          RADIUS Extensions for Port Set Configuration and Reporting
                 draft-cheng-behave-cgn-cfg-radius-ext-06

Abstract

   This document defines new RADIUS attributes that can be used by a
   device implementing port ranges to communicate with a RADIUS server
   to configure and/or report TCP/UDP port sets and ICMP identifiers
   mapping behavior for specific hosts. This mechanism can be used in
   various deployment scenarios such as CGN, NAT64, Provider WiFi
   Gateway, etc.

   This document does not make any assumption about the deployment
   context.

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] and at the time when a user initiates an IP
   connection request, the RADIUS server will populate the user's
   configuration information to the Network Access Server (NAS), which
   is usually co-located with the Border Network Gateway (BNG), after

the connection request is granted. The Carrier Grade NAT (CGN)
function may also implemented on the BNG, and therefore CGN TCP/UDP
port (or ICMP identifier) mapping behavior can be configured on the
RADIUS server as part of the user profile, and populated to the NAS
in the same manner. In addition, during the operation, the CGN can
also convey port/identifier mapping behavior specific to a user to
the RADIUS server, as part of the normal RADIUS accounting process.

The CGN device that communicates with a RADIUS server using RADIUS
extensions defined in this document may perform NAT44 [RFC3022],
NAT64 [RFC6146], or Dual-Stack Lite AFTR [RFC6333] function.

For the CGN example, when IP packets traverse a CGN, it would perform
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 subject to port quota.

The attributes defined in this document may also be used to report
the assigned port set in some deployment such as Provider Wi-Fi
[I-D.gundavelli-v6ops-community-wifi-svcs]. For example, a visiting
host can be managed by a CPE which will need to report the assigned
port set to the service platform. This is required for
identification purposes (see WT-146 for example).

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

o A session limit is configured on a RADIUS server based on service
   agreement with a subscriber, and this parameter imposes the limit
   of total number of TCP/UDP ports and/or ICMP identifiers that the
   subscriber can use. Alternately, a separate session limit may be
   configured to limit the number of TCP ports, UDP ports, or the sum
   of the two, and ICMP identifiers, respectively, that the user can
   use. The session limit is carried by a new RADIUS attribute Port-
   Session-Limit, which is included in a RADIUS Access-Accept message
   sent by the RADIUS server to port-based device. This new RADIUS
   attribute can also be included in a RADIUS CoA message sent by the
   RADIUS server to the port-based device in order to change the
   session limit previously configured.

o A port-based device may allocate or de-allocate a set of TCP/UDP
   ports or ICMP identifiers for a specific subscriber. When it does

so, the associated session range along with the shared IPv4
address can be conveyed to the RADIUS server as part of the
accounting process. These parameters are carried by a new RADIUS
attribute Port-Session-Range, which is included in a RADIUS
Accounting- Request message sent by the port-based device to the
RADIUS server.

o A user may require the port-based device to perform port
   forwarding function, i.e., a port mapping is pre-configured on the
   port-based so that inbound IP packets sent by some applications
   from the port-based external realm can pass through that device
   and reach the user. The port mapping information includes the
   port-based device internal port, external port, and may also
   include the associated internal IPv4 or IPv6 address, and is
   carried by a new RADIUS attribute Port- Forwarding-Map, which is
   included in a RADIUS Access-Accept message sent by the RADIUS
   server to the port-based device. This new RADIUS attribute can
   also be included in a RADIUS CoA message sent by the RADIUS server
   to the port-based device in order to change the forwarding port
   mapping previously configured.

[2](). **Terminology**

Some terms that are used in this document are listed as follows:

o Session Limit - This is the maximum number of TCP ports, or UDP
   ports, or the total of the two, or ICMP identifiers, or the total
   of the three, that a device supporting port ranges can use when
   performing mapping on TCP/ UDP ports or ICMP identifiers for a
   specific user.

o Session Range - This specifies a set of TCP/UDP port numbers or
   ICMP identifiers, indicated by the port/identifier with the
   smallest numerical number and the port/identifier with the largest
   numerical number, inclusively.

o Internal IP Address - The IP address that is used as a source IP
   address in an outbound IP packet sent toward a device supporting
   port ranges in the internal realm. In IPv4 case, it is typically
   a private address [RFC1918].

o External IP Address - 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. In IPv4 case, it is
   typically a global and routable IP address.

o Internal Port - The 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 - The 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 - The networking segment where IPv4 public
   addresses are used in respective of the device supporting port
   ranges.

o Internal realm - The networking segment that is behind a device
   supporting port ranges and where IPv4 private addresses are used.

o Mapping - This term in this document 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 TCP/UDP port mapping services and in particular, with
   the granularity of one or more subsets within the 16-bit TCP/UDP
   port number range. A typical example of this device can be a CGN,
   CPE, Provider Wi-Fi Gateway, etc.

Note the terms "internal IP address", "internal port", "internal
realm", "external IP address", "external port", "external realm", and
"mapping" and their semantics are the same as in [RFC6887], and
[RFC6888].

3. RADIUS Attributes

   [Discussion: should these attributes be allocated from the
   extended RADIUS attribute code space?]

   [Discussion: Should we define a dedicated attribute
   (port_set_policies) to configure the following policies: (1)
   enforce port randomization, (2) include/exclude the WKP in the
   port assignment, (3) preserve parity, (4) quota for explicit port
   mapping, (5) DSCP marking policy, (6) Port hold down timer, (7)
   port hold down pool, etc. Perhaps we don't need to cover all
   these parameters.]

3.1. Port-Session-Limit Attribute

This attribute is of type complex [RFC6158] and specifies the limit
of TCP ports, or UDP ports, or the sum of the two, or ICMP
identifiers, or the sum of the three, which is configured on a device
supporting port ranges corresponding to a specific subscriber.

The Port-Session-Limit MAY appear in an Access-Accept packet, it MAY
also appear in an Access-Request packet as a hint by the device
supporting port ranges, which is co-allocated with the NAS, to the
RADIUS server as a preference, although the server is not required to
honor such a hint.

The Port-Session-Limit MAY appear in an CoA-Request packet.

The Port-Session-Limit MAY appear in an Accounting-Request packet.

The Port-Session-Limit MUST NOT appear in any other RADIUS packets.

The format of the Port-Session-Limit RADIUS attribute format is shown
below. The fields are transmitted from left to right.

```
 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    |      ST       |    Session
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      Limit     |
+-+-+-+-+-+-+-+-+
```

Type:

   TBA1 for Port-Session-Limit.

Length:

   5 octets. This field indicates the total length in octets of this
   attribute including the Type and the Length field.

ST (Session Type):

   This one octet field contains an enumerated value that indicates
   the applicability of the Session Limit as follows:

   0:

      The limit as specified is applied to each transport protocol
      (TCP/UDP) and ICMP Identifiers as a whole.

   1:

The limit as specified is applied to TCP and UDP ports.

2:

The limit as specified is applied to TCP ports.

3:

The limit as specified is applied to UDP ports.

4:

The limit as specified is applied to ICMP Identifiers.

5-255:

These values are undefined.

Session Limit:

This field contains the maximum number that is assigned to the transport sessions depending on the value in the Session Type (ST) field, that the specific user can use.

3.2. Port-Session-Range Attribute

This attribute is of type complex [RFC6158] and contains a range of numbers for TCP ports or UDP ports, or both, or for ICMP Identifiers, which has been allocated or de-allocated by a device supporting port ranges for a given subscriber, along with an external IPv4 address that is associated with any TCP/UDP port or ICMP identifier in the range.

In some CGN deployment scenarios as described such as L2NAT [I-D.miles-behave-l2nat], DS-Extra-Lite [RFC6619] and Lightweight 4over6 [I-D.ietf-softwire-lw4over6], 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.

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

The Port-Session-Range MUST NOT appear in any other RADIUS packets.

The port range follows the encoding specified in [RFC6431]; as such both contiguous and non-contiguous port sets are supported.

The format of the Port-Session-Range RADIUS attribute format is shown
below. The fields are transmitted from left to right.

```
 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     |      ST       |A| Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Port Range Mask          |       Port Range Value        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     External IPv4 Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Local Session ID ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+--
```

Type:

   TBA2 for Port-Session-Range.

Length:

   12 octets plus the length of optional field Local Session ID.
   This field indicates the total length in octets of this attribute
   including the Type and the Length field.

ST (Session Type):

   This one octet field contains an enumerated value that indicates
   the semantics of the session range. The values follow the Session
   Type encoding defined in [Section 3.1](#) except that the following
   values are not valid in scope of this attribute:

   0:

      The limit as specified is applied to the sum of TCP ports, UDP
      ports, and ICMP Identifiers as a whole.

A-bit Flag:

   This field is set to 0 or 1, indicates that the session range has
   been allocated or de-allocated, respectively, by the device
   supporting port ranges.

Reserved:

   This field MUST be set to zero by the sender and ignored by the
   receiver.

Port Range Mask:

   The Port Range Mask indicates the position of the bits that are
   used to build the Port Range Value. By default, no PRM value is
   assigned. The 1 values in the Port Range Mask indicate by their
   position the significant bits of the Port Range Value. Refer to
   [RFC6431] for more details.

Port Range Value:

   The PRV indicates the value of the significant bits of the Port
   Mask. By default, no PRV is assigned. Refer to [RFC6431] for
   more details.

External IPv4 Address:

   This is an optional field. If present, this field contains the
   IPv4 address assigned to the associated subscriber to be used in
   the external realm. If set to 0/0, the allocation address policy
   is local to the device supporting port ranges.

Local Session ID:

   This is an optional field and if presents, it 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. The length of this field equals to the total
   attribute length minus 12 octets. If this field is not present,
   the port range policies must be enforced to all subscribers using
   a local subscriber identifier.

3.3. Port-Forwarding-Map Attribute

This attribute is type of complex [RFC6158] and contains a 16-bit
Internal Port that identifies the source TCP/UDP port number of an IP
packet sent by the user, or the destination port number of an IP
packet destined to the user, and in both cases, the IP packet travels
behind the NAT device. Also they contain a 16-bit Configured
External Port that identifies the source TCP/UDP port number of an IP
packet sent by the user, or the destination port number of an IP
packet destined to the user, and in both cases, the IP packet travels
outside of the NAT device. In addition, the attribute may contain a
32-bit IPv4 address or a 128-bit IPv6 address, respectively, as their
respective NAT mappings internal IP address. Together, the port pair
and IP address determine the port mapping rule for a specific IP flow
that traverses a NAT device.

The attribute MAY appear in an Access-Accept packet, and may also
appear in an Accounting-Request packet. In either case, the
attribute MUST NOT appear more than once in a single packet.

The attribute MUST NOT appear in any other RADIUS packets.

The format of the Port-Forwarding-Map RADIUS attribute format is
shown below. The fields are transmitted from left to right.

```
 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     |      AF       |    Reserved   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Internal Port          |    Configured External Port   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Internal IP Address  .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

   TBA3 for Port-Forwarding-Map.

Length:

   This field indicates the total length in octets of this attribute
   including the Type and the Length field. Depending on the value
   of the AF field, the length could be 8, 12 or 24 octets.

AF (Address Family):

   This one octet field contains a value that indicates address
   family of the internal IP address at the mapping as follows:

   0:

      There is no internal address attached.

   1:

      The internal address is an IPv4 address.

   2:

      The internal address is an IPv6 address.

   3-255:

      Unused.

   [Discussion: should we use IANA assigned protocol numbers here?]

   Reserved:

      This field is set to zero by the sender and ignored by the
      receiver.

   Internal Port:

      This field contains the internal port for the CGN mapping.

   Configured External Port:

      This field contains the external port for the CGN mapping.

   Internal IP Address:

      This field may or may not present, and when it does, contains the
      internal IPv4 or IPv6 address for the CGN mapping.

4. Applications, Use Cases and Examples

   This section describes some applications and use cases to illustrate
   the use of the RADIUS port set attributes.

4.1. Managing CGN Port Behavior using RADIUS

   In a broadband network, customer information is usually stored on a
   RADIUS server, and the BNG hosts the NAS. The communication between
   the NAS and the RADIUS server is triggered by a subscriber when the
   user 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 reside 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
de-allocation 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 CGN Session Limit

In the face of IPv4 address shortage, there are currently proposals
to multiplex multiple subscribers' 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
subscribers. As indicated in [RFC6269], it is therefore necessary to
impose limits on the total number of ports available to an individual
subscriber to ensure that the shared resource, i.e., the IPv4 address
remains available in some capacity to all the subscribers using it,
and port limiting is also documented in [RFC6888] as a requirement.

There are two practical granularities to impose such a limit. One is
to define a session limit that is imposed to the total number of TCP
and UDP ports, plus the number of ICMP identifiers, for a specific
subscriber. Alternatively, a session limit can be specified for the
sum of TCP ports and UDP ports, or a separate session limit for TCP
ports and UDP ports, respectively, and another session limit for ICMP
identifiers.

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

When a subscriber signs in to the Internet service successfully, the
session limit(s) for the subscriber is passed to the BNG based NAS,
where CGN also locates, using a new RADIUS attribute called Port-
Session-Limit (defined in Section 3.1), along with other
configuration parameters. While some parameters are passed to the
subscriber, the session limit(s) is recorded on the CGN device for
imposing the usage of TCP/UDP ports and ICMP identifiers for that
subscriber.

Figure 1 illustrates how RADIUS protocol is used to configure the maximum number of TCP/UDP ports for a given subscriber on a NAT44 device.

```
User                        NAT44/NAS                     AAA
 |                            BNG                         Server
 |                            |                             |
 |                            |                             |
 |----Service Request------>|                             |
 |                            |                             |
 |                            |-----Access-Request -------->|
 |                            |                             |
 |                            |<----Access-Accept-----------|
 |                            |     (Port-Session-Limit)    |
 |                            |     (for TCP/UDP ports)     |
 |<---Service Granted ------|                             |
 |     (other parameters)    |                             |
 |                            |                             |
 |                 (NAT44 external port                     |
 |                  allocation and                          |
 |                  IPv4 address assignment)                |
 |                            |                             |
```
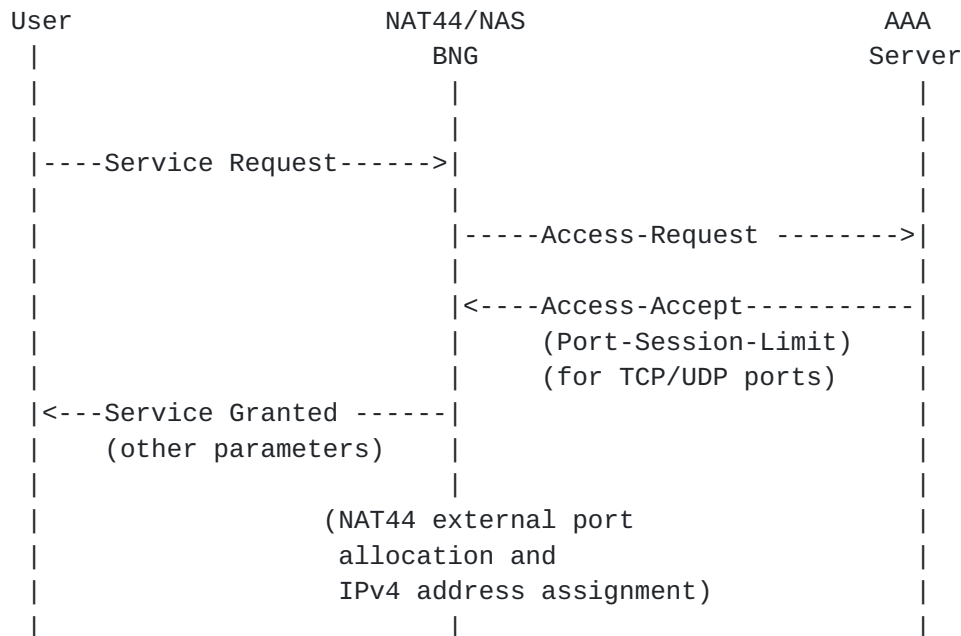
Figure 1: RADIUS Message Flow for Configuring NAT44 Port Limit

The session limit(s) 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 session limit replaces the previous one.

Figure 2 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                        NAT/NAS                       AAA
    |                           BNG                         Server
    |                            |                            |
    |           TCP/UDP Port Limit (1024)                     |
    |                            |                            |
    |                            |<---------CoA Request----------|
    |                            |          (Port-Session-Limit)  |
    |                            |          (for TCP/UDP ports)   |
    |                            |                            |
    |           TCP/UDP Port Limit (2048)                     |
    |                            |                            |
    |                            |--------CoA Response--------->|
    |                            |                            |
```
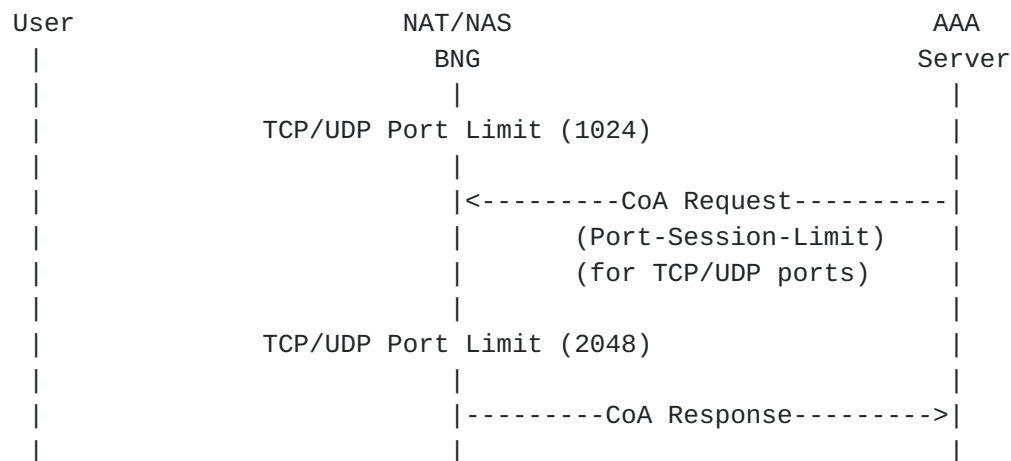
        Figure 2: RADIUS Message Flow for changing a user's NAT44 port limit

4.1.2. Report CGN Session Allocation or De-allocation

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

   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 session 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 CGN-Session-Range
   (defined in Section 3.2). The CGN device may allocate one or more
   TCP/UDP port ranges or ICMP identifier ranges, or generally called
   session ranges, where each range contains a set of numbers
   representing TCP/UDP ports or ICMP identifiers, and the total number
   of sessions must be less or equal to the associated session limit
   defined for that subscriber. A CGN device may choose to allocate a
   small session 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 subscriber. The shared IPv4 address and the pre-
   allocated session range are both passed to the RADIUS server.

   When a subscriber initiates an IP flow, the CGN device randomly
   selects a TCP/UDP port or ICMP identifier from the associated and
   pre-allocated session range for that subscriber 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
subscriber but not currently in use, and with that, the CGN device
must send the information of the de-allocated session range along
with the shared IPv4 address to the RADIUS server.

Figure 3 illustrates how RADIUS protocol is used to report a set of
ports allocated and de-allocated, 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----->|
 |                            |     (Port-Session-Range      |
 |                            |        for allocation)       |
...                          ...                           ...
 |                            |                             |
 |            (NAT44 decides to de-allocate                 |
 |              a TCP/UDP port range for the user)          |
 |                            |                             |
 |                            |-----Accounting-Request----->|
 |                            |     (Port-Session-Range      |
 |                            |        for de-allocation)    |
 |                            |                             |
```
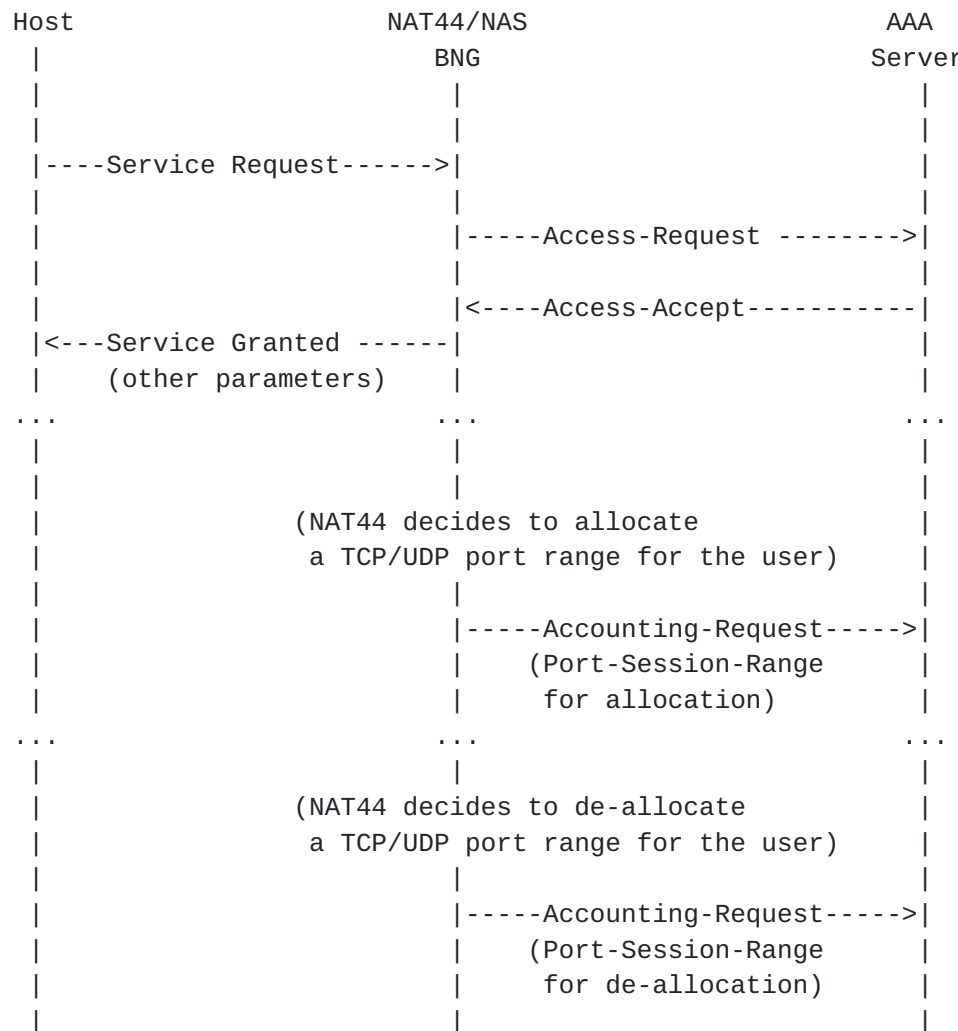
       Figure 3: RADIUS Message Flow for reporting NAT44 allocation/de-
                        allocation of a port set

4.1.3. Configure CGN 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 4 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---------|
      |                          |    (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------>|
      |                          |    (Port-Forwarding-Map)      |
```
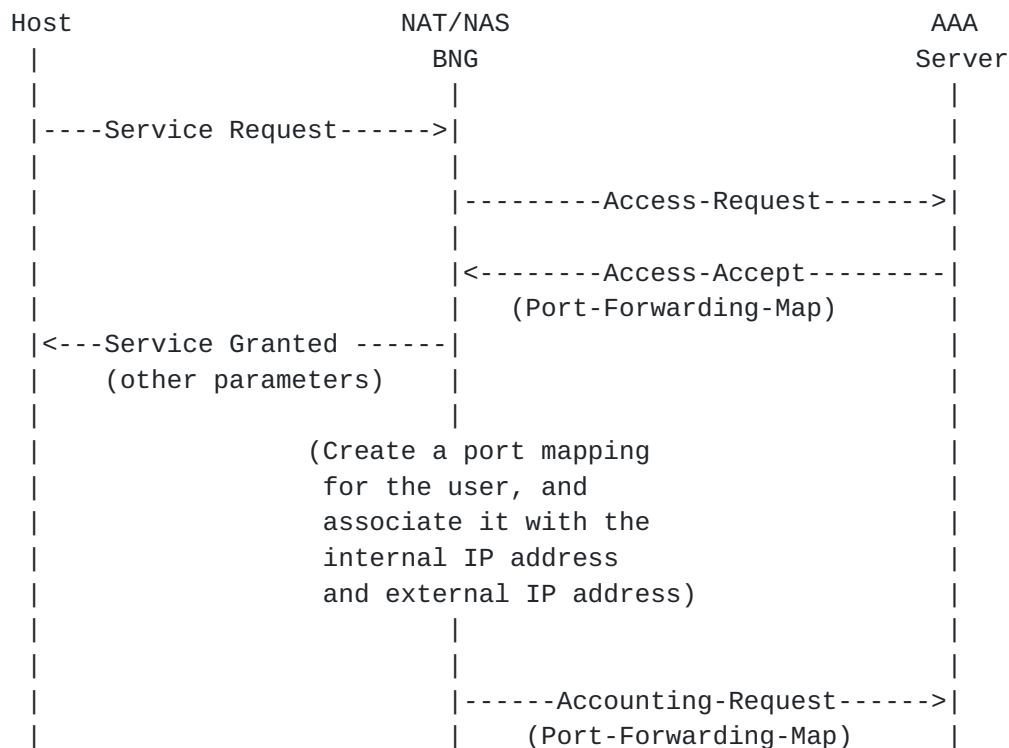
                Figure 4: RADIUS Message Flow for configuring a forwarding port
                                     mapping

   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 5 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----------|
      |                  |     (Port-Forwarding-Map)     |
      |                  |                             |
      |                  Internal IP Address                    |
      |                  Port Map (a:Y)                         |
      |                           |                             |
      |                  |---------CoA Response--------->|
      |                  |     (Port-Forwarding-Map)     |
      |                           |                             |
```
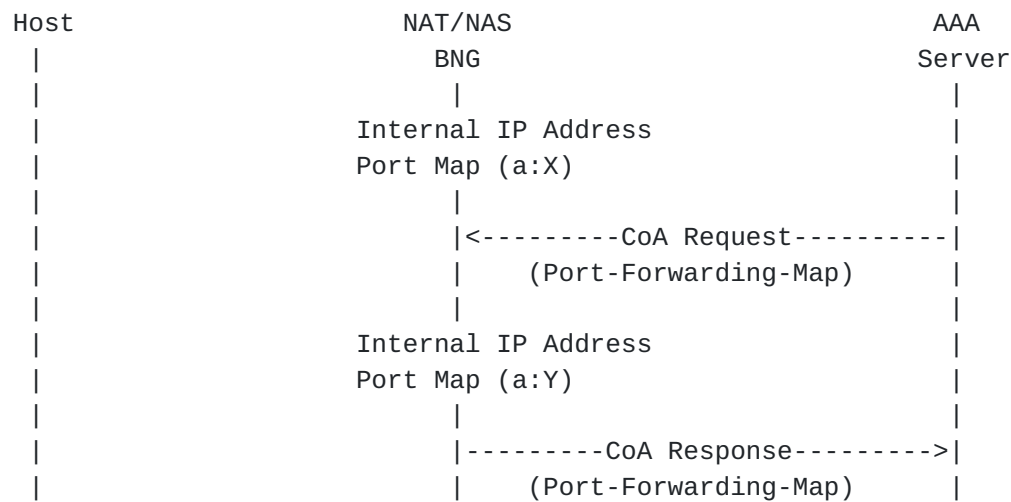
           Figure 5: RADIUS Message Flow for changing a user's forwarding port
                                   mapping

4.1.4. An Example

   An Internet Service Provider (ISP) assigns TCP/UDP 500 ports for the
   subscriber 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 Port-Session-Limit attribute and 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 Port-Session-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 Port-Session-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 Port-Session-Limit 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 Port-
Session-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
de-allocate 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 6 illustrates an example of the flow exchange which occurs
when a visiting UE connects to a CPE offering Wi-Fi service.

For identification purposes (see [RFC6967]), once the CPE assigns a
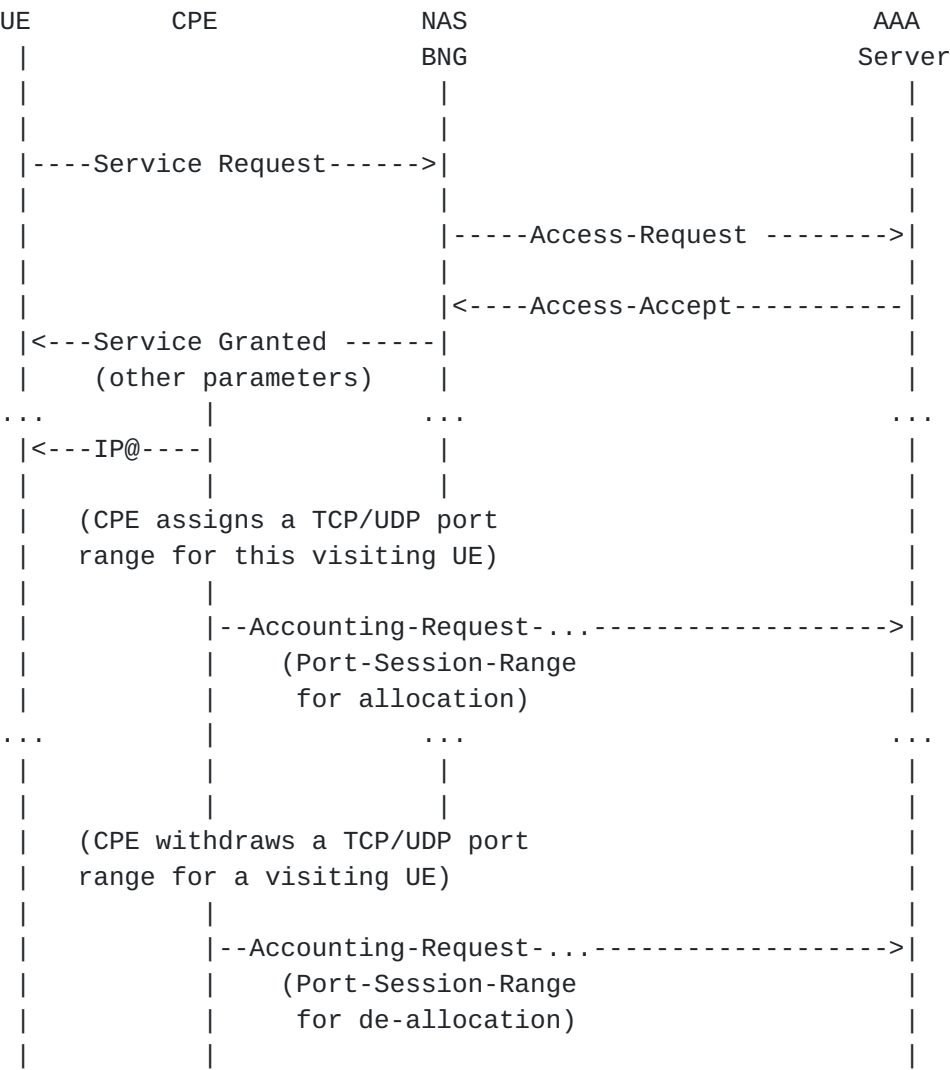port set, it issues a RADIUS message to report the assigned port set.

```
   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-...------------------->|
    |           |      (Port-Session-Range                  |
    |           |       for allocation)                     |
   ...          |               ...                        ...
    |           |                |                          |
    |           |                |                          |
    |    (CPE withdraws a TCP/UDP port                      |
    |     range for a visiting UE)                          |
    |           |                |                          |
    |           |--Accounting-Request-...------------------->|
    |           |      (Port-Session-Range                  |
    |           |       for de-allocation)                  |
    |           |                                          |
```

        Figure 6: RADIUS Message Flow for reporting CPE allocation/de-
                 allocation of a port set to a visiting UE

5. Table of Attributes

   The following table provides a guide as the attributes may be found
   in which kinds of RADIUS packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct. Request	#	Attribute
0-1	0-1	0	0	0-1	TBA1	Port-Session-Limit
0	0	0	0	0-1	TBA2	Port-Session-Range
0-1	0-1	0	0	0-1	TBA3	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.
0-1 Zero or one instance of this attribute MAY be present in packet.

6. Security Considerations

This document does not introduce any security issue than what has
been identified in [RFC2865].

7. IANA Considerations

7.1. RADIUS Attributes

This document requires new code point assignment for the three new
RADIUS attributes as follows:

o Port-Session-Limit

o Port-Session-Range

o Port-Forwarding-Map

7.2. Name Spaces

This document establishes a new name space for Session Type (see
Section 3.1 for the initial reservation of values. The allocation of
future values is according to RFC Required policy [RFC5226].

8. Acknowledgements

Many thanks to Dan Wing, Roberta Maglione, Daniel Derksen, and David
Thaler for their useful comments and suggestions.

9. References

9.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
           E. Lear, "Address Allocation for Private Internets", BCP
           5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, 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.

   [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,
              January 2008.

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.

   [I-D.ietf-softwire-lw4over6]
              Cui, Y., Qiong, Q., Boucadair, M., Tsou, T., Lee, Y., and
              I. Farrer, "Lightweight 4over6: An Extension to the DS-
              Lite Architecture", draft-ietf-softwire-lw4over6-03 (work
              in progress), November 2013.

   [I-D.miles-behave-l2nat]
              Miles, D. and M. Townsley, "Layer2-Aware NAT", draft-
              miles-behave-l2nat-00 (work in progress), March 2009.

   [RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network
              Address Translator (Traditional NAT)", RFC 3022, January
              2001.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              May 2008.

   [RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful
              NAT64: Network Address and Protocol Translation from IPv6
              Clients to IPv4 Servers", RFC 6146, April 2011.

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

   [RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P.
              Roberts, "Issues with IP Address Sharing", RFC 6269, June
              2011.

   [RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
              Stack Lite Broadband Deployments Following IPv4
              Exhaustion", RFC 6333, August 2011.

   [RFC6431]   Boucadair, M., Levis, P., Bajko, G., Savolainen, T., and
               T. Tsou, "Huawei Port Range Configuration Options for PPP
               IP Control Protocol (IPCP)", RFC 6431, November 2011.

   [RFC6619]   Arkko, J., Eggert, L., and M. Townsley, "Scalable
               Operation of Address Translators with Per-Interface
               Bindings", RFC 6619, June 2012.

   [RFC6887]   Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P.
               Selkirk, "Port Control Protocol (PCP)", RFC 6887, April
               2013.

   [RFC6888]   Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A.,
               and H. Ashida, "Common Requirements for Carrier-Grade NATs
               (CGNs)", BCP 127, RFC 6888, April 2013.

   [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, June 2013.

Authors' Addresses

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

   Email: dean.cheng@huawei.com

   Jouni Korhonen
   Nokia Siemens Networks
   Linnoitustie 6
   Espoo FIN-02600
   Finland

   Email: jouni.nospam@gmail.com

   Mohamed Boucadair
   France Telecom
   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