6929] Section 11. In short, RADIUS has known issues which are discussed there.

This specification adds one new attribute, and defines new behavior for RADIUS proxying. As this behavior mirrors existing RADIUS proxying, we do not believe that it introduces any new security issues.

Operator-NAS-Identifier should remain secure. We don't say how.

7. IANA Considerations

IANA is instructed to allocated one new RADIUS attribute, as per Section 3.1, above.

8. References

8.1. Normative References

[RFC2119]
    Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

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

[RFC5580]
    Tschofenig H., Ed. "Carrying Location Objects in RADIUS and Diameter", RFC 5580, August 2009.

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

[RFC7542]
    DeKok A., "The Network Access Identifier", RFC 7542, May 2015.

[DATA]
     DeKok A., "Data Types in the Remote Authentication Dial-In User
     Service Protocol (RADIUS)", draft-ietf-radext-datatypes-02.txt,
     November 2015

8.2.   Informative References

[RFC2866]
     Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC5176]
     Chiba, M. et al, "Dynamic Authorization Extensions to Remote
     Authentication Dial In User Service (RADIUS)", RFC 5176, January
     2008.

Acknowledgments

   Stuff

Authors' Addresses

   Alan DeKok
   The FreeRADIUS Server Project

   Email: aland@freeradius.org

   Jouni Korhonen
   Broadcom Corporation
   3151 Zanker Road
   San Jose, California 95134
   United States
   EMail: jouni.nospam@gmail.com

Network Working Group   D. Cheng
Internet-Draft   Huawei
Intended status: Standards Track   J. Korhonen
Expires: September 15, 2016   Broadcom Corporation
                                                           M. Boucadair
                                                                 Orange
                                                           S. Sivakumar
                                                          Cisco Systems
                                                         March 14, 2016

        RADIUS Extensions for IP Port Configuration and Reporting
                draft-ietf-radext-ip-port-radius-ext-08

Abstract

   This document defines three new RADIUS attributes. For devices that
   implementing IP port ranges, these attributes are used to communicate
   with a RADIUS server in order to configure and report TCP/UDP ports
   and ICMP identifiers, as well as mapping behavior for specific hosts.
   This mechanism can be used in various deployment scenarios such as
   Carrier-Grade NAT, IPv4/IPv6 translators, Provider WLAN Gateway, etc.

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].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   In a broadband network, customer information is usually stored on a
   RADIUS server [RFC2865]. At the time when a user initiates an IP
   connection request, if this request is authorized, the RADIUS server
   will populate the user's configuration information to the Network
   Access Server (NAS), which is often referred to as a Broadband
   Network Gateway (BNG) in broadband access networks. The Carrier-
   Grade NAT (CGN) function may also be implemented on the BNG. Within
   this document, the CGN may perform NAT44 [RFC3022], NAT64 [RFC6146],
   or Dual-Stack Lite AFTR [RFC6333] function. In such case, the CGN
   TCP/UDP port (or ICMP identifier) mapping(s) behavior(s) can be part
   of the configuration information sent from the RADIUS server to the
   NAS/BNG. The NAS/BNG may also report to the RADIUS Server the port/
   identifier mapping behavior applied by the CGN to a user session to
   the RADIUS server, as part of the accounting information sent from
   the NAS/BNG to a RADIUS server.

   When IP packets traverse the CGN, it performs TCP/UDP source port
   mapping or ICMP identifier mapping as required. A TCP/ UDP source
   port or ICMP identifier, along with source IP address, destination IP
   address, destination port and protocol identifier if applicable,
   uniquely identify a session. Since the number space of TCP/UDP ports
   and ICMP identifiers in CGN's external realm is shared among multiple
   users assigned with the same IPv4 address, the total number of a
   user's simultaneous IP sessions is likely to be subject to port quota
   (see Section 5 of [RFC6269]).

   The attributes defined in this document may also be used to report
   the assigned port range in some deployments such as Provider WLAN
   [I-D.gundavelli-v6ops-community-wifi-svcs]. For example, a visiting
   host can be managed by a CPE (Customer Premises Equipment) which
   will need to report the assigned port range to the service platform.
   This is required for identification purposes (see TR-146 [TR-146] for
   more details).

   This document proposes three new attributes as RADIUS protocol's
   extensions, and they are used for separate purposes as follows:

   1. IP-Port-Limit-Info: This attribute may be carried in RADIUS
       Access-Accept, Access-Request, Accounting-Request or CoA-Request

packet. The purpose of this attribute is to limit the total
number of TCP/UDP ports and/or ICMP identifiers allocated to a
user, associated with one or more IPv4 addresses.

2. IP-Port-Range: This attribute may be carried in RADIUS
Accounting-Request packet. The purpose of this attribute is to
report by an address sharing device (e.g., a CGN) to the RADIUS
server the range of TCP/UDP ports and/or ICMP identifiers that
have been allocated or deallocated associated with a given IPv4
address for a user.

3. IP-Port-Forwarding-Map: This attribute may be carried in RADIUS
Access-Accept, Access-Request, Accounting-Request or CoA-Request
packet. The purpose of this attribute is to specify how an IPv4
address and a TCP/ UDP port (or an ICMP identifier) is mapped to
another IPv4 address and a TCP/UDP port (or an ICMP identifier).

IPFIX Information Elements [RFC7012] can be used for IP flow
identification and representation over RADIUS. This document
provides a mapping between RADIUS TLV and IPFIX Information Element
Identifiers. As a consequence, new IPFIX Information Elements are
defined by this document (see Section 3).

2. Terminology

This document makes use of the following terms:

o IP Port: refers to the port numbers of IP transport protocols,
including TCP port, UDP port and ICMP identifier.

o IP Port Type: refers to one of the following: (1) TCP/UDP port and
ICMP identifier, (2) TCP port and UDP port, (3) TCP port, (4) UDP
port, or (5) ICMP identifier.

o IP Port Limit: denotes the maximum number of IP ports for a
specific IP port type, that a device supporting port ranges can
use when performing port number mapping for a specific user.
Note, this limit is usually associated with one or more IPv4
addresses.

o IP Port Range: specifies a set of contiguous IP ports, indicated
by the lowest numerical number and the highest numerical number,
inclusively.

o Internal IP Address: refers to the IP address that is used as a
source IP address in an outbound IP packet sent towards a device
supporting port ranges in the internal realm.

   o External IP Address: refers to the IP address that is used as a
      source IP address in an outbound IP packet after traversing a
      device supporting port ranges in the external realm.

   o Internal Port: is a UDP or TCP port, or an ICMP identifier, which
      is allocated by a host or application behind a device supporting
      port ranges for an outbound IP packet in the internal realm.

   o External Port: is a UDP or TCP port, or an ICMP identifier, which
      is allocated by a device supporting port ranges upon receiving an
      outbound IP packet in the internal realm, and is used to replace
      the internal port that is allocated by a user or application.

   o External realm: refers to the networking segment where external IP
      addresses are used in respective of the device supporting port
      ranges.

   o Internal realm: refers to the networking segment that is behind a
      device supporting port ranges and where internal IP addresses are
      used.

   o Mapping: associates with a device supporting port ranges for a
      relationship between an internal IP address, internal port and the
      protocol, and an external IP address, external port, and the
      protocol.

   o Port-based device: a device that is capable of providing IP
      address and IP port mapping services and in particular, with the
      granularity of one or more subsets within the 16-bit IP port
      number range. A typical example of this device is a CGN, CPE,
      Provider WLAN Gateway, etc.

   Note that the definitions of "internal IP address", "internal port",
   "internal realm", "external IP address", "external port", "external
   realm", and "mapping" are the same as defined in Port Control
   Protocol (PCP) [RFC6887], and the Common Requirements for Carrier-
   Grade NATs (CGNs) [RFC6888].

3. Extensions of RADIUS Attributes and TLVs

   These three new attributes are defined in the following sub-sections:

   1. IP-Port-Limit-Info Attribute

   2. IP-Port-Range Attribute

   3. IP-Port-Forwarding-Map Attribute

All these attributes are allocated from the RADIUS "Extended Type" code space per [RFC6929].

These attributes and their embedded TLVs (refer to Section 3.2) are defined with globally unique names and follow the guideline in Section 2.7.1 of [RFC6929].

In all the figures describing the RADIUS attributes and TLV formats in the following sub-sections, the fields are transmitted from left to right.

3.1. Extended Attributes for IP Ports

3.1.1. IP-Port-Limit-Info Attribute

This attribute is of type "TLV" as defined in the RADIUS Protocol Extensions [RFC6929]. It contains the following sub-attributes:

o   an IP-Port-Type TLV (see Section 3.2.1),

o   an IP-Port-Limit TLV (see Section 3.2.2),

o   an optional IP-Port-Ext-IPv4-Addr TLV (see Section 3.2.3).

It specifies the maximum number of IP ports as indicated in IP-Port-Limit TLV, of a specific port type as indicated in IP-Port-Type TLV, and associated with a given IPv4 address as indicated in IP-Port-Ext-IPv4-Addr TLV for an end user.

Note that when IP-Port-Ext-IPv4-Addr TLV is not included as part of the IP-Port-Limit-Info Attribute, the port limit applies to all the IPv4 addresses managed by the port device, e.g., a CGN or NAT64 device.

The IP-Port-Limit-Info Attribute MAY appear in an Access-Accept packet. It MAY also appear in an Access-Request packet as a preferred maximum number of IP ports indicated by the device supporting port ranges co-located with the NAS, e.g., a CGN or NAT64. However, the RADIUS server is not required to honor such a preference.

The IP-Port-Limit-Info Attribute MAY appear in a CoA-Request packet.

The IP-Port-Limit-Info Attribute MAY appear in an Accounting-Request packet.

The IP-Port-Limit-Info Attribute MUST NOT appear in any other RADIUS packet.

The format of the IP-Port-Limit-Info Attribute is shown in Figure 1.

```
 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     | Extended-Type |   Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1

Type

   241 (To be confirmed by IANA).

Length

   This field indicates the total length in bytes of all fields of
   this attribute, including the Type, Length, Extended-Type, and the
   entire length of the embedded TLVs.

Extended-Type

   TBD1.

Value

   This field contains a set of TLVs as follows:

   IP-Port-Type TLV

      This TLV contains a value that indicates the IP port type.
      Refer to Section 3.2.1.

   IP-Port-Limit TLV

      This TLV contains the maximum number of IP ports of a specific
      IP port type and associated with a given IPv4 address for an
      end user. This TLV must be included in the IP-Port-Limit-Info
      Attribute. Refer to Section 3.2.2.

   IP-Port-Ext-IPv4-Addr TLV

      This TLV contains the IPv4 address that is associated with the
      IP port limit contained in the IP-Port-Limit TLV. This TLV is
      optionally included as part of the IP-Port-Limit-Info
      Attribute. Refer to Section 3.2.3.

   IP-Port-Limit-Info Attribute is associated with the following
   identifier: 241.Extended-Type(TBD1).

3.1.2. IP-Port-Range Attribute

   This attribute is of type "TLV" as defined in the RADIUS Protocol
   Extensions [RFC6929]. It contains the following sub-attributes:

   o an IP-Port-Type TLV (see Section 3.2.1),

   o an IP-Port-Range-Start TLV (see Section 3.2.9),

   o an IP-Port-Range-End TLV (see Section 3.2.10),

   o an IP-Port-Alloc TLV (see Section 3.2.8),

   o an optional IP-Port-Ext-IPv4-Addr TLV (see Section 3.2.3),

   o an optional IP-Port-Local-Id TLV (see Section 3.2.11).

   This attribute contains a range of contiguous IP ports of a specific
   port type and associated with an IPv4 address that are either
   allocated or deallocated by a device for a given user, and the
   information is intended to be sent to RADIUS server.

   This attribute can be used to convey a single IP port number; in such
   case IP-Port-Range-Start and IP-Port-Range-End conveys the same
   value.

   Within an IP-Port-Range Attribute, the IP-Port-Alloc TLV is always
   included. For port allocation, both IP-Port-Range-Start TLV and IP-
   Port-Range-End TLV must be included; for port deallocation, the
   inclusion of these two TLVs is optional and if not included, it
   implies that all ports that are previously allocated are now
   deallocated. Both IP-Port-Ext-IPv4-Addr TLV and IP-Port-Local-Id TLV
   are optional and if included, they are used by a port device (e.g., a
   CGN device) to identify the end user.

   The IP-Port-Range Attribute MAY appear in an Accounting-Request
   packet.

   The IP-Port-Range Attribute MUST NOT appear in any other RADIUS
   packet.

   The format of the IP-Port-Range Attribute is shown in Figure 2.

```
 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      | Extended-Type |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
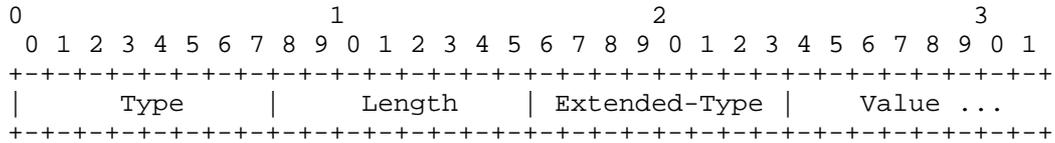

                             Figure 2

   Type

      241 (To be confirmed by IANA).

   Length

      This field indicates the total length in bytes of all fields of
      this attribute, including the Type, Length, Extended-Type, and the
      entire length of the embedded TLVs.

   Extended-Type

      TBD2.

   Value

      This field contains a set of TLVs as follows:

      IP-Port-Type TLV

         This TLV contains a value that indicates the IP port type.
         Refer to Section 3.2.1.

      IP-Port-Alloc TLV

         This TLV contains a flag to indicate that the range of the
         specified IP ports for either allocation or deallocation. This
         TLV must be included as part of the IP-Port-Range Attribute.
         Refer to Section 3.2.8.

      IP-Port-Range-Start TLV

         This TLV contains the smallest port number of a range of
         contiguous IP ports. To report the port allocation, this TLV
         must be included together with IP-Port-Range-End TLV as part of
         the IP-Port-Range Attribute. Refer to Section 3.2.9.

      IP-Port-Range-End TLV

This TLV contains the largest port number of a range of
contiguous IP ports. To report the port allocation, this TLV
must be included together with IP-Port-Range-Start TLV as part
of the IP-Port-Range Attribute. Refer to Section 3.2.10.

IP-Port-Ext-IPv4-Addr TLV

This TLV contains the IPv4 address that is associated with the
IP port range, as collectively indicated in the IP-Port-Range-
Start TLV and the IP-Port-Range-End TLV. This TLV is
optionally included as part of the IP-Port-Range Attribute.
Refer to Section 3.2.3.

IP-Port-Local-Id TLV

This TLV contains a local session identifier at the customer
premise, such as MAC address, interface ID, VLAN ID, PPP
sessions ID, VRF ID, IPv6 address/prefix, etc. This TLV is
optionally included as part of the IP-Port-Range Attribute.
Refer to Section 3.2.11.

The IP-Port-Range attribute is associated with the following
identifier: 241.Extended-Type(TBD2).

3.1.3. IP-Port-Forwarding-Map Attribute

This attribute is of type "TLV" as defined in the RADIUS Protocol
Extensions [RFC6929]. It contains the following sub-attributes:

o an IP-Port-Type TLV (see Section 3.2.1),

o an IP-Port-Int-Port TLV (see Section 3.2.6),

o an IP-Port-Ext-Port TLV (see Section 3.2.7),

o either an IP-Port-Int-IPv4-Addr TLV (see Section 3.2.4) or an IP-
   Port-Local-Id TLV (see Section 3.2.11),

o either an IP-Port-Int-IPv6-Addr TLV (see Section 3.2.5) or an IP-
   Port-Local-Id TLV (see Section 3.2.11),

o an IP-Port-Ext-IPv4-Addr TLV (see Section 3.2.3).

The attribute contains a 2-byte IP internal port number that is
associated with an internal IPv4 or IPv6 address, or a locally
significant identifier at the customer site, and a 2-byte IP external
port number that is associated with an external IPv4 address. The

internal IPv4 or IPv6 address, or the local identifier must be
included; the external IPv4 address may also be included.

The IP-Port-Forwarding-Map Attribute MAY appear in an Access-Accept
packet. It MAY also appear in an Access-Request packet to indicate a
preferred port mapping by the device co-located with NAS. However
the server is not required to honor such a preference.

The IP-Port-Forwarding-Map Attribute MAY appear in a CoA-Request
packet.

The IP-Port-Forwarding-Map Attribute MAY also appear in an
Accounting-Request packet.

The IP-Port-Forwarding-Map Attribute MUST NOT appear in any other
RADIUS packet.

The format of the IP-Port-Forwarding-Map Attribute is shown in
Figure 3.

```
 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     | Extended-Type |   Value ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
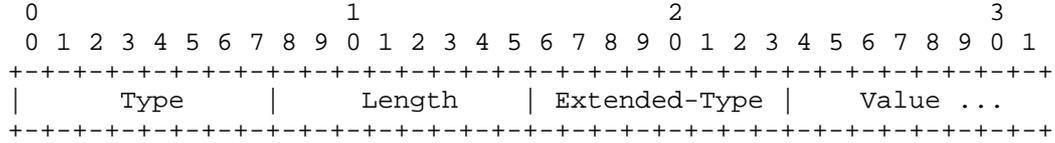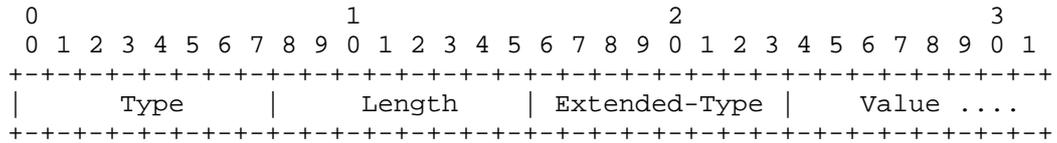
Figure 3

Type

   241 (To be confirmed by IANA).

Length

   This field indicates the total length in bytes of all fields of
   this attribute, including the Type, Length, Extended-Type, and the
   entire length of the embedded TLVs.

Extended-Type

   TBD3.

Value

   This field contains a set of TLVs as follows:

   IP-Port-Type TLV

This TLV contains a value that indicates the IP port type.
Refer to Section 3.2.1.

IP-Port-Int-Port TLV

This TLV contains an internal IP port number associated with an
internal IPv4 or IPv6 address. This TLV must be included
together with IP-Port-Ext-Port TLV as part of the IP-Port-
Forwarding-Map attribute. Refer to Section 3.2.6.

IP-Port-Ext-Port TLV

This TLV contains an external IP port number associated with an
external IPv4 address. This TLV must be included together with
IP-Port-Int-Port TLV as part of the IP-Port-Forwarding-Map
attribute. Refer to Section 3.2.7.

IP-Port-Int-IPv4-Addr TLV

This TLV contains an IPv4 address that is associated with the
internal IP port number contained in the IP-Port-Int-Port TLV.
For IPv4 network, either this TLV or IP-Port-Local-Id TLV must
be included as part of the IP-Port-Forwarding-Map Attribute.
Refer to Section 3.2.4.

IP-Port-Int-IPv6-Addr TLV

This TLV contains an IPv4 address that is associated with the
internal IP port number contained in the IP-Port-Int-Port TLV.
For IPv6 network, either this TLV or IP-Port-Local-Id TLV must
be included as part of the IP-Port-Forwarding-Map Attribute.
Refer to Section 3.2.5.

IP-Port-Local-Id TLV

This TLV contains a local session identifier at the customer
premise, such as MAC address, interface ID, VLAN ID, PPP
sessions ID, VRF ID, IPv6 address/prefix, etc. Either this TLV
or IP-Port-Int-IP-Addr TLV must be included as part of the IP-
Port-Forwarding-Map Attribute. Refer to Section 3.2.11.

IP-Port-Ext-IPv4-Addr TLV

This TLV contains an IPv4 address that is associated with the
external IP port number contained in the IP-Port-Ext-Port TLV.
This TLV may be included as part of the IP-Port-Forwarding-Map
Attribute. Refer to Section 3.2.3.

   The IP-Port-Forwarding-Map Attribute is associated with the following
   identifier: 241.Extended-Type(TBD3).

3.2. RADIUS TLVs for IP Ports

   The TLVs that are included in the three attributes (see Section 3.1)
   are defined in the following sub-sections. These TLVs use the format
   defined in [RFC6929].

3.2.1. IP-Port-Type TLV

   The format of IP-Port-Type TLV is shown in Figure 4. Its "Type"
   field contains a value that uniquely refers to IPFIX Information
   Element "transportType" (TBAx1), and its "Value" field contains the
   values defined for the IPFIX Information Element "transportType",
   which indicates the type of IP transport as follows:

   1:

      Refer to TCP port, UDP port, and ICMP identifier as a whole.

   2:

      Refer to TCP port and UDP port as a whole.

   3:

      Refer to TCP port only.

   4:

      Refer to UDP port only.

   5:

      Refer to ICMP identifier only.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   TLV-Type    |    Length     |          transportType
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         transportType         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
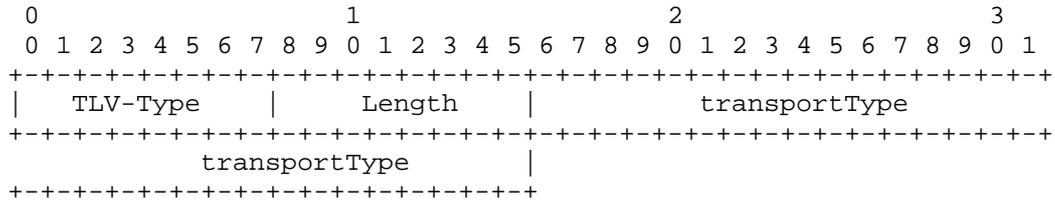
                             Figure 4

   TLV-Type

   1. This MUST uniquely refer to the IPFIX Information Element
       identifier TBAx1.

Length

   6.

transportType

   Integer. This field contains the data (unsigned8) of
   transportType (TBAx1) defined in IPFIX, right justified, and the
   unused bits in this field MUST be set to zero.

IP-Port-Type TLV is included in the following Attributes:

o IP-Port-Limit-Info Attribute, identified as 241.TBD1.1 (see
   Section 3.1.1).

o IP-Port-Range Attribute, identified as 241.TBD2.1 (see
   Section 3.1.2).

o IP-Port-Forwarding-Mapping Attribute, identified as 241.TBD3.1
   (see Section 3.1.3).

3.2.2. IP-Port-Limit TLV

The format of IP-Port-Limit TLV is shown in Figure 5. Its "Type"
field contains a value that uniquely refers to IPFIX Information
Element natTransportLimit (TBAx2), and its "Value" field contains
IPFIX Information Element natTransportLimit, which indicates the
maximum number of ports for a given IPv4 address assigned to a user
for a specified IP-Port-Type.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type   |     Length    |         natTransportLimit
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        natTransportLimit       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                            Figure 5

TLV-Type

   2. It MUST uniquely refer to the IPFIX Information Element
       identifier TBAx2.

Length

   6.

natTransportLimit

   Integer. This field contains the data (unsigned16) of
   natTransportLimit (TBAx2) defined in IPFIX, right justified, and
   the unused bits in this field MUST be set to zero.

IP-Port-Limit TLV is included as part of the IP-Port-Limit-Info
Attribute (refer to Section 3.1.1), identified as 241.TBD1.2.

3.2.3. IP-Port-Ext-IPv4-Addr TLV

The format of IP-Port-Ext-IPv4-Addr TLV is shown in Figure 6. Its
"Type" field contains a value that uniquely refers to IPFIX
Information Element postNATSourceIPv4Address(225), and its "Value"
field contains IPFIX Information Element postNATSourceIPv4Address,
which is the IPv4 source address after NAT operation (refer to
[IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   TLV-Type    |    Length     |    postNATSourceIPv4Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    postNATSourceIPv4Address   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                          Figure 6

TLV-Type

   3. This MUST uniquely refer to the IPFIX Information Element
   identifier 225.

Length

   6

postNATSourceIPv4Address

   Integer. This field contains the data (ipv4Address) of
   postNATSourceIPv4Address (225) defined in IPFIX.

IP-Port-Ext-IPv4-Addr TLV MAY be included in the following
Attributes:

   o IP-Port-Limit-Info Attribute, identified as 241.TBD1.3 (see
      Section 3.1.1).

   o IP-Port-Range Attribute, identified as 241.TBD2.3 (see
      Section 3.1.2).

   o IP-Port-Forwarding-Mapping Attribute, identified as 241.TBD3.3
      (see Section 3.1.3).

3.2.4. IP-Port-Int-IPv4-Addr TLV

   The format of IP-Port-Int-IPv4 TLV is shown in Figure 7. Its "Type"
   field contains a value that uniquely refers to IPFIX Information
   Element sourceIPv4Address (8), and its "Value" field contains IPFIX
   Information Element sourceIPv4Address, which is the IPv4 source
   address before NAT operation (refer to [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type    |     Length    |         sourceIPv4Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       sourceIPv4Address         |
+-+--+-+-+-+-+-++-+-+-+-+-+-+-+-+-+
```

                                Figure 7

   TLV-Type

      4. It MUST uniquely refer to the IPFIX Information Element
      identifier 8.

   Length

      6.

   sourceIPv4Address

      Integer. This field contains the data (ipv4Address) of
      sourceIPv4Address (8) defined in IPFIX.

   IP-Port-Int-IPv4-Addr TLV MAY be included as part of the IP-Port-
   Forwarding-Map Attribute (refer to Section 3.1.3), identified as
   241.TBD3.4.

3.2.5. IP-Port-Int-IPv6-Addr TLV

   The format of IP-Port-Int-IPv6-Addr TLV is shown in Figure 8. Its
   "Type" field contains a value that uniquely refers to IPFIX
   Information Element sourceIPv6Address(27), and its "Value" field
   contains IPFIX Information Element sourceIPv6Address, which is the
   IPv6 source address before NAT operation (refer to [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type    |      Length     |         sourceIPv6Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                     sourceIPv6Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                     sourceIPv6Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                     sourceIPv6Address
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        sourceIPv6Address      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                              Figure 8

   TLV-Type

      5. It MUST uniquely refer to the IPFIX Information Element
      identifier 27.

   Length

      18.

   sourceIPv6Address

      IPv6 address (128 bits). This field contains the data
      (ipv6Address) of sourceIPv6Address (27) defined in IPFIX.

   IP-Port-Int-IPv6-Addr TLV MAY be included as part of the IP-Port-
   Forwarding-Map Attribute (refer to Section 3.1.3), identified as
   241.TBD3.5.

3.2.6. IP-Port-Int-Port TLV

   The format of IP-Port-Int-Port TLV is shown in Figure 9. Its "Type"
   field contains a value that uniquely refers to IPFIX Information
   Element sourceTransportPort (7), and its "Value" field contains IPFIX
   Information Element sourceTransportPort, which is the source

transport number associated with an internal IPv4 or IPv6 address
(refer to [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type   |    Length    |       sourceTransportPort
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       sourceTransportPort    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
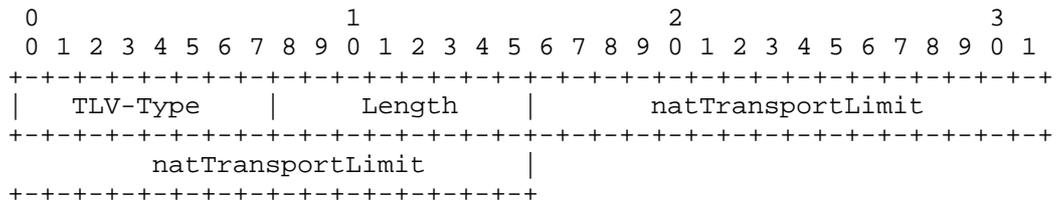
Figure 9

TLV-Type

   6. It MUST uniquely refer to the IPFIX Information Element
   identifier 7.

Length

   4.

sourceTransportPort

   Integer. This field contains the data (unsigned16) of
   sourceTrasnportPort (7) defined in IPFIX, right justified, and
   unused bits MUST be set to zero.

   IP-Port-Int-Port TLV is included as part of the IP-Port-Forwarding-
   Map Attribute (refer to Section 3.1.3), identified as 241.TBD3.6.

3.2.7. IP-Port-Ext-Port TLV

   The format of IP-Port-Ext-Port TLV is shown in Figure 10. Its "Type"
   field contains a value that uniquely refers to IPFIX Information
   Element postNAPTSourceTransportPort (227), and its "Value" field
   contains IPFIX Information Element postNAPTSourceTransportPort, which
   is the transport number associated with an external IPv4
   address(refer to [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type    |     Length    |   postNAPTSourceTransportPort
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   postNAPTSourceTransportPort   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

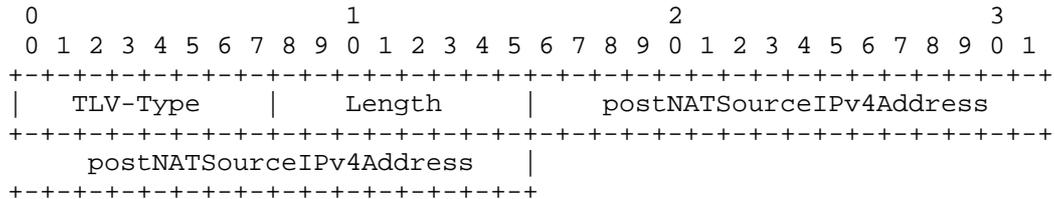   Figure 10

   TLV-Type

      7. It MUST uniquely refer to the IPFIX Information Element
      identifier 227 .

   Length

      6.

   postNAPTSourceTransportPort

      Integer. This field contains the data (unsigned16) of
      postNAPTSourceTrasnportPort (227) defined in IPFIX, right
      justified, and unused bits must be set to zero.

   IP-Port-Ext-Port TLV is included as part of the IP-Port-Forwarding-
   Map Attribute (refer to Section 3.1.3), identified as 241.TBD3.7.

3.2.8. IP-Port-Alloc TLV

   The format of IP-Port-Alloc TLV is shown in Figure 11. Its "Type"
   field contains a value that uniquely refers to IPFIX Information
   Element natEvent (230), and its "Value" field contains IPFIX
   Information Element "natEvent", which is a flag to indicate an action
   of NAT operation (refer to [IPFIX]).

   When the value of natEvent is "1" (Create event), it means to
   allocate a range of transport ports; when the value is "2", it means
   to deallocate a range of transports ports. For the purpose of this
   TLV, no other value is used.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type   |     Length    |              natEvent
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           natEvent            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
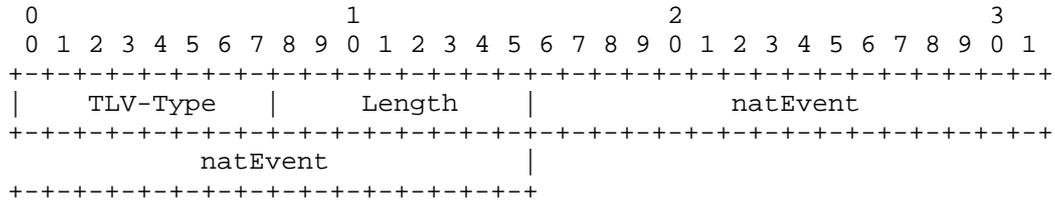
                          Figure 11
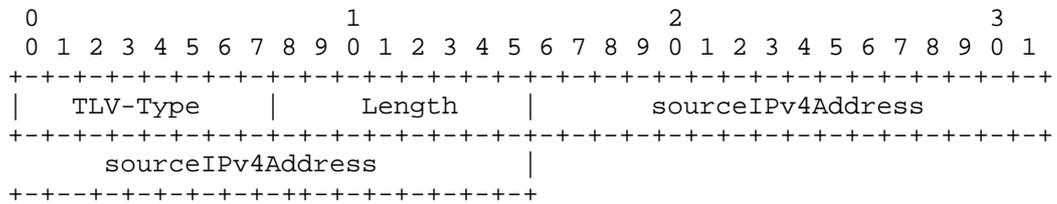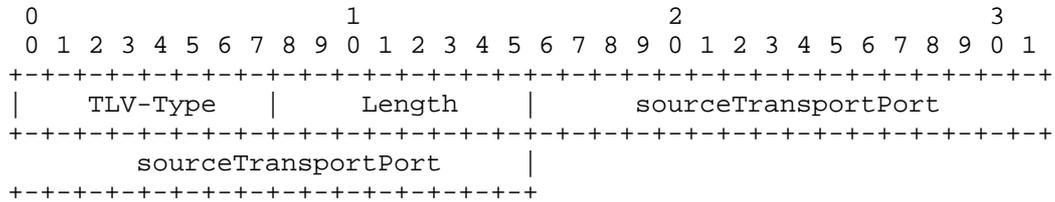
   TLV-Type

      8. It MUST uniquely refer to the IPFIX Information Element
      identifier 230 .

   Length

      3.

   natEvent

      Integer. This field contains the data (unsigned8) of natEvent
      (230) defined in IPFIX, right justified, and unused bits must be
      set to zero. It indicates the allocation or deallocation of a
      range of IP ports as follows:

      1:

         Allocation

      2:

         Deallocation

   Reserved:

      0.

   IP-Port-Alloc TLV is included as part of the IP-Port-Range Attribute
   (refer to Section 3.1.2), identified as 241.TBD2.8.

3.2.9. IP-Port-Range-Start TLV

   The format of IP-Port-Range-Start TLV is shown in Figure 12. Its
   "Type" field contains a value that uniquely refers to IPFIX
   Information Element portRangeStart (361), and its "Value" field
   contains IPFIX Information Element portRangeStart, which is the

smallest port number of a range of contiguous transport ports (refer
to [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type   |     Length    |          portRangeStart
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         portRangeStart         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
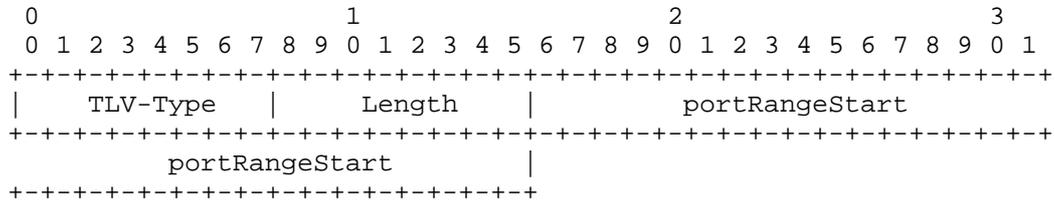

                             Figure 12
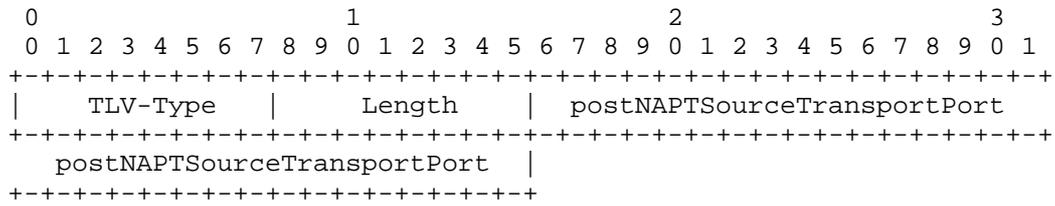
   TLV-Type

      9. It MUST uniquely refer to the IPFIX Information Element
      identifier 361.

   Length

      4.

   portRangeStart

      Integer. This field contains the data (unsigned16) of (361)
      defined in IPFIX, right justified, and unused bits must be set to
      zero.

   IP-Port-Range-Start TLV is included as part of the IP-Port-Range
   Attribute (refer to Section 3.1.2), identified as 241.TBD2.9.

3.2.10. IP-Port-Range-End TLV

   The format of IP-Port-Range-End TLV is shown in Figure 13. Its
   "Type" field contains a value that uniquely refers to IPFIX
   Information Element portRangeEnd (362), and its "Value" field
   contains IPFIX Information Element portRangeEnd, which is the largest
   port number of a range of contiguous transport ports (refer to
   [IPFIX]).

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    TLV-Type   |    Length     |          portRangeEnd
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         portRangeEnd           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
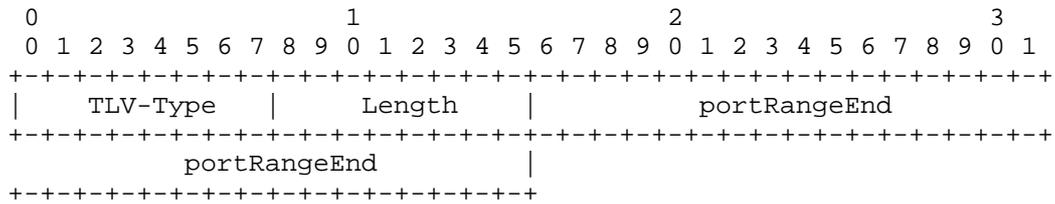
                          Figure 13

   TLV-Type

      10. It MUST uniquely refer to the IPFIX Information Element
      identifier 362.

   Length

      4. The Length field for IP-Port-Range-End TLV.

   portRangeEnd

      Integer. This field contains the data (unsigned16) of (362)
      defined in IPFIX, right justified, and unused bits must be set to
      zero.

   IP-Port-Range-End TLV is included as part of the IP-Port-Range
   Attribute (refer to Section 3.1.2), identified as 241.TBD2.10.

3.2.11. IP-Port-Local-Id TLV

   The format of IP-Port-Local-Id TLV is shown in Figure 14. Its "Type"
   field contains a value that uniquely refers to the IPFIX Information
   Element localID (TBAx3), and its "Value" field contains IPFIX
   Information Element localID, which is a local significant identifier
   as explained below.

   In some CGN deployment scenarios such as DS-Extra-Lite [RFC6619] and
   Lightweight 4over6 [RFC7596], parameters at a customer premise such
   as MAC address, interface ID, VLAN ID, PPP session ID, IPv6 prefix,
   VRF ID, etc., may also be required to pass to the RADIUS server as
   part of the accounting record.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   TLV-Type    |     Length    |          localID ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
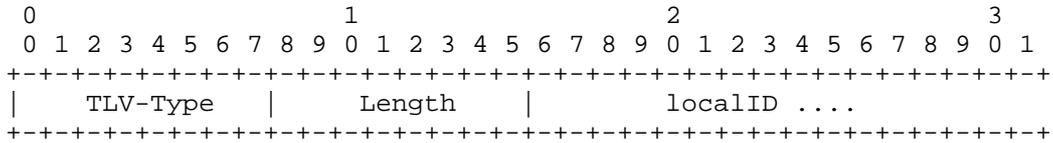
                             Figure 14

   TLV-Type

      11. This MUST uniquely refer to the IPFIX Information Element
      identifier TBAx3.

   Length

      Variable number of bytes.

   localID

      string. This field contains the data (string) of (TBAx3) defined
      in IPFIX. This is a local session identifier at the customer
      premise, such as MAC address, interface ID, VLAN ID, PPP sessions
      ID, VRF ID, IPv6 address/prefix, etc.

   IP-Port-Local-Id TLV MAY be included in the following Attributes:

   o IP-Port-Range Attribute, identified as 241.TBD2.11 (see
      Section 3.1.2).

   o IP-Port-Forwarding-Mapping Attribute, identified as 241.TBD3.11
      (see Section 3.1.3).

4. Applications, Use Cases and Examples

   This section describes some applications and use cases to illustrate
   the use of the attributes proposed in this document.

4.1. Managing CGN Port Behavior using RADIUS

   In a broadband network, customer information is usually stored on a
   RADIUS server, and the BNG acts as a NAS. The communication between
   the NAS and the RADIUS server is triggered by a user when it signs in
   to the Internet service, where either PPP or DHCP/DHCPv6 is used.
   When a user signs in, the NAS sends a RADIUS Access-Request message
   to the RADIUS server. The RADIUS server validates the request, and
   if the validation succeeds, it in turn sends back a RADIUS Access-
   Accept message. The Access-Accept message carries configuration

information specific to that user, back to the NAS, where some of the
information would pass on to the requesting user via PPP or DHCP/
DHCPv6.

A CGN function in a broadband network would most likely co-located on
a BNG. In that case, parameters for CGN port/identifier mapping
behavior for users can be configured on the RADIUS server. When a
user signs in to the Internet service, the associated parameters can
be conveyed to the NAS, and proper configuration is accomplished on
the CGN device for that user.

Also, CGN operation status such as CGN port/identifier allocation and
deallocation for a specific user on the BNG can also be transmitted
back to the RADIUS server for accounting purpose using the RADIUS
protocol.

RADIUS protocol has already been widely deployed in broadband
networks to manage BNG, thus the functionality described in this
specification introduces little overhead to the existing network
operation.

In the following sub-sections, we describe how to manage CGN behavior
using RADIUS protocol, with required RADIUS extensions proposed in
Section 3.

4.1.1. Configure IP Port Limit for a User

In the face of IPv4 address shortage, there are currently proposals
to multiplex multiple users' connections over a smaller number of
shared IPv4 addresses, such as Carrier Grade NAT [RFC6888], Dual-
Stack Lite [RFC6333], NAT64 [RFC6146], etc. As a result, a single
IPv4 public address may be shared by hundreds or even thousands of
users. As indicated in [RFC6269], it is therefore necessary to
impose limits on the total number of ports available to an individual
user to ensure that the shared resource, i.e., the IPv4 address,
remains available in some capacity to all the users using it. The
support of IP port limit is also documented in [RFC6888] as a
requirement for CGN.

The IP port limit imposed to a specific user may be on the total
number of TCP and UDP ports plus the number of ICMP identifiers, or
with other granularities as defined in Section 3.1.1.

The per-user based IP port limit is configured on a RADIUS server,
along with other user information such as credentials. The value of
this IP port limit is based on service agreement and its
specification is out of the scope of this document.

When a user signs in to the Internet service successfully, the IP
port limit for the subscriber is passed by the RADIUS server to the
BNG, acting as a NAS and co-located with the CGN, using a new RADIUS
attribute called IP-Port-Limit-Info (defined in Section 3.1.1), along
with other configuration parameters. While some parameters are
passed to the user, the IP port limit is recorded on the CGN device
for imposing the usage of TCP/UDP ports and ICMP identifiers for that
user.

Figure 15 illustrates how RADIUS protocol is used to configure the
maximum number of TCP/UDP ports for a given user on a NAT44 device.

```
User                         NAT44/NAS                    AAA
                               BNG                        Server
 |                             |                            |
 |                             |                            |
 |----Service Request------>|                            |
 |                             |                            |
 |                             |-----Access-Request -------->|
 |                             |                            |
 |                             |<----Access-Accept-----------|
 |                             |     (IP-Port-Limit-Info)    |
 |                             |     (for TCP/UDP ports)     |
 |<---Service Granted ------|                            |
 |     (other parameters)      |                            |
 |                             |                            |
 |               (NAT44 external port                       |
 |                allocation and                            |
 |                IPv4 address assignment)                  |
 |                             |                            |
```
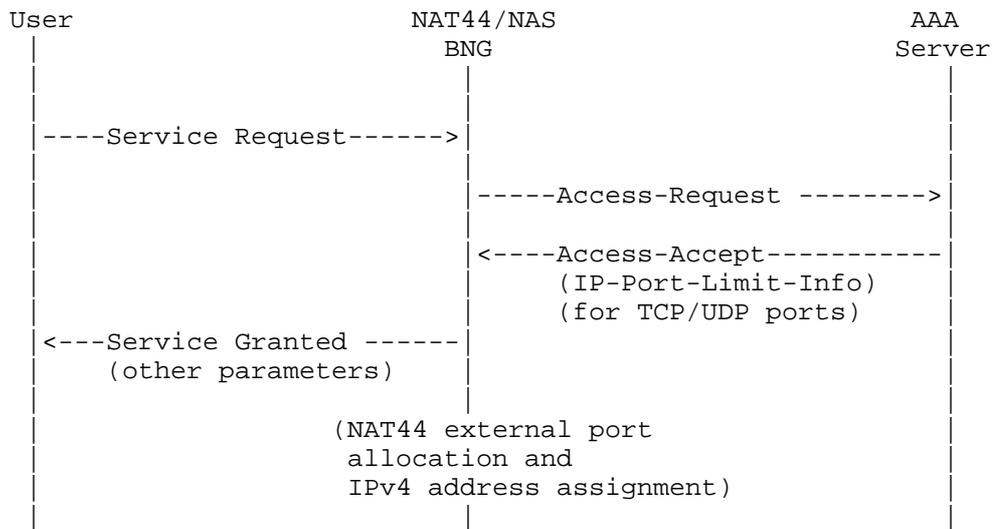
       Figure 15: RADIUS Message Flow for Configuring NAT44 Port Limit

The IP port limit created on a CGN device for a specific user using
RADIUS extension may be changed using RADIUS CoA message [RFC5176]
that carries the same RADIUS attribute. The CoA message may be sent
from the RADIUS server directly to the NAS, which once accepts and
sends back a RADIUS CoA ACK message, the new IP port limit replaces
the previous one.

Figure 16 illustrates how RADIUS protocol is used to increase the
TCP/UDP port limit from 1024 to 2048 on a NAT44 device for a specific
user.

```
        User                    NAT44/NAS                    AAA
          |                        BNG                      Server
          |                         |                          |
          |        TCP/UDP Port Limit (1024)                   |
          |                         |                          |
          |                         |<---------CoA Request----------|
          |                         |          (IP-Port-Limit-Info)  |
          |                         |          (for TCP/UDP ports)   |
          |                         |                          |
          |        TCP/UDP Port Limit (2048)                   |
          |                         |                          |
          |                         |--------CoA Response--------->|
          |                         |                          |
```

    Figure 16: RADIUS Message Flow for changing a user's NAT44 port limit

4.1.2. Report IP Port Allocation/Deallocation

   Upon obtaining the IP port limit for a user, the CGN device needs to
   allocate a TCP/UDP port or an ICMP identifiers for the user when
   receiving a new IP flow sent from that user.

   As one practice, a CGN may allocate a bulk of TCP/UDP ports or ICMP
   identifiers once at a time for a specific user, instead of one port/
   identifier at a time, and within each port bulk, the ports/
   identifiers may be randomly distributed or in consecutive fashion.
   When a CGN device allocates bulk of TCP/UDP ports and ICMP
   identifiers, the information can be easily conveyed to the RADIUS
   server by a new RADIUS attribute called the IP-Port-Range (defined in
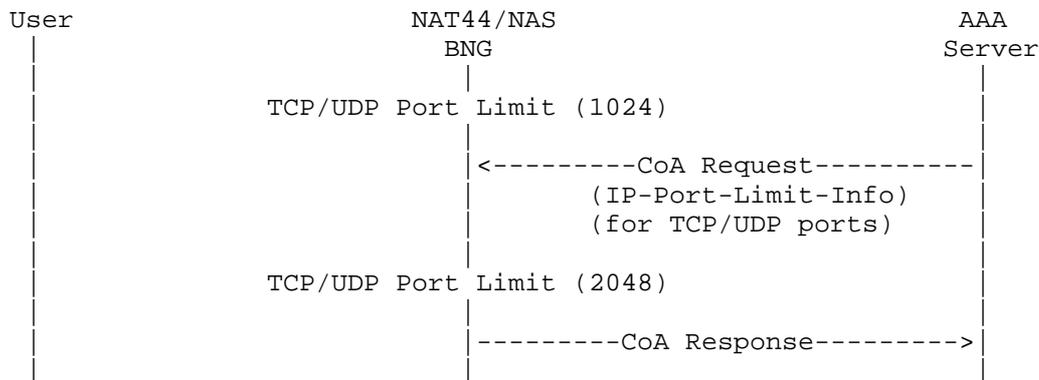   Section 3.1.2). The CGN device may allocate one or more TCP/UDP port
   ranges or ICMP identifier ranges, or generally called IP port ranges,
   where each range contains a set of numbers representing TCP/UDP ports
   or ICMP identifiers, and the total number of ports/identifiers must
   be less or equal to the associated IP port limit imposed for that
   user. A CGN device may choose to allocate a small port range, and
   allocate more at a later time as needed; such practice is good
   because its randomization in nature.

   At the same time, the CGN device also needs to decide the shared IPv4
   address for that user. The shared IPv4 address and the pre-allocated
   IP port range are both passed to the RADIUS server.

   When a user initiates an IP flow, the CGN device randomly selects a
   TCP/UDP port or ICMP identifier from the associated and pre-allocated
   IP port range for that user to replace the original source TCP/UDP
   port or ICMP identifier, along with the replacement of the source IP
   address by the shared IPv4 address.

A CGN device may decide to "free" a previously assigned set of TCP/
UDP ports or ICMP identifiers that have been allocated for a specific
user but not currently in use, and with that, the CGN device must
send the information of the deallocated IP port range along with the
shared IPv4 address to the RADIUS server.

Figure 17 illustrates how RADIUS protocol is used to report a set of
ports allocated and deallocated, respectively, by a NAT44 device for
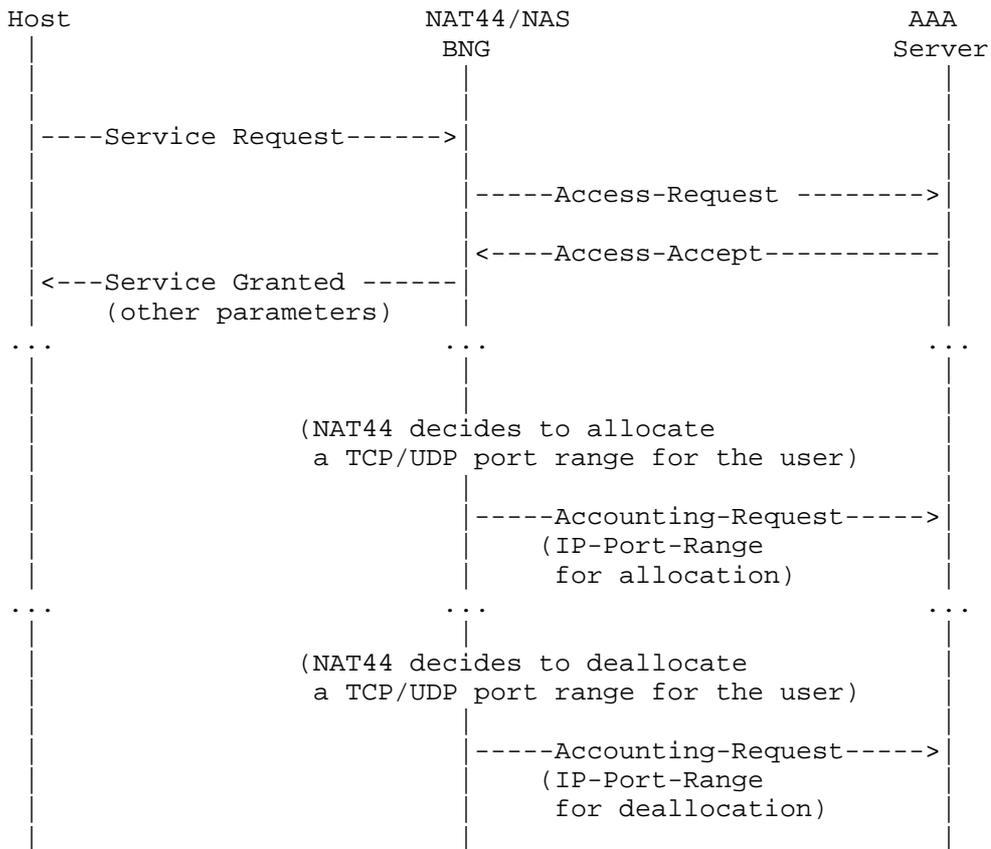a specific user to the RADIUS server.

```
Host                      NAT44/NAS                 AAA
                          BNG                       Server
 |                         |                         |
 |                         |                         |
 |----Service Request----->|                         |
 |                         |                         |
 |                         |-----Access-Request -------->|
 |                         |                         |
 |                         |<----Access-Accept-----------|
 |<---Service Granted ------|                         |
 |     (other parameters)  |                         |
 ...                       ...                       ...
 |                         |                         |
 |                         |                         |
 |              (NAT44 decides to allocate           |
 |               a TCP/UDP port range for the user)  |
 |                         |                         |
 |                         |-----Accounting-Request----->|
 |                         |     (IP-Port-Range      |
 |                         |      for allocation)    |
 ...                       ...                       ...
 |                         |                         |
 |              (NAT44 decides to deallocate         |
 |               a TCP/UDP port range for the user)  |
 |                         |                         |
 |                         |-----Accounting-Request----->|
 |                         |     (IP-Port-Range      |
 |                         |      for deallocation)  |
 |                         |                         |
```

Figure 17: RADIUS Message Flow for reporting NAT44 allocation/
                  deallocation of a port set

4.1.3. Configure Forwarding Port Mapping

In most scenarios, the port mapping on a NAT device is dynamically
created when the IP packets of an IP connection initiated by a user
arrives. For some applications, the port mapping needs to be pre-

defined allowing IP packets of applications from outside a CGN device
to pass through and "port forwarded" to the correct user located
behind the CGN device.

Port Control Protocol [RFC6887], provides a mechanism to create a
mapping from an external IP address and port to an internal IP
address and port on a CGN device just to achieve the "port
forwarding" purpose. PCP is a server-client protocol capable of
creating or deleting a mapping along with a rich set of features on a
CGN device in dynamic fashion. In some deployment, all users need is
a few, typically just one pre-configured port mapping for
applications such as web cam at home, and the lifetime of such a port
mapping remains valid throughout the duration of the customer's
Internet service connection time. In such an environment, it is
possible to statically configure a port mapping on the RADIUS server
for a user and let the RADIUS protocol to propagate the information
to the associated CGN device.

Figure 18 illustrates how RADIUS protocol is used to configure a
forwarding port mapping on a NAT44 device by using RADIUS protocol.

```
Host                        NAT/NAS                        AAA
 |                            BNG                          Server
 |                             |                             |
 |----Service Request------>|                             |
 |                             |                             |
 |                             |---------Access-Request------->|
 |                             |                             |
 |                             |<--------Access-Accept---------|
 |                             |     (IP-Port-Forwarding-Map)  |
 |<---Service Granted ------|                             |
 |     (other parameters)      |                             |
 |                             |                             |
 |              (Create a port mapping                       |
 |               for the user, and                          |
 |               associate it with the                      |
 |               internal IP address                        |
 |               and external IP address)                   |
 |                             |                             |
 |                             |                             |
 |                             |------Accounting-Request------>|
 |                             |     (IP-Port-Forwarding-Map)  |
```

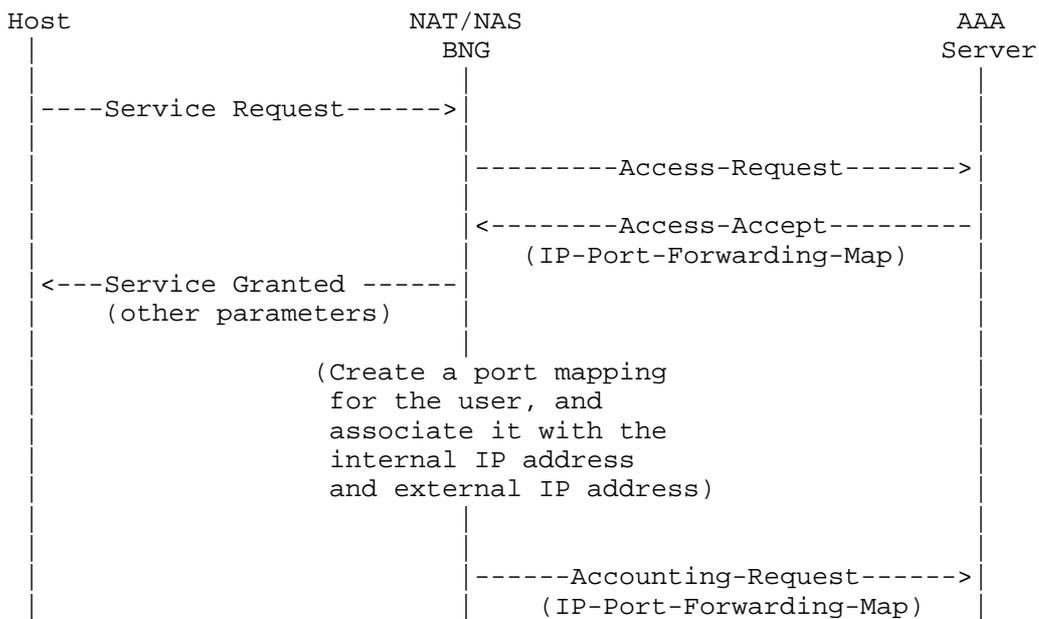   Figure 18: RADIUS Message Flow for configuring a forwarding port
                                    mapping

A port forwarding mapping that is created on a CGN device using
RADIUS extension as described above may also be changed using RADIUS

CoA message [RFC5176] that carries the same RADIUS associate. The
CoA message may be sent from the RADIUS server directly to the NAS,
which once accepts and sends back a RADIUS CoA ACK message, the new
port forwarding mapping then replaces the previous one.

Figure 19 illustrates how RADIUS protocol is used to change an
existing port mapping from (a:X) to (a:Y), where "a" is an internal
port, and "X" and "Y" are external ports, respectively, for a
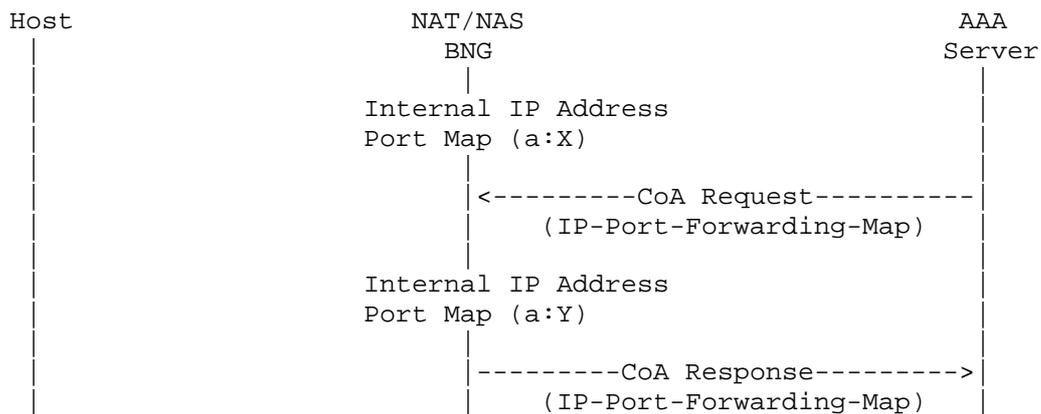specific user with a specific IP address

```
Host                        NAT/NAS                    AAA
|                             BNG                    Server
|                             |                         |
|                     Internal IP Address              |
|                     Port Map (a:X)                   |
|                             |                         |
|                             |<---------CoA Request----------|
|                             |    (IP-Port-Forwarding-Map)   |
|                             |                         |
|                     Internal IP Address              |
|                     Port Map (a:Y)                   |
|                             |                         |
|                             |---------CoA Response--------->|
|                             |    (IP-Port-Forwarding-Map)   |
```

Figure 19: RADIUS Message Flow for changing a user's forwarding port
mapping

4.1.4. An Example

An Internet Service Provider (ISP) assigns TCP/UDP 500 ports for the
user Joe. This number is the limit that can be used for TCP/UDP ports
on a NAT44 device for Joe, and is configured on a RADIUS server.
Also, Joe asks for a pre-defined port forwarding mapping on the NAT44
device for his web cam applications (external port 5000 maps to
internal port 80).

When Joe successfully connects to the Internet service, the RADIUS
server conveys the TCP/UDP port limit (1000) and the forwarding port
mapping (external port 5000 to internal port 80) to the NAT44 device,
using IP-Port-Limit-Info Attribute and IP-Port-Forwarding-Map
attribute, respectively, carried by an Access-Accept message to the
BNG where NAS and CGN co-located.

Upon receiving the first outbound IP packet sent from Joe's laptop,
the NAT44 device decides to allocate a small port pool that contains
40 consecutive ports, from 3500 to 3540, inclusively, and also assign
a shared IPv4 address 192.0.2.15, for Joe. The NAT44 device also

randomly selects one port from the allocated range (say 3519) and use that port to replace the original source port in outbound IP packets.

For accounting purpose, the NAT44 device passes this port range (3500-3540) and the shared IPv4 address 192.0.2.15 together to the RADIUS server using IP-Port-Range attribute carried by an Accounting-Request message.

When Joe works on more applications with more outbound IP sessions and the port pool (3500-3540) is close to exhaust, the NAT44 device allocates a second port pool (8500-8800) in a similar fashion, and also passes the new port range (8500-8800) and IPv4 address 192.0.2.15 together to the RADIUS server using IP-Port-Range attribute carried by an Accounting-Request message. Note when the CGN allocates more ports, it needs to assure that the total number of ports allocated for Joe is within the limit.

Joe decides to upgrade his service agreement with more TCP/UDP ports allowed (up to 1000 ports). The ISP updates the information in Joe's profile on the RADIUS server, which then sends a CoA-Request message that carries the IP-Port-Limit-Info Attribute with 1000 ports to the NAT44 device; the NAT44 device in turn sends back a CoA-ACK message. With that, Joe enjoys more available TCP/UDP ports for his applications.

When Joe travels, most of the IP sessions are closed with their associated TCP/UDP ports released on the NAT44 device, which then sends the relevant information back to the RADIUS server using IP-Port-Range attribute carried by Accounting-Request message.

Throughout Joe's connection with his ISP Internet service, applications can communicate with his web cam at home from external realm directly traversing the pre-configured mapping on the CGN device.

When Joe disconnects from his Internet service, the CGN device will deallocate all TCP/UDP ports as well as the port-forwarding mapping, and send the relevant information to the RADIUS server.

4.2. Report Assigned Port Set for a Visiting UE

Figure 20 illustrates an example of the flow exchange which occurs when a visiting UE connects to a CPE offering WLAN service.

For identification purposes (see [RFC6967]), once the CPE assigns a port set, it issues a RADIUS message to report the assigned port set.
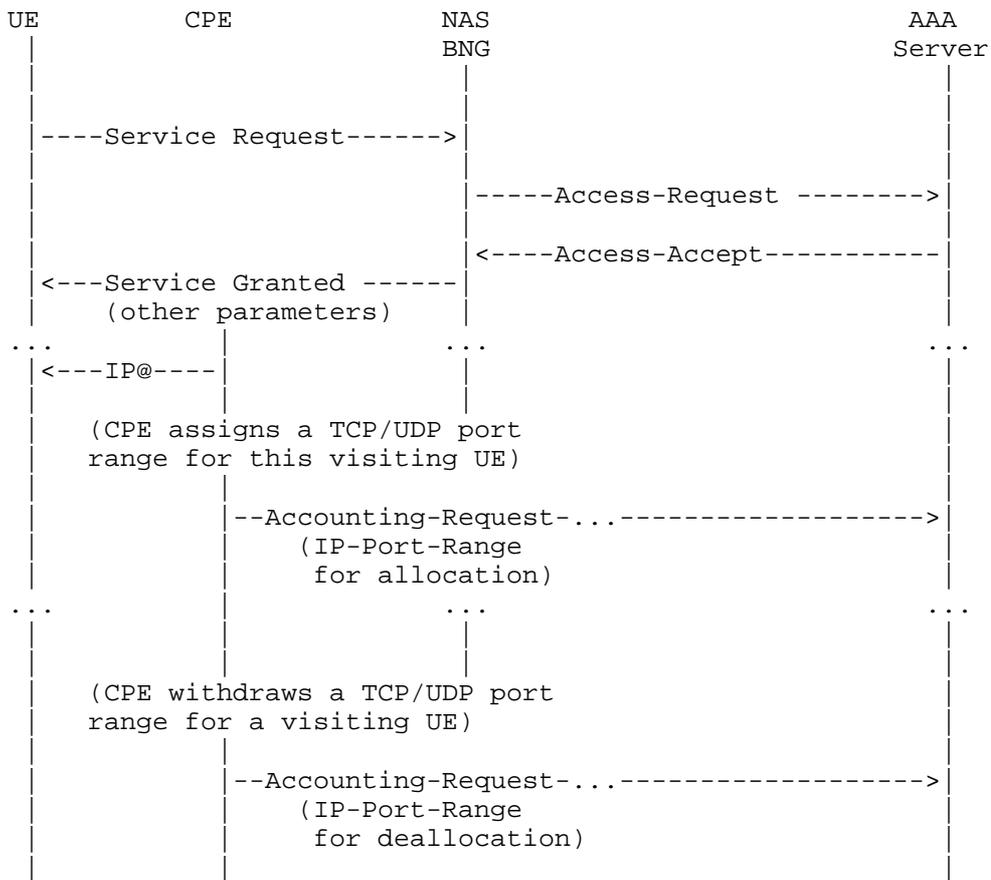
```
   UE           CPE              NAS                        AAA
                                 BNG                        Server
    |            |                |                          |
    |            |                |                          |
    |----Service Request------>|                          |
    |            |                |                          |
    |            |                |-----Access-Request -------->|
    |            |                |                          |
    |            |                |<----Access-Accept-----------|
    |<---Service Granted ------|                          |
    |      (other parameters)  |                          |
   ...           |               ...                        ...
    |<---IP@----|                |                          |
    |            |                |                          |
    |     (CPE assigns a TCP/UDP port                        |
    |      range for this visiting UE)                       |
    |            |                |                          |
    |            |--Accounting-Request-...----------------->|
    |            |      (IP-Port-Range                      |
    |            |       for allocation)                    |
   ...           |               ...                        ...
    |            |                |                          |
    |            |                |                          |
    |     (CPE withdraws a TCP/UDP port                      |
    |      range for a visiting UE)                          |
    |            |                |                          |
    |            |--Accounting-Request-...----------------->|
    |            |      (IP-Port-Range                      |
    |            |       for deallocation)                  |
    |            |                |                          |
```

              Figure 20: RADIUS Message Flow for reporting CPE allocation/
                    deallocation of a port set to a visiting UE

5. Table of Attributes

   This document proposes three new RADIUS attributes and their formats
   are as follows:

   o IP-Port-Limit-Info: 241.TBD1.

   o IP-Port-Range: 241.TBD2.

   o IP-Port-Forwarding-Map: 241.TBD3.

   Note to IANA: it is assumed that Extended-Type-1 "241" will be used
   for these attributes.

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

Request	Accept	Reject	Challenge	Acct. Request	#	Attribute
0+	0+	0	0	0+	TBA	IP-Port-Limit-Info
0	0	0	0	0+	TBA	IP-Port-Range
0+	0+	0	0	0+	TBA	IP-Port-Forwarding-Map

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. Security Considerations

This document does not introduce any security issue other than the
ones already identified in RADIUS [RFC2865].

7. IANA Considerations

This document requires new code point assignments for both IPFIX
Information Elements and RADIUS attributes as explained in the
following sub-sections.

It is assumed that Extended-Type-1 "241" will be used for RADIUS
attributes in Section 7.2.

7.1. IANA Considerations on New IPFIX Information Elements

The following are code point assignments for new IPFIX Information
Elements as requested by this document:

o transportType (refer to Section 3.2.1): The identifier of this
   IPFIX Information Element is TBAx1. The data type of this IPFIX
   Information Element is unsigned8, and the Element's value
   indicates TCP/UDP ports and ICMP Identifiers (1), TCP/UDP ports
   (2), TCP ports (3), UDP ports (4) or ICMP identifiers (5).

o natTransportLimit (refer to Section 3.2.2): The identifier of this
   IPFIX Information Element is TBAx2. The data type of this IPFIX
   Information Element is unsigned16, and the Element's value is the
   max number of IP transport ports to be assigned to an end user
   associated with one or more IPv4 addresses.

o localID (refer to Section 3.2.11): The identifier of this IPFIX
   Information Element is TBAx3. The data type of this IPFIX

Information Element is string, and the Element's value is an IPv4
or IPv6 address, a MAC address, a VLAN ID, etc.

7.2. IANA Considerations on New RADIUS Attributes

The authors request that Attribute Types and Attribute Values defined
in this document be registered by the Internet Assigned Numbers
Authority (IANA) from the RADIUS namespaces as described in the "IANA
Considerations" section of [RFC3575], in accordance with BCP 26
[RFC5226]. For RADIUS packets, attributes and registries created by
this document IANA is requested to place them at
http://www.iana.org/assignments/radius-types.

In particular, this document defines three new RADIUS attributes,
entitled "IP-Port-Limit-Info" (see Section 3.1.1), "IP-Port-Range"
(see Section 3.1.2) and "IP-Port-Forwarding-Map" (see Section 3.1.3),
with assigned values of 241.TBD1, 241.TBD2 and 241.TBD3 from the
Short Extended Space of [RFC6929]:

```
      Type        Name                  Meaning
      ----        ----                  -------
      241.TBD1    IP-Port-Limit-Info    see Section 3.1.1
      241.TBD2    IP-Port-Range         see Section 3.1.2
      241.TBD3    IP-Port-Forwarding-Map see Section 3.1.3
```

7.3. IANA Considerations on New RADIUS TLVs

This specification requests allocation of the following TLVs:

```
      Name                    Value   Meaning
      ----                    -----   -------
      IP-Port-Type            1       see Section 3.2.1
      IP-Port-Limit           2       see Section 3.2.2
      IP-Port-Ext-IPv4-Addr   3       see Section 3.2.3
      IP-Port-Int-IPv4-Addr   4       see Section 3.2.4
      IP-Port-Int-IPv6-Addr   5       see Section 3.2.5
      IP-Port-Int-Port        6       see Section 3.2.6
      IP-Port-Ext-Port        7       see Section 3.2.7
      IP-Port-Alloc           8       see Section 3.2.8
      IP-Port-Range-Start     9       see Section 3.2.9
      IP-Port-Range-End       10      see Section 3.2.10
      IP-Port-Local-Id        11      see Section 3.2.11
```

8. Acknowledgements

Many thanks to Dan Wing, Roberta Maglione, Daniel Derksen, David
Thaler, Alan Dekok, Lionel Morand, and Peter Deacon for their useful
comments and suggestions.

Special thanks to Lionel Morand for the Shepherd review.

9. References

9.1. Normative References

   [IPFIX]   IANA, "IP Flow Information Export (IPFIX) Entities",
               <http://www.iana.org/assignments/ipfix/ipfix.xhtml>.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119,
               DOI 10.17487/RFC2119, March 1997,
               <http://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,
               <http://www.rfc-editor.org/info/rfc2865>.

   [RFC3575]   Aboba, B., "IANA Considerations for RADIUS (Remote
               Authentication Dial In User Service)", RFC 3575,
               DOI 10.17487/RFC3575, July 2003,
               <http://www.rfc-editor.org/info/rfc3575>.

   [RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
               IANA Considerations Section in RFCs", BCP 26, RFC 5226,
               DOI 10.17487/RFC5226, May 2008,
               <http://www.rfc-editor.org/info/rfc5226>.

   [RFC6929]   DeKok, A. and A. Lior, "Remote Authentication Dial In User
               Service (RADIUS) Protocol Extensions", RFC 6929,
               DOI 10.17487/RFC6929, April 2013,
               <http://www.rfc-editor.org/info/rfc6929>.

   [RFC7012]   Claise, B., Ed. and B. Trammell, Ed., "Information Model
               for IP Flow Information Export (IPFIX)", RFC 7012,
               DOI 10.17487/RFC7012, September 2013,
               <http://www.rfc-editor.org/info/rfc7012>.

9.2. Informative References

   [I-D.gundavelli-v6ops-community-wifi-svcs]
               Gundavelli, S., Grayson, M., Seite, P., and Y. Lee,
               "Service Provider Wi-Fi Services Over Residential
               Architectures", draft-gundavelli-v6ops-community-wifi-
               svcs-06 (work in progress), April 2013.

   [RFC3022]   Srisuresh, P. and K. Egevang, "Traditional IP Network
               Address Translator (Traditional NAT)", RFC 3022,
               DOI 10.17487/RFC3022, January 2001,
               <http://www.rfc-editor.org/info/rfc3022>.

   [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,
               <http://www.rfc-editor.org/info/rfc5176>.

   [RFC6146]   Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful
               NAT64: Network Address and Protocol Translation from IPv6
               Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146,
               April 2011, <http://www.rfc-editor.org/info/rfc6146>.

   [RFC6269]   Ford, M., Ed., Boucadair, M., Durand, A., Levis, P., and
               P. Roberts, "Issues with IP Address Sharing", RFC 6269,
               DOI 10.17487/RFC6269, June 2011,
               <http://www.rfc-editor.org/info/rfc6269>.

   [RFC6333]   Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
               Stack Lite Broadband Deployments Following IPv4
               Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011,
               <http://www.rfc-editor.org/info/rfc6333>.

   [RFC6619]   Arkko, J., Eggert, L., and M. Townsley, "Scalable
               Operation of Address Translators with Per-Interface
               Bindings", RFC 6619, DOI 10.17487/RFC6619, June 2012,
               <http://www.rfc-editor.org/info/rfc6619>.

   [RFC6887]   Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and
               P. Selkirk, "Port Control Protocol (PCP)", RFC 6887,
               DOI 10.17487/RFC6887, April 2013,
               <http://www.rfc-editor.org/info/rfc6887>.

   [RFC6888]   Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa,
               A., and H. Ashida, "Common Requirements for Carrier-Grade
               NATs (CGNs)", BCP 127, RFC 6888, DOI 10.17487/RFC6888,
               April 2013, <http://www.rfc-editor.org/info/rfc6888>.

   [RFC6967]   Boucadair, M., Touch, J., Levis, P., and R. Penno,
               "Analysis of Potential Solutions for Revealing a Host
               Identifier (HOST_ID) in Shared Address Deployments",
               RFC 6967, DOI 10.17487/RFC6967, June 2013,
               <http://www.rfc-editor.org/info/rfc6967>.

   [RFC7596]   Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I.
               Farrer, "Lightweight 4over6: An Extension to the Dual-
               Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596,
               July 2015, <http://www.rfc-editor.org/info/rfc7596>.

   [TR-146]   Broadband Forum, "TR-146: Subscriber Sessions",
               <http://www.broadband-forum.org/technical/download/
               TR-146.pdf>.

Authors' Addresses

   Dean Cheng
   Huawei
   2330 Central Expressway
   Santa Clara, California 95050
   USA

   Email: dean.cheng@huawei.com

   Jouni Korhonen
   Broadcom Corporation
   3151 Zanker Road
   San Jose 95134
   USA

   Email: jouni.nospam@gmail.com

   Mohamed Boucadair
   Orange
   Rennes
   France

   Email: mohamed.boucadair@orange.com

   Senthil Sivakumar
   Cisco Systems
   7100-8 Kit Creek Road
   Research Triangle Park, North Carolina
   USA

   Email: ssenthil@cisco.com

RADIUS Extensions Working Group   S. Winter
Internet-Draft   RESTENA
Intended status: Best Current Practice   March 21, 2016
Expires: September 22, 2016

            Considerations regarding the correct use of EAP-Response/Identity
                 draft-ietf-radext-populating-eapidentity-00

Abstract

   There are some subtle considerations for an EAP peer regarding the
   content of the EAP-Response/Identity packet when authenticating with
   EAP to an EAP server. This document describes two such
   considerations and suggests workarounds to the associated problems.

Status of This Memo

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

   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 http://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 September 22, 2016.

Table of Contents

1. Introduction

1.1. Problem Statement

   An Extensible Authentication Protocol (EAP, [RFC3748]) conversation
   between an EAP peer and an EAP server starts with an (optional)
   request for identity information by the EAP server (EAP-Request/
   Identity) followed by the peer's response with identity information
   (EAP-Response/Identity). Only after this identity exchange are EAP
   types negotiated.

   EAP-Response/Identity is sent before EAP type negotiation takes
   place, but it is not independent of the later-negotiated EAP type.
   Two entanglements between EAP-Response/Identity and EAP methods'
   notions of a user identifier are described in this document.

   1. The choice of identity to send in EAP-Response/Identity may have
       detrimental effects on the subsequent EAP type negotiation.

   2. Using identity information from the preferred EAP type without
       thoughtful conversion of character encoding may have detrimental
       effects on the outcome of the authentication.

   The following two chapters describe each of these issues in detail.
   The last chapter contains recommendations for implementers of EAP
   peers to avoid these issues.

1.2. Taxonomy of identities in EAP

   The notion of identity occurs numerous times in the EAP protocol
   stack (EAP-Response/Identity, Outer identity, method-specific

identity, tunneled identity). This document uses the following
terminology when discussing EAP identities.

o Method-specific Identity: Each EAP method has a means to identify
   the user or machine that tries to authenticate. There are no
   restrictions on the format or encoding of this method-specific
   identity. If an EAP methods distinguishes between this actual
   identity and a outer identity (see next bullet), then the Method-
   specific Identity is also often called the Inner Identity.

o Method-specific Outer Identity: Some EAP methods allow privacy-
   preserving enhancements where a string is sent as "identity" which
   is actually not necessarily related to the user or machine that
   tries to authenticate. There is often a relationship between the
   Method-specific Outer Identity and the Inner Identity (e.g. they
   often share the same NAI realm suffix); but this is not a
   requirement. There are no restrictions on the format or encoding
   of this method-specific identity. Method-specific outer
   identities are either

   * explicitly configured (e.g. string input UI: "Outer Identity")

   * implicitly configured by copying the actual Method-specific
      (Inner) Identity

   * implicitly configured by copying the NAI realm of the Method-
      specific (Inner) Identity and prefixing it non-configurably
      with a fixed privacy-preserving local username part like
      "anonymous" or the empty string (see [RFC7542])

   * configured in a mixed way, e.g. using a explicit string input
      UI for the local part of the outer identity and combining it
      implicitly with a copy of the NAI realm part of the Method-
      specific (Inner) Identity

o EAP-Response/Identity: a string representing the user or machine
   that tries to authenticate, used outside the EAP method-specific
   context for the entire EAP session. There can be only one EAP-
   Response/Identity per EAP session, even if that session is
   configured with more than one EAP method to authenticate with. As
   per [RFC3748] there is no encoding requirement on EAP-Response/
   Identity. In AAA protocol routing contexts, the content of EAP-
   Response/Identity is often used for request routing purposes.
   EAP-Response/Identity is chosen from the set:

   * all method-specific outer identities from all configured EAP
      types supporting the notion of an outer identity union

> * all method-specific identities from all configured EAP types
>   without the notion of an outer identity

One of the two problems addressed in this document stems from this
fact: the set of identities may contain more than one element.
The resulting EAP-Response/Identity always routes all configured
EAP types to only one destination, even if different EAP types
would need routing to different destinations.

o User-Name: when using EAP in AAA protocol contexts (e.g. RADIUS
  [RFC2865], Diameter [RFC6733]), this additional identity is
  created outside the EAP peer (typically in a pass-through
  authenticator) by copying EAP-Response/Identity content to the AAA
  protocol's User-Name attribute. There is no format requirement on
  User-Name, but there is an encoding requirement: the string MUST
  be UTF-8 encoded. One of the two problems addressed in this
  document stems from this fact: EAP-Response/Identity does not have
  an encoding requirement, nor does it carry meta-information about
  the encoding used - and yet, it needs to be coerced into a UTF-8
  encoding.

o Further identities: Some EAP methods establish an EAP session
  inside EAP (e.g. PEAP first establishes a TLS tunnel using a
  method-specific outer identity, and then starts an EAP exchange
  inside the tunnel). This being a new, independent EAP session, it
  contains its own EAP-Response/Identity, can invoke EAP method
  negotiation with different (inner) EAP types (this happens e.g.
  with EAP-FAST and its configurable choice of EAP-GTC or EAP-
  MSCHAPv2 inside the inner EAP session), and those inner EAP
  methods then have their own (inner) method-specific identities.
  Where the inner EAP method itself supports the notion of method-
  specific outer identities, another identity could be configured.
  For the purposes of this document, none of those details are
  considered and the process by which the (outer) EAP method selects
  its method-specific identity is left entirely to that EAP type.
  This document does not consider the (inner) EAP-Response/Identity
  in scope; the recommendations in this document to not apply to
  such (inner) occurences of EAP-Response/Identity.

1.3. Requirements Language

In this document, several words are used to signify the requirements
of the specification. 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. EAP-Response/Identity: Effects on EAP type negotiation

   Assuming the EAP peer's EAP type selection is not the trivial case
   (i.e. it has more than one configured EAP type for a given network or
   application, and needs to make a decision which one to use), an issue
   arises when the configured EAP types are not all configured with the
   same method-specific outer identity (or method-specific identity for
   EAP types not supporting the notion of an outer identity).

   Issue: if the identities in the set of configured EAP types differ
   (e.g. have a different [RFC7542] "realm" portion), and the
   authenticator does not send identity selection hints as per
   [RFC7542], then EAP type negotiation may be limited to those EAP
   types which are terminated in the same EAP server. The reason for
   that is because the information in the EAP-Response/Identity is used
   for request routing decisions and thus determines the EAP server - a
   given user identifier may be routed to a server which exclusively
   serves the matching EAP type. Negotiating another EAP type from the
   set of configured EAP types during the running EAP conversation is
   then not possible.

   Example:

   Assume an EAP peer is configured to support two EAP types:

   o EAP-AKA' [RFC5448] with user identifier imsi@mnc123.mcc123.3gpp-
      network.org

   o EAP-TTLS [RFC5281] with user identifier john@realm.example

   The user connects to hotspot of a roaming consortium which could
   authenticate him with EAP-TTLS and his john@realm.example identity.
   The hotspot operator has no business relationship at all with the
   3GPP consortium; incoming authentication requests for realms ending
   in 3gppnetwork.org will be immediately rejected. Identity selection
   hints are not sent.

   Consequence: If the EAP peer consistently chooses the
   imsi@mnc123.mcc123.3gpp-network.org user identifier as choice for its
   initial EAP-Response/Identity, the user will be consistently and
   perpetually rejected, even though in possession of a valid credential
   for the hotspot.

   An EAP peer should always try all options to authenticate. As the
   example above shows, it may not be sufficient to rely on EAP method
   negotiation alone to iterate through all configured EAP types and
   come to a conclusive outcome of the authentication attempt. Multiple
   new EAP authentications, each using an EAP-Response/Identity from a

different element of the set of method-specific outer identities, may
be required to fully iterate through the list of usable identities.

3. Character (re-)encoding may be required

The method-specific identities as configured in the EAP method
configuration are not always suited as identities to choose as EAP-
Response/Identity: EAP methods define the encoding of their method-
specific outer identities at their leisure; in particular, the chosen
encoding may or may not be UTF-8.

It is not the intention of EAP, as a mere method-agnostic container
which simply carries EAP types, to restrict an EAP method's choice of
encoding of method-specific identities. However, there are
restrictions in what should be contained in the EAP-Response/
Identity: EAP is very often carried over a AAA protocol (e.g over
RADIUS as per [RFC3579]). The typical use for the contents of EAP-
Response/Identity inside AAA protocols like RADIUS [RFC2865] and
Diameter [RFC6733] is to copy the content of EAP-Response/Identity
into a "User-Name" attribute; the encoding of the User-Name attribute
is required to be UTF-8. EAP-Response/Identity does not carry
encoding information itself, so a conversion between a non-UTF-8
encoding and UTF-8 is not possible for the AAA entity doing the EAP-
Response/Identity to User-Name copying.

Consequence: If an EAP method's method-specific identity is not
encoded in UTF-8, and the EAP peer verbatimly uses that method-
specific identity for its EAP-Response/Identity field, then the AAA
entity is forced to violate its own specification because it has to,
but can not use UTF-8 for its own User-Name attribute. If the EAP
method supports a method-specific outer identity in a non UTF-8
character set, and the EAP peer verbatimly uses that outer identity
for its EAP-Response/Identity field, then the same violation occurs.

This jeopardizes the subsequent EAP authentication as a whole;
request routing may fail, lead to a wrong destination or introduce
routing loops due to differing interpretations of the User-Name in
EAP pass-through authenticators and AAA proxies.

4. Recommendations for EAP peer implementations

Where method-specific identities or method-specific outer identities
in configured EAP types in an EAP peer differ, the EAP peer can not
rely on the EAP type negotiation mechanism alone to provide useful
results. If an EAP authentication gets rejected, the EAP peer SHOULD
re-try the authentication using a different EAP-Response/Identity
than before. The EAP peer SHOULD try all possible EAP-Response/

Identity contents from the entire set of configured EAP types before
declaring final authentication failure.

EAP peers need to maintain state on the encoding of the method-
specific identities and outer identities which are used in their
locally configured EAP types. When constructing an EAP-Response/
Identity from the set of identities, they MUST (re-)encode the
corresponding identity as UTF-8 and use the resulting value for the
EAP-Response/Identity.

5. Privacy Considerations

   Because the EAP-Response/Identity content is not encrypted, the
   backtracking to a new EAP-Response/Identity will systematically
   reveal all configured identities to intermediate passive listeners on
   the path between the EAP peer and the EAP server (until one
   authentication round succeeds).

   This additional leakage of identity information is not very
   significant though because where privacy is considered important, the
   additional option for identity privacy which is present in most
   modern EAP methods can be used.

   If the EAP peer implementation is certain that all EAP types will be
   terminated at the same EAP server (e.g. with a corresponding
   configuration option) then the iteration over all identities can be
   avoided, because the EAP type negotiation is then sufficient.

   If a choice of which identity information to disclose needs to be
   made by the EAP peer, when iterating through the list of identities
   the EAP peer SHOULD

      in first priority honour a manually configured order of preference
      of EAP types, if any

      in second priority try EAP types in order of less leakage first;
      that is, EAP types with a method-specific outer identity that
      differs from the method-specific identity should be tried before
      other EAP types which would reveal actual user identities.

6. Security Considerations

   The security of an EAP conversation is determined by the EAP method
   which is used to authenticate. This document does not change the
   actual authentication with an EAP method, and all the security
   properties of the chosen EAP method remain. The format requirements
   (character encoding) and operational considerations (re-try EAP with

a different EAP-Response/Identity) do not lead to new or different
security properties.

7. IANA Considerations

There are no IANA actions in 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.

8.2. Informative References

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

[RFC3579]   Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication
Dial In User Service) Support For Extensible
Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748]   Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.
Levkowetz, "Extensible Authentication Protocol (EAP)", RFC
3748, June 2004.

[RFC5281]   Funk, P. and S. Blake-Wilson, "Extensible Authentication
Protocol Tunneled Transport Layer Security Authenticated
Protocol Version 0 (EAP-TTLSv0)", RFC 5281, August 2008.

[RFC5448]   Arkko, J., Lehtovirta, V., and P. Eronen, "Improved
Extensible Authentication Protocol Method for 3rd
Generation Authentication and Key Agreement (EAP-AKA')",
RFC 5448, May 2009.

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

[RFC7542]   DeKok, A., "The Network Access Identifier", RFC 7542, DOI
10.17487/RFC7542, May 2015,
<http://www.rfc-editor.org/info/rfc7542>.

Author's Address

   Stefan Winter
   Fondation RESTENA
   6, rue Richard Coudenhove-Kalergi
   Luxembourg 1359
   LUXEMBOURG

   Phone: +352 424409 1
   Fax: +352 422473
   EMail: stefan.winter@restena.lu
   URI: http://www.restena.lu.