Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2016

D. Cheng
Huawei
J. Korhonen
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

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:

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

- 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.

- 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.

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

- 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.

- 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.

- 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.

- 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.

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

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

- 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.

- 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:

- an IP-Port-Type TLV (see Section 3.2.1),
- an IP-Port-Limit TLV (see Section 3.2.2),
- 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.

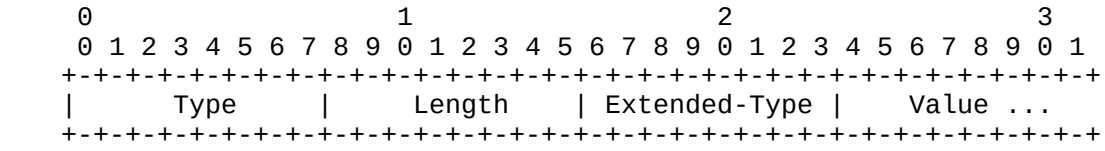

Figure 1

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:

- an IP-Port-Type TLV (see Section 3.2.1),
- an IP-Port-Range-Start TLV (see Section 3.2.9),
- an IP-Port-Range-End TLV (see Section 3.2.10),
- an IP-Port-Alloc TLV (see Section 3.2.8),
- an optional IP-Port-Ext-IPv4-Addr TLV (see Section 3.2.3),
- 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.

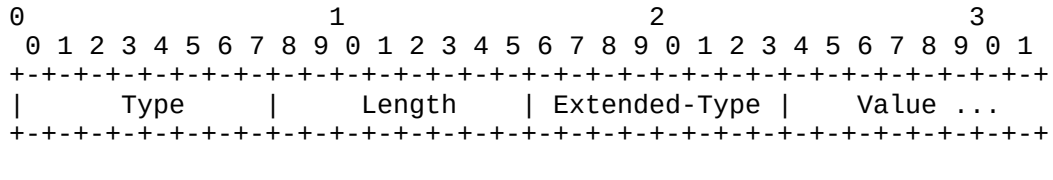

Figure 2

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:

- an IP-Port-Type TLV (see Section 3.2.1),
- an IP-Port-Int-Port TLV (see Section 3.2.6),
- an IP-Port-Ext-Port TLV (see Section 3.2.7),
- 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),
- 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),
- 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.

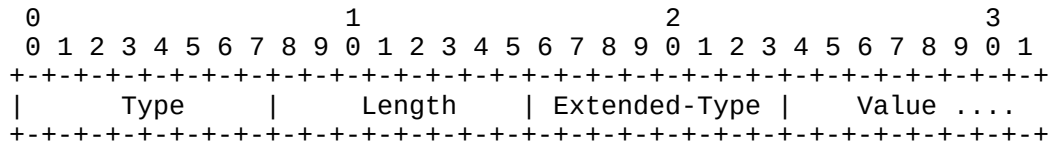

Figure 3

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.

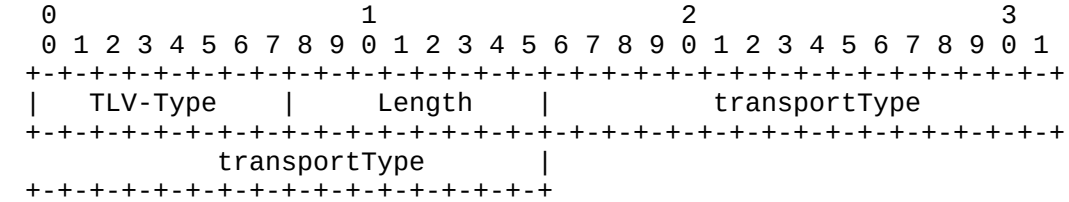

Figure 4

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:

- IP-Port-Limit-Info Attribute, identified as 241.TBD1.1 (see Section 3.1.1).
- IP-Port-Range Attribute, identified as 241.TBD2.1 (see Section 3.1.2).
- 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.

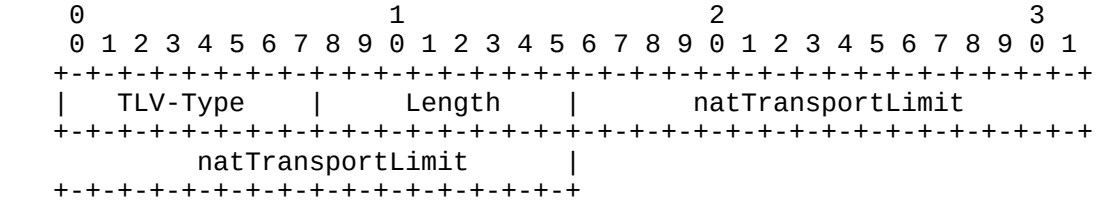

Figure 5

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]).

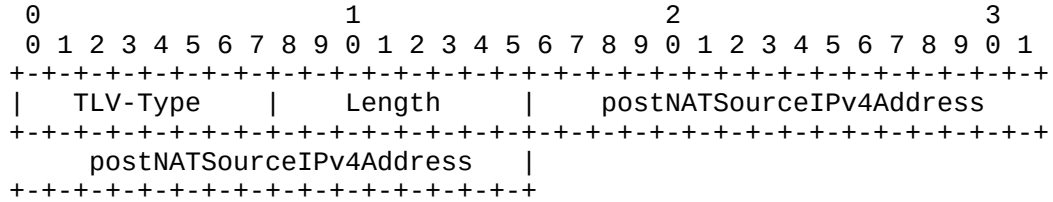

Figure 6

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:

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

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

- 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]).

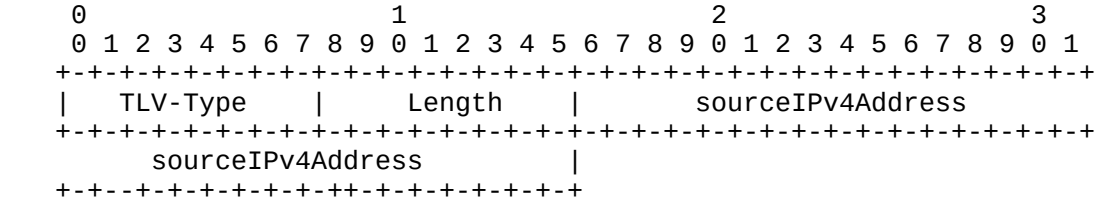

Figure 7

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]).

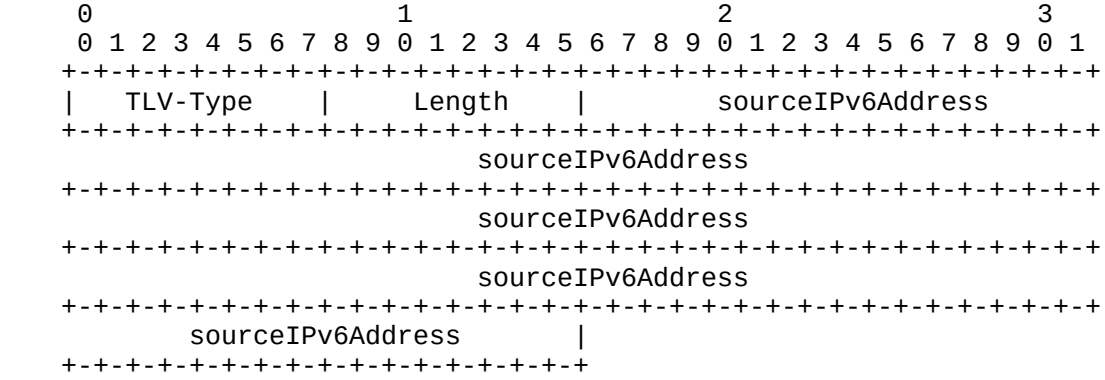

Figure 8

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]).

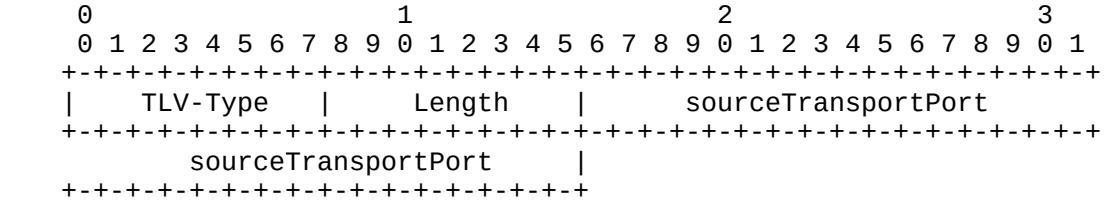

Figure 9

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]).

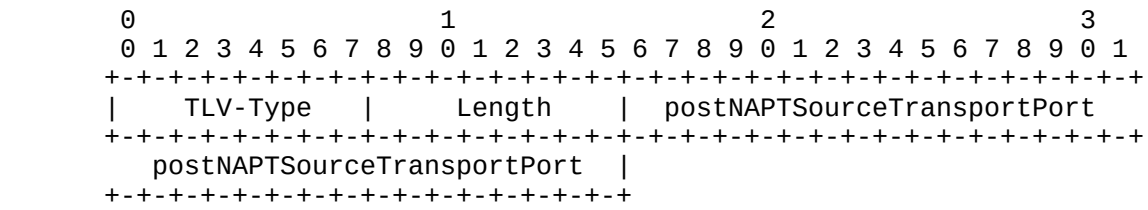

Figure 10

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.

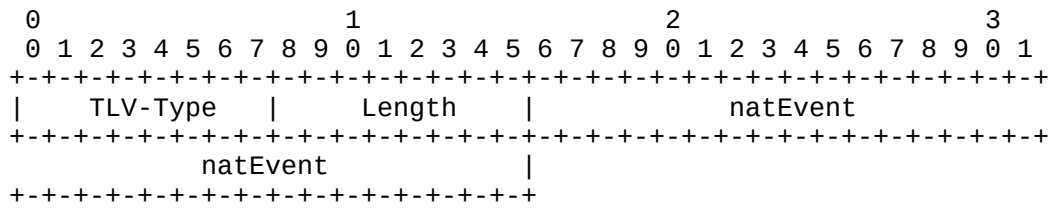

Figure 11

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]).

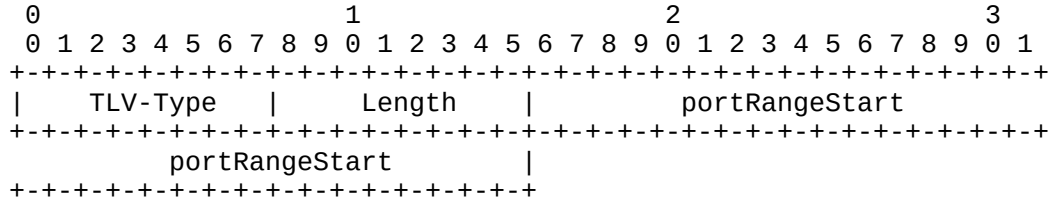

Figure 12

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]).

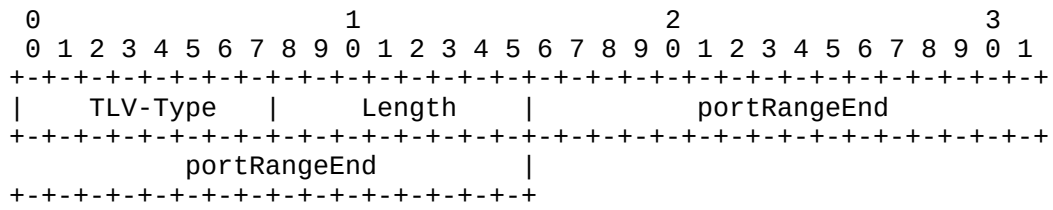

Figure 13

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.

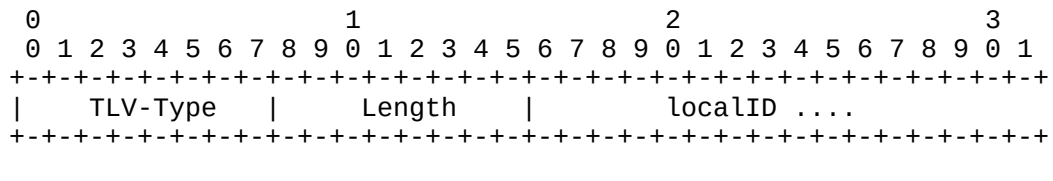

Figure 14

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:

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

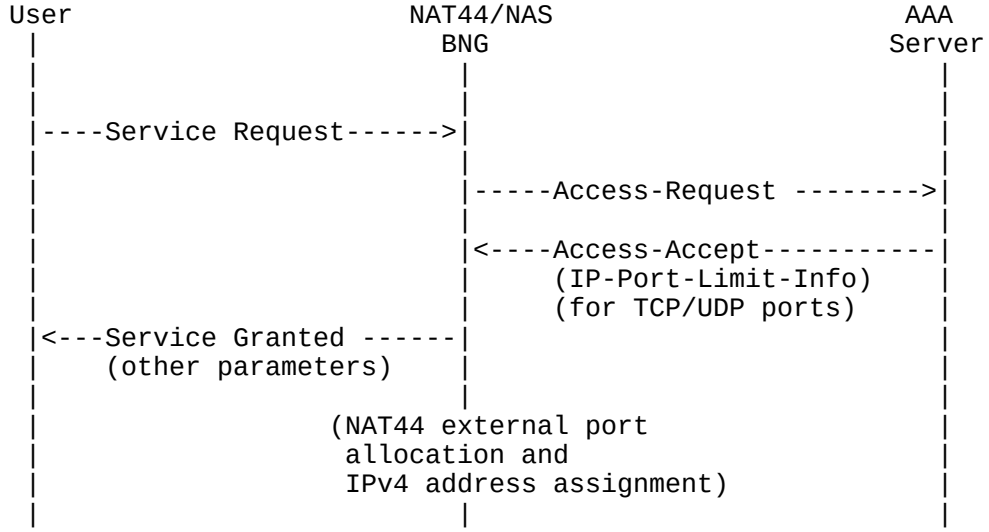

Figure 15: RADIUS Message Flow for Configuring NAT44 Port Limit

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.

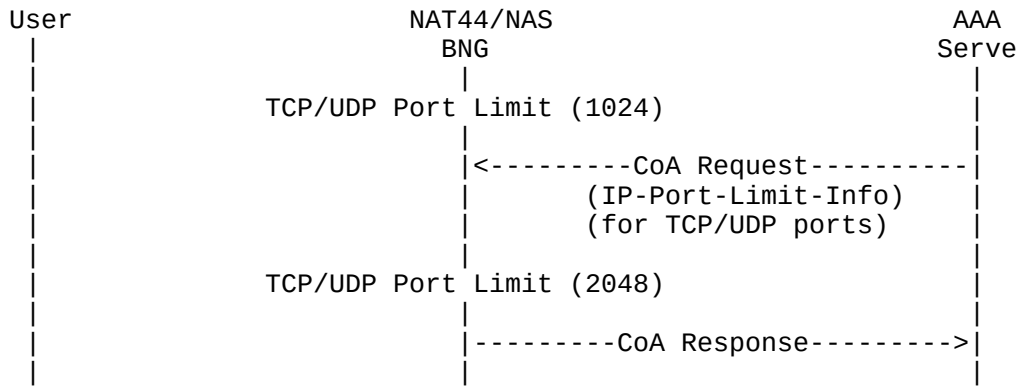

Figure 16: RADIUS Message Flow for changing a user's NAT44 port limit

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.

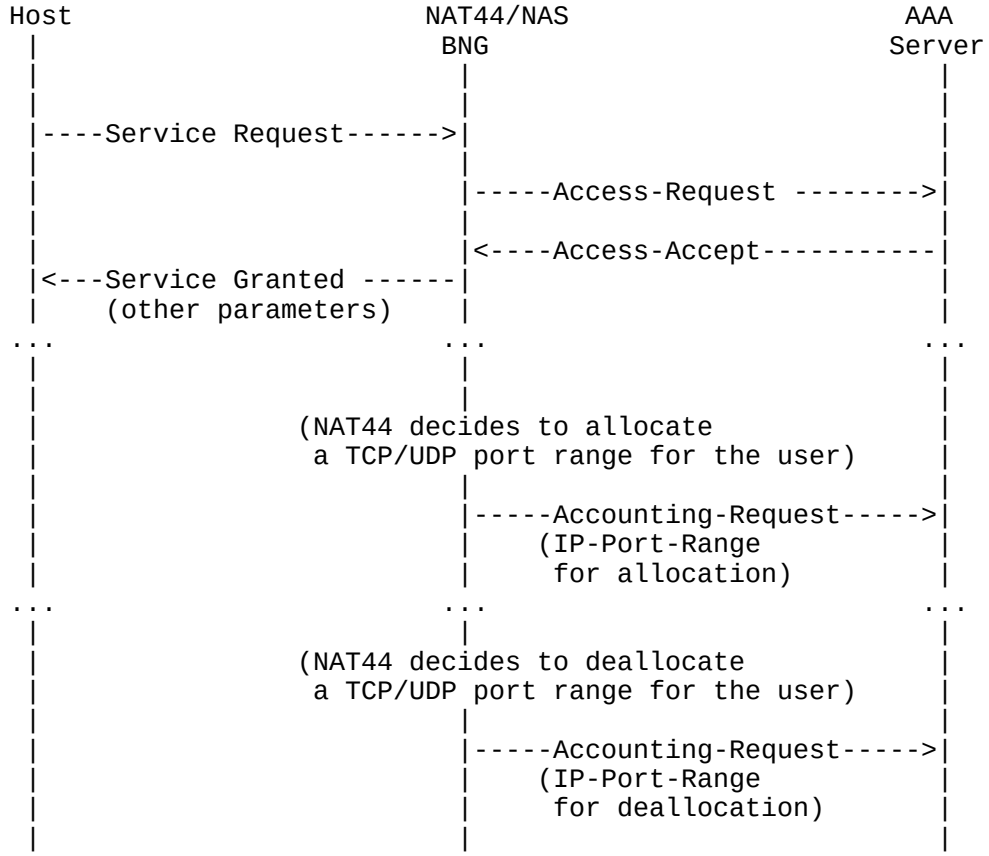

Figure 17: RADIUS Message Flow for reporting NAT44 allocation/ deallocation of a port set

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.

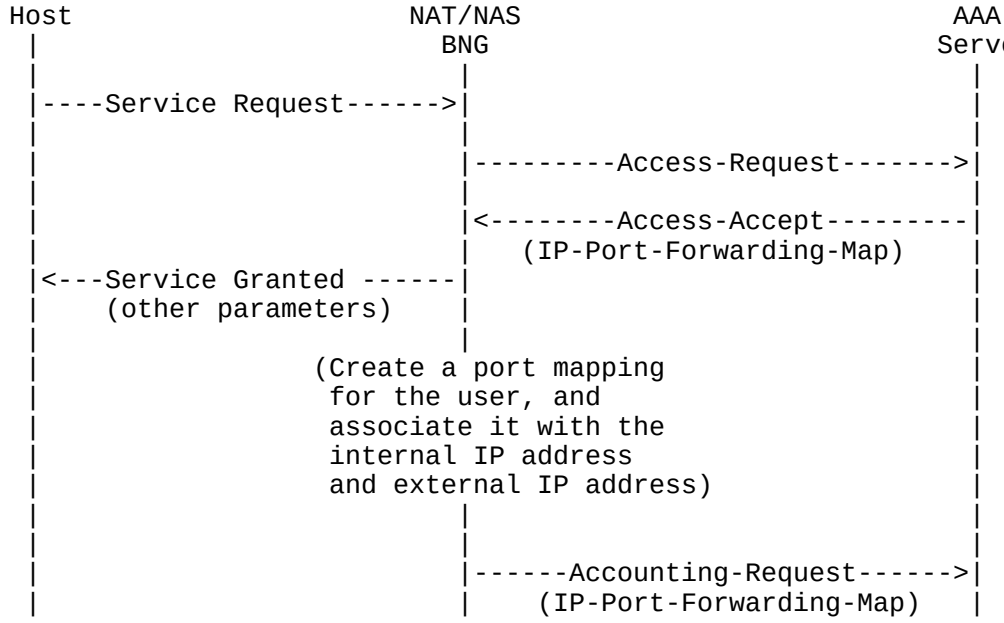

Figure 18: RADIUS Message Flow for configuring a forwarding port mapping

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

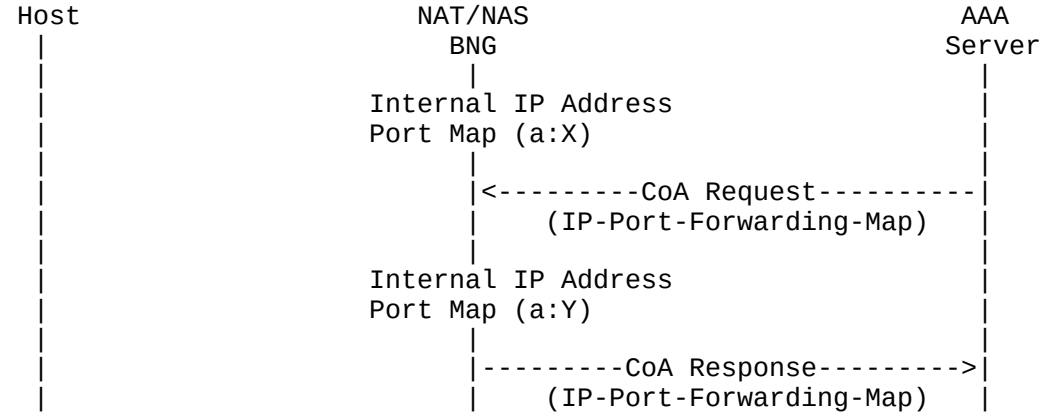

Figure 19: RADIUS Message Flow for changing a user’s forwarding port mapping

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.

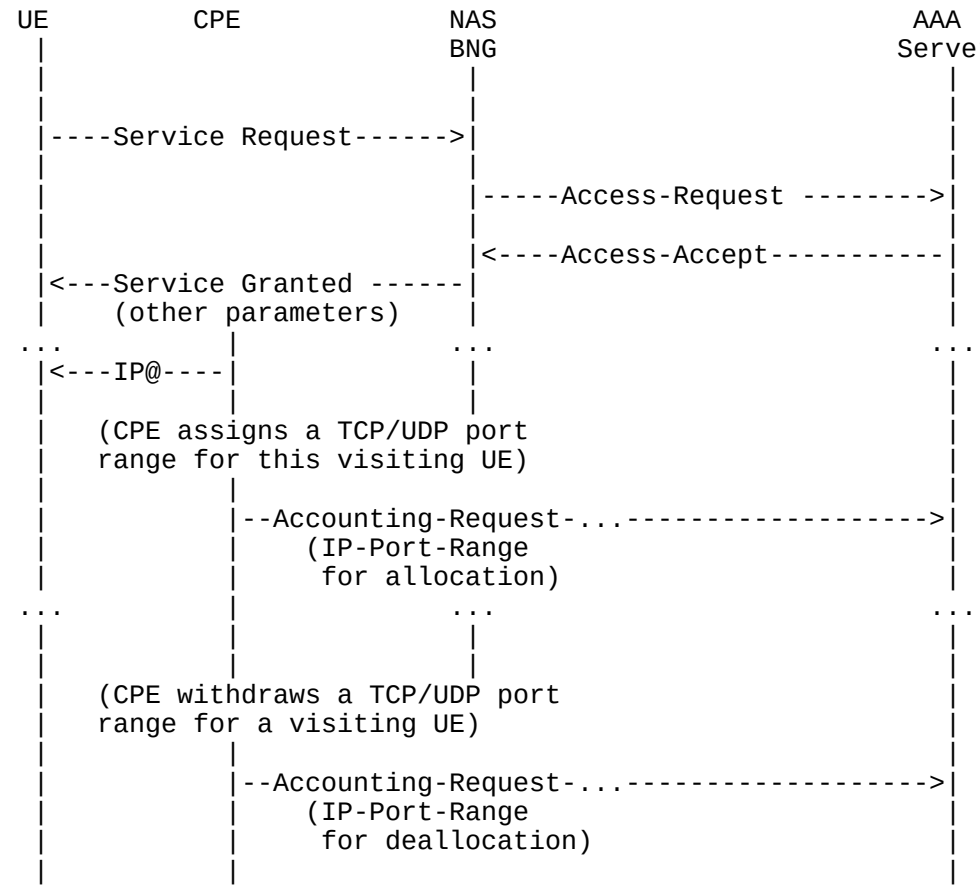

Figure 20: RADIUS Message Flow for reporting CPE allocation/ deallocation of a port set to a visiting UE

5. Table of Attributes

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

- IP-Port-Limit-Info: 241.TBD1.
- IP-Port-Range: 241.TBD2.
- 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:

- 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).

- 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.

- 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