Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: October 22, 2012

F. Brockners
S. Bhandari
Cisco
V. Singh

V. Fajardo
Telcordia Technologies

April 20, 2012

Diameter Network Address and Port Translation Control Application
draft-ietf-dime-nat-control-17

Abstract

This document describes the framework, messages, and procedures for the Diameter Network address and port translation Control Application. This Diameter application allows per endpoint control of Network Address Translators and Network Address and Port Translators, which are added to networks to cope with IPv4-address space depletion. This Diameter application allows external devices to configure and manage a Network Address Translator device - expanding the existing Diameter-based AAA and policy control capabilities with a Network Address Translators and Network Address and Port Translators control component. These external devices can be network elements in the data plane such as a Network Access Server, or can be more centralized control plane devices such as AAA-servers. This Diameter application establishes a context to commonly identify and manage endpoints on a gateway or server, and a Network Address Translator and Network Address and Port Translator device. This includes, for example, the control of the total number of Network Address Translator bindings allowed or the allocation of a specific Network Address Translator binding for a particular endpoint. In addition, it allows Network Address Translator devices to provide information relevant to accounting purposes.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on October 22, 2012.

Copyright Notice

Table of Contents

1. Introduction

Internet service providers deploy Network Address Translators (NATs) and Network Address and Port Translators (NAPTs) [RFC3022] in their networks. A key motivation for doing so is the depletion of available public IPv4 addresses. This document defines a Diameter application allowing providers to control the behavior of NAT and NAPT devices that implement IPv4-to-IPv4 network address and port translation [RFC2663] as well as stateful IPv6-to-IPv4 address family translation as defined in [RFC2663], [RFC6145], and [RFC6146]. The use of a Diameter application allows for simple integration into the existing Authentication, Authorization and Accounting (AAA) environment of a provider.

The Diameter Network address and port translation Control Application (DNCA) offers the following capabilities:

1. Limits or defines the number of NAPT/NAT bindings made available to an individual endpoint. The main motivation for restricting the number of bindings on a per endpoint basis is to protect the service of the service provider against denial of service attacks. If multiple endpoints share a single public IP address, these endpoints can share fate. If one endpoint would (either intentionally, or due to mis-behavior, mis-configuration, mal-ware, etc.) be able to consume all available bindings for a given single public IP address, service would be hampered (or might even become unavailable) for those other endpoints sharing the same public IP address. The efficiency of a NAPT deployment depends on the maximum number of bindings an endpoint could use. Given that the typical number of bindings an endpoint uses depends on the type of endpoint (e.g. a personal computer of a broadband user is expected to use a higher number of bindings than a simple mobile phone) and a NAPT device is often shared by different types of endpoints, it is desirable to actively manage the maximum number of bindings. This requirement is specified in REQ-3 of [I-D.ietf-behave-lsn-requirements]

2. Supports the allocation of specific NAPT/NAT bindings. Two types of specific bindings can be distinguished:

   * Allocation of a pre-defined NAT binding: Both the internal and external IP address and 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.

   * Allocation of an external IP address for a given internal IP address: The allocated external IP address is reported 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; for example, SIP-proxy server deployments.

3. Defines the external address pool(s) to be used for allocating an external IP address: External address pools can either be pre-assigned at the NAPT/NAT device, or specified within a request. If pre-assigned address pools are used, a request needs to include a reference to identify the pool. Otherwise, the request contains a description of the IP address pool(s) to be used; for example, a list of IP-subnets. Such external address pools can be used to select the external IP address in NAPT/NAT bindings for multiple subscribers.

4. Generates reports and accounting records: Reports established bindings for a particular endpoint. The collected information is used by accounting systems for statistical purposes.

5. Queries and retrieves details about bindings on demand: This feature complements the previously mentioned accounting functionality (see item 4). This feature can be used by an entity to find NAT-bindings belonging to one or multiple endpoints on the NAT-device. The entity is not required to create a DNCA control session to perform the query, but would obviously still need to create a Diameter session complying to the security requirements.

6. Identifies a subscriber or endpoint on multiple network devices (NAT/NAPT device, the AAA-server, or the Network Access Server (NAS)): Endpoint identification is facilitated through a Global Endpoint ID. Endpoints are identified through a single or a set of classifiers, such as IP address, Virtual Local Area Network (VLAN) identifier, or interface identifier which uniquely identify the traffic associated with a particular global endpoint.

With the above capabilities, DNCA qualifies as a MIDCOM protocol [RFC3303], [RFC3304], [RFC5189] for middle boxes which perform NAT. The MIDCOM protocol evaluation [RFC4097] evaluated Diameter as a candidate protocol for MIDCOM. DNCA provides the extensions to the Diameter base protocol [RFC3588] following the MIDCOM protocol requirements, such as the support of NAT-specific rule transport, support for oddity of mapped ports, as well as support for consecutive range port numbers. DNCA adds to the MIDCOM protocol capabilities in that it allows to maintain the reference to an endpoint representing a user or subscriber in the control operation,

enabling the control of the behavior of a NAT-device on a per endpoint basis. Following the requirements of different operators and deployments, different management protocols are employed. Examples include e.g. SNMP [RFC3411] and NETCONF [RFC6241] which can both be used for device configuration. Similarly, DNCA is complementing existing MIDCOM implementations, offering a MIDCOM protocol option for operators with an operational environment that is Diameter-focused which desire to use Diameter to perform per endpoint NAT control. Note that in case an operator uses multiple methods and protocols to configure a NAT-device, such as for example command line interface, SNMP, NETCONF, or PCP, along with DNCA specified in this document, the operator MUST ensure that the configurations performed using the different methods and protocols do not conflict in order to ensure a proper operation of the NAT service.

This document is structured as follows: Section 2 lists terminology, while Section 3 provides an introduction to DNCA and its overall deployment framework. Sections 4 to 8 cover DNCA specifics, with Section 4 describing session management, Section 5 the use of the Diameter base protocol, Section 6 new commands, Section 7 Attribute Value Pairs(AVPs) used, and Section 8 accounting aspects. Section 9 presents AVP occurrence tables. IANA and security considerations are addressed in Sections 10 and 11.

2. Conventions

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 used in this document:

AAA: Authentication, Authorization, Accounting

DNCA: Diameter Network address and port translation Control Application

Endpoint: Managed entity of the DNCA. An endpoint represents a network element or device, associated with a subscriber, a user or a group of users. An endpoint is represented by a single access-session on a NAS. DNCA assumes a 1:1 relationship between an endpoint, the access-session it represents, and the associated DNCA session.

NAPT: Network Address and Port Translation, see also [RFC3022]

NAT: Network Address Translation (NAT and NAPT are used in this document interchangeably)

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

NAT binding predefined template: Is a policy template or configuration that is predefined at the NAT-device. It may contain NAT-bindings, IP-address pools for allocating the external IP-address of a NAT-binding, the maximum number of allowed NAT-bindings for end-points, etc.

NAT-device: Network Address Translator or Network Address and Port Translator: An entity performing NAT or NAPT.

NAT-controller: Entity controlling the behavior of a NAT-device.

NAS: Network Access Server

NCR: NAT Control Request

NCA: NAT Control Answer

NAT44: IPv4 to IPv4 network address and port translation, see [RFC2663]

NAT64: IPv6 to IPv4 address family translation, see [RFC6145] and [RFC6146]

PPP: Point-to-Point Protocol [RFC1661]

3. Deployment Framework

3.1. Deployment Scenario

Figure 1 shows a typical network deployment for IPv4-Internet access. A user's IPv4 host (i.e. endpoint) gains access to the Internet though a NAS, which facilitates the authentication of the endpoint and configures the endpoints'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. DNCA manages an endpoint that represents a network element or device or IPv4 host, associated with a subscriber, a user or a group of users. An endpoint is represented by a single access-session on a NAS. DNCA assumes a 1:1 relationship between an endpoint, the access-session it represents, and the associated DNCA

session.

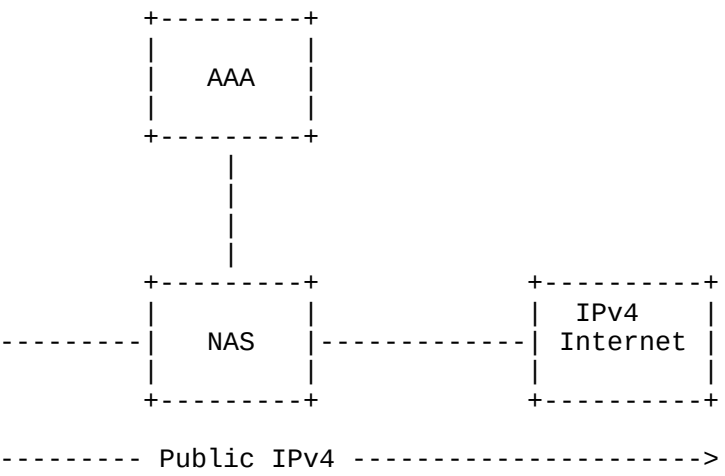


Figure 1: Typical network deployment for internet access

Figure 2 depicts the deployment scenario where a service provider places a NAT between the host and the public Internet. The objective is to provide the customer with connectivity to the public IPv4 Internet. The NAT-device performs network address and port (and optionally address family) translation, depending on whether the access network uses private IPv4 addresses or public IPv6 addresses, to public IPv4 addresses. Note that there may be more than one NAS, NAT-device, or AAA-entity in a deployment, although the figures only depict one entity each for clarity.

If the NAT-device would be put in place without any endpoint awareness, the service offerings of the service provider could be impacted as detailed in [I-D.ietf-behave-lsn-requirements]. This includes cases like:

- Provisioning static NAT bindings for particular endpoints
- Using different public IP address pools for different set of endpoints (for example, residential or business customers)
- Reporting allocated bindings on a per endpoint basis
- Integrate control of the NAT-device into the already existing per endpoint management infrastructure of the service provider

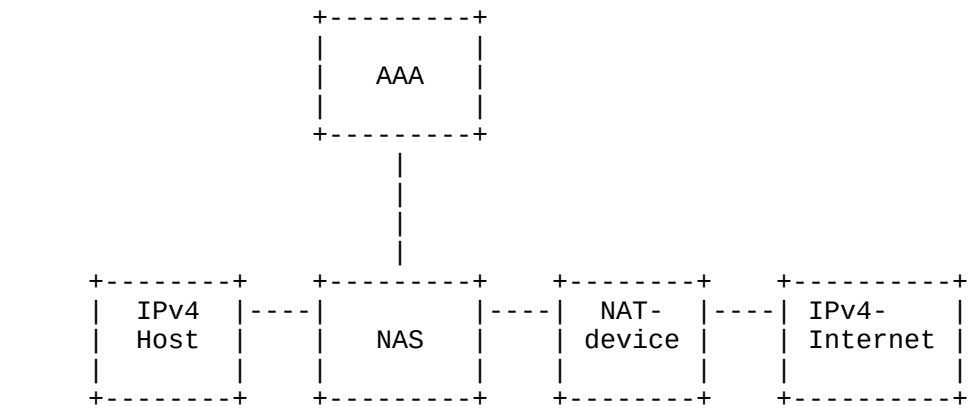


Figure 2: Access network deployment with NAT

Figure 2 shows a typical deployment for IPv4-Internet access involving a NAT-device within the service provider network. The figure describes two scenarios: One where an IPv4-host (with a private IPv4 address) accesses the IPv4-Internet, as well as one where an IPv6-host accesses the IPv4-Internet.

3.2. Diameter NAPT Control Application Overview

DNCA runs between two DNCA Diameter peers. One DNCA Diameter peer resides within the NAT-device, the other DNCA Diameter peer resides within a NAT-controller (discussed in Section 3.3). DNCA allows per endpoint control and management of NAT within the NAT-device. 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.

- Provides per endpoint reporting of the allocated NAT bindings.

- o Provides unique identification of an endpoint on NAT-device, AAA-server and NAS, to simplify correlation of accounting data streams.

DNCA allows controlling the behavior of a NAT-device on a per endpoint basis during initial session establishment and 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 NAT.

3.3. Deployment Scenarios For DNCA

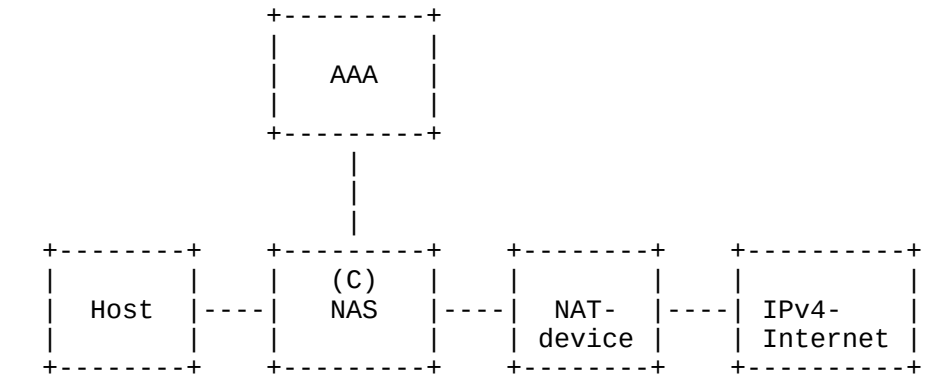
DNCA can be deployed in different ways. DNCA supports deployments with "n" NAT-controllers and "m" NAT-devices, with n and m equal to or greater than 1. From a DNCA perspective an operator should ensure that the session representing a particular endpoint is atomic. Any deployment MUST ensure that for any given endpoint only a single DNCA NAT-controller and is active at any point in time. This is to ensure that NAT-devices controlled by multiple NAT-controllers do not receive conflicting control requests for a particular endpoint, or would be unclear which NAT-controller to send accounting information to. Operational considerations MAY require an operator to use alternate control mechanisms or protocols such as SNMP or manual configuration via a Command-Line-Interface to apply per-endpoint NAT-specific configuration, like for example static NAT-bindings. For these cases, the NAT-device MUST allow the operator to configure a policy how configuration conflicts are resolved. Such a policy could for example specify that manually configured NAT-bindings using the Command-Line-Interface always take precedence over those configured using DNCA.

Two common deployment scenarios are outlined in Figure 3 ("integrated deployment") and Figure 4 ("autonomous deployment"). Per the note above, multiple instances of NAT-controllers and NAT-devices could be deployed. The figures only show single instances for reasons of clarity. The two shown scenarios differ in which entity fulfills the role of the NAT-controller. Within the figures (C) denotes the network element performing the role of the NAT-controller.

The integrated deployment approach hides the existence of the NAT-device from external servers, such as the AAA-server. It is suited for environments where minimal changes to the existing AAA deployment are desired. The NAS and the NAT-device are Diameter peers supporting the DNCA. The Diameter peer within the NAS, performing the role of the NAT-controller, initiates and manages sessions with the NAT-device, exchanges NAT specific configuration information and handles reporting and accounting information. The NAS receives

reporting and accounting information from the NAT-device. With this information, the NAS can provide a single accounting record for the endpoint. A system correlating the accounting information received from the NAS and NAT-device would not be needed.

An example network attachment for an integrated NAT deployment can be described as follows: An endpoint connects to the network, with the NAS being the point of attachment. After successful authentication, the 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 NAT-device. The NAS initiates a DNCA session to the NAT-device and sends relevant authorization and configuration information for the particular endpoint to the NAT-device. This can comprise 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. The NAT-device sends its per endpoint accounting information to the NAS, which aggregates the accounting information received from the NAT-device with its local accounting information for the endpoint into a single accounting stream towards the AAA-server.



For NAT44 deployments (IPv4 host):
<----- Private IPv4 ----------><--- Public IPv4 --->

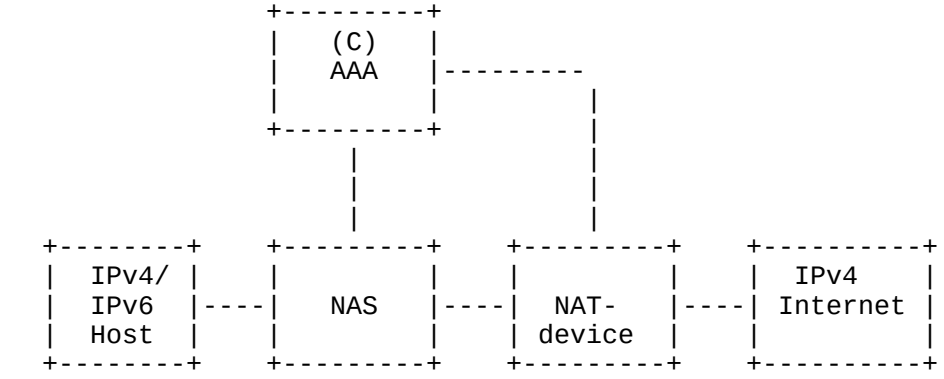
For NAT64 deployments (IPv6 host):
<----- Public IPv6 ----------><--- Public IPv4 --->

Figure 3: NAT control deployment: Integrated deployment

Figure 3 shows examples of integrated deployments. The figure describes two scenarios: One where an IPv4-host (with a private IPv4 address) accesses the IPv4-Internet, as well as one where an IPv6-

host accesses the IPv4-Internet.

The autonomous deployment approach decouples endpoint management on the NAS and NAT-device. In the autonomous deployment approach, the AAA-system and the NAT-device are the Diameter peers running the DNCA. The AAA-system also serves as NAT-controller. It manages the connection to the NAT-device, controls the per endpoint configuration, and also receives accounting and reporting information from the NAT-device. Different from the integrated deployment scenario, the autonomous deployment scenario does not "hide" the existence of the NAT-device 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 NAT-device.



For NAT44 deployments (IPv4 host):
<----- Private IPv4 ----------><--- Public IPv4 --->

For NAT64 deployments (IPv6 host):
<----- Public IPv6 ----------><--- Public IPv4 --->

Figure 4: NAT control deployment: Autonomous deployment

Figure 4 shows examples of autonomous deployments. The figure describes two scenarios: One where an IPv4-host (with a private IPv4 address) accesses the IPv4-Internet, as well as one where an IPv6-host accesses the IPv4-Internet.

4. DNCA Session Establishment and Management

Note that this section forward references some of the commands and AVPs defined for DNCA. Please refer to Section 6 and Section 8 for details. DNCA runs between a Diameter peer residing in a NAT-controller and a Diameter peer residing in a NAT-device. Note that,

per what was already mentioned above, each DNCA session between Diameter peers in a NAT-controller and a NAT-device represents a single endpoint, with an endpoint being either a network element, a device or an IPv4 host associated with a subscriber, a user, or a group of users. The Diameter peer within the NAT-controller is always the control requesting entity: It initiates, updates, or terminates the sessions. Sessions are initiated when the NAT-controller learns about a new endpoint (i.e., host) that requires a NAT service. This could for example be due to the entity hosting the NAT-controller receiving authentication, authorization, or accounting requests for or from the endpoint. Alternate methods that could trigger session setup include local configuration, receipt of a packet from a formerly unknown IP-address, etc.

4.1. Session Establishment

The DNCA Diameter peer within the NAT-controller establishes a session with the DNCA Diameter peer within the NAT-device to control the behavior of the NAT function within the NAT-device. During session establishment, the DNCA Diameter peer within the NAT-controller passes along configuration information to DNCA Diameter peer within the NAT-device. The session configuration information comprises 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, that external addresses are to be allocated from.

The DNCA Diameter peer within the NAT-controller generates a NAT-Control Request (NCR) message to the DNCA Diameter peer within the NAT-device with NC-Request-Type AVP set to INITIAL_REQUEST to initiate a Diameter NAT control session. On receipt of a NCR the DNCA Diameter peer within the NAT-device sets up a new session for the endpoint associated with the endpoint classifier(s) contained in the NCR. The DNCA Diameter peer within the NAT-device notifies its DNCA Diameter peer within the NAT-controller about successful session setup using a NAT-Control Answer (NCA) message with Result-Code set to DIAMETER_SUCCESS. Figure 5 shows the initial protocol interaction between the two DNCA Diameter peers.

The initial NAT-Control-Request MAY contain configuration information for the session, which specifies the behavior of the NAT-device for the session. The configuration information that MAY be included, comprises:

- A list of NAT bindings, which should be pre-allocated for the session; for example, in case an endpoint requires a fixed external IP-address/port pair for an application.

- The maximum number of NAT-bindings allowed for an endpoint.

- A description of the external IP-address pool(s) to be used for the session.

- A reference to a NAT Binding Predefined template on the NAT-device, which is applied to the session. Such a NAT Binding Predefined template on the NAT-device may contain, for example, the name of the IP-address pool that external IP-addresses should be allocated from, the maximum number of bindings permitted for the endpoint, etc.

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

- If a DNCA Diameter peer within the NAT-device receives a NCR from a DNCA Diameter peer within a NAT-controller with NC-Request-Type AVP set to INITIAL_REQUEST that identifies an already existing session; that is endpoint identifier match an already existing session, the DNCA Diameter peer within the NAT-device MUST return an NCA with Result-Code set to SESSION_EXISTS, and provide the Session-Id of the existing session in the Duplicate-Session-Id AVP.

- If a DNCA Diameter peer within the NAT-device receives a NCR from a DNCA Diameter peer within a NAT-controller with NC-Request-Type AVP set to INITIAL_REQUEST that matches more than one of the already existing sessions; that is, DNCA Diameter peer and endpoint identifier match already existing sessions, the DNCA Diameter peer within the NAT-device MUST return an NCA with Result-Code set to INSUFFICIENT-CLASSIFIERS. In case a DNCA Diameter peer receives a NCA that reports Insufficient-Classifiers, it MAY choose to retry establishing a new session using additional or more specific classifiers.

- If the NCR contains a NAT Binding predefined template not defined on the NAT-device, the DNCA Diameter peer within the NAT-device MUST return an NCA with Result-Code AVP set to UNKNOWN_BINDING_TEMPLATE_NAME.

- In case the NAT-device is unable to establish all of the bindings requested in the NCR, the DNCA Diameter peer MUST return an NCA with Result-Code set to BINDING_FAILURE. A DNCA Diameter peer within a NAT-device MUST treat a NCR as an atomic operation; hence none of the requested bindings will be established by the NAT-device. Either all requested actions within a NCR MUST be completed successfully, or the entire request fails.

- If a NAT-device cannot conform to a request to set the maximum number of NAT bindings allowed for a session, the DNCA Diameter peer in the NAT-device MUST return an NCA with Result-Code AVP set to MAX_BINDINGS_SET_FAILURE. Such a condition can for example occur if the operator specified the maximum number of NAT bindings through another mechanism, which per the operator's policy, takes precedence over DNCA.

- If a NAT-device does not have sufficient resources to process a request, the DNCA Diameter peer MUST return an NCA with Result-Code set to RESOURCE_FAILURE.

- In case Max-NAT-Bindings, NAT-Control-Definition as well as NAT-Control-Binding-Template are included in the NCR, and the values in Max-NAT-Bindings and NAT-Control-Definition contradict those specified in the pre-provisioned template on the NAT-device which NAT-Control-Binding-Template references, Max-NAT-Bindings and NAT-Control-Definition MUST override the values specified in the template that NAT-Control-Binding-Template refers to.

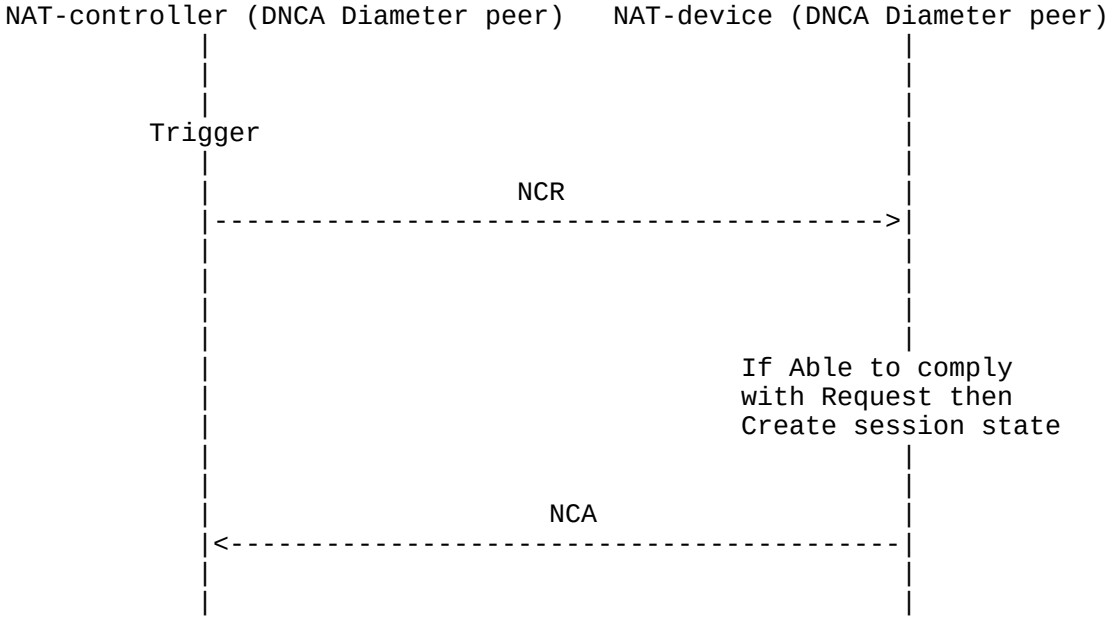


Figure 5: Initial NAT control request and session establishment

Note: The DNCA Diameter peer within the NAT-device creates session state only if it is able to comply with the NCR. On success it will reply with an NCA with Result-Code set to DIAMETER_SUCCESS.

4.2. Session Update

Session update is performed if the NAT-controller desires to change the behavior of the NAT-device for an existing session. Session update 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 Diameter peer within the NAT-controller generates a NCR message to the DNCA Diameter peer within the NAT-device with NC-Request-Type AVP set to UPDATE_REQUEST upon receiving a trigger signal. If the session is updated successfully, the DNCA Diameter peer within the NAT-device notifies the DNCA Diameter peer within the NAT-controller about the 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 two DNCA Diameter peers.

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

- If DNCA Diameter peer within a NAT-device receives an NCR update or query request for a non-existent session, it MUST set Result-Code in the answer to DIAMETER_UNKNOWN_SESSION_ID.

- If the NCR contains a NAT Binding Predefined template not defined on the NAT-device, an NCA with Result-Code AVP set to UNKNOWN_BINDING_TEMPLATE_NAME MUST be returned.

- If the NAT-device cannot establish the requested binding because the maximum number of allowed bindings has been reached for the endpoint classifier, an NCA with Result-Code AVP set to MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT MUST be returned to the DNCA Diameter peer.

- If the NAT-device cannot establish some or all of the bindings requested in an NCR, but has not yet reached the maximum number of allowed bindings for the endpoint, an NCA with Result-Code set to BINDING_FAILURE MUST be returned. As already noted, the DNCA Diameter peer in a NAT-device MUST treat an NCR as an atomic operation. Hence none of the requested bindings will be established by the NAT-device in case of failure. Actions requested within a NCR are either all successful or all fail.

- If the NAT-device cannot conform to a request to set the maximum number of bindings allowed for a session as specified by the Max-NAT-Bindings, the DNCA Diameter peer in the NAT-device MUST return an NCA with Result-Code AVP set to MAX_BINDINGS_SET_FAILURE.

- If the NAT-device does not have sufficient resources to process a request, an NCA with Result-Code set to RESOURCE_FAILURE MUST be returned.

- If an NCR changes the maximum number of NAT-bindings allowed for the endpoint defined through an earlier NCR, the new value MUST override any previously defined limit on the maximum number of NAT bindings set through DNCA. Note that prior to overwriting an existing value, the NAT-device MUST check whether the overwrite action conforms to the locally configured policy. Deployment dependent, an existing value could have been set by a protocol or mechanism different from DNCA and with higher priority. In which case, the NAT-device will refuse the change and the DNCA Diameter peer in the NAT-device MUST return an NCA with Result-Code AVP set to MAX_BINDINGS_SET_FAILURE. It depends on the implementation of the NAT-device on how the NAT-device copes with a case where the new value is lower than the actual number of allocated bindings. The NAT-device SHOULD refrain from enforcing the new limit immediately (that is, actively remove bindings), but rather disallows the establishment of new bindings until the current number of bindings is lower than the newly established maximum number of allowed bindings.

- If an NCR specifies a new NAT Binding Predefined template on the NAT-device, the NAT Binding Predefined template overrides any previously defined rule for the session. Existing NAT-bindings SHOULD NOT be impacted by the change of templates.

- In case Max-NAT-Binding, NAT-Control-Definition as well as NAT-Control-Binding-Template are included in the NCR, and the values in Max-NAT-Bindings and NAT-Control-Definition contradict those specified in the pre-provisioned template on the NAT-device which NAT-Control-Binding-Template references, Max-NAT-Bindings and NAT-Control-Definition MUST override the values specified in the template that the NAT-Control-Binding-Template refers to.

Note: Already established bindings for the session SHOULD NOT be affected in case the tasks requested within the NCR cannot be completed.

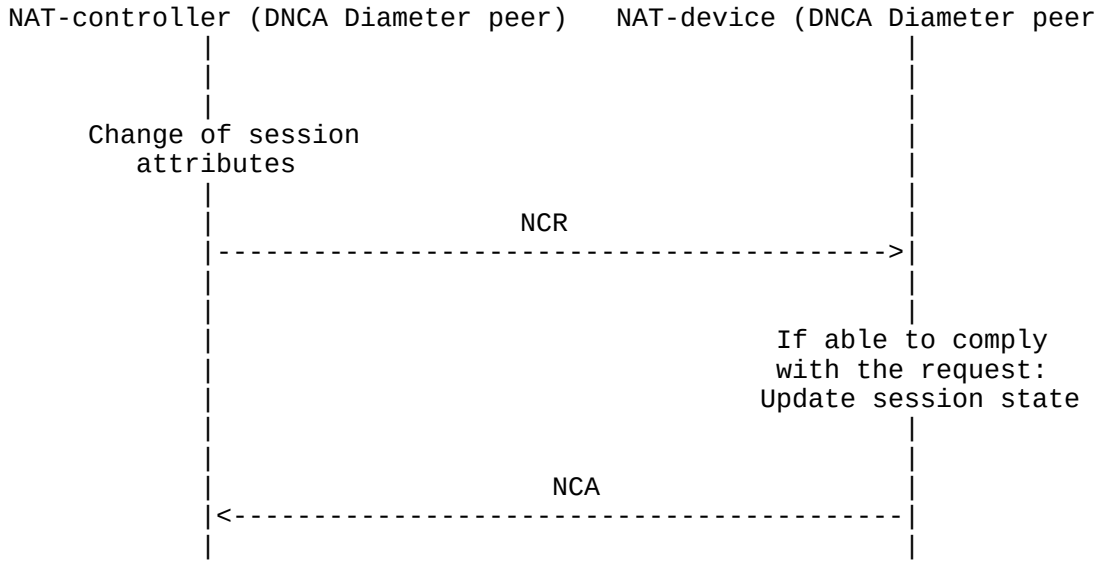


Figure 6: NAT control request for session update

4.3. Session and Binding Query

A Session and NAT-binding query MAY be used by the DNCA Diameter peer within the NAT-controller to either retrieve information on the current bindings for a particular session at the NAT-device or discover the session identifier for a particular external IP address/ port pair.

A DNCA Diameter peer within the NAT-controller starts a session query by sending an NCR message with NC-Request-Type AVP set to QUERY_REQUEST. Figure 7 shows the protocol interaction between the DNCA Diameter peers.

Two types of query requests exist. The first type of query request uses the session ID as input parameter to the query. It is to allow the DNCA Diameter peer within the NAT-controller to retrieve the current set of bindings for a specific session. The second type of query request is used to retrieve the session identifiers, along with the associated bindings, matching a criteria. This enables the DNCA Diameter peer within the NAT-controller to find those sessions, which utilize a specific external or internal IP-address.

1. Request a list of currently allocated NAT bindings for a particular session: On receiving a NCR, the NAT-device SHOULD look up the session information for the session ID contained in the NCR, and report all currently active NAT-bindings for the

session using an 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 is reported in a NAT-Control-Definition AVP. In case the session ID is unknown, the DNCA Diameter peer within the NAT-device MUST return an NCA message with Result-Code set to DIAMETER_UNKNOWN_SESSION_ID.

2. Retrieve session IDs and bindings for internal IP-address or one or multiple external IP-address/port pairs: If the DNCA Diameter peer within the NAT-controller wishes to retrieve the session ID(s) for internal IP-address or one or multiple external IP-address/port pairs, it MUST include the internal IP-address as part of Framed-IP-Address or external IP-address/port pair(s) as part of the NAT-External-Address AVP of the NCR. The external IP-address/port pair(s) are pre-known to the controller via configuration, AAA interactions, or other means. The session ID is not included in the NCR or the NCA for this type of a query. The DNCA Diameter peer within the NAT-device SHOULD report the NAT-bindings and associated session IDs corresponding to the internal IP-address or external IP-address/port pairs in an NCA message using one or multiple instances of the NAT-Control-Definition AVP. The Result-Code is set to DIAMETER_SUCCESS. 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.

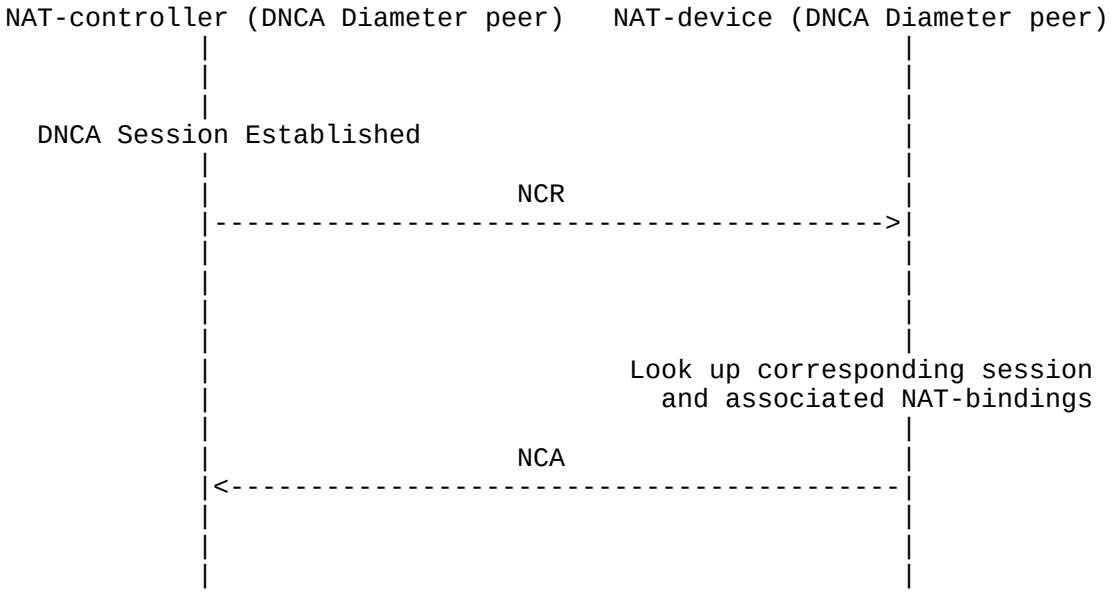


Figure 7: Session query

4.4. Session Termination

Similar to session initiation, session tear down MUST be initiated by the DNCA Diameter peer within the NAT-controller. The DNCA Diameter peer sends a Session Terminate Request (STR) message to its peer within the NAT-device upon receiving a trigger signal. The source of the trigger signal is outside the scope of this document. As part of STR message processing the DNCA Diameter peer within the NAT-device MAY send an accounting stop record reporting all bindings. All the NAT-bindings belonging to the session MUST be removed and the session state MUST be cleaned up. The DNCA Diameter peer within the NAT-device MUST notify its DNCA Diameter peer in the NAT-controller about successful session termination using a Session Terminate Answer (STA) message with Result-Code set to DIAMETER_SUCCESS. Figure 8 shows the protocol interaction between the two DNCA Diameter peers.

If a DNCA Diameter peer within a NAT-device receives a STR and fails to find a matching session, the DNCA Diameter peer MUST return a STA with Result-Code set to DIAMETER_UNKNOWN_SESSION_ID.

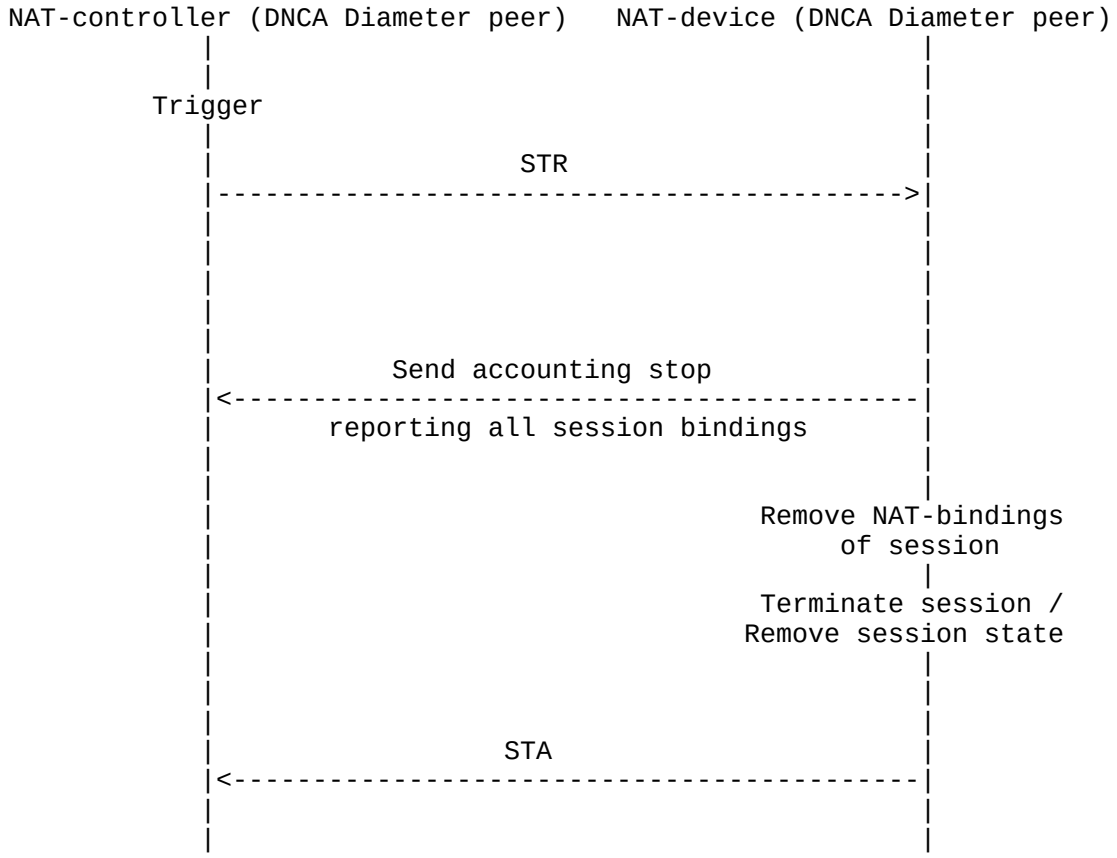


Figure 8: Terminate NAT control session

4.5. Session Abort

An Abort-Session-Request (ASR) message is sent from the DNCA Diameter peer within the NAT-device to the DNCA Diameter peer within the NAT-controller when it is unable to maintain a session due to resource limitations. The DNCA Diameter peer within the NAT-controller MUST acknowledge successful session abort using a Abort Session Answer (ASA) message with Result-Code set to DIAMETER_SUCCESS. Figure 9 shows the protocol interaction between the DNCA Diameter peers. The DNCA Diameter peers will start a session termination procedure as described in Section 4.4 following an ASA with Result-Code set to DIAMETER_SUCCESS.

If the DNCA Diameter peer within a NAT-controller receives an ASR but fails to find a matching session, it MUST return an ASA with Result-Code set to DIAMETER_UNKNOWN_SESSION_ID. If the DNCA Diameter peer

within the NAT-controller is unable to comply with the ASR for any other reason, an ASA with Result-Code set to DIAMETER_UNABLE_TO_COMPLY MUST be returned.

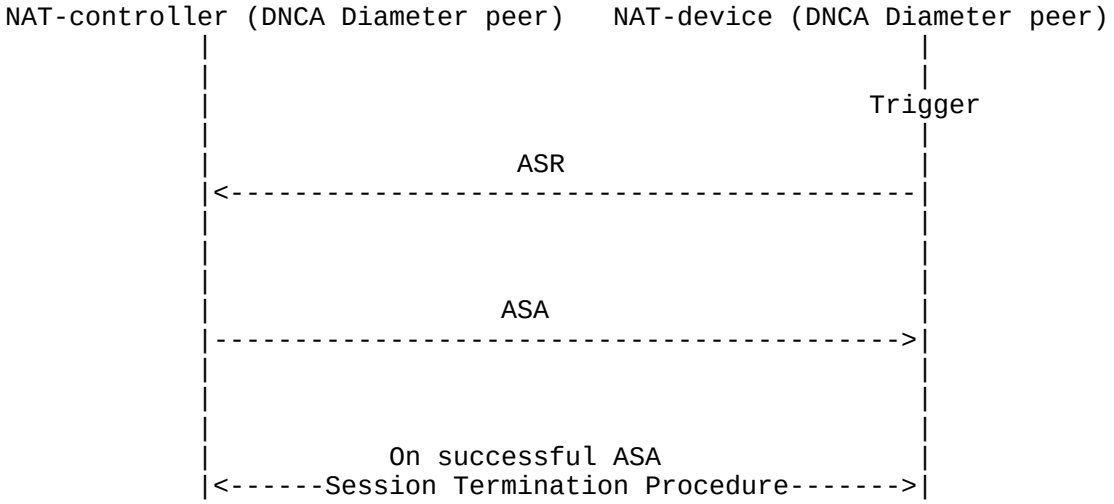


Figure 9: Abort NAT control session

4.6. Failure cases of the DNCA Diameter peers

This document does not specify the behavior in case the NAT-device and NAT-controller, or their respective DNCA Diameter peers are out of sync or lose state. This could happen for example if one of the entities restarts, in case of a (temporary) loss of network connectivity etc. Example failure cases include the following:

- o NAT-controller and the DNCA Diameter peer within the NAT-controller lose state (e.g., due to a restart). In this case,
  - * the DNCA Diameter peer within the NAT-device MAY receive an NCR with NC-Request-Type AVP set to INITIAL_REQUEST that matches an existing session of the DNCA Diameter peer within the NAT-device. The DNCA Diameter peer within the NAT-device MUST return Result-Code that contains Duplicate-Session-Id AVP to report the Session-ID of the existing session. The DNCA Diameter peer within the NAT-controller MAY send an explicit Session Terminate Request (STR) for the older session, which was lost.
  - * a DNCA Diameter peer MAY receive accounting records for a session that does not exist. The DNCA Diameter peer sends an accounting answer with Result-Code set to

DIAMETER_UNKNOWN_SESSION_ID in response. On receiving the response, the DNCA Diameter peer SHOULD clear the session and remove associated session state.

- o NAT-device and the DNCA Diameter peer within NAT-device lose state. In such a case, the DNCA Diameter peer MAY receive a NCR with NC-Request-Type AVP set to UPDATE_REQUEST for a non-existent session. The DNCA Diameter peer MUST return an NCA with Result-Code set to DIAMETER_UNKNOWN_SESSION_ID. When DNCA application within NAT-controller receives this NCA within Result-Code set to DIAMETER_UNKNOWN_SESSION_ID, it MAY try to reestablish DNCA session or disconnect corresponding access session.

- o The DNCA Diameter peer within the NAT-controller is unreachable, for example detected by Diameter device watchdog messages (as defined in Section 5.5 of [RFC3588]), or accounting requests from the DNCA Diameter peer fail to get a response, NAT-bindings and NAT-device state pertaining to that session MUST be cleaned up after a grace period that is configurable on the NAT-device. The grace period can be configured as zero or higher, depending on operator preference.

- o The DNCA Diameter peer within the NAT-device is unreachable or down and NCR fails to get a response. Handling of this case depends on the actual service offering of the service provider. The service provider could for example choose to stop offering connectivity service.

- o A discussion of the mechanisms how a NAT-device cleans up state in case the DNCA Diameter peer within the NAT-device crashes is outside the scope of this document. Implementers of NAT-devices could choose from a variety of options such as coupling the state (e.g. NAT bindings) to timers which require periodic refresh, or time out otherwise, operating system watchdogs for applications, etc.

5. Use of the Diameter Base Protocol

The Diameter Base Protocol defined by [RFC3588] applies with the clarifications listed in the present specification.

5.1. Securing Diameter Messages

For secure transport of Diameter messages, the recommendations in [RFC3588] apply.

DNCA Diameter peers SHOULD verify their identity during the

Capabilities Exchange Request procedure.

A DNCA Diameter peer within the NAT-device SHOULD verify that a DNCA Diameter peer that issues a NCR command is allowed to do so based on:

- The identity of the DNCA Diameter peer
- 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 9 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. The DNCA Diameter peers maintain state associated with the Session-ID. This globally unique Session-ID is used for updating, accounting, and terminating the session. A DNCA session MUST NOT have more than one outstanding request at any given instant. A DNCA Diameter peer 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 Diameter peer within a NAT-controller knows the DiameterIdentity of the Diameter peer within a NAT-device for a given endpoint. Both the Destination-Realm and Destination-Host AVPs are present in the request from a DNCA Diameter peer within a NAT-controller to a DNCA Diameter peer within a NAT-device.

5.5. Advertising Application Support

Diameter nodes conforming to this specification MUST advertise support for DNCA by including the value of TBD.APP-ID in the Auth-Application-Id of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command[RFC3588].

6. DNCA Commands

The following commands are used to establish, maintain and query NAT-bindings.

6.1. NAT-Control Request (NCR) Command

The NAT-Control Request (NCR) command, indicated by the command field set to TBD.COM-CODE and the "R" bit set in the Command Flags field, is sent from the DNCA Diameter peer within the NAT-controller to the DNCA Diameter peer within the NAT-device in order to install NAT-bindings.

User-Name, Logical-Access-Id, Physical-Access-ID, Framed-IP-Address, Framed-IPv6-Prefix, Framed-Interface-Id, EGRESS-VLANID, NAS-Port-ID, Address-Realm, Calling-Station-ID AVPs serve as identifiers for the endpoint.

Message format:

```
   < NC-Request > ::= < Diameter Header: TBD.COM-CODE, REQ, PXY>
                     { Auth-Application-Id }
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { Destination-Host }
                     { NC-Request-Type }
                     [ Session-Id ]
                     [ Origin-State-Id ]
                   *1 [ NAT-Control-Remove ]
                   *1 [ NAT-Control-Install ]
                     [ NAT-External-Address ]
                     [ User-Name ]
                     [ Logical-Access-Id ]
                     [ Physical-Access-ID ]
                     [ Framed-IP-Address ]
                     [ Framed-IPv6-Prefix ]
                     [ Framed-Interface-Id ]
                     [ EGRESS-VLANID]
                     [ NAS-Port-ID]
                     [ Address-Realm ]
                     [ Calling-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.COM-CODE and the "R" bit cleared in the Command Flags field, is sent by the DNCA Diameter peer within the NAT-device in response to NAT-Control-Request command.

Message format:

```
<NC-Answer> ::= < Diameter Header: TBD.COM-CODE, PXY >
                { Origin-Host }
                { Origin-Realm }
                { Result-Code }
                [ Session-Id ]
                [ NC-Request-Type ]
              * [ NAT-Control-Definition ]
                [ Current-NAT-Bindings ]
                [ Origin-State-Id ]
                [ Error-Message ]
                [ Error-Reporting-Host ]
              * [ Failed-AVP ]
              * [ Proxy-Info ]
                [ Duplicate-Session-ID ]
              * [ Redirect-Host]
                [ Redirect-Host-Usage ]
                [ Redirect-Max-Cache-Time ]
              * [ Proxy-Info ]
              * [ Route-Record ]
              * [ Failed-AVP ]
              * [ AVP ]
```

7. NAT Control Application Session State Machine

This section contains a set of finite state machines, representing the life cycle of a DNCA session, which MUST be observed by all implementations of the DNCA Diameter application. The DNCA Diameter peers are stateful and the state machine maintained is similar to the stateful Client and Server authorization state machine described in [RFC3588]. When a session is moved to the Idle state, any resources that were allocated for the particular session must be released. Any event not listed in the state machines MUST be considered as an error condition, and an answer, if applicable, MUST be returned to the originator of the message.

In the state table, the event ’Failure to send NCR’ means that the DNCA Diameter peer within the NAT-controller is unable to send the NCR command to the desired destination. This could be due to the

peer being down, or due to the peer sending back the transient failure or temporary protocol error notification DIAMETER_TOO_BUSY or DIAMETER_LOOP_DETECTED in the Result-Code AVP of an NCA.

In the state table "FAILED NCA" means that the DNCA Diameter peer within the NAT-device was not able to honor the corresponding NCR. This can happen due to any transient and permanent error at the NAT-device or its associated DNCA Diameter peer within indicated by the following error Result-Code values: RESOURCE_FAILURE, UNKNOWN_BINDING_TEMPLATE_NAME, MAX_BINDINGS_SET_FAILURE, BINDING_FAILURE, MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT, SESSION_EXISTS, INSUFFICIENT_CLASSIFIERS.

The following state machine is observed by a DNCA Diameter peer within a NAT-controller. The state machine description uses the term "access session" to describe the connectivity service offered to the endpoint or host. "Access session" should not be confused with the Diameter session ID.

DNCA Diameter peer within a NAT-controller

State	Event	Action	New State
Idle	New endpoint detected that requires NAT Control	Send NCR Initial Request	Pending
Idle	ASR Received for unknown session	Send ASA with Result-Code = UNKNOWN_ SESSION_ID	Idle
Pending	Successful NCA received	Setup complete	Open
Pending	Successful NCA received but peer unable to provide service	Send STR	Discon
Pending	Error processing successful NCA	Send STR	Discon
Pending	Failed NCA received	Clean up	Idle
Open	NAT control	Send	Open

	update required	NCR Update Request	
Open	Successful NCA received		Open
Open	Failed NCA received	Clean up	Idle
Open	Access session end detected	Send STR	Discon
Open	ASR Received, access session will be terminated	Send ASA with Result-Code = SUCCESS, Send STR	Discon
Open	ASR Received, access session will not be terminated	Send ASA with Result-Code != SUCCESS	Open
Discon	ASR Received	Send ASA	Idle
Discon	STA Received	Discon. endpoint	Idle

The following state machine is observed by a DNCA Diameter peer within a NAT-device.

DNCA Diameter peer within a NAT-device

State	Event	Action	New State
Idle	NCR Query request received, and able to provide requested NAT Binding report	Send successful NCA	Idle
Idle	NCR received and able to provide requested NAT control service	Send successful NCA	Open
Idle	NCR request received, and unable to provide requested NAT control service	Send failed NCA	Idle

Open	NCR request received, and able to provide requested NAT control service	Send successful NCA	Open
Open	NCR request received, and unable to provide requested NAT control service	Send failed NCA, Clean up	Idle
Open	Unable to continue providing requested NAT control service	Send ASR	Discon
Open	Unplanned loss of session/ connection to DNCA Diameter peer in NAT controller detected (e.g. due to Diameter watchdog notification)	Clean up	Idle
Discon	Failure to send ASR	Wait, resend ASR	Discon
Discon	ASR successfully sent and ASA Received with Result-Code	Clean up	Idle
Not Discon	ASA Received	None	No change
Any	STR Received	Send STA, Clean up	Idle

8. DNCA AVPs

8.1. Reused Base Protocol AVPs

The following table describes the AVPs reused from Diameter Base Protocol [RFC3588]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the [RFC3588], section 4.

Attribute Name	AVP Code	Data Type	AVP Flag rules: MUST	MAY	Encr
Acct-Interim-Interval	85	Unsigned32	M	P	Y
Auth-Application-Id	258	Unsigned32	M	P	N
Destination-Host	293	DiamIdent	M	P	N
Destination-Realm	283	DiamIdent	M	P	N
Error-Message	281	UTF8String	M	P	N
Error-Reporting-Host	294	DiamIdent	M	P	N
Failed-AVP	279	Grouped	M	P	N
Origin-Host	264	DiamIdent	M	P	N
Origin-Realm	296	DiamIdent	M	P	N
Origin-State-Id	278	Unsigned32	M	P	N
Proxy-Info	284	Grouped	M	P	N
Result-Code	268	Unsigned32	M	P	N
Route-Record	282	DiamIdent	M		N
Session-Id	263	UTF8String	M	P	Y
User-Name	1	UTF8String	M	P	Y

Table 1: DIAMETER AVPs used from Diameter base

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.APP-ID. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.2. Additional Result-Code AVP Values

This section defines new values for the Result-Code AVP that SHALL be supported by all Diameter implementations that conform to the present document.

8.2.1. Success

No new Result-Code AVP value is defined within this category.

8.2.2. Transient Failures

Result-Code AVP values 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.

The following new values of the Result-Code AVP are defined:

RESOURCE_FAILURE (TBD.RCX)

The DNCA Diameter peer within the NAT-device indicates that the binding could not be installed or a new session could not be created due to resource shortage.

8.2.3. Permanent Failures

The Result-Code AVP values, which fall within the permanent failures category are used to inform the peer that the request failed, and should not be attempted again. The request may be able to be satisfied in the future.

The following new values of the Result-Code AVP are defined:

UNKNOWN_BINDING_TEMPLATE_NAME (TBD.RCX)

The DNCA Diameter peer within the NAT-device indicates that the binding could not be installed or a new session could not be created because the specified NAT-Control-Binding-Template AVP, that refers to a predefined policy template in the NAT-device, is unknown.

BINDING_FAILURE (TBD.RCX)

The DNCA Diameter peer within the NAT-device indicates that the requested binding(s) could not be installed. For example: Requested ports are already in use.

MAX_BINDINGS_SET_FAILURE (TBD.RCX)

The DNCA Diameter peer within the NAT-device indicates that it failed to conform to a request to configure the maximum number of bindings for a session. For example: An operator defined the maximum number of bindings on the NAT-device using a method or protocol which takes precendence over DNCA.

MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT (TBD.RCX)

The DNCA Diameter peer within the NAT-device denies the request because the maximum number of allowed bindings has been reached for the specified endpoint classifier.

SESSION_EXISTS (TBD.RCX)

The DNCA Diameter peer within the NAT-device denies request to initialize a new session, if it already has a DNCA session that uses the same set of classifiers as indicated by the DNCA Diameter peer within the NAT-controller in the new session initialization request.

INSUFFICIENT_CLASSIFIERS (TBD.RCX)

The DNCA Diameter peer within the NAT-device requests to initialize a new session, if the classifiers in the request match more than one of the existing sessions on the DNCA Diameter peer within the NAT-device.

8.3. Reused NASREQ Diameter Application AVPs

The following table describes the AVPs reused from the Diameter Network Access Server Application [RFC4005]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the [RFC3588], section 4.

			AVP Flag rules				
Attribute Name	AVP Code	Value Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
NAS-Port	5	Unsigned32	M	P		V	Y
NAS-Port-Id	87	UTF8String	M	P		V	Y
Calling-Station-Id	31	UTF8String	M	P		V	Y
Framed-IP-Address	8	OctetString	M	P		V	Y
Framed-Interface-Id	96	Unsigned64	M	P		V	Y
Framed-IPv6-Prefix	97	OctetString	M	P		V	Y

Table 2: Reused NASREQ Diameter application AVPs. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.4. Reused AVPs from RFC 4675

The following table describes the AVPs reused from "RADIUS Attributes for Virtual LAN and Priority Support" specification [RFC4675]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the

[RFC3588], section 4.

Attribute Name	AVP Code	Value Type	AVP Flag rules: MUST	MAY	SHLD NOT	MUST NOT	Encr
Egress-VLANID	56	OctetString	M	P		V	Y

Table 3: Reused attributes from RFC 4675. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.5. Reused AVPs from Diameter QoS Application

The following table describes the AVPs reused from the Traffic Classification and Quality of Service (QoS) Attributes for Diameter [RFC5777]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the [RFC3588], section 4.

Attribute Name	AVP Code	Data Type	AVP Flag rules: MUST	MAY	Encr
Port	530	Integer32	M	P	Y
Protocol	513	Enumerated	M	P	Y
Direction	514	Enumerated	M	P	Y

Table 4: Reused QoS-attributes. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.6. Reused AVPs from ETSI ES 283 034, e4 Diameter Application

The following table describes the AVPs reused from the Diameter e4 Application [ETSIES283034]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the [RFC3588], section 4. The Vendor-ID field in these AVP header will be set to ETSI (13019).

			AVP Flag rules		
Attribute Name	AVP Code	Data Type	MUST	MAY	Encr
Address-Realm	301	OctetString	M,V		Y
Logical-Access-Id	302	OctetString	V	M	Y
Physical-Access-ID	313	UTF8String	V	M	Y

Table 5: Reused AVPs from Diameter e4 application. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.7. DNCA Defined AVPs

The following table describes the new Diameter AVPs defined in this document; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. The [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5. The Diameter AVP rules are defined in the [RFC3588], section 4. The AVPs defined here MUST NOT have the V bit in the AVP Flag set.

Attribute Name	AVP Code		Data Type	AVP Flag rules: MUST	MAY	Encr
NC-Request-Type	TBD.AX	8.7.1	Enumerated	M	P	Y
NAT-Control-Install	TBD.AX	8.7.2	Grouped	M	P	Y
NAT-Control-Remove	TBD.AX	8.7.3	Grouped	M	P	Y
NAT-Control-Definition	TBD.AX	8.7.4	Grouped	M	P	Y
NAT-Internal-Address	TBD.AX	8.7.5	Grouped	M	P	Y
NAT-External-Address	TBD.AX	8.7.6	Grouped	M	P	Y
Max-NAT-Bindings	TBD.AX	8.7.7	Unsigned32	M	P	Y
NAT-Control-Binding-Template	TBD.AX	8.7.8	OctetString	M	P	Y
Duplicate-Session-ID	TBD.AX	8.7.9	UTF8String	M	P	Y
NAT-External-Port-Style	TBD.AX	8.7.10	Enumerated	M	P	Y
NAT-Control-Record	TBD.AX	9.2.1	Grouped	M	P	Y
NAT-Control-Binding-Status	TBD.AX	9.2.2	Enumerated	M	P	Y
Current-NAT-Bindings	TBD.AX	9.2.3	Unsigned32	M	P	Y

Table 6: New Diameter AVPs. Please refer to [RFC3588] for the definition of the Diameter AVP flag rules and the associated abbreviations used in the table.

8.7.1. NC-Request-Type AVP

The NC-Request-Type AVP (AVP Code TBD.AX) 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 to initiate a Diameter NAT control session between the DNCA Diameter peers.

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.

QUERY_REQUEST (3)

Query Request is used to query a NAT-device about the currently installed bindings for an endpoint classifier.

8.7.2. NAT-Control-Install AVP

The NAT-Control AVP (AVP code TBD.AX) is of type Grouped, and it is used to activate or install NAT bindings. It also contains Max-NAT-Bindings that defines the maximum number of NAT bindings allowed for an endpoint and the NAT-Control-Binding-Template that references a predefined template on the NAT-device that may contain static binding, a maximum number of bindings allowed, an IP-address pool from which external binding addresses should be allocated, etc. If the NAT-External-Port-Style AVP is present, then the NAT-device MUST select the external ports for the NAT-Bindings as per the style specified. The NAT-External-Port-Style is applicable for NAT-Bindings defined by the NAT-Control-Definition AVPs whose NAT-External-Address or Port AVPs within the NAT-External-Address are unspecified.

AVP format:

```
NAT-Control-Install ::= < AVP Header: TBD.AX >
                         * [ NAT-Control-Definition ]
                           [ NAT-Control-Binding-Template ]
                           [ Max-NAT-Bindings ]
                           [ NAT-External-Port-Style ]
                         * [ AVP ]
```

8.7.3. NAT-Control-Remove AVP

The NAT-Control-Remove AVP (AVP code TBD.AX) is of type Grouped, and it is used to deactivate or remove NAT-bindings. At least one of the two AVPs (NAT-Control-Definition AVP, NAT-Control-Binding-Template AVP) SHOULD be present in the NAT-Control-Remove AVP.

AVP format:

```
NAT-Control-Remove ::= < AVP Header: TBD.AX >
                        * [ NAT-Control-Definition ]
                          [ NAT-Control-Binding-Template ]
                        * [ AVP ]
```

8.7.4. NAT-Control-Definition AVP

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

The NAT-Control-Definition AVP uniquely identifies the binding between the DNCA Diameter peers.

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

If the NAT-External-Address AVP is not specified then the NAT-device MUST select the external port as per the NAT-External-Port-Style AVP, if present in the NAT-Control-Definition AVP.

The Protocol AVP describes the transport protocol for the binding. The NAT-Control-Definition AVP can contain either zero or one Protocol AVP. If the Protocol AVP is omitted and if both internal and external IP-address are specified then the binding reserves the IP-addresses for all transport protocols.

The Direction AVP is of type Enumerated. It specifies the direction for the binding. The values of the enumeration applicable in this context are: "IN","OUT". If Direction AVP is OUT or absent, the NAT-Internal-Address refers to the IP-address of the endpoint that needs to be translated. If Direction AVP is "IN", NAT-Internal-Address is the destination IP-address that has to be translated.

AVP format:

```
  NAT-Control-Definition ::= < AVP Header: TBD.AX >
                              { NAT-Internal-Address }
                              [ Protocol ]
                              [ Direction ]
                              [ NAT-External-Address ]
                              [ Session-Id ]
                             * [ AVP ]
```

8.7.5. NAT-Internal-Address AVP

The NAT-Internal-Address AVP (AVP code TBD.AX) is of type Grouped. It describes the internal IP-address and port for a binding. Framed-IPV6-Prefix and Framed-IP-Address AVPs are mutually exclusive. The endpoint identifier Framed-IP-Address, Framed-IPv6-Prefix and the internal address in this NAT-Internal-Address AVP to install NAT-bindings for the session MUST match.

AVP format:

```
NAT-Internal-Address ::= < AVP Header: TBD.AX >
                           [ Framed-IP-Address ]
                           [ Framed-IPv6-Prefix ]
                           [ Port]
                         * [ AVP ]
```

8.7.6. NAT-External-Address AVP

The NAT-External-Address AVP (AVP code TBD.AX) is of type Grouped, and it describes the external IP-address and port for a binding. The external IP-address specified in this attribute can be reused for multiple endpoints by specifying the same address in the respective NAT-External-Address AVPs. If the external IP-address is not specified and the NAT-External-Port-Style AVP is specified in the NAT-Control-Definition AVP then the NAT-device MUST select external port as per the NAT-External-Port-Style AVP.

AVP format:

```
NAT-External-Address ::= < AVP Header: TBD.AX >
                           [ Framed-IP-Address ]
                           [ Port ]
                         * [ AVP ]
```

8.7.7. Max-NAT-Bindings

The Max-NAT-Bindings AVP (AVP code TBD.AX) is of type Unsigned32. It indicates the maximum number of NAT-bindings allowed for a particular endpoint.

8.7.8. NAT-Control-Binding-Template AVP

The NAT-Control-Binding-Template AVP (AVP code TBD.AX) is of type OctetString. It defines a name for a policy template that is predefined at the NAT-device. Details on the contents and structure of the template and configuration are outside the scope of this document. The policy to which this AVP refers to may contain NAT-bindings, IP-address pool for allocating the external IP-address of a NAT-binding, and maximum number of allowed NAT-bindings. Such policy template can be reused by specifying the same NAT-Control-Binding-Template AVP in the corresponding NAT-Control-Install AVPs of multiple endpoints.

8.7.9. Duplicate-Session-Id AVP

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

8.7.10. NAT-External-Port-Style AVP

The NAT-External-Port-Style AVP (AVP Code TBD.AX) is of type Enumerated and contains the style to be followed while selecting the external port for a NAT-Binding relative to the internal port.

The following values are defined:

FOLLOW_INTERNAL_PORT_STYLE (1)

External port numbers selected MUST follow the same sequence and oddity as the internal ports of the NAT-bindings. The port odditity is required to support protocols like RTP and RTCP as defined in [RFC3550]. If for example the internal port in a requested NAT-binding is odd numbered then the external port allocated MUST also be odd numbered, and vice versa for an even numbered port. In addition, the sequence of port numbering is maintained: If internal ports are consecutive, then the NAT-device MUST choose consecutive external ports for the NAT-bindings.

9. Accounting Commands

The DNCA reuses session based accounting as defined in the Diameter Base Protocol[RFC3588] to report the bindings per endpoint. This reporting is achieved by sending Diameter Accounting Requests (ACR) [Start, Interim and Stop] from the DNCA Diameter peer within the NAT-device to its associated DNCA Diameter peer within the NAT-controller.

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

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

The DNCA Diameter peer within the NAT-device may trigger an interim accounting record when the maximum number of bindings, if received in an NCR, is reached.

9.1. NAT Control Accounting Messages

The ACR and ACA messages are reused as defined in the Diameter Base Protocol [RFC3588] for exchanging endpoint NAT binding details between the DNCA Diameter peers. The DNCA Application IDs is used in the accounting commands. ACR contains one or more optional NAT-Control-Record AVPs to report the bindings. The NAT-device indicates the number of allocated NAT bindings to the NAT-controller using the Current-NAT-Bindings AVP. This number needs to match the number of bindings identified as active within the NAT-Control-Record AVP.

9.2. NAT Control Accounting AVPs

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

9.2.1. NAT-Control-Record

The NAT-Control-Record AVP (AVP code TBD.AX) is of type Grouped. It describes a binding and its status. If NAT-Control-Binding-Status is set to Created, Event-Timestamp indicates the binding creation time. If NAT-Control-Binding-Status is set to Removed, Event-Timestamp indicates the binding removal time. If NAT-Control-Binding-Status is active, Event-Timestamp need not be present; if a value is present, it indicates that binding is active at the given time.

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

9.2.2. NAT-Control-Binding-Status

The NAT-Control-Binding-Status AVP (AVP code TBD.AX) is of type enumerated. It indicates the status of the binding - created, removed, or active.

The following values are defined:

Created (1)

NAT binding is created.

Active (2)

NAT binding is active.

Removed (3)

NAT binding was removed.

9.2.3. Current-NAT-Bindings

The Current-NAT-Bindings AVP (AVP code TBD.AX) is of type Unsigned32. It indicates the number of NAT bindings active on the NAT-device.

10. AVP Occurrence Table

The following sections present the AVPs defined in this document and specify the Diameter messages in which they can be present. Note: 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 can be present in the message.
0-1	Zero or one instance of the AVP can 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.

10.1. DNCA AVP Table for NAT Control Initial and Update Requests

The following table lists DNCA specific AVPs that have to be present in NCRs and NCAs with NC-Request-Type set to INITIAL_REQUEST or UPDATE_REQUEST.

	Command Code	
Attribute Name	NCR	NCA
NC-Request-Type	1	1
NAT-Control-Install	0-1	0
NAT-Control-Remove	0-1	0
NAT-Control-Definition	0	0
Current-NAT-Bindings	0	0
Duplicate-Session-Id	0	0-1

Note that any combination of "NAT-Control-Install" and "NAT-Control-Remove" AVPs could be present in an update or initial requests. Consider the following examples:

Neither "NAT-Control-Install AVP" nor "NAT-Control-Remove AVP" are present: This could for example be the case if the NAT-controller would only want to receive accounting information, but not control NAT-bindings.

Only "NAT-Control-Install AVP" is present: This could for example be the case if a new NAT-binding is installed for an existing session.

Only "NAT-Control-Remove AVP" is present: This could for example be the case if a new NAT-binding is removed from an existing session.

Both, "NAT-Control-Install AVP" and "NAT-Control-Remove AVP" are present: This could for example be the case if a formerly created NAT-binding is removed and a new NAT-binding is established within the same request.

10.2. DNCA AVP Table for Session Query request

The following table lists DNCA specific AVPs that have to be present in NCRs and NCAs with NC-Request-Type set to QUERY_REQUEST.

	Command Code	
Attribute Name	NCR	NCA
NC-Request-Type	1	1
NAT-Control-Install	0	0
NAT-Control-Remove	0	0
NAT-Control-Definition	0	0+
NAT-External-Address	0+	0
Current-NAT-Bindings	0	1
Duplicate-Session-Id	0	0

10.3. DNCA AVP Table for Accounting Message

The following table lists DNCA specific AVPs, which may or may not be present in ACR and ACA messages.

	Command Code	
Attribute Name	ACR	ACA
NAT-Control-Record	0+	0
Current-NAT-Bindings	1	0

11. IANA Considerations

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

In the subsections below, when we speak about review by a Designated Expert, please note that the designated expert will be assigned by the IESG. Initially, such Expert discussions take place on the AAA WG mailing list.

11.1. Application Identifier

This specification assigns the value <TBD.APP-ID>, 'Diameter NAT Control Application', to the Application Identifier namespace defined in [RFC3588]. See Section 4 for more information.

11.2. Command Codes

This specification uses the value <TBD.COM-CODE> from the Command code namespace defined in [RFC3588] for the NAT-Control-Request (NCR), NAT-Control-Answer (NCA) commands. See Section 6.1 and Section 6.2 for more information on these commands.

11.3. AVP Codes

This specification assigns the values <TBD.AX> from the AVP code namespace defined in [RFC3588]. See Section 8.7 for the assignment of the namespace in this specification.

11.4. Result-Code AVP Values

This specification assigns the values <TBD.RCX> (4xxx, 5xxx, 5xxx, 5xxx, 5xxx,5xxx) from the Result-Code AVP value namespace defined in [RFC3588]. See Section 8.2 for the assignment of the namespace in this specification.

11.5. NC-Request-Type AVP

As defined in Section 8.7.1, the NC-Request-Type AVP includes Enumerated type values 1 - 3. IANA has created and is maintaining a namespace for this AVP. All remaining values are available for assignment by a Designated Expert [RFC5226].

11.6. NAT-External-Port-Style AVP

As defined in Section 8.7.10, the NAT-External-Port-Style AVP includes Enumerated type value 1. IANA has created and is maintaining a namespace for this AVP. All remaining values are available for assignment by a Designated Expert [RFC5226].

11.7. NAT-Control-Binding-Status AVP

As defined in Section 8.7.1, the NAT-Control-Binding-Status AVP includes Enumerated type values 1 - 3. IANA has created and is maintaining a namespace for this AVP. All remaining values are available for assignment by a Designated Expert [RFC5226].

12. Security Considerations

This document describes procedures for controlling NAT related attributes and parameters by an entity, which is non-local to the device performing NAT. This section discusses security considerations for DNCA. This includes the interactions between the

Diameter peers within a NAT-controller and a NAT-device as well as general considerations for NAT-control in a service provider network.

Security between a NAT-controller and a NAT-device has a number of components: authentication, authorization, integrity, and confidentiality.

Authentication refers to confirming the identity of an originator for all datagrams received from the originator. Lack of authentication of Diameter messages between the Diameter peers can jeopardize the fundamental service of the peering network elements. A consequence of not authenticating the message sender by the recipient would be that an attacker could spoof the identity of a "legitimate" authorizing entity in order to change the behavior of the receiver. An attacker could for example launch a denial of service attack by setting the maximum number of bindings for a session on the NAT-device to zero; provision bindings on a NAT-device which include IP-addresses already in use in other parts of the network; or request session termination of the Diameter session and hamper an endpoint’s (i.e. a user’s) connectivity. Lack of authentication of a NAT-device to a NAT-controller could lead to situations where the NAT-device could provide a wrong view of the resources (i.e. NAT-bindings). In addition, NAT Binding Predefined template on the NAT-device could be configured differently than expected by the NAT-controller. Failing of any of the two DNCA Diameter peers to provide the required credentials should be subject to logging. The corresponding logging infrastructure of the operator SHOULD be built in a way that it can mitigate potential denial of service attacks resulting from large amounts of logging events. This could include proper dimensioning of the logging infrastructure combined with policing the maximum amount of logging events accepted by the logging system to a threshold which the system is known to be able to handle.

Authorization refers to whether a particular authorizing entity is authorized to signal a network element requests for one or more applications, adhering to a certain policy profile. Failing the authorization process might indicate a resource theft attempt or failure due to administrative and/or credential deficiencies. In either case, the network element should take the proper measures to log such attempts.

Integrity is required to ensure that a Diameter message exchanged between the Diameter peers has not been maliciously altered by intermediate devices. The result of a lack of data integrity enforcement in an untrusted environment could be that an impostor will alter the messages exchanged between the peers. This could cause a change of behavior of the peers, including the potential of a denial of service.

Confidentiality protection of Diameter messages ensures that the signaling data is accessible only to the authorized entities. When signaling messages between the DNCA Diameter peers traverse untrusted networks, lack of confidentiality will allow eavesdropping and traffic analysis.

Diameter offers security mechanisms to deal with the functionality demanded above. DNCA makes use of the capabilities offered by Diameter and the underlying transport protocols to deliver these requirements (see Section 5.1). If the DNCA communication traverses untrusted networks, messages between DNCA Diameter peers SHOULD be secured using either IPsec or TLS. Please refer to [RFC3588], section 13 for details. DNCA Diameter peers SHOULD perform bilateral authentication, authorization as well as procedures to ensure integrity and confidentiality of the information exchange. In addition the Session-Id chosen for a particular Diameter session SHOULD be chosen in a way that it is hard to guess in order to mitigate issues through potential message replay.

DNCA Diameter peers SHOULD have a mutual trust setup. This document does not specify a mechanisms for authorization between the DNCA Diameter peers. The DNCA Diameter peers SHOULD be provided with sufficient information to make an authorization decision. The information can come from various sources, for example the peering devices could store local authentication policy, listing the identities of authorized peers.

Any mechanism or protocol providing control of a NAT-device, and DNCA is an example of such a control mechanism, could allow for misuse of the NAT-device given that it enables the definition of per-destination or per-source rules. Misuse could include anti-competitive practices among providers, censorship, crime, etc. NAT-control could be used as a tool for preventing or redirecting access to particular sites. For instance, by controlling the NAT bindings, one could ensure that endpoints aren’t able to receive particular flows, or that those flows are redirected to a relay that snoops or tampers with traffic instead of directly forwarding the traffic to the intended endpoint. In addition one could set up a binding in a way that the source IP address used is one of a relay so that traffic coming back can be snooped on or interfered with. The operator also needs to consider security threats resulting from unplanned termination of the DNCA session. Unplanned session termination, which could e.g. happen due to an attacker taking down the NAT-controller, leads to the NAT-device cleaning up the state associated with this session after a grace period. If the grace period is set to zero, the endpoint will experience an immediate loss of connectivity to services reachable through the NAT-device following the termination of the DNCA session.The protections on DNCA and its

Diameter protocol exchanges don’t prevent such abuses of NAT-control. Prevention of mis-use or mis-configuration of a NAT-device by an authorized NAT-controller is beyond the scope of this protocol specification. A service provider deploying DNCA needs to make sure that higher layer processes and procedures are put in place which allow them to detect and mitigate misuses.

13. Examples

This section shows example DNCA message content and exchange.

13.1. DNCA Session Establishment Example

Figure 15 depicts a typical call flow for DNCA session establishment.

In this example, the NAT-controller:

a. requests a maximum of 100 NAT-bindings for the endpoint.

b. defines a static binding for a TCP connection which associates the internal IP-Address:Port 192.0.2.1:80 with the external IP-Address:Port 198.51.100.1:80 for the endpoint.

c. requests the use of a preconfigured template called "local-policy" while creating NAT-bindings for the endpoint.

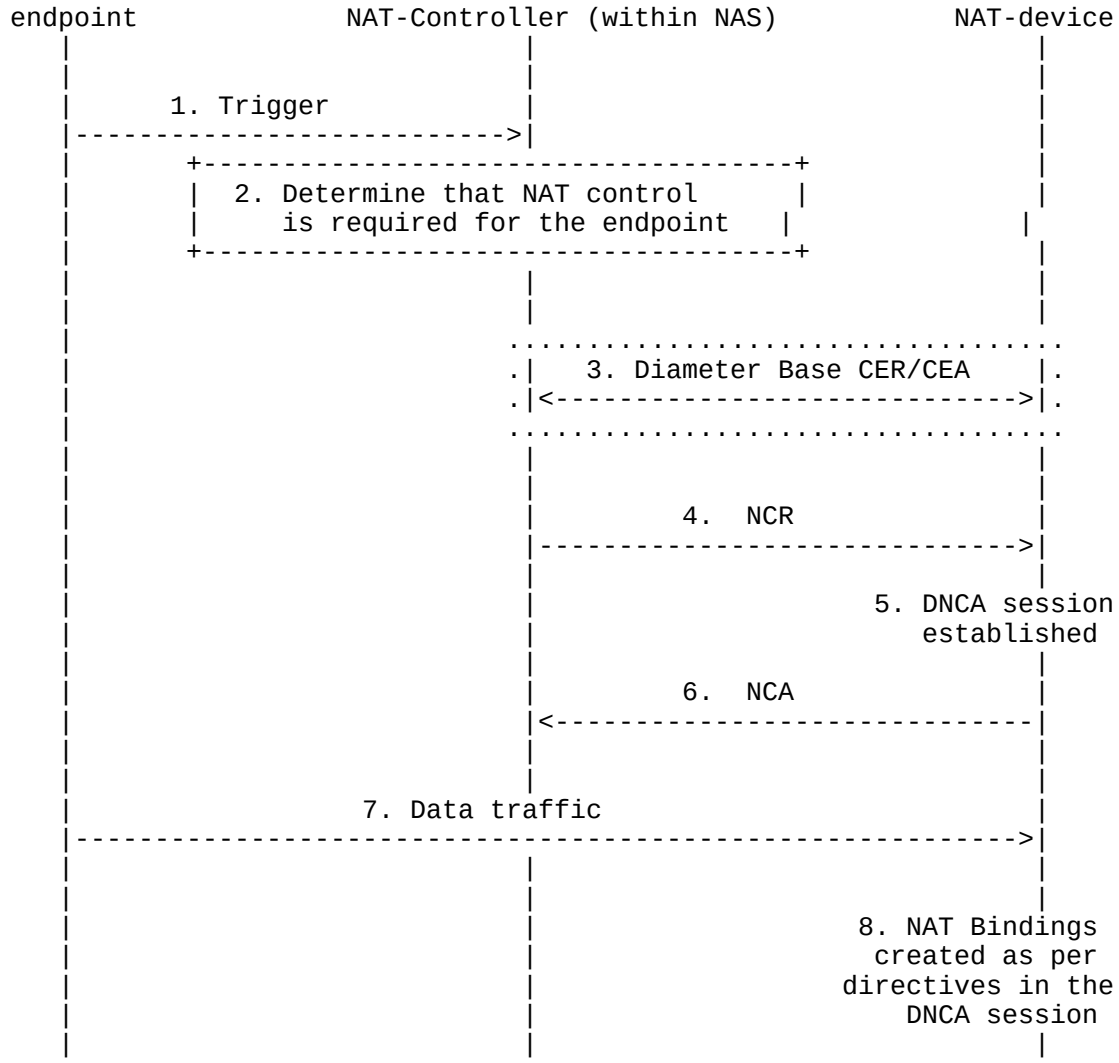


Figure 15: Initial NAT control request and session establishment example

Detailed description of the steps shown in Figure 15:

1. The NAT-controller (co-located with the NAS here) creates state for an endpoint based on a trigger. This could for example be the successful establishment of a Point-to-Point Protocol (PPP) [RFC1661] access session.

2. Based on the configuration of the DNCA Diameter peer within the NAT-controller, the NAT-controller determines that NAT-control is required and is to be enforced at a NAT-device.

3. If there is no Diameter session already established with the DNCA Diameter peer within NAT-device, a Diameter connection is established and Diameter Base CER/CEA are exchanged.

4. The NAT-Controller creates an NCR message (see below) and sends it to the NAT-device. This example shows IPv4 to IPv4 address and port translation. For IPv6 to IPv4 translation, the Framed-IP-Address AVP would be replaced by the Framed-IPv6-Address AVP with the value set to the IPv6 address of the endpoint.

```
< NC-Request > ::= < Diameter Header: TBD.COM-CODE, REQ, PXY>
                   Session-Id =  "natC.example.com:33041;23432;"
                   Auth-Application-Id = <DNCA Application ID>
                   Origin-Host = "natC.example.com"
                   Origin-Realm = "example.com"
                   Destination-Realm = "example.com"
                   Destination-Host = "nat-device.example.com"
                   NC-Request-Type = INITIAL_REQUEST
                   User-Name = "subscriber_example1"
                   Framed-IP-Address = "192.0.2.1"
                   NAT-Control-Install = {
                        NAT-Control-Definition = {
                           Protocol = TCP
                           Direction = OUT
                           NAT-Internal-Address = {
                                Framed-IP-Address = "192.0.2.1"
                                Port = 80
                           }
                           NAT-External-Address = {
                                Framed-IP-Address = "198.51.100.1"
                                Port = 80
                           }
                        }
                        Max-NAT-Bindings = 100
                        NAT-Control-Binding-Template = "local-policy"
                  }
```

5. The NAT-device establishes a DNCA session as it is able to comply with the request.

6. The NAT-device sends an NCA to indicate the successful completion of the request.

```
<NC-Answer> ::= < Diameter Header: TBD.COM-CODE, PXY >
                  Session-Id =  "natC.example.com:33041;23432;"
                  Origin-Host = "nat-device.example.com"
                  Origin-Realm = "example.com"
                  NC-Request-Type = INITIAL_REQUEST
                  Result-Code = DIAMETER_SUCCESS
```

7. The endpoint sends packets that reach the NAT-device.

8. The NAT-device performs NAT for traffic received from the endpoint with source address 192.0.2.1. Traffic with source IP-address 192.0.2.1 and port 80 are translated to the external IP-address 198.51.100.1 and port 80. Traffic with source IP-address 192.0.2.1 and a source port different from 80 will be translated to IP-address 198.51.100.1 and a port chosen by the NAT-device. Note that this example assumes that the NAT-device follows typical binding allocation rules for endpoints, in that only a single external IP-address is used for all traffic received from a single IP-address of an endpoint. The NAT-device will allow a maximum of 100 NAT-bindings be created for the endpoint.

13.2. DNCA Session Update with Port Style Example

This section gives an example for a DNCA session update: A new set of NAT-bindings is requested for an existing session. The request contains a directive (the "NAT-External-Port-Style" AVP set to FOLLOW_INTERNAL_PORT_STYLE) that directs the NAT-device to maintain port-sequence and port-oddity for the newly created NAT-bindings. In the example shown, the internal ports are UDP port 1036 and 1037. The NAT-device follows the directive selects the external ports accordingly. The NAT-device would for example create a mapping of 192.0.2.1:1036 to 198.51.100.1:5056 and 192.0.2.1:1037 to 198.51.100.1:5057, thereby maintaining port oddity (1036->5056, 1037->5057) and sequence (the consecutive internal ports 1036 and 1037 map to the consecutive external ports 5056 and 5057).

```
< NC-Request > ::= < Diameter Header: TBD.COM-CODE, REQ, PXY>
                   Session-Id =  "natC.example.com:33041;23432;"
                   Auth-Application-Id = <DNCA Application ID>
                   Origin-Host = "natC.example.com"
                   Origin-Realm = "example.com"
                   Destination-Realm = "example.com"
                   Destination-Host = "nat-device.example.com"
                   NC-Request-Type = UPDATE_REQUEST
                   NAT-Control-Install = {
                       NAT-Control-Definition = {
                           Protocol = UDP
                           Direction = OUT
                           NAT-Internal-Address = {
                                Framed-IP-Address = "192.0.2.1"
                                Port = 1035
                           }
                       }
                       NAT-Control-Definition = {
                           Protocol = UDP
                           Direction = OUT
                           NAT-Internal-Address = {
                                Framed-IP-Address = "192.0.2.1"
                                Port = 1036
                           }
                       }
                       NAT-External-Port-
                              Style = FOLLOW_INTERNAL_PORT_STYLE
                   }
```

13.3. DNCA Session Query Example

This section shows an example for DNCA session query for a subscriber whose internal IP-Address is 192.0.2.1.

```
< NC-Request > ::= < Diameter Header: TBD.COM-CODE, REQ, PXY>
                   Auth-Application-Id = <DNCA Application ID>
                   Origin-Host = "natC.example.com"
                   Origin-Realm = "example.com"
                   Destination-Realm = "example.com"
                   Destination-Host = "nat-device.example.com"
                   NC-Request-Type = QUERY_REQUEST
                   Framed-IP-Address = "192.0.2.1"
```

The NAT-device constructs an NCA to report all currently active NAT-bindings whose internal address is 192.0.2.1.

```
      <NC-Answer> ::= < Diameter Header: TBD.COM-CODE, PXY >
                     Origin-Host = "nat-device.example.com"
                     Origin-Realm = "example.com"
                     NC-Request-Type = QUERY_REQUEST
                     NAT-Control-Definition = {
                             Protocol = TCP
                             Direction = OUT
                             NAT-Internal-Address = {
                                 Framed-IP-Address = "192.0.2.1"
                                 Port = 80
                                }
                             NAT-External-Address = {
                                  Framed-IP-Address = "198.51.100.1"
                                  Port = 80
                                }
                             Session-Id = "natC.example.com:33041;23432;"
                     }
                     NAT-Control-Definition = {
                             Protocol = TCP
                             Direction = OUT
                             NAT-Internal-Address = {
                                 Framed-IP-Address = "192.0.2.1"
                                 Port = 1036
                                }
                             NAT-External-Address = {
                                  Framed-IP-Address = "198.51.100.1"
                                  Port = 5056
                                }
                             Session-Id = "natC.example.com:33041;23432;"
                     }
                     NAT-Control-Definition = {
                             Protocol = TCP
                             Direction = OUT
                             NAT-Internal-Address = {
                                 Framed-IP-Address = "192.0.2.1"
                                 Port = 1037
                                }
                             NAT-External-Address = {
                                  Framed-IP-Address = "198.51.100.1"
                                  Port = 5057
                                }
                             Session-Id = "natC.example.com:33041;23432;"
                     }
```

13.4. DNCA Session Termination Example

In this example the NAT-controller decides to terminate the previously established DNCA session. This could for example be the

case as a result of an access session (e.g. a PPP session) associated with an endpoint been torn down.

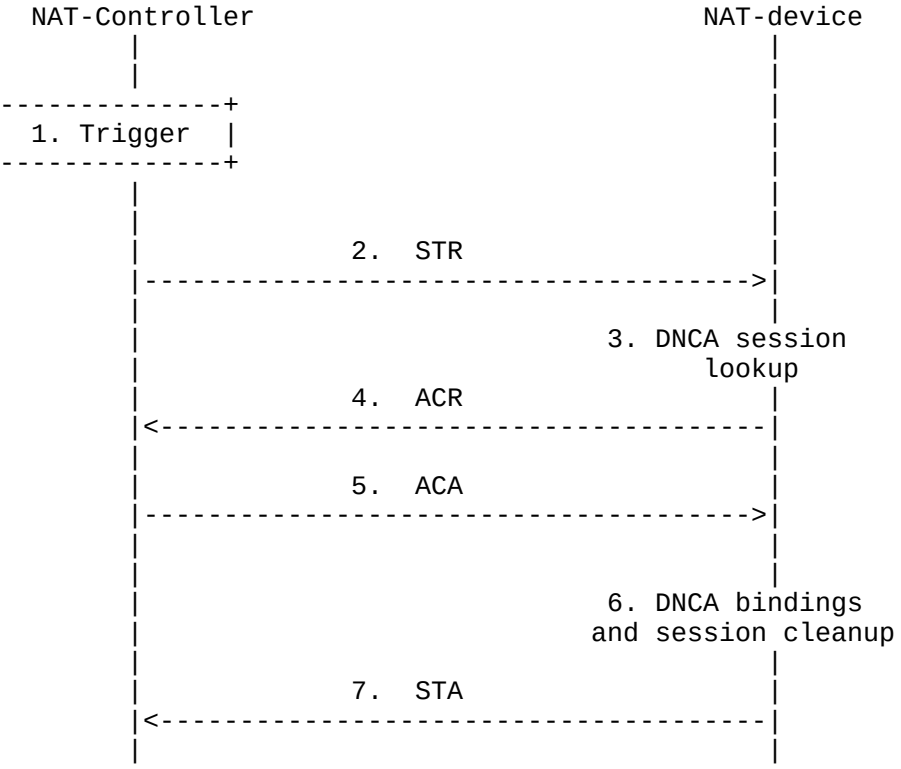


Figure 20: NAT control session termination example

The following steps describe the sequence of events for tearing down the DNCA session in the example above:

1. The NAT-controller receives a trigger that a DNCA session associated with a specific endpoint should be terminated. An example event could be the termination of the PPP [RFC1661] access session to an endpoint in a NAS. The NAS correspondingly triggers the NAT-controller request tear-down of the associated DNCA session.

2. The NAT-controller creates the required NCR message and sends it to the NAT-device:

```
< STR >     ::= < Diameter Header: 275, REQ, PXY>
                Session-Id =  "natC.example.com:33041;23432;"
                Auth-Application-Id = <DNCA Application ID>
                Origin-Host = "natC.example.com"
                Origin-Realm = "example.com"
                Destination-Realm = "example.com"
                Destination-Host = "nat-device.example.com"
                Termination-Cause = DIAMETER_LOGOUT
```

3. The NAT-device looks up the DNCA session based on the Session-Id AVP and finds a previously established active session.

4. The NAT-device reports all NAT-bindings established for that subscriber using an ACR:

```
< ACR >     ::= < Diameter Header: 271, REQ, PXY>
                Session-Id =  "natC.example.com:33041;23432;"
                Auth-Application-Id = <DNCA Application ID>
                Origin-Host = "nat-device.example.com"
                Origin-Realm = "example.com"
                Destination-Realm = "example.com"
                Destination-Host = "natC.example.com"
                Accounting-Record-Type = STOP_RECORD
                Accounting-Record-Number = 1
                NAT-Control-Record = {
                    NAT-Control-Definition = {
                        Protocol = TCP
                        Direction = OUT
                        NAT-Internal-Address = {
                            Framed-IP-Address = "192.0.2.1"
                            Port = 5001
                           }
                        NAT-External-Address = {
                             Framed-IP-Address = "198.51.100.1"
                             Port = 7777
                           }
                       }
                      NAT-Control-Binding-Status = Removed
                   }
```

5. The NAT-controller receives and processes the ACR as per its configuration. It responds with an ACA to the NAT-device.

```
<ACA>      ::= < Diameter Header: 271, PXY >
                 Session-Id =  "natC.example.com:33041;23432;"
                 Origin-Host = "natC.example.com"
                 Origin-Realm = "example.com"
                 Result-Code = DIAMETER_SUCCESS
                 Accounting-Record-Type = STOP_RECORD
                 Accounting-Record-Number = 1
```

6. On receipt of the ACA the NAT-device cleans up all NAT-bindings and associated session state for the endpoint.

7. NAT-device sends an STA. On receipt of the STA the NAT-controller will clean up the corresponding session state.

```
<STA>      ::= < Diameter Header: 275, PXY >
                 Session-Id =  "natC.example.com:33041;23432;"
                 Origin-Host = "nat-device.example.com"
                 Origin-Realm = "example.com"
                 Result-Code = DIAMETER_SUCCESS
```

14. Acknowledgements

The authors would like to thank Jari Arkko, Wesley Eddy, Stephen Farrell, Miguel A. Garcia, David Harrington, Jouni Korhonen, Matt Lepinski, Avi Lior, Chris Metz, Pallavi Mishra, Lionel Morand, Robert Sparks, Martin Stiemerling, Dave Thaler, Hannes Tschofenig, Sean Turner, Shashank Vikram, Greg Weber, and Glen Zorn for their input on this document.

15. Change History (to be removed prior to publication as an RFC)

Changes from -00 to -01

a. new values for Result-Code AVP used - instead of Experimental-Result AVP

b. added support for transport specific binding (UDP/TCP)

c. added support for twice-NAT

d. clarified the use of the two different types of query-requests

Changes from -01 to -02

a. Reference to pull mode removed, session initiation event clarified in section 4.1

b. added Redirect-* AVPs in NCA command

c. Removed reference to Called-Station-Id AVP in NCR command

d. Editorial changes

e. added support for bindings providing AFT (NAT64)

Changes from -02 to -03

a. Editorial changes

Changes from -03 to -04

a. Editorial changes suggested in WG last call review

b. Removed NCR Request type terminate and replaced with STR

c. All references to Auth-Session-State are removed and a new section to describe FSM for Manager and Agent has been added

d. Clarified reuse of External address and address pools among multiple subscribers

Changes from -04 to -05

a. Removed references to Large Scale NAT as per review comments

Changes from -05 to -06

a. Editorial changes

Changes from -06 to -07

a. Added a note in section 4.3 stating the state of pre-existing bindings on update failure

b. Security considerations are made consistent between sections 5.1 and 12

c. Editorial changes

Changes from -07 to -08

a. Added section 4.6 to describe session abort

b. Editorial changes

c. Nomenclature change: From DNCA Agent/Manager to DNCA Diameter peers identifying the location where they reside (NAT-controller or NAT-device)

d. IANA consideration Section format changes

e. Updated security section (included considerations directly, rather than referring to Diameter QoS similarities).

Changes from -08 to -09

a. expanded on the need for an SP controlling the maximum number of bindings of an endpoint (see introduction section)

b. added a paragraph in the security section outlining general mis-uses of NAT-control (non specific to DNCA), with DNCA being an example of such a NAT-control protocol

c. editorial changes

Changes from -09 to -10

a. Section 4 and security considerations updated with RFC 2119 language

b. NAT-External-Port-Style AVP added to aid external port oddity requirement as per MIDCOM framework

c. NAT related RFCs added in normative reference

d. Section 13 added to provide example DNCA message exchange flows

e. Added a description to provide DNCA comparison with MIDCOM

f. n:1 deployment model for NAT-controllers and NAT-devices explicitly specified

g. editorial changes as per IESG DISCUSS comments

Changes from -10 to -11

a. clarified DNCA session query to be done after Diameter session is established

b. Section 4.4 Session Termination updated to specify resource cleanup at NAT-Device upon session termination

c. Removed Framed-IP-Netmask AVP from NAT-External-Address as external address is fully defined by Framed-IP-Address AVP

d. Updated Section 12 to highlight Session-Id to be chosen such that it is hard to guess

e. editorial changes as per IESG DISCUSS

Changes from -11 to -12

a. endpoint replaces references to end point and user and defines what Endpoint means in this draft

b. editorial changes as per IESG DISCUSS

Changes from -12 to -13

a. Section 4.3 session query updated to use NAT-External-Address for external IP-address based query

Changes from -13 to -14

a. Added NAT-External-Address in NC-request for session query by external IP-address

b. Reordered all mandatory AVPs in NCR and NCA to appear before optional AVPs

Changes from -14 to -15

a. As part of IESG discuss - clarified that multiple methods if used along with DNCA for NAT control should be configured to prevent conflict.

b. Clarified misuse of NAT-device by a Diameter authorized NAT-controller using DNCA is beyond the scope of this protocol specification.

c. Editorial updates.

Changes from -15 to -16

a. Extended section covering case of a single NAT-device controlled by multiple NAT-ontrollers which use different protocols for configuring the NAT-device.

b. Added NAT-device state cleanup in case of unexpected/unplanned termination of Diameter session or application either on NAT-controller or NAT-device.

c. Added MAX_BINDINGS_SET_FAILURE failure case (for those scenarios where the maximum number of bindings cannot be set by the controller)

Change from -16 to -17

a. Clarified that the endpoint identifier Framed-IP-Address and the internal address in NAT-Internal-Address specified to install NAT-bindings for the session MUST match.

16. References

16.1. Normative References

[ETSIES283034] ETSI, "Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN),Network Attachment Sub-System (NASS),e4 interface based on the Diameter protocol.", September 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4675] Congdon, P., Sanchez, M., and B. Aboba, "RADIUS Attributes for Virtual LAN and Priority Support", RFC 4675, September 2006.

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

[RFC5777] Korhonen, J., Tschofenig, H., Arumaithurai, M., Jones, M., and A. Lior, "Traffic Classification and Quality of Service (QoS) Attributes for Diameter", RFC 5777, February 2010.

16.2. Informative References

[I-D.ietf-behave-lsn-requirements]
Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-05 (work in progress), November 2011.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

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

[RFC3303] Srisuresh, P., Kuthan, J., Rosenberg, J., Molitor, A., and A. Rayhan, "Middlebox communication architecture and framework", RFC 3303, August 2002.

[RFC3304] Swale, R., Mart, P., Sijben, P., Brim, S., and M. Shore, "Middlebox Communications (midcom) Protocol Requirements", RFC 3304, August 2002.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC4097] Barnes, M., "Middlebox Communications (MIDCOM) Protocol Evaluation", RFC 4097, June 2005.

[RFC5189] Stiemerling, M., Quittek, J., and T. Taylor, "Middlebox Communication (MIDCOM) Protocol Semantics", RFC 5189, March 2008.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6

Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

Authors' Addresses

Frank Brockners
Cisco
Hansaallee 249, 3rd Floor
DUESSELDORF, NORDRHEIN-WESTFALEN 40549
Germany

Email: fbrockne@cisco.com

Shwetha Bhandari
Cisco
Cessna Business Park, Sarjapura Marathalli Outer Ring Road
Bangalore, KARNATAKA 560 087
India

Email: shwethab@cisco.com

Vaneeta Singh
18, Cambridge Road
Bangalore 560008
India

Email: vaneeta.singh@gmail.com

Victor Fajardo
Telcordia Technologies
1 Telcordia Drive #1S-222
Piscataway, NJ 08854
USA

Email: vf0213@gmail.com