

RADIUS Extensions for IP Port Configuration and Reporting

draft-ietf-radext-ip-port-radius-ext-01

Dean Cheng (dean.cheng@huawei.com)

Jouni Korhonen (jouni.nospam@gmail.com)

Mehamed Boucadair (mohamed.boucadair@oragne.com)

Senthil Sivakumar (ssenthil@cisco.com)

IETF Toronto

July, 2014

Draft Status

- **Adopted as a WG document in May 2014**
- **00.txt was posted on May 9 2014 (based on individual draft).**
- **Comments received on mailing list since London meeting**
 - Thanks to Alan DeKok, Lionel Morand, Peter Deacon, etc.
- **01.txt was posted on June 12 2014 with significant changes incorporating most of the comments including:**
 - Defined IP-Port-Type TLV.
 - Defined one TLV for each data field.
 - Changed to allow multiple instances for all proposed attributes.
 - Defined mandatory and optional TLVs within each proposed attribute.

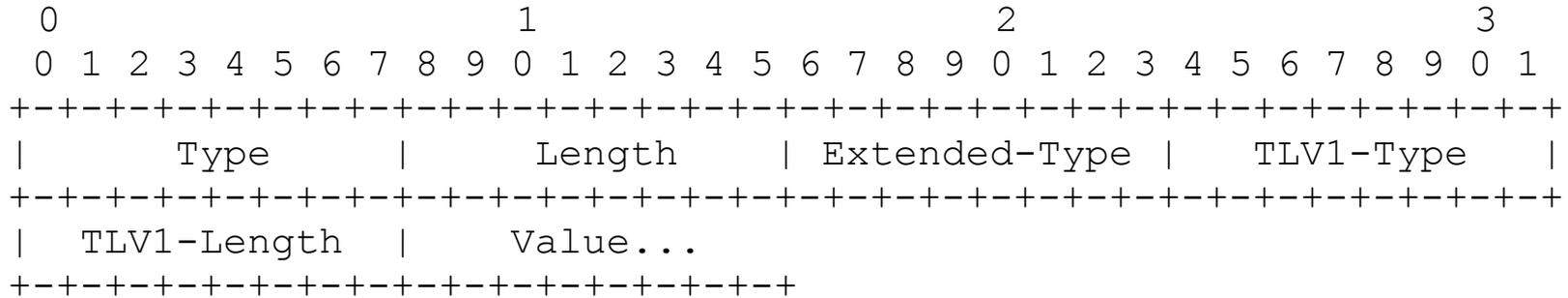
Motivation

- **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**
- **Use RADIUS protocol for communication between a RADIUS server and a port-set device where NAS resides**

Proposed Radius Attributes

- **IP-Port-Limit Attribute**
 - To configure the max number of IP ports associated with a specific or all IPv4 address for an IP service subscriber.
- **IP-Port-Range Attribute**
 - To report to the Radius server that a range IP ports that have been allocated or de-allocated associated with a specific IPv4 address for an IP service subscriber by a port set device.
- **IP-Port-Forwarding-Map Attribute**
 - To define the mapping between an internal IP port (associated with an internal IP address or customer's local identifier) and an external IP port (associated with an external IPv4 address).

Extended Type & IP-Port-Type TLV



Type:

TBA1 - Extended-Type-1 (241), Extended-Type-2 (242), Extended-Type-3 (243), or Extended-Type-4 (244) per [RFC6929].

Length:

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

Extended-Type:

TBA2.

TLV1-Type:

Type field of IP-Port-Type TLV. This one byte field indicates the IP port type as follows:

Extended Type & IP-Port-Type TLV (cont.)

TBA2-1:

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

TBA2-2:

Refer to TCP port and UDP port as a whole.

TBA2-3:

Refer to TCP port only.

TBA2-4:

Refer to UDP port only.

TBA2-5:

Refer to ICMP identifier only.

TLV1-Length:

Length field of IP-Port-Type TLV. This field indicates the total length in bytes of the TLV1, including the field of TLV1-Type, TLV1-Length, and the Value.

Value:

Value field of IP-Port-Type TLV. This field contains one or more TLVs.

Proposed Radius TLVs

- **IP-Port-Limit TLV**
 - To specify the max number of IP ports.
- **IP-Port-Ext-IPv4-Addr TLV**
 - To specify the external IPv4 address.
- **IP-Port-Int-IP-Addr TLV**
 - To specify the internal IPv4 or IPv6 address.
- **IP-Port-Alloc TLV**
 - To specify either allocation or de-allocation of IP ports.
- **IP-Port-Range-Start TLV**
 - To specify the largest port number of a contiguous IP ports.
- **IP-Port-Range-End TLV**
 - To specify the smallest port number of a contiguous IP ports.
- **IP-Port-Int-Port TLV**
 - To specify an internal IP port (associated with an internal IP address).
- **IP-Port-Ext-Port TLV**
 - To specify an external IP port (associated with an external IPv4 address).
- **IP-Port-Local-Id TLV**
 - To specify a customer-local significant identifier (e.g., a MAC address).

Attributes and Embedded TLVs

	IP-Port-Limit Attribute	IP-Port-Range Attribute	IP-Port-Forwarding-Map Attribute
IP-Port-Limit TLV	M	n/a	n/a
IP-Port-Ext-IPv4-Addr TLV	O ⁿ¹	O	O
IP-Port-Int-IP-Addr TLV	n/a	n/a	M ⁿ³
IP-Port-Int-Port TLV	n/a	n/a	M
IP-Port-Ext-Port TLV	n/a	n/a	M
IP-Port-Alloc TLV	n/a	M	n/a
IP-Port-Range-Start TLV	n/a	M ⁿ²	n/a
IP-Port-Range-End TLV	n/a	M ⁿ²	n/a
IP-Port-Local-Id TLV	n/a	O	M ⁿ³

n1: If not included, the port limit as specified in IP-Port-Limit TLV applied to IPv4 addresses.

n2: For port allocation, these two TLVs are mandatory.

For port de-allocation, if these two TLVs are present, all ports are de-allocated.

n3: Either IP-Port-Int-IP-Addr TLV or IP-Port-Local-Id TLV must be included.

Identifiers of the three Attributes

- **IP-Port-Limit Attribute**

- Type.Extended-Type.IP-Port-Type TLV {TBA2-1..TBA2-5}.

- [IP-Port-Limit TLV, {IP-Port-Ext-IPv4-Addr TLV }].

- **IP-Port-Range Attribute**

- Type.Extended-Type.IP-Port-Type TLV {TBA2-1..TBA2-5}.

- [IP-Port-Alloc TLV, {IP-Port-Range-Start TLV, IP-Port-Range-End TLV},

- {IP-Port-Ext-IPv4-Addr TLV}, {IP-Port-Local-Id TLV}].

- **IP-Port-Forwarding-Map Attribute**

- Type.Extended-Type.IP-Port-Type TLV {TBA2-1..TBA2-5}.

- [IP-Port-Int-Port TLV, IP-Port-Ext-Port TLV, {IP-Port-Int-IP-Addr TLV},

- {IP-Port-Ext-IPv4-Addr TLV}].

IANA Considerations

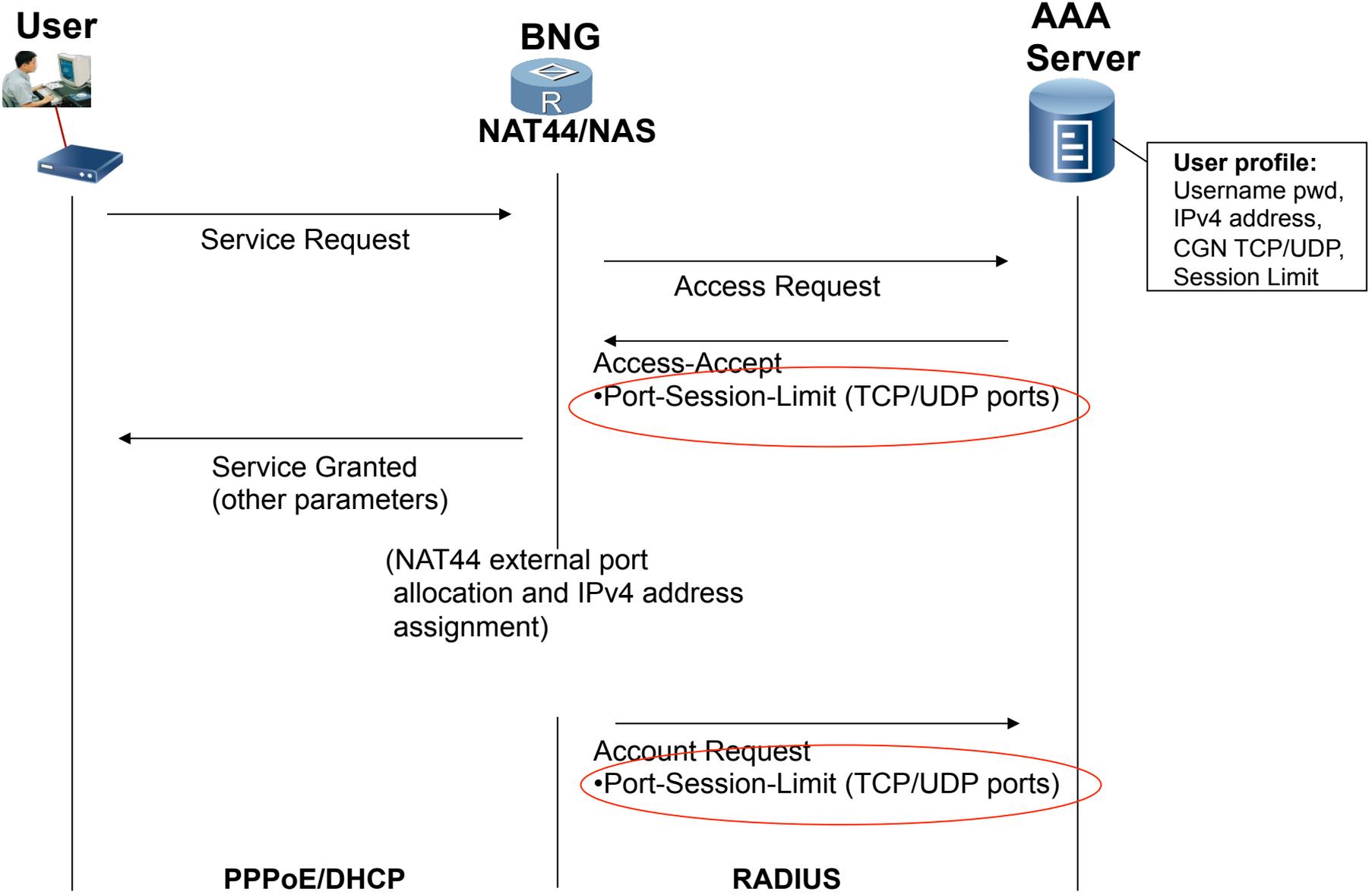
Name	Reference	Value
Type Field	Section 3.1.1	TBA1
Extended Field	Section 3.1.1	TBA2
IP-Port-Type TLV	Section 3.1.1	TBA2-1:TCP/UDP port and ICMP identifier TBA2-2:TCP/UDP port TBA2-3:TCP port TBA2-4:UDP port TBA2-5:ICMP identifier
IP-Port-Limit TLV	Section 3.1.2	TBA3
IP-Port-Ext-IPv4-Addr TLV	Section 3.2.2	TBA4
IP-Port-Int-IP-Addr TLV	Section 3.2.3	TBA5
IP-Port-Int-Port TLV	Section 3.2.4	TBA6
IP-Port-Ext-Port TLV	Section 3.2.5	TBA7
IP-Port-Alloc TLV	Section 3.2.6	TBA8
IP-Port-Range-Start TLV	Section 3.2.7	TBA9
IP-Port-Range-End TLV	Section 3.2.8	TBA10
IP-Port-Local-Id TLV	Section 3.2.9	TBA11

Next step ...

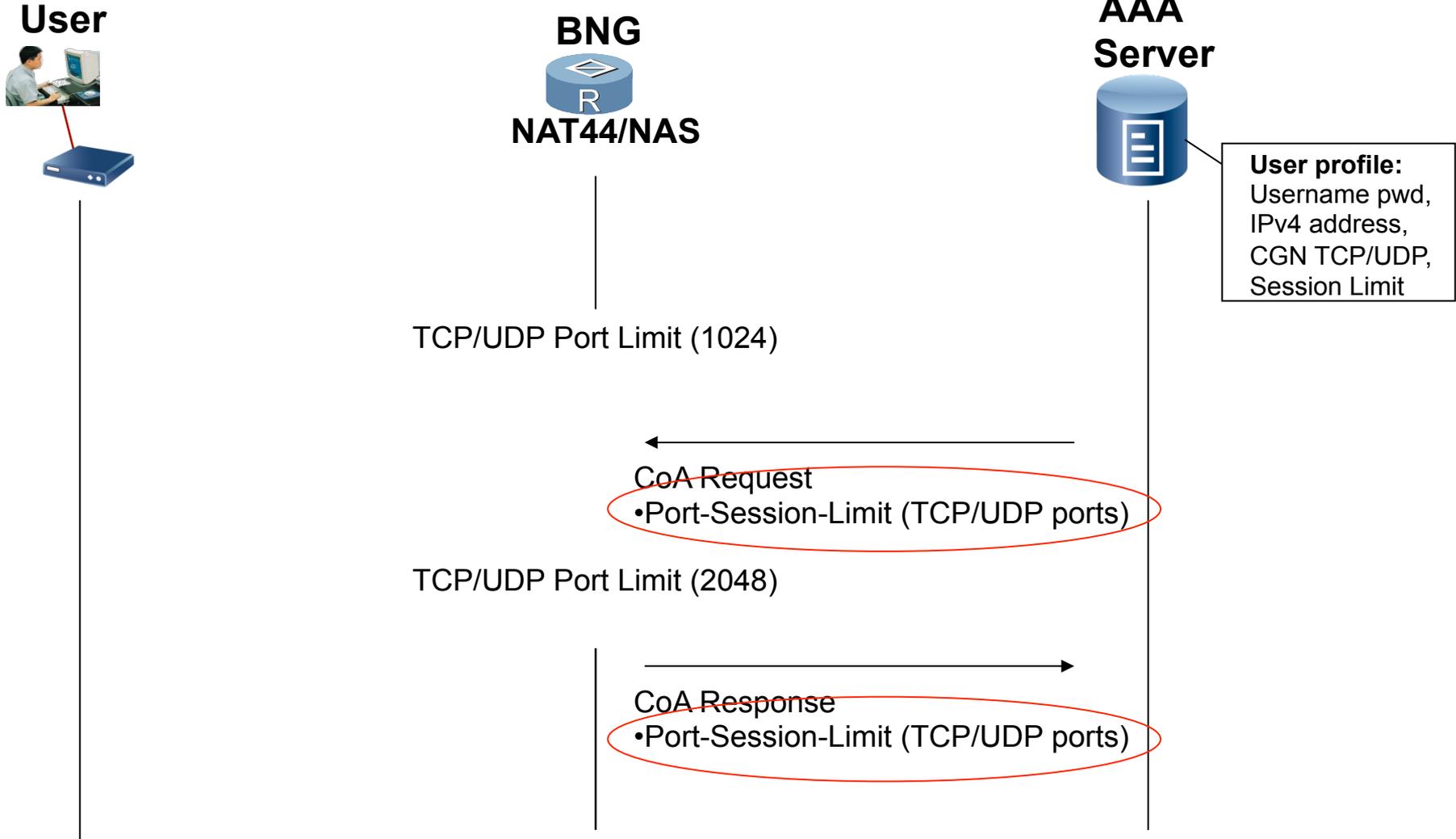
- Request the WG to review and provide comments....

Backup Slides

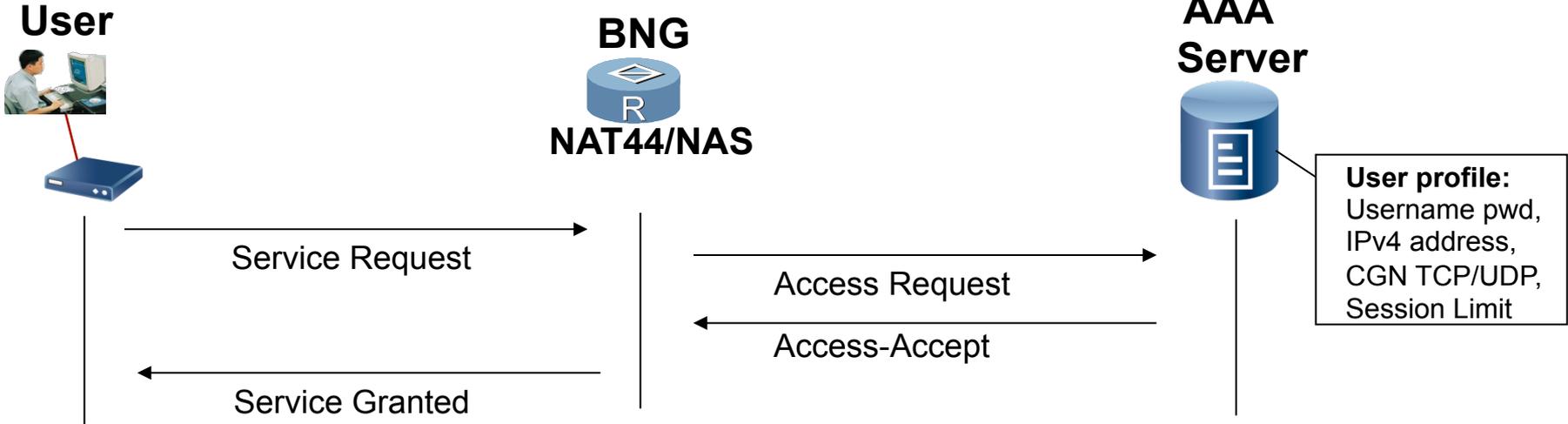
Configure NAT44 TCP/UDP Session Limit via RADIUS



Change NAT44 TCP/UDP Session Limit via RADIUS



Report NAT44 TCP/UDP Port Allocation Range via RADIUS



CGN allocates a TCP/UDP port range for the user

Account Request
•Port-Session-Range for allocation

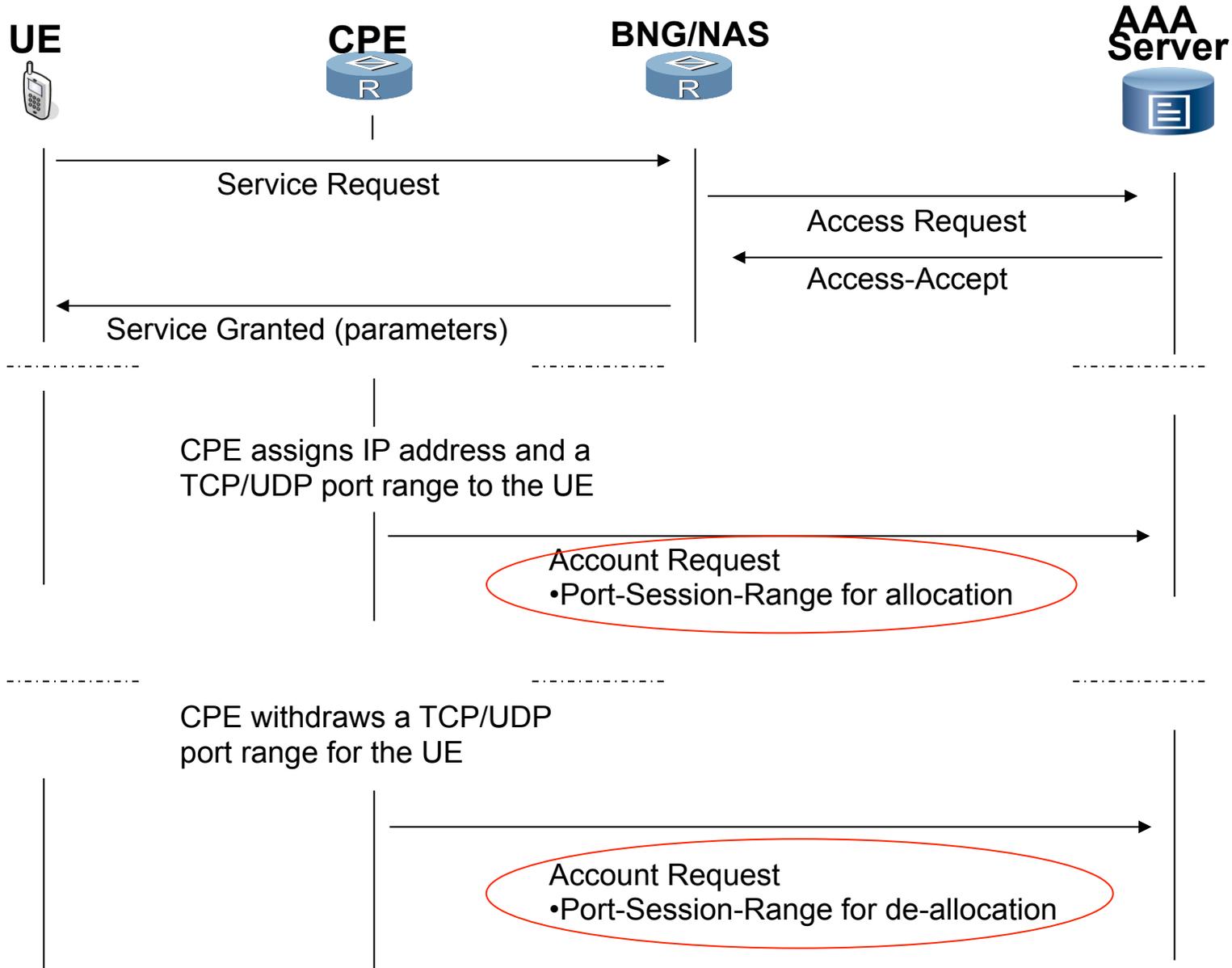
CGN de-allocates a TCP/UDP port range for the user

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

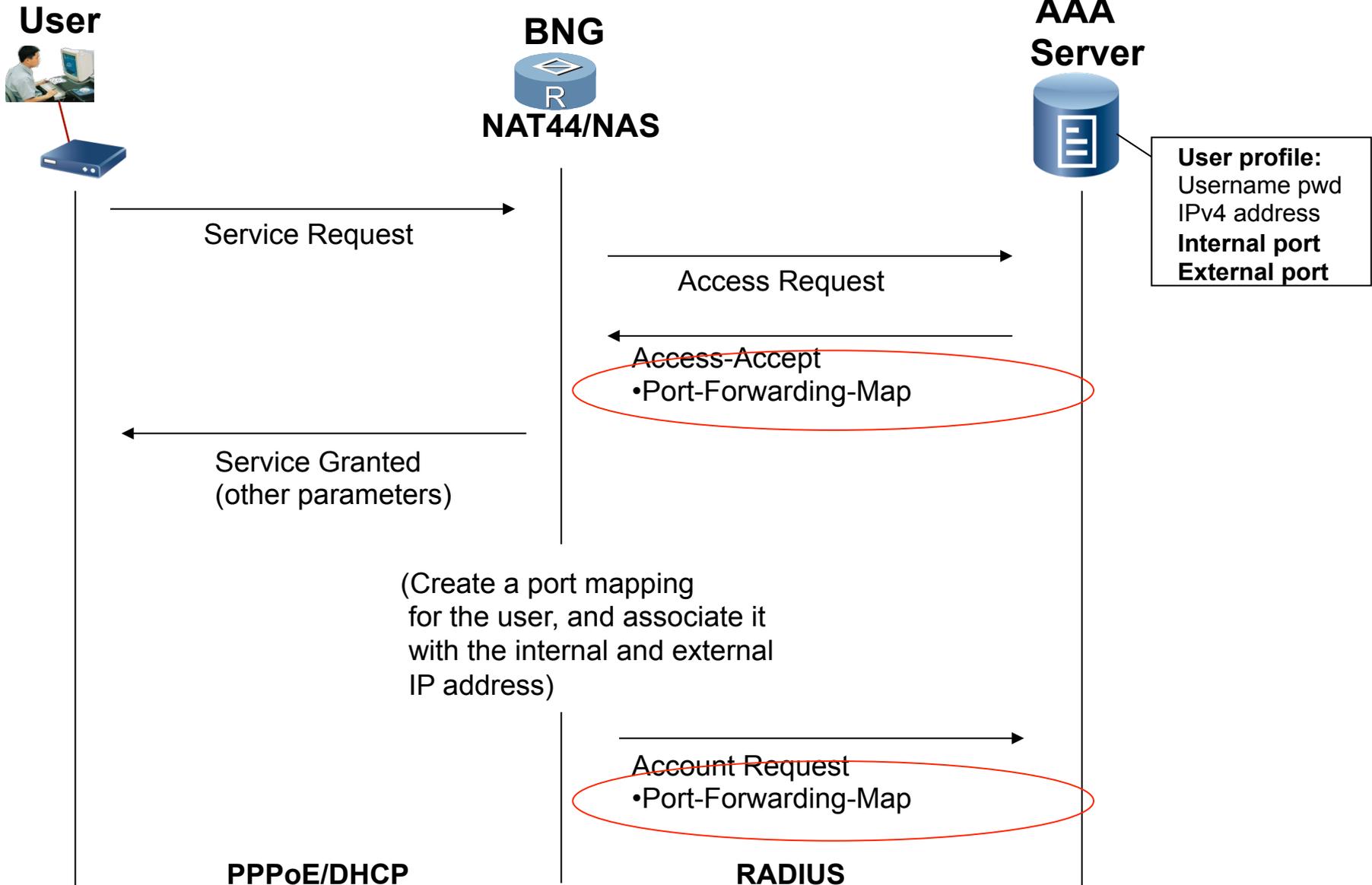
PPPoE/DHCP

RADIUS

Report Port Allocation/De-allocation for a UE



NAT44 Port Forwarding Configuration via RADIUS



Change NAT44 TCP/UDP Port Mapping via RADIUS

