Diameter NAT Control Application

draft-brockners-diameter-nat-control-00.txt

Status of this Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

This Internet-Draft will expire on August 29, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

This document describes the framework, messages, and procedures for the Diameter NAT Control Application (DNCA), allowing for per-endpoint control of large scale NAT devices, which are put in place to cope with IPv4-address space completion. The Diameter NAT Control Application allows external devices to configure and manage a Large Scale NAT (LSN) device - expanding the existing Diameter-based AAA and policy control capabilities with a NAT control component. These external devices can be network elements in the data plane such as a Network Access Server (NAS), or can be more centralized control plane devices such as AAA-servers. DNCA establishes a context to commonly identify and manage endpoints on a gateway or server, and a large scale NAT device. This includes, for example, the control of the total number of NAT-bindings allowed or the allocation of a specific NAT-binding for a particular endpoint. In addition, it allows large scale NAT devices to provide information relevant to accounting purposes.

Table of Contents

Copyright Notice...............................................1
Abstract......................................................2
1. Introduction.................................................5
2. Terminology..................................................6
3. Deployment framework and DNCA capabilities...............6
   3.1. Diameter NAT Control Application capabilities........6
   3.2. LSN Control Deployment Framework......................8
      3.2.1. LSN Deployment Scenario..........................8
      3.2.2. Diameter NAT Control Application overview.........9
      3.2.3. Deployment scenarios for the Diameter NAT Control Application.................................................10
4. Diameter NAT Control Application Session Establishment and Management.........................................12
   4.1. Parties involved........................................12
   4.2. Session Establishment....................................13
   4.3. Session Re-Authorization................................16
   4.4. Session and Binding Query...............................18
   4.5. Session Termination.....................................20
4.6. DNCA Manager/Agent failures.................................21
5. Use of the DIAMETER base protocol..............................22
  5.1. Securing DIAMETER messages................................22
  5.2. Accounting functionality................................22
  5.3. Use of sessions.........................................22
  5.4. Routing considerations...................................23
  5.5. Advertising Application support...........................23
6. Diameter NAT Control Application Commands.....................23
  6.1. NAT-Control Request (NCR) Command........................23
  6.2. NAT-Control Answer (NCA) Command........................25
7. Diameter NAT Control Application AVPs.........................26
  7.1. Reused Base Protocol AVPs................................26
  7.2. Experimental-Result-Code AVP values.......................26
    7.2.1. Success............................................27
    7.2.2. Transient failures................................27
    7.2.3. Permanent failures................................27
  7.3. Reused NASREQ Diameter application AVPs..................28
  7.4. Reused from RFC 4675....................................29
  7.5. Reused from Diameter QoS Application [I-D.ietf-dime-qos-attributes]....................................................29
  7.6. Reused from ETSI ES 283 034, e4 Diameter application.....30
  7.7. Diameter NAT Control Application Defined AVPs............31
    7.7.1. NC-Request-Type AVP................................31
    7.7.2. NAT-Control-Install AVP............................32
    7.7.3. NAT-Control-Remove AVP............................33
    7.7.4. NAT-Control-Definition AVP........................33
    7.7.5. NAT-Internal-Address AVP..........................33
    7.7.6. NAT-External-Address AVP..........................33
    7.7.7. Max-NAT-Bindings..................................34
    7.7.8. NAT-Control-Binding-Rule..........................34
    7.7.9. Duplicate-Session-Id AVP............................34
  8. Accounting Commands...........................................34
  8.1. NAT Control Accounting Messages...........................35
  8.2. NAT Control Accounting AVPs................................35
    8.2.1. NAT-Control-Record................................35
    8.2.2. NAT-Control-Binding-Status........................35
    8.2.3. Current-NAT-Bindings................................36
  9. AVP Occurrence Table..........................................36
  9.1. DNCA AVP Table for NAT control initial & update requests 37
  9.2. DNCA AVP Table for Session Query request..................37
  9.3. DNCA AVP Table for NAT Control Terminate requests........37
  9.4. DNCA AVP Table for accounting message......................38
10. IANA Considerations............................................38
  10.1. Command Codes.........................................38
  10.2. AVP Codes..............................................39
  10.3. Application IDs........................................39
11. Security Considerations........................................39

12. References.........................................................40
  12.1. Normative References........................................40
  12.2. Informative References....................................40
13. Author’s Addresses..............................................41
1. Introduction

With the foreseeable depletion of available IPv4 addresses from the IANA pool, service providers are starting to consider network designs which no longer assign unique global IPv4 addresses to their subscribers. One of the approaches considered, is the deployment of a provider-operated large scale NAT device between the end-users and the Internet. Nishitani et al. [I-D.nishitani-cgn] call this NAT device a ‘‘Large Scale NAT (LSN)’’.

LSNs will be inserted into the existing subscriber access and aggregation networks which typically provide for per-endpoint service management and control as well as per-endpoint accounting. Per-endpoint rules include those which relate to service offerings of the SP (e.g. access bandwidth, time or volume based access restrictions) as well as rules which follow legal regulations of the ‘‘National Regulation Authorities (NRA)’’. The introduction of a LSN impacts the per-endpoint service offerings as well as the regulatory requirements and gives rise to new control requirements within the service provider network: Service providers need to manage the behavior of the LSN on a per-endpoint basis.

The per-endpoint management capabilities of a LSN comprise, for example the control of the number of NAT-address-port pairs (often called ‘‘NAT-bindings’’ or simply ‘‘bindings’’) allocated to a single endpoint. Given that global IPv4 address-port pairs are becoming a scarce resource, several service providers intend to restrict the number of NAT-bindings on a per endpoint basis and thus increase address utilization efficiency. The number of bindings an endpoint can consume becomes another parameter within a tiered-service offering. In addition, the service provider might offer static bindings to endpoints or pre-allocate external IP-address/port-ranges to certain endpoints. One of the NRA requirements is that a service provider needs to provide the identity of a user (which e.g. translates to the public IP address and ports leveraged by the user at a given point in time) upon request.

Dynamic per-endpoint management at the LSN requires an associated interface that has to be tightly integrated with the existing per-endpoint authentication, authorization, and accounting (AAA) environment of the service provider.

This document describes the framework, messages and procedures for the Diameter carrier-grade NAT Control Application (DNCA). The DNCA interacts with the LSN to coordinate per-endpoint configuration and management of subscriber traffic traversing the LSN. Use of a
Diameter application allows for simple integration into the existing AAA environment of a service provider.

2. Terminology

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Abbreviations are used in this document:

AAA: Authentication, Authorization, Accounting
DNCA: Diameter NAT Control Application
LSN: Large Scale NAT device
NAT: Network Address Translation
NAS: Network Access Server
NAT-Binding or Binding: Association of two IP-address/port pairs (with one IP-address typically being private and the other one public) to facilitate NAT
NRA: National Regulatory Authority

3. Deployment framework and DNCA capabilities

3.1. Diameter NAT Control Application capabilities

The Diameter NAT control application offers the following capabilities:

1. Limit the number of NAT-bindings per endpoint:
   Define/restrict the maximum number of NAT-bindings on a per-endpoint basis. This enables service providers to offer differentiated services based on the number of bindings and hence optimize the consumption of IP-address/port-ranges.
2 Request the allocation of specific NAT-bindings: Under normal operation the LSN would allocate NAT-bindings based on rules and algorithms local to the LSN. Fixed or pre-defined bindings would be the exception rather than the rule but are essential for certain deployment scenarios. Requests for NAT-binding allocation could happen either at or after initial session establishment. Two cases could be distinguished:

- Request the allocation of a pre-defined NAT-binding. Both the internal as well as the external IP-address/port pair are specified within the request. Some deployment cases, such as access to a web-server within a user's home network with IP-address and port, benefit from statically configured bindings.

- Request the allocation of an external IP-address for a given internal IP-address and report the allocated external IP-address back to the requestor. In some deployment scenarios, the application requires immediate knowledge of the allocated binding for a given internal IP-address but does not control the allocation of the external IP-address (e.g. SIP-proxy server deployments).

3 Define the external address-pool(s) to be used for allocating an external IP-address. External address-pools can either be pre-defined on the LSN, or specified within a request. If pre-defined address-pools are used, a request would just include a reference (e.g. name) to an already defined address pool on LSN. Otherwise, the request will contain a description of the IP-address pool(s) to be used (e.g. list of IP-subnets).

4 Accounting/Reporting: Report established bindings for a particular user. Apart from statistical and charging purposes, binding reporting is also required for legal reasons. Most National Regulatory Authorities (NRA) require that service providers provide the identity of a user upon request. The service provider needs to be able to correlate a tuple (public IP-address, port, time) to a particular user or endpoint.

5 Flexible Information Query: Report details and statistics of bindings for a single endpoint or a set of endpoints through an external interface which integrates with the overall per-endpoint management suite. Hence this information query capability of the DNCA potentially complements alternative information query mechanisms such as SNMP-based mechanisms.
6 Global Endpoint ID: The global endpoint ID will allow for common identification of an endpoint on a LSN as well as other endpoint-or subscriber-aware devices such as a Network Access Server (NAS) or an AAA system. Endpoints are identified through a single or a set of classifiers such as IP address, VLAN identifier, or interface identifier which uniquely identify the traffic associated with a particular global endpoint.

3.2. LSN Control Deployment Framework

3.2.1. LSN Deployment Scenario

Figure 1 shows a typical network deployment for internet access. A user's IPv4-host gains access to the internet through a Network Access Server (NAS) which facilitates the authentication of the endpoint and configures the user's connection according to the authorization and configuration data received from the AAA-server upon successful authentication. Public IPv4 addresses are used throughout the network.

Figure 1: Typical network deployment for internet access

Figure 2 depicts the deployment scenario when a service provider introduces a LSN to increase the efficiency of the global IPv4 address pool utilization. The objective is to provide the customer with connectivity to the public IPv4 Internet. The LSN performs
network address translation between private IPv4 addresses and public IPv4 addresses. If the LSN would be put in place without any endpoint awareness, the service offerings of the service provider would be hampered. Provisioning static NAT-bindings for particular endpoints, using different public IP-address pools for different set of endpoints (e.g. residential or business customers), as well as reporting on the allocated bindings on a per-endpoint basis would be burdensome for a service provider if the LSN would not be aware of endpoints and allow for per-endpoint control and management which easily integrates with the already existing per-endpoint management infrastructure of the service provider.

```
+---------+
|         |
|   AAA   |
|         |
+---------+

+---------+    +---------+    +---------+    +----------+
|  IPv4   |    |         |    |         |    |  IPv4    |
|  Host   |----|   NAS   |----|   LSN   |----| Internet |
+---------+    +---------+    +---------+    +----------+

<-------- Private IPv4 ------------> <-------- Public IPv4 ----->

Figure 2: Access network deployment with LSN

3.2.2. Diameter NAT Control Application overview

The Diameter NAT Control Application runs between a Diameter NAT Control Application Agent on the LSN and the Diameter NAT Control Application Manager. DNCA allows for per-endpoint control and management of a LSN. Being based on Diameter, DNCA integrates well with the suite of Diameter applications deployed for per-endpoint authentication, authorization, accounting, and policy control in service provider networks.
DNCA offers request and answer commands to control the allowed number of NAT-bindings per endpoint, to request the allocation of specific bindings for an endpoint, to define the address pool to be used for an endpoint, to provide per endpoint reporting on the allocated NAT-bindings, as well as to provide for unique identification of an endpoint on both LSN, AAA-server and NAS, thus simplifying the correlation of accounting data streams.

DNCA allows for controlling the behavior of a LSN on a per-endpoint basis during initial session establishment as well as at later stages by providing an update procedure for already established sessions. Using DNCA, per-endpoint NAT-binding information can be retrieved either using accounting mechanisms or through an explicit session query to the LSN.

3.2.3. Deployment scenarios for the Diameter NAT Control Application

Deployment dependent, the role of the Diameter NAT Control Manager can be fulfilled by either the NAS or by an external server such as an AAA-server. The two deployment scenarios are outlined in Figure 3 ("integrated deployment") and Figure 4 ("autonomous deployment").

Within the figures (M) denotes the network element which takes on the DNCA manager role. Similarly, (A) identifies the network element which performs the DNCA agent role.

The integrated deployment approach hides the existence of the LSN from external servers such as the AAA-server as much as possible. It is suited for environments where minimal changes to the existing AAA deployment are desired. The NAS, taking the role of the DNCA manager, is in charge of initiating and managing the session to the LSN, exchanging LSN specific configuration information as well as handling reporting and accounting information. The NAS receives reporting and accounting information from LSN. This way the NAS can provide for a single accounting record for the user - offloading external accounting systems from correlating accounting information received from multiple sources.

An example network attachment for an integrated LSN deployment could be described as follows: An endpoint connects to the network, with the NAS being the point of attachment. After successful authentication, NAS receives endpoint related authorization data from the AAA-server. A portion of the authorization data applies to per-endpoint configuration on the NAS itself, another portion describes authorization and configuration information for NAT control aimed at the LSN. NAS will initiate a DNCA session to the LSN and send the relevant authorization and configuration information for the
particular endpoint to the LSN. This could comprise e.g. NAT-bindings which have to be pre-established for the endpoint, or management related configuration, such as the maximum number of NAT-bindings allowed for the endpoint or accounting requirements. The LSN will send its per-endpoint accounting information to the NAS which aggregates the accounting information received from the LSN with its local accounting information for the endpoint into a single accounting stream towards the AAA-server.

Figure 3: LSN Control deployment: Integrated deployment

The autonomous deployment approach decouples user management on NAS and LSN. The AAA system performing the role of the DNCA manager manages the connection to the LSN, controls the per-endpoint configuration, and also receives accounting and reporting information from LSN. Different from the integrated deployment scenario, the autonomous deployment scenario does not "hide" the existence of the LSN from the AAA infrastructure. Here two accounting streams are received by the AAA-server for one particular endpoint - one from the NAS, and one from the LSN.
4. Diameter NAT Control Application Session Establishment and Management

Note that this section forward references some of the commands and AVPs defined for the DNCA. Please refer to sections 6. and 7. for details.

4.1. Parties involved

Authorization and control models supported by this application include the following parties:

- Diameter NAT Control Application (DNCA) agent: The DNCA agent is part of the Large scale NAT (LSN) device
- Diameter NAT Control Application (DNCA) manager
The current version of the draft assumes that the NAT control requesting entity is always the DNCA manager. Sessions will always be initiated, updated, or terminated by the DNCA manager. This mode of operation is sometimes also referred to as ‘‘push mode’’. Session initiation by the DNCA agent (sometimes referred to as ‘‘pull mode’’) will be covered in a future version of this draft.

4.2. Session Establishment

The DNCA manager establishes a session to the DNCA agent to control the behavior of the NAT device. During session establishment, the DNCA manager will pass along configuration information to the DNCA agent. Session configuration information could for example comprise the maximum number of bindings allowed for the endpoint associated with this session, a set of pre-defined NAT-bindings to be established for this endpoint, or a description of the address pool, external addresses should be allocated from.

The DNCA manager initiates the Diameter NAT Control session to the DNCA agent. The DNCA manager generates a NAT-Control Request (NCR) message to the DNCA agent with NC-Request-Type AVP set to INITIAL_REQUEST. On receipt of the NCR the DNCA agent will setup a new session for the endpoint associated with the endpoint classifier(s) contained in the NCR. The DNCA agent notifies the DNCA manager about successful session setup using a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS. Figure 5 shows the protocol interaction between the DNCA manager and the DNCA agent.

The initial NAT-Control-Request can contain configuration information for the session which specifies the behavior of the LSN for the session. Configuration information which can be included comprises:

- A list of NAT-bindings which should be pre-allocated for the session (e.g. in case a subscriber requires a fixed external IP-address/port pair for one of his applications).
- The maximum number of NAT bindings allowed for an endpoint.
- A description of the external address pool(s) to be used for the session.
A reference to a predefined binding rule on DNCA agent that will be applied to the session. Such a predefined binding rule on DNCA agent may contain, for example, the name of the IP-address pool that external IP-addresses should be allocated from, maximum number of bindings permitted for the endpoint etc.

In certain cases, the DNCA agent may not be able to perform the tasks requested within the NCR. These include the following:

- If a DNCA agent receives a NCR from a DNCA manager with NC-Request-Type AVP set to INITIAL_REQUEST that identifies an already existing session (i.e. DNCA manager and endpoint identifier match an already existing session), the DNCA agent will return NCA with Experimental-Result-Code set to Session-Exists, and provides Session-Id of the existing session in Duplicate-Session-Id AVP.

- If a DNCA agent receives an NCR from a DNCA manager with NC-Request-Type AVP set to INITIAL_REQUEST that matches more than one of the already existing sessions (i.e. DNCA manager and endpoint identifier match already existing sessions), the DNCA agent will return a NCA with Experimental-Result-Code set to Insufficient-Classifiers. In case a DNCA manager receives a NCA that reports Insufficient-Classifiers, it may choose to retry establishing a new session using additional/more specific classifiers.

- If the NCR contains a binding rule not defined on the LSN, the DNCA agent will return a NCA with Experimental-Result-Code AVP set to UNKNOWN_BINDING_RULE.

- In case the DNCA agent is unable to establish all of the bindings requested in the NCR, it will return a NCA with Experimental-Result-Code set to BINDING_FAILURE. The DNCA agent (i.e. LSN) treats a NCR as an atomic operation; hence none of the requested bindings will be established by LSN. Either all requested actions within a NCR are completed successfully, or the entire request fails.

- If DNCA agent does not have sufficient resources to process a request, it will return NCA with Experimental-Result-Code set to RESOURCE_FAILURE.

- In case Max-NAT-Binding and Nat-Control-Definition are included in the NCR along with a reference to a binding rule (i.e. a predefined template on LSN) and the values in Max-NAT-Binding and Nat-Control-Definition contradict those specified in the predefined binding rule, Max-NAT-Binding and Nat-Control-Definition override the values specified in the binding rule.
Figure 5: Initial NAT Control request and session establishment
4.3. Session Re-Authorization

Session re-authorization is performed if the DNCA manager desires to change the behavior of the LSN for an existing session. Re-authorization could be used, for example, to change the number of allowed bindings for a particular session, or establish or remove a pre-defined binding.

The DNCA manager generates a NAT-Control Request (NCR) message to the DNCA agent with NC-Request-Type AVP set to UPDATE_REQUEST upon receiving a trigger signal. In case the session is updated successfully, the DNCA agent notifies the DNCA manager about successful session update using a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS. Figure 6 shows the protocol interaction between the DNCA manager and the DNCA agent.

In certain cases, the DNCA agent may not be able to perform the tasks requested within the NCR. These include the following:

- If DNCA agent receives a NCR update/query request for non-existent session it will set error code in answer, to DIAMETER_UNKNOWN_SESSION_ID.
- If the NCR contains a binding rule not defined on the LSN, the DNCA agent will return a NCA with Experimental-Result-Code AVP set to UNKNOWN_BINDING_RULE.
- If the DNCA agent cannot establish the requested binding because the maximum number of allowed bindings has been reached for the Endpoint Classifier, it will return NCA with Experimental-Result-Code AVP set to MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT.
- In case the DNCA agent cannot establish some or all of the bindings requested in a NCR, but has not yet reached the maximum number of allowed bindings for the subscriber, it will return a NCA with Experimental-Result-Code set to BINDING_FAILURE. The DNCA agent (i.e. LSN) treats a NCR as an atomic operation; hence none of the requested bindings will be established by LSN. Either all requested actions within a NCR are completed successfully, or the entire request fails.
- If DNCA agent does not have sufficient resources to process a request, it will return a NCA with Experimental-Result-Code set to RESOURCE_FAILURE.
o If a NCR redefines the maximum number of NAT bindings allowed for the endpoint, the new value will override any previously defined limit on NAT-bindings. It depends on the implementation of the LSN how LSN would cope with a case where the new value is lower than the actual number of allocated bindings. Typically the LSN would refrain from enforcing the new limit immediately (i.e. actively remove bindings) but rather disallow the establishment of new bindings until the current number of bindings is lower than the newly established maximum number of allowed bindings.

o If a NCR specifies a new binding rule, predefined on the DNCA agent, the binding rule will override any previously defined rules for the session.

o In case Max-NAT-Binding and Nat-Control-Definition are included in the NCR along with a reference to a binding rule (i.e. a predefined template on LSN) and the values in Max-NAT-Binding and Nat-Control-Definition contradict those specified in the pre-defined binding rule, Max-NAT-Binding and NAT-Control-Definition override the values specified in the binding rule.

```
<table>
<thead>
<tr>
<th>DNCA Manager</th>
<th>DNCA Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change of session attributes</td>
<td></td>
</tr>
<tr>
<td>NCR</td>
<td>(UPDATE_REQUEST session id, NAT control config data)</td>
</tr>
<tr>
<td>Update session state</td>
<td></td>
</tr>
<tr>
<td>NCA</td>
<td>(result code)</td>
</tr>
</tbody>
</table>
```

Figure 6: NAT Control request for session update
4.4. Session and Binding Query

Session query can be used by the DNCA manager to either retrieve information on the current bindings for a particular session at the LSN or discover the session identifier for a particular external IP-address/port pair.

The DNCA manager initiates a session query by sending a NAT-Control Request (NCR) message to the DNCA agent with NC-Request-Type AVP set to QUERY_REQUEST. Figure 7 shows the protocol interaction between the DNCA manager and the DNCA agent.

Two types of query requests exist:

- Request a list of currently allocated NAT-bindings for a particular session:
  The DNCA agent will, on receipt of the NCR, lookup the session information for the session id contained in the NCR, and will report all currently active NAT-bindings for the session using a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS. In this case the NCR MUST NOT contain a NAT-Control-Definition AVP. Each NAT-Binding will be reported in a NAT-Control-Definition AVP. In case the session id is unknown to the DNCA agent a DIAMETER_UNKNOWN_SESSION_ID error is returned.

- Retrieve session ids and internal IP-address/port pairs for one or multiple external IP-address/port pairs:
  If the DNCA manager wishes to retrieve the session id(s) for one or multiple external IP-address/port pairs, it MUST include the external IP-address/port pair(s) as part of the NAT-Control-Definition AVP of the NCR. The session id used within the NCR is not meaningful for this type of a query. The DNCA agent will report the NAT-bindings and associated session ids corresponding to the external IP-address/port pairs in a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS and the same session id as the one used in the NCR. In case an external IP-address/port pair has no associated existing NAT-binding, the NAT-Control-Definition AVP contained in the reply just contains the NAT-External-Address AVP.
Figure 7: Session Query
4.5. Session Termination

The DNCA manager generates a NAT-Control Request (NCR) message to the DNCA agent with NC-Request-Type AVP set to TERMINATE REQUEST upon receiving a trigger signal. The DNCA agent sends accounting stop record reporting all the bindings and notifies the DNCA manager about successful session termination using a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS. Figure 8 shows the protocol interaction between the DNCA manager and the DNCA agent.

If a DNCA agent receives a NCR from a DNCA manager with NC-Request-Type AVP set to Terminate REQUEST and fails to find a matching session, the DNCA agent returns DIAMETER_UNKNOWN_SESSION_ID error.

Figure 8: Terminate NAT Control session
4.6. DNCA Manager/Agent failures

Disclaimer: This version of the draft does not cover details in case DNCA manager and DNCA agent go out of sync, which could happen for example due to DNCA manager or DNCA agent restart, (temporary) loss of network connectivity etc. Future versions of this draft will cover failure cases and corresponding behavior of DNCA manager and DNCA agent in detail.

Example failure cases include the following:

- The DNCA manager loses session state (e.g. due to a restart). In this case,
  - the DNCA agent may receive a NCR with NC-Request-Type AVP set to INITIAL_REQUEST that matches an existing session of DNCA agent. The DNCA agent will return an error that contains Duplicate-Session-Id AVP to report Session-Id of existing session. The DNCA manager may then send an explicit TERMINATE_REQUEST for the older session that was lost.
  - the DNCA manager may receive accounting records for a session that does not exist. The DNCA manager will send an accounting answer with error-code set to DIAMETER_UNKNOWN_SESSION_ID. On receipt of which the DNCA agent clears the session and removes the associated session state.

- The DNCA agent loses session state. In such a case, the DNCA agent could receive a NCR with NC-Request-Type AVP set to UPDATE_REQUEST for a non-existent session. The DNCA agent will return NCA with error code set to DIAMETER_UNKNOWN_SESSION_ID. State recovery procedures of the DNCA agent will be covered in a future version of this document.

- The DNCA manager is unreachable (as e.g. detected by Diameter watchdog) or down and accounting requests from the DNCA agent fail to get a response. The current version of the draft does not specify procedures for DNCA agent session state clean up or recovery. The mechanism to ensure that a DNCA manager no longer has associated state for a session being cleared at the DNCA agent is beyond the scope of this document.
5. Use of the DIAMETER base protocol

The DIAMETER Base Protocol defined by [RFC3588] shall apply, with the clarifications listed in the present specification.

5.1. Securing DIAMETER messages

For secure transport of DIAMETER messages, IPSec may be used.

The DNCA agent may verify the identity of the DNCA Manager during the Capabilities Exchange Request procedure.

The DNCA agent may verify if the DNCA Manager that issues a NCR command is allowed to do so, based on:

- The Identity of the DNCA Manager
- The Type of NCR Command
- The content of the NCR Command
- Any combination of the above

5.2. Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is defined in section 8 below.

5.3. Use of sessions

Each DNCA session MUST have a globally unique Session-Id as defined in [RFC3588], which MUST NOT be changed during the lifetime of a DNCA session. The Diameter Session-Id serves as the global endpoint identifier (see also capabilities section 3.1. The DNCA agent and DNCA manager maintain state associated with the Session-Id. This globally unique Session-Id is used for updating, accounting for and terminating the session. DNCA session MUST NOT have more than one outstanding request at any given instant.
The DNCA agent sends an Abort-Session-Request as defined in [RFC3588] if it is unable to maintain sessions due to resource limitation.

5.4. Routing considerations

It is assumed that the DNCA manager knows the address/name of the DNCA agent for a given endpoint. Both the Destination-Realm and Destination-Host AVPs are present in the Request from the DNCA manager to the DNCA agent.

5.5. Advertising Application support

Diameter applications conforming to this specification MUST advertise support by including the value of TBD in:

- Auth-Application-Id and Acct-Application-Id of Capabilities-Exchange-Request (CER)

- Auth-Application-Id of NC-request (NCR), NC-Answer (NCA), Abort-Session-Request (ASR), Abort-Session-Answer (AAA) messages

- Acct-Application-Id in Accounting-Request (ACR) and Accounting-Answer (AAA) messages.

6. Diameter NAT Control Application Commands

The following commands are used to establish, maintain and clear LSN bindings.

6.1. NAT-Control Request (NCR) Command

The NAT-Control Request (NCR) command, indicated by the command field set to TBD and the "R" bit set in the Command Flags field, is sent from the DNCA manager to the DNCA agent in order to install NAT bindings.
Message Format:

< NC-Request > ::= < Diameter Header: TBD, REQ, PXY>

   < Session-Id >
     { Auth-Application-Id }
     { Origin-Host   }
     { Origin-Realm }
     { Destination-Realm }
     { Destination-Host }
     { NC-Request-Type }
     { Origin-State-Id }
     { Auth-Session-State }
     * [ NAT-Control-Remove ]
     * [ NAT-Control-Install ]
     [ User-Name ]
     [ Logical-Access-Id ]
     [ Physical-Access-ID ]
     [ Framed-IP-Address ]
     [ Framed-Interface-ID ]
     [ EGRESS-VLANID]
     [ NAS-Port-ID]
     [ Address-Realm ]
     [ Called-Station-ID ]
     * [ Proxy-Info ]
     * [ Route-Record ]
     * [ AVP ]
6.2. NAT-Control Answer (NCA) Command

The NAT-Control-Answer (NCA) command, indicated by the Command-Code field set to TBD and the "R" bit cleared in the Command Flags field, is sent by the DNCA agent in response to NAT-Control-Request command.

Message Format:
<NC-Answer> ::= < Diameter Header: TBD, PXY >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ NC-Request-Type }
[ Result-Code ]
* [ NAT-Control-Definition ]
[ Current-NAT-Bindings ]
[ Experimental-Result ]
[ Origin-State-Id ]
[ Error-Message ]
[ Error-Reporting-Host ]
* [ Failed-AVP ]
* [ Proxy-Info ]
* [ Duplicate-Session-ID ]
* [ AVP ]
7. Diameter NAT Control Application AVPs

7.1. Reused Base Protocol AVPs

AVPs reused from Diameter Base Protocol [RFC3588] are listed below.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Data Type</th>
<th>MUST</th>
<th>MAY</th>
<th>May encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct-Interim-Interval</td>
<td>85</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Auth-Application-Id</td>
<td>258</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Auth-Session-State</td>
<td>277</td>
<td>Enumerated</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Destination-Host</td>
<td>293</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Destination-Realm</td>
<td>283</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Error-Message</td>
<td>281</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Error-Reporting-Host</td>
<td>294</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Experimental-Result</td>
<td>297</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Experimental-Result-Code</td>
<td>298</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Failed-AVP</td>
<td>279</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Origin-Host</td>
<td>264</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Origin-Realm</td>
<td>296</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Origin-State-Id</td>
<td>278</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Proxy-Info</td>
<td>284</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Result-Code</td>
<td>268</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Route-Record</td>
<td>282</td>
<td>DiamIdent</td>
<td>M</td>
<td>P</td>
<td>N</td>
</tr>
<tr>
<td>Session-Id</td>
<td>263</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>User-Name</td>
<td>1</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
</tbody>
</table>

M - Mandatory bit. An AVP with "M" bit set and its value MUST be supported and recognized by a Diameter entity in order the message, which carries this AVP, to be accepted.
P - Indicates the need for encryption for end-to-end security.

Table 1: DIAMETER AVPs used from Diameter base [RFC3588]

The Auth-Application-Id AVP (AVP Code 258) is assigned by IANA to Diameter applications. The value of the Auth-Application-Id for the Diameter NAT Control Application is TBD.

7.2. Experimental-Result-Code AVP values

This section defines new Experimental-Result-Code values that shall be supported by all DIAMETER implementations that conform to the
present document. When one of the Experimental Result Code defined in
the present section is included in a response, it shall be inside an
Experimental-Result AVP and the Result-Code AVP shall be absent.

7.2.1. Success

Experimental Result Codes that fall within the success category are
used to inform a peer that a request has been successfully completed.

No new Result Code has been defined within this category.

7.2.2. Transient failures

Experimental Result Codes that fall within the transient failures
category are those used to inform a peer that the request could not
be satisfied at the time that it was received. The request may be
able to be satisfied in the future.

This document defines the following new values of the Experimental-
Result-Code AVP:

RESOURCE_FAILURE (TBD)

The DNCA agent indicates that the binding could not be
installed or a new session could not be created due to resource
shortage.

7.2.3. Permanent failures

Experimental Result Codes that fall within the Permanent Failures
category are used to inform the peer that the request failed, and
should not be attempted again.

This document defines the following new values of the Experimental-
Result-Code AVP:

UNKNOWN_BINDING_RULE_NAME (TBD)

The DNCA agent indicates that the specified NAT-Binding-Rule
AVP is unknown.

BINDING_FAILURE (TBD)

The DNCA indicates that the requested binding(s) could not be
installed.

MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT (TBD)
The DNCA agent denies the request because the maximum number of allowed bindings has been reached for the specified Endpoint Classifier.

SESSION_EXISTS (TBD)

The DNCA agent denies request to initialize a new session, if it already has a DNCA session that uses the same set of classifiers as indicated by DNCA manager in the new session init request.

INSUFFICIENT_CLASSIFIERS (TBD)

The DNCA agent defines request to initialize a new session, if the classifiers in the request match more than one of the existing sessions on DNCA agent.

7.3. Reused NASREQ Diameter application AVPs

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Code</th>
<th>Value Type</th>
<th>MUST</th>
<th>MAY</th>
<th>SHLD</th>
<th>MUST</th>
<th>Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-Port</td>
<td>5</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>NAS-Port-Id</td>
<td>87</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td>30</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>31</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>8</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>Framed-Interface-ID</td>
<td>96</td>
<td>Unsigned64</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
</tbody>
</table>

Table 2: Reused NASREQ Diameter application AVPs
7.4. Reused from RFC 4675

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Value Type</th>
<th>MUST</th>
<th>MAY</th>
<th>SHLD</th>
<th>MUST</th>
<th>Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress-VLANID</td>
<td>56</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td>V</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

7.5. Reused from Diameter QoS Application [I-D.ietf-dime-qos-attributes]

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Code</th>
<th>Data Type</th>
<th>MUST</th>
<th>MAY</th>
<th>May encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>TBD</td>
<td>Integer32</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>IP-Address Mask</td>
<td>TBD</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
</tbody>
</table>

M - Mandatory bit. An AVP with "M" bit set and its value MUST be supported and recognized by a Diameter entity in order the message, which carries this AVP, to be accepted.
P - Indicates the need for encryption for end-to-end security.
V - Indicates whether the optional Vendor-ID field is present in the AVP header. Vendor-Id header of all AVPs in this table will be set to ETSI (13019)

Table 3: Reused QoS-attributes
7.6. Reused from ETSI ES 283 034, e4 Diameter application

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Code</th>
<th>Data Type</th>
<th>MUST</th>
<th>MAY</th>
<th>encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address-Realm</td>
<td>301</td>
<td>OctetString</td>
<td>M,V</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Logical-Access-Id</td>
<td>302</td>
<td>OctetString</td>
<td>V</td>
<td>M</td>
<td>Y</td>
</tr>
<tr>
<td>Physical-Access-ID</td>
<td>313</td>
<td>UTF8String</td>
<td>V</td>
<td>M</td>
<td>Y</td>
</tr>
</tbody>
</table>

M - Mandatory bit. An AVP with "M" bit set and its value MUST be supported and recognized by a Diameter entity in order the message, which carries this AVP, to be accepted.
P - Indicates the need for encryption for end-to-end security.
V - Indicates whether the optional Vendor-ID field is present in the AVP header. Vendor-Id header of all AVPs in this table will be set to ETSI (13019)

Table 4: Reused AVPs from Diameter e4 application
7.7. Diameter NAT Control Application Defined AVPs

The following table describes the new Diameter AVPs used in the present document, their AVP Code values, types, possible flag values and whether the AVP may or not be encrypted.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Section</th>
<th>Data Type</th>
<th>MUST</th>
<th>MAY</th>
<th>encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC-Request-Type</td>
<td>TBD</td>
<td>7.7.1</td>
<td>Enumerated</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Install</td>
<td>TBD</td>
<td>7.7.2</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Remove</td>
<td>TBD</td>
<td>7.7.3</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Definition</td>
<td>TBD</td>
<td>7.7.4</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Internal-Address</td>
<td>TBD</td>
<td>7.7.5</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-External-Address</td>
<td>TBD</td>
<td>7.7.6</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Max-NAT-Bindings</td>
<td>TBD</td>
<td>7.7.7</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Binding-Rule</td>
<td>TBD</td>
<td>7.7.8</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Duplicate-Session-ID</td>
<td>TBD</td>
<td>7.7.9</td>
<td>UTF8String</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Record</td>
<td>TBD</td>
<td>8.2.1</td>
<td>Grouped</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>NAT-Control-Binding-Status</td>
<td>TBD</td>
<td>8.2.2</td>
<td>Enumerated</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
<tr>
<td>Current-NAT-Bindings</td>
<td>TBD</td>
<td>8.2.3</td>
<td>Unsigned32</td>
<td>M</td>
<td>P</td>
<td>Y</td>
</tr>
</tbody>
</table>

M - Mandatory bit. An AVP with "M" bit set and its value MUST be supported and recognized by a Diameter entity in order the message, which carries this AVP, to be accepted.

P - Indicates the need for encryption for end-to-end security.

V - Vendor specific bit that indicates whether the optional Vendor-ID field is present in the AVP header.

Table 5: New Diameter AVPs

7.7.1. NC-Request-Type AVP

The NC-Request-Type AVP (AVP Code TBD) is of type Enumerated and contains the reason for sending the NAT-Control-Request command. It shall be present in all NAT-Control-Request messages.

The following values are defined:
INITIAL_REQUEST (1)

An Initial Request is used to install binding at the DNCA agent on a successful access session setup.

UPDATE_REQUEST (2)

An Update Request is used to update bindings previously installed on a given access session, to add new binding on a given access session, or to remove one or several binding(s) activated on a given access session.

TERMINATION_REQUEST (3)

Termination Request is used to deactivate and remove all bindings previously activated on a given access session.

QUERY_REQUEST (4)

Query Request is used to query the DNCA agent about the currently installed bindings for an endpoint classifier.

7.7.2. NAT-Control-Install AVP

The NAT-Control AVP (AVP code TBD) is of type Grouped, and it is used to activate or install NAT bindings. It also contains Max-NAT-Bindings that defines maximum number of NAT bindings to be allowed for a subscriber and NAT-Control-Binding-Rule that references predefined policy template on DNCA agent that may contain static bindings, maximum number of bindings to be allowed, address pool from which external binding address should be allocated.

AVP Format:

NAT-Control-Install ::= < AVP Header: TBD >
* [ NAT-Control-Definition ]
[ NAT-Control-Binding-Rule ]
[ Max-NAT-Bindings]
* [ AVP ]
7.7.3. NAT-Control-Remove AVP

The NAT-Control-Remove AVP (AVP code TBD) is of type Grouped, and it is used to deactivate or remove NAT bindings.

AVP Format:

\[
\text{NAT-Control-Remove ::= < AVP Header: TBD >}
\]
\[
* \ [ \text{NAT-Control-Definition } ]
\]
\[
* \ [ \text{NAT-Control-Binding-Rule } ]
\]
\[
* \ [ \text{AVP } ]
\]

7.7.4. NAT-Control-Definition AVP

The NAT-Control-Definition AVP (AVP code TBD) is of type Grouped, and it describes a binding.

The NAT-Control-Definition AVP uniquely identifies the binding between the DNCA agent and the DNCA manager.

If both the NAT-Internal-Address and NAT-External-Address AVP(s) are supplied, it is a pre-defined binding.

AVP Format:

\[
\text{NAT-Control-Definition ::= < AVP Header: TBD >}
\]
\[
\{ \text{NAT-Internal-Address } \}
\]
\[
\{ \text{NAT-External-Address } \}
\]
\[
\{ \text{Session-Id } \}
\]
\[
* \ [ \text{AVP } ]
\]

7.7.5. NAT-Internal-Address AVP

The NAT-Internal-Address AVP (AVP code TBD) is of type Grouped, and it describes the internal IP address and port for a binding.

AVP Format:

\[
\text{NAT-Internal-Address ::= < AVP Header: TBD >}
\]
\[
* \ [ \text{Framed-IP-Address } ]
\]
\[
* \ [ \text{Port} ]
\]
\[
* \ [ \text{AVP } ]
\]

7.7.6. NAT-External-Address AVP

The NAT-External-Address AVP (AVP code TBD) is of type Grouped, and it describes the external IP address and port for a binding. IP-
Address-Mask AVP can only be specified when Framed-IP-Address AVP is present.

AVP Format:

\[
\text{NAT-External-Address ::= < AVP Header: TBD >}
\begin{align*}
&\text{[ Framed-IP-Address ]} \\
&\text{[ IP-Address-Mask ]} \\
&\text{[ Port ]} \\
&\text{[ AVP ]}
\end{align*}
\]

7.7.7. Max-NAT-Bindings

The Max-NAT-Bindings AVP (AVP code TBD) is of type Unsigned32, and it indicates the maximum number of NAT bindings allowed.

7.7.8. NAT-Control-Binding-Rule

The NAT-Control-Binding-Rule AVP (AVP code TBD) is of type OctetString, and it defines a name for a policy template that will be predefined at LSN. Details on the contents and structure of the template as well as how it would be configured are outside the scope of this document. The policy to which this AVP refers to may contain NAT Bindings, address pool for external address allocation of NAT binding, maximum allowed NAT bindings etc.

7.7.9. Duplicate-Session-Id AVP

The Duplicate-Session-Id AVP (AVP Code TBD) is of type UTF8String. It is used to report error and contains the Session-Id of an existing session.

8. Accounting Commands

The Diameter NAT Control Application reuses session based accounting as defined in Diameter Base Protocol [RFC3588] to report the bindings used per endpoint. This reporting is achieved by sending Diameter Accounting Requests (ACR) [Start, Interim and Stop] from the DNCA agent to DNCA manager.

The DNCA agent sends an ACR Start on receiving an NCR with NC-Request-Type AVP set to INITIAL_REQUEST received for a session, or on creation of the first binding for a session requested in an earlier NCR. The DNCA may send ACR Interim updates, if required, either due to a change in bindings resulting from an NCR with NC-Request-Type AVP set to UPDATE_REQUEST, or periodically as specified in Acct-Interim-Interval by DNCA Manager or when it creates/tears down bindings.
An ACR Stop is sent by the DNCA agent on receiving an NCR with NC-Request-Type AVP set to TERMINATION_REQUEST.

The function of correlating the multiple bindings used by an endpoint at any given time is relegated to the post processor.

DNCA agent may trigger an interim accounting record when maximum number of bindings, if received in NCR, is reached.

8.1. NAT Control Accounting Messages

The ACR and ACA messages are reused as defined in Diameter Base Protocol [RFC3588] for exchanging endpoint NAT binding details between the DNCA agent and the CDF. ACR will contain one or more optional NAT-Control-Record AVP to report the bindings. The DNCA agent indicates the number of the currently allocated NAT bindings to the DNCA manager using the Current-NAT-Bindings AVP. This number needs to match the number of bindings identified as active within the NAT-Control-Record AVP.

8.2. NAT Control Accounting AVPs

In addition to AVPs for ACR specified in [RFC3588], the DNCA agent must add the NAT-Control-Record AVP.

8.2.1. NAT-Control-Record

The NAT-Control-Record AVP (AVP code TBD) is of type Grouped, and it describes a binding and its status. Event-Timestamp indicates the time at which binding was created if NAT-Control-Binding-Status is set to Created, or time at which the binding was removed if NAT-Control-Binding-Status is set to removed. If the NAT-Control-Binding-Status is active Event-Timestamp need not be present, if present it indicates that binding is active at the mentioned time.

NAT-Control-Record ::= < AVP Header: TBD >
{ NAT-Control-Definition }
{ NAT-Control-Binding-Status }
[ Event-Timestamp ]

8.2.2. NAT-Control-Binding-Status

The NAT-Control-Binding-Status AVP (AVP code TBD) is of type enumerated and it describes whether the binding being reported was created or removed or simply indicates that it is active.

The following values are defined:
Created (1)

Indicates that NAT binding is created.

Active (2)

Indicates that NAT binding is active.

Removed (3)

Indicates that the NAT binding was removed.

8.2.3. Current-NAT-Bindings

The Current-NAT-Bindings AVP (AVP code TBD) is of type Unsigned32, and it indicates number of NAT bindings active on LSN.

9. AVP Occurrence Table

The following sections presents the AVPs defined in this document and specifies in which Diameter messages they MAY be present. Note that AVPs that can only be present within a Grouped AVP are not represented in this table.

The table uses the following symbols:

0     The AVP MUST NOT be present in the message.

0+    Zero or more instances of the AVP MAY be present in the message.

0-1   Zero or one instance of the AVP MAY be present in the message. It is considered an error if there is more than one instance of the AVP.

1     One instance of the AVP MUST be present in the message.

1+    At least one instance of the AVP MUST be present in the message.
9.1. DNCA AVP Table for NAT control initial and update requests

Following table presents which NAT control application specific AVPs are to be present in NCR/NCA with NC-Request-Type set to INITIAL_REQUEST or UPDATE_REQUEST

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>NCR</th>
<th>NCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC-Request-Type</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NAT-Control-Install</td>
<td>0-1</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Remove</td>
<td>0-1</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Definition</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Record</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Current-NAT-Bindings</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate-Session-Id</td>
<td>0</td>
<td>0-1</td>
</tr>
</tbody>
</table>

9.2. DNCA AVP Table for Session Query request

Following table presents which NAT control application specific AVPs are to be present in NCR/NCA with NC-Request-Type set to QUERY_REQUEST

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>NCR</th>
<th>NCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC-Request-Type</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NAT-Control-Install</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Remove</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Definition</td>
<td>0</td>
<td>0+</td>
</tr>
<tr>
<td>NAT-Control-Record</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Current-NAT-Bindings</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Duplicate-Session-Id</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

9.3. DNCA AVP Table for NAT Control Terminate requests

Following table presents which NAT control application specific AVPs are to be present in NCR/NCA with NC-Request-Type set to TERMINATION_REQUEST
9.4. DNCA AVP Table for accounting message

Following table presents which NAT control application specific AVPs May or May Not be present in ACR/ACA messages.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>ACR</th>
<th>ACA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NC-Request-Type</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Install</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Remove</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NAT-Control-Definition</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Current-NAT-Bindings</td>
<td>1+</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate-Session-Id</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

10. IANA Considerations

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

10.1. Command Codes

IANA is requested to allocate command code values for the following.
Registry:

<table>
<thead>
<tr>
<th>Code Value</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>NAT-Control-Request (NCR)</td>
<td>Section 6.1</td>
</tr>
<tr>
<td>to be assigned</td>
<td>NAT-Control-Answer (NCA)</td>
<td>Section 6.2</td>
</tr>
</tbody>
</table>

### 10.2. AVP Codes

IANA is requested to allocate AVP codes for the following AVPs that are defined in this document.

<table>
<thead>
<tr>
<th>Code Value</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>NC-Request-Type</td>
<td>7.7.1</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Install</td>
<td>7.7.2</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Remove</td>
<td>7.7.3</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Definition</td>
<td>7.7.4</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Internal-Address</td>
<td>7.7.5</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-External-Address</td>
<td>7.7.6</td>
</tr>
<tr>
<td>TBD</td>
<td>Max-NAT-Bindings</td>
<td>7.7.7</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Binding-Rule</td>
<td>7.7.8</td>
</tr>
<tr>
<td>TBD</td>
<td>Duplicate-Session-Id</td>
<td>7.7.9</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Record</td>
<td>8.2.1</td>
</tr>
<tr>
<td>TBD</td>
<td>NAT-Control-Binding-Status</td>
<td>8.2.2</td>
</tr>
<tr>
<td>TBD</td>
<td>Current-NAT-Bindings</td>
<td>8.2.3</td>
</tr>
</tbody>
</table>

### 10.3. Application IDs

IANA is requested to allocate the following application ID using the next value from the 7-16777215 range.

<table>
<thead>
<tr>
<th>ID values</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>Diameter NAT Control Application</td>
<td>Section 4</td>
</tr>
</tbody>
</table>

### 11. Security Considerations

Similar to what the Diameter QoS application (see [I-D.sun-dqa]) does for authorization of QoS reservations, this document describes procedures for authorizing network address translation related attributes and parameters by an entity which is non-local to the device performing network address translation. The security considerations for the Diameter QoS application (see [I-D.sun-dqa], section 11) apply in a similar way to the DNCA. Securing the information exchange between the authorizing entity (the DNCA manager) as well as the NAT device requires bilateral authentication.
of the involved parties, authorization of the involved parties to perform the required procedures and functions, as well as procedures to ensure integrity and confidentiality of the information exchange. DNCA makes use of the capabilities offered by Diameter as well as the underlying transport protocols to deliver on these requirements (see section 5.1.).

It is assumed that the DNCA agent and DNCA manager are in the same domain and have a mutual trust set up. Authorization between the DNCA agent and DNCA manager is beyond the scope of this document.

12. References

12.1. Normative References


[ETSI ES 283 034] Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN), Network Attachment Sub-System (NASS), e4 interface based on the Diameter protocol.

12.2. Informative References


13. Author’s Addresses

Frank Brockners
Cisco Systems, Inc.
Hansaallee 249
40549 Duesseldorf
Germany
Email: fbrockne@cisco.com

Vaneeta Singh
Cisco Systems, Inc.
Cessna Business Park,
Sarjapura Marathalli Outer Ring Road
Bangalore, KARNATAKA 560 087
India
Email: vansingh@cisco.com

Shwetha Bhandari
Cisco Systems, Inc.
Cessna Business Park,
Sarjapura Marathalli Outer Ring Road
Bangalore, KARNATAKA 560 087
India
Email: shwethab@cisco.com