# RADIUS Extensions
# for
# Port Set Configuration and Reporting

**draft-cheng-behave-cgn-cfg-radius-ext-07**

**Dean Cheng (dean.cheng@huawei.com)**

**Jouni Korhonen (jouni.nospam@gmail.com)**

**Mehamed Boucadair (mohamed.boucadair@oragne.com)**

**Senthil Sivakumar (ssenthil@cisco.com)**

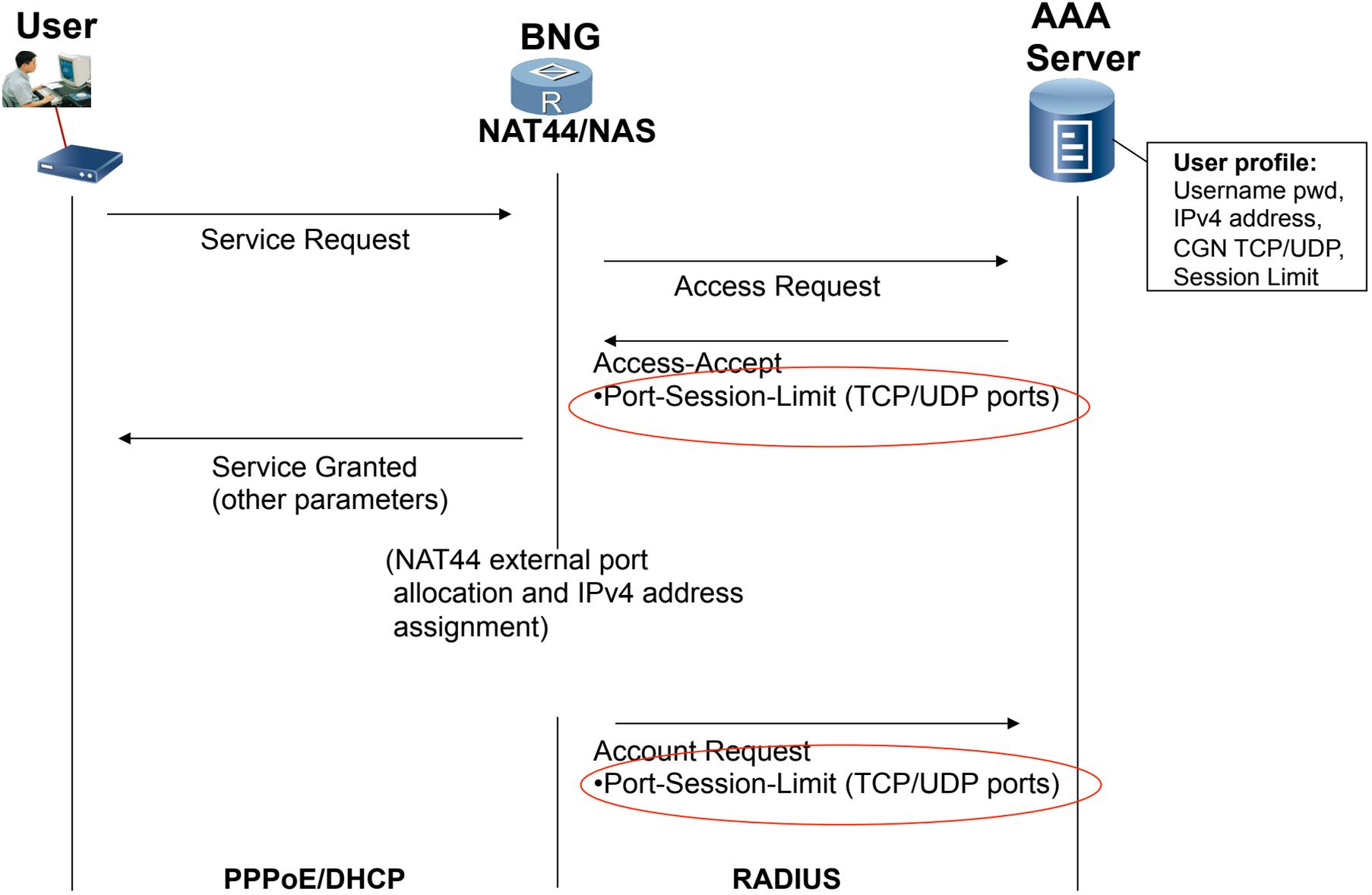**IETF London**

**March, 2014**

# History

- 00 text - merged from two earlier drafts per suggestions
  - draft-cheng-behave-nat44-pre-allocated-ports-02
  - draft-cheng-behave-nat-fwd-port-radius-ext-00
- 00 text presented at RADEXT WG at Quebec meeting
- 00 text was listed as one "potential work" on BEHAVE WG Chairs' slide at Quebec meeting
- Jouni Korhonen joined the work with much help
- 01 text posted in October 2011
- 01 text presented at BEHAVE WG at Taipei meeting
- 02 text posted in January 2012 (minor editorial changes)
- 03 text posted in April 2012
  - Med Boucadair joined as a co-author with contributing text
  - Focus on RADIUS extensions that can be used for any port-based devices
  - Changed the title of the document (CGN ->port-based device)
    - Was – "Radius Extensions for CGN Configurations"
    - Now – "RADIUS Extensions for Port Set Configuration and Reporting"
  - Added Section 4.2 for WiFi application using the proposed RADIUS extensions
- 04 text posted in October 2012
- Senthil Sivakumar joined the work & helped the edits (05 text) in May 2013
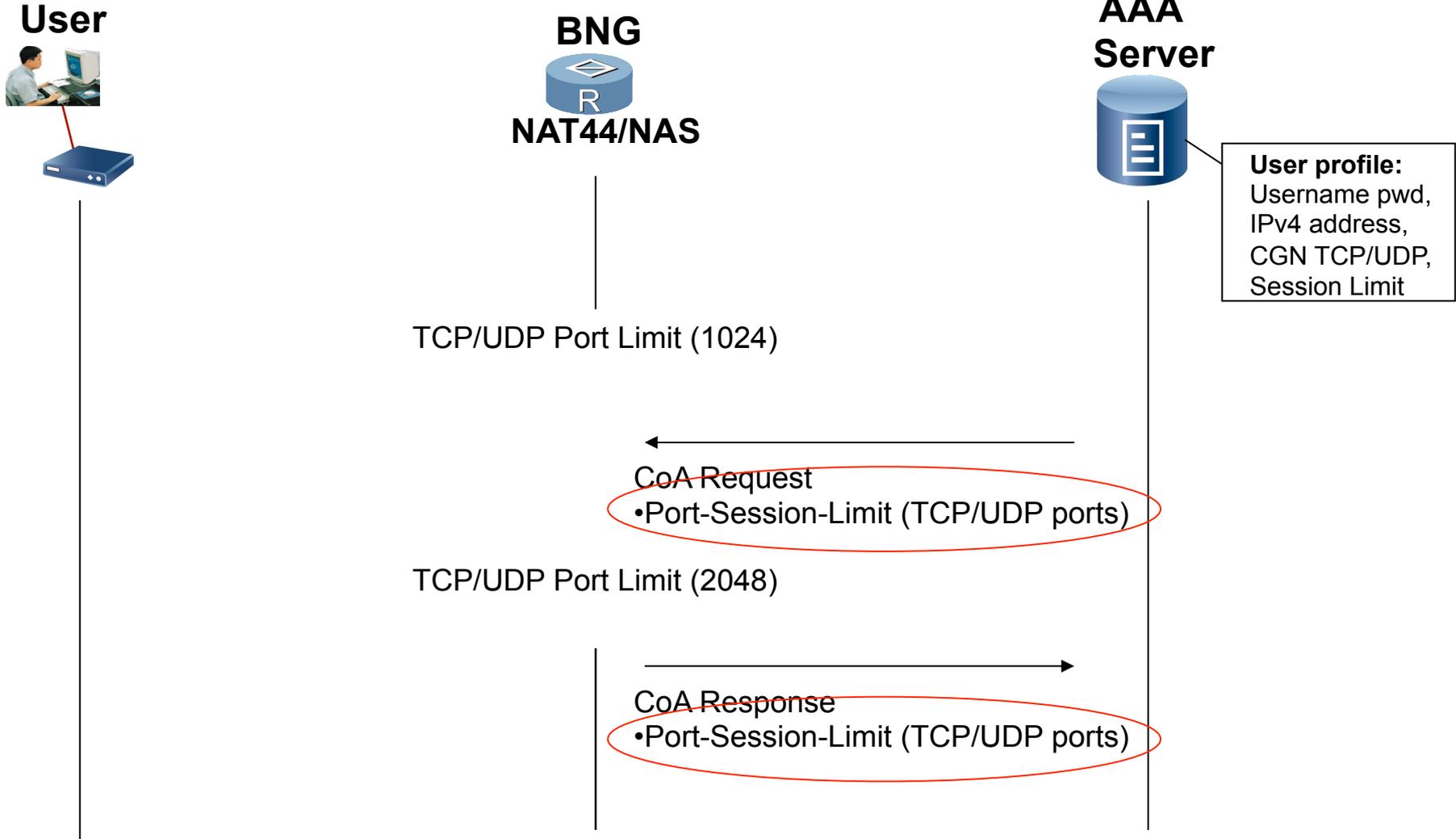- 06/07 text -  Minor updates in December 2013

# Motivation

- **Scenario (in a broadband network, WiFi network, etc.)**
  - ➤ **A port-set device, capable of performing mapping on IP address and port need to communicate with a RADIUS server.**
  - ➤ **Examples:**
    - ➤ **A CGN acquires TCP/UDP port limit for a given user from the RADIUS server**
    - ➤ **A CGN reports a range of TCP/UDP ports allocated/de-allocated for a given user to the RADIUS server**
    - ➤ **A CGN acquires a forwarding port for a given user from the RADIUS server**
    - ➤ **A WiFi server (CPE) reports a range of TCP/UDP ports allocated/de-allocated for a visiting UE to the RADIUS server**
- **Proposed solutions**
  - ➤ **Use RADIUS protocol for communication between a RADIUS server and a port-set device where NAS resides**
  - ➤ **Proposing three new RADIUS attributes**
    - ➤ **Limit for an end user on TCP/UDP ports (or ICMP identifiers) usage**
    - ➤ **The range of TCP/UDP ports (or ICMP identifiers) allocated or de-allocated for an end user**
    - ➤ **The forwarding port mapping definition for an end user**

**3**

# Configure NAT44 TCP/UDP Session Limit via RADIUS

# Change NAT44 TCP/UDP Session Limit via RADIUS

**User**

**BNG**

**NAT44/NAS**

**AAA Server**

**User profile:**
Username pwd,
IPv4 address,
CGN TCP/UDP,
Session Limit

TCP/UDP Port Limit (1024)

CoA Request
•Port-Session-Limit (TCP/UDP ports)

TCP/UDP Port Limit (2048)

CoA Response
•Port-Session-Limit (TCP/UDP ports)

5

# Port-Session-Limit Attribute

```
 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      |
+-+-+-+-+-+-+-+-+-+
```
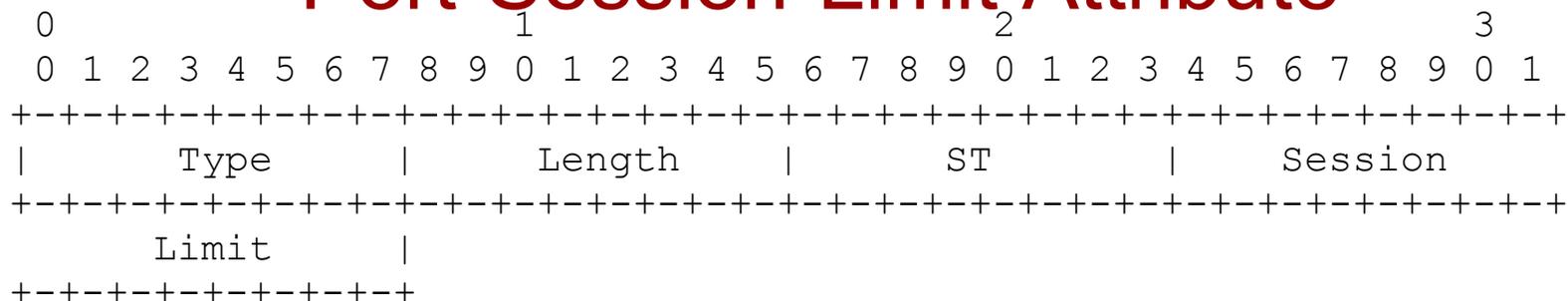
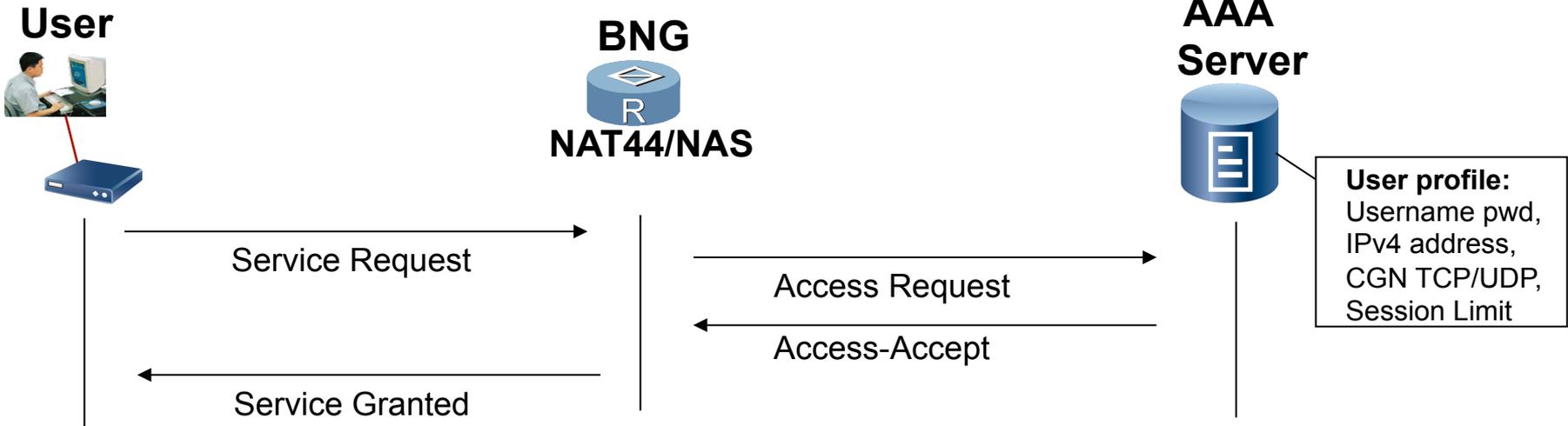Type – TBA1 for Port-Session-Limit

Length – 5 octets, total length of this attributes including Type and Length

ST – Session Type(8 bit) contains an enumerated value that indicates the
     applicability of the Session Limit as follows:
   0: The limit as specified is applied to the sum of TCP ports, UDP
      ports and ICMP identifiers.
   1: The limit as specified is applied to the sum of TCP ports
      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 imposed to the
        total number of TCP ports, or UDP ports, or the sum of the two,
        or ICMP Identifiers, or the sum of the three, depending on the
        value in the Session Type field, that the specific user can use
        during CGN operation.

**6**

# Report NAT44 TCP/UDP Port Allocation Range via RADIUS

**User**

**BNG**

NAT44/NAS

**AAA Server**

**User profile:**
Username pwd,
IPv4 address,
CGN TCP/UDP,
Session Limit

Service Request

Access Request

Access-Accept

Service Granted

CGN allocates a TCP/UDP
port range for the user
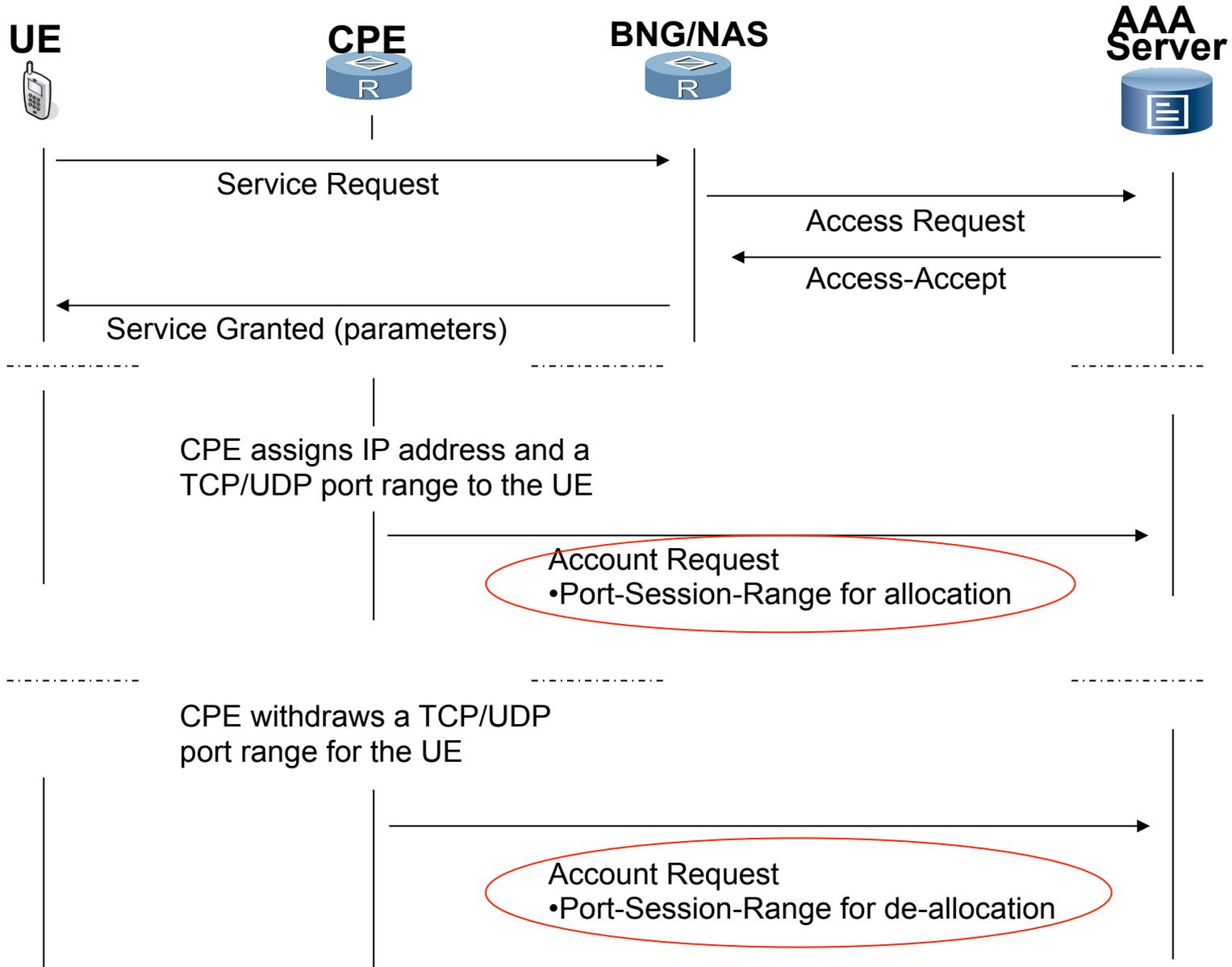
Account Request
•Port-Session-Range for allocation

CGN de-allocates a TCP/UDP
port range for the user

Account Request
•Port-Session-Range for de-allocation

**PPPoE/DHCP**

**RADIUS**

# Report Port Allocation/De-allocation for a UE



**UE**     **CPE**     **BNG/NAS**     **AAA Server**

Service Request

Access Request

Access-Accept

Service Granted (parameters)

CPE assigns IP address and a TCP/UDP port range to the UE

Account Request
- Port-Session-Range for allocation

CPE withdraws a TCP/UDP port range for the UE
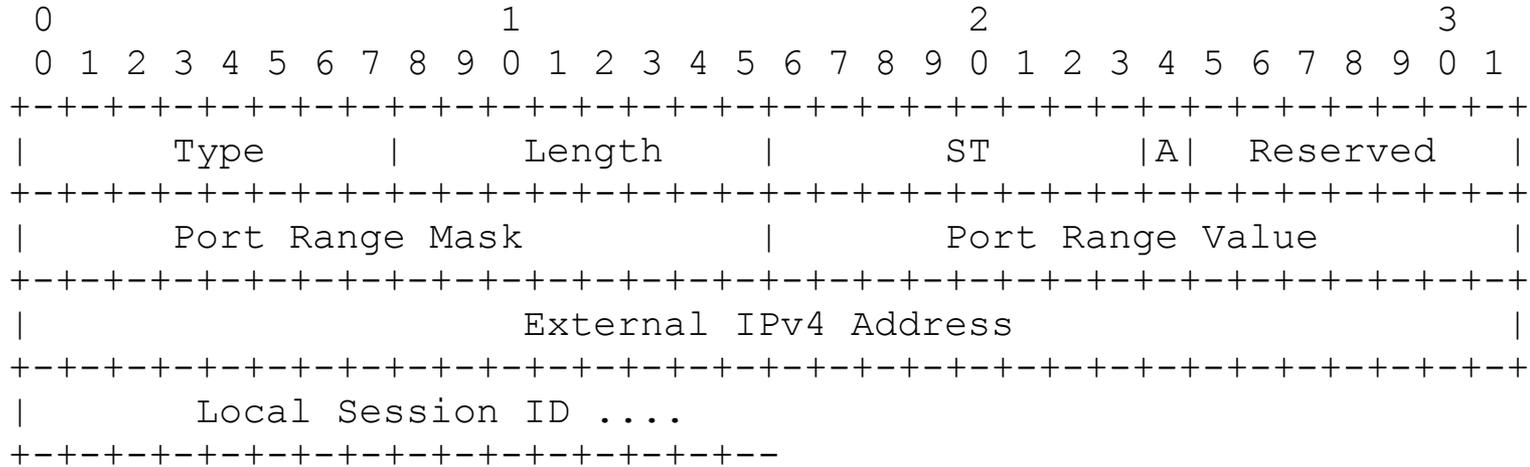
Account Request
- Port-Session-Range for de-allocation

# Port-Session-Range Attribute

```
 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 plus the length of Local Session ID) octets

ST (Session Type)- 8 bits,
   This field contains an enumerated value (refer to Section 3.1) that
   indicates the semantics of the Session Range.

A-bit Flag –
    0: The specified range is for allocation.
    1: The specified range is for de-allocation.

# CGN-Session-Range Attribute (Cont.)

Reserved – set to zero by sender and ignored by receiver.

Port Range Mask:
> The Port Range Mask (PRM) 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 Port Range Value (PRV) indicates the value of the significant bits of the Port Range Mask.  By default, no PRV is assigned. Refer to [RFC6431] for more details.
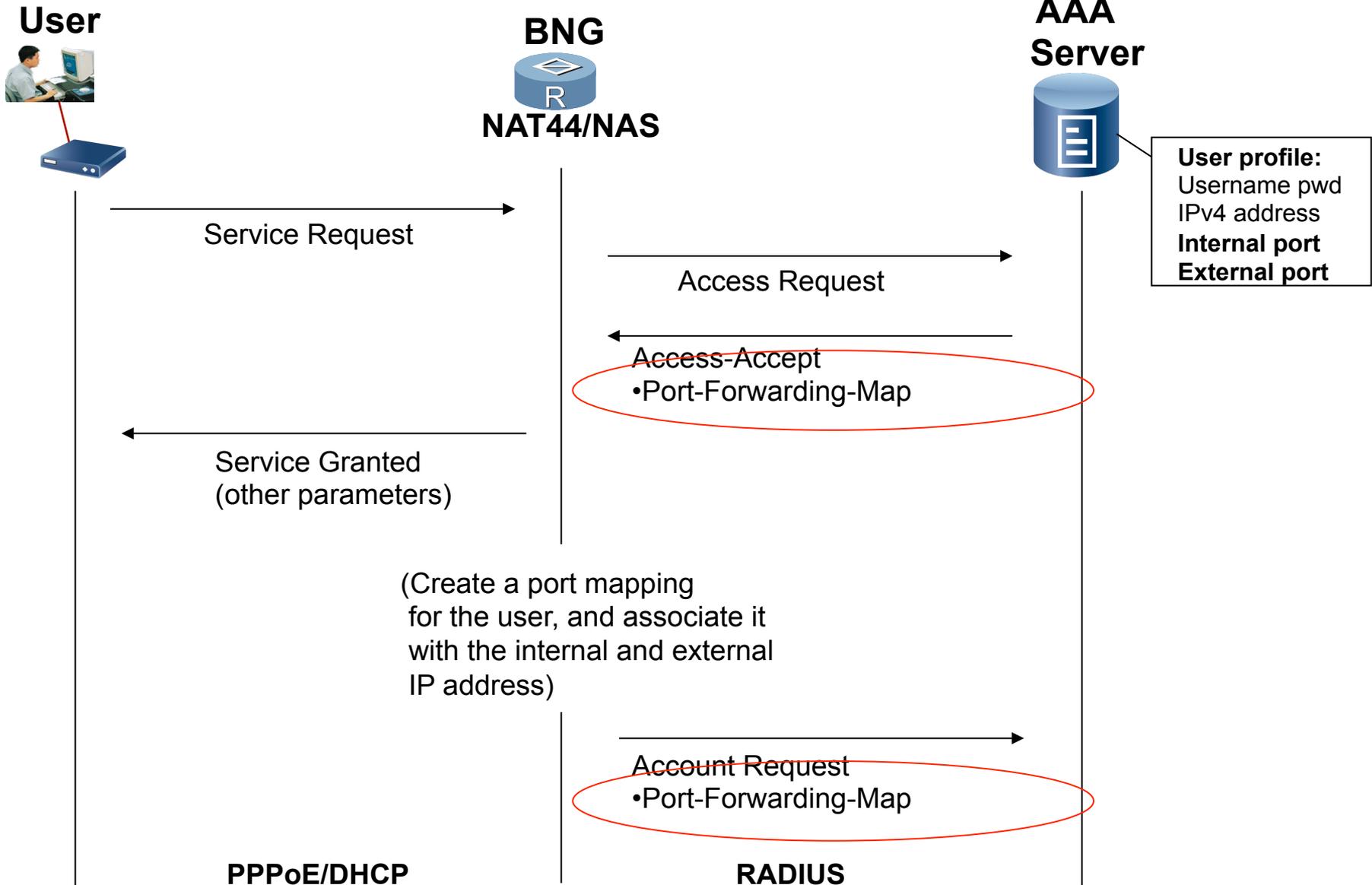
External IPv4 Address:
> This field contains the IPv4 address assigned to the associated subscriber to be used in the external realm.
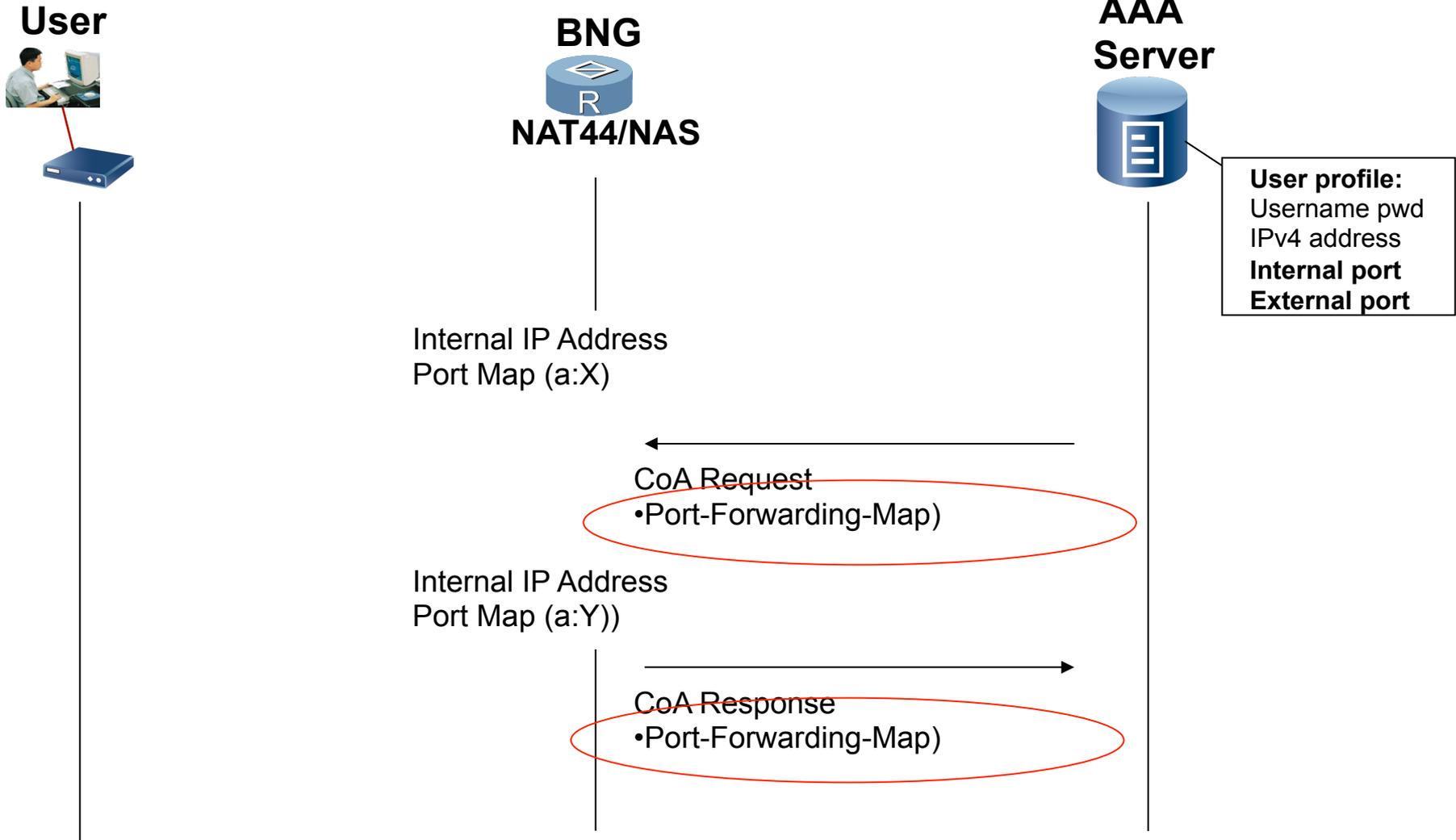
Local Session ID:
> This is an optional field and if presents, it contains a local session identifier at the customer premise, such as MAC address, interface ID, VLAN ID, PPP sessions ID, VRF ID, etc. The length of this field equals to the total attribute length minus 12 octets.

# NAT44 Port Forwarding Configuration via RADIUS

# Change NAT44 TCP/UDP Port Mapping via RADIUS

**User**

**BNG**

R

**NAT44/NAS**

**AAA Server**

User profile:
Username pwd
IPv4 address
**Internal port**
**External port**

Internal IP Address
Port Map (a:X)

CoA Request
•Port-Forwarding-Map)

Internal IP Address
Port Map (a:Y))

CoA Response
•Port-Forwarding-Map)

**PPPoE/DHCP**                    **RADIUS**

# Port-Forwarding-Map Attribute

```
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  .....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
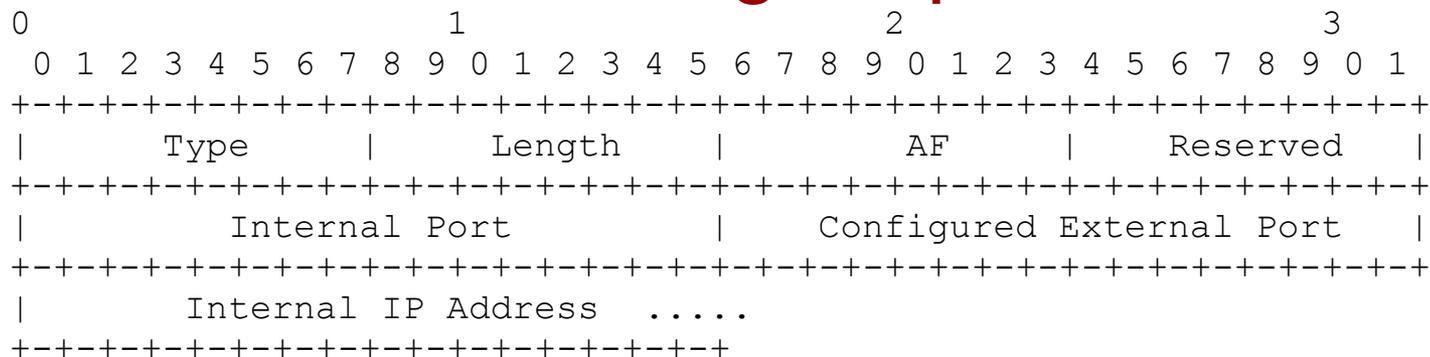
Type – TBA3 for Port-Forwarding-Map

Length – Depending on the value of the AF field, the length could be
        8, 12 or 24 octets.

AF (Address Family)- 8 bits. This field contains an enumerated value
   that indicates the address family of the internal IP address for
   the mapping as follows:
   0: no internal IP address
   1: The internal address is an IPv4 address.
   2: The internal address is an IPv6 address.
   3-255: Values not defined.

Internal Port – The internal port for the CGN mapping.

External Port – The external port for the CGN mapping.

Internal IP address – if exists, contains the internal IPv4 or IPv6
    address for the CGN mapping.

**13**

# IANA Considerations (code point request)

- New RADIUS attributes:
  - **Port-Session-Limit (Section 3.1)**
  - **Port-Session-Range (Section 3.2)**
  - **Port-Forwarding-Map (Section 3.3)**

- Session type (Section 3.1)
  - **0: Applicable to TCP/UDP port number and ICMP identifier**
  - **1: Applicable to TCP/UDP port number only**
  - **2: Applicable to TCP port number only**
  - **3: Applicable to UDP port number only**
  - **4: Applicable to ICMP identifier only**
  - **5-255: Undefined**

# Next step …

- Requesting to be adopted as a RADEXT WG document…

- Update the draft with clarification that the new RADIUS attribute types as requested are in the *extended type code space* per RFC6929.