

Internet Engineering Task Force (IETF)
Request for Comments: 6736
Category: Standards Track
ISSN: 2070-1721

F. Brockners
S. Bhandari
Cisco
V. Singh

V. Fajardo
Telcordia Technologies
October 2012

Diameter Network Address and Port Translation Control Application

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 Authentication, Authorization, and Accounting (AAA) and policy control capabilities with a Network Address Translator and Network Address and Port Translator 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6736>.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Conventions	6
3. Deployment Framework	7
3.1. Deployment Scenario	7
3.2. Diameter NAPT Control Application Overview	9
3.3. Deployment Scenarios for DNCA	10
4. DNCA Session Establishment and Management	12
4.1. Session Establishment	13
4.2. Session Update	16
4.3. Session and Binding Query	18
4.4. Session Termination	20
4.5. Session Abort	21
4.6. Failure Cases of the DNCA Diameter Peers	22
5. Use of the Diameter Base Protocol	23
5.1. Securing Diameter Messages	23
5.2. Accounting Functionality	24
5.3. Use of Sessions	24
5.4. Routing Considerations	24
5.5. Advertising Application Support	24
6. DNCA Commands	25
6.1. NAT-Control-Request (NCR) Command	25
6.2. NAT-Control-Answer (NCA) Command	26
7. NAT Control Application Session State Machine	26
8. DNCA AVPs	29
8.1. Reused Base Protocol AVPs	29
8.2. Additional Result-Code AVP Values	30
8.2.1. Success	30
8.2.2. Transient Failures	30
8.2.3. Permanent Failures	31

8.3. Reused NASREQ Diameter Application AVPs	32
8.4. Reused AVPs from RFC 4675	33
8.5. Reused AVPs from Diameter QoS Application	33
8.6. Reused AVPs from ETSI ES 283 034, e4 Diameter Application	34
8.7. DNCA-Defined AVPs	35
8.7.1. NC-Request-Type AVP	36
8.7.2. NAT-Control-Install AVP	36
8.7.3. NAT-Control-Remove AVP	37
8.7.4. NAT-Control-Definition AVP	37
8.7.5. NAT-Internal-Address AVP	38
8.7.6. NAT-External-Address AVP	38
8.7.7. Max-NAT-Bindings	39
8.7.8. NAT-Control-Binding-Template AVP	39
8.7.9. Duplicate-Session-Id AVP	39
8.7.10. NAT-External-Port-Style AVP	39
9. Accounting Commands	40
9.1. NAT Control Accounting Messages	40
9.2. NAT Control Accounting AVPs	40
9.2.1. NAT-Control-Record	41
9.2.2. NAT-Control-Binding-Status	41
9.2.3. Current-NAT-Bindings	41
10. AVP Occurrence Tables	41
10.1. DNCA AVP Table for NAT Control Initial and Update Requests	42
10.2. DNCA AVP Table for Session Query Requests	43
10.3. DNCA AVP Table for Accounting Messages	43
11. IANA Considerations	44
11.1. Application Identifier	44
11.2. Command Codes	44
11.3. AVP Codes	44
11.4. Result-Code AVP Values	44
11.5. NC-Request-Type AVP	44
11.6. NAT-External-Port-Style AVP	45
11.7. NAT-Control-Binding-Status AVP	45
12. Security Considerations	45
13. Examples	47
13.1. DNCA Session Establishment Example	47
13.2. DNCA Session Update with Port Style Example	50
13.3. DNCA Session Query Example	51
13.4. DNCA Session Termination Example	53
14. Acknowledgements	55
15. References	55
15.1. Normative References	55
15.2. Informative References	56

1. Introduction

Internet service providers deploy Network Address Translators (NATs) and Network Address and Port Translators (NAPT) [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 (DoS) attacks. If multiple endpoints share a single public IP address, these endpoints can share fate. If one endpoint would (either intentionally, or due to misbehavior, misconfiguration, malware, 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 [CGN-REQS].
2. Supports the allocation of specific NAPT/NAT-bindings. Two types of specific bindings can be distinguished:
 - * Allocation of a predefined NAT-binding: The internal and external IP addresses as well as the 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 requester. 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 be either pre-assigned at the NAT/NAPT 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 NAT/NAPT-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 classifier or a set of classifiers, such as IP address, Virtual Local Area Network (VLAN) identifier, or interface identifier that uniquely identify the traffic associated with a particular global endpoint.

With the above capabilities, DNCA qualifies as a Middlebox Communications (MIDCOM) protocol [RFC3303], [RFC3304], [RFC5189] for middleboxes that perform NAT. The MIDCOM protocol evaluation [RFC4097] evaluated Diameter as a candidate protocol for MIDCOM. DNCA provides the extensions to the Diameter base protocol [RFC6733] 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 the maintenance of 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, for example, Simple Network Management Protocol (SNMP) [RFC3411] and Network Configuration (NETCONF) [RFC6241], which can both be used for device configuration. Similarly, DNCA complements existing MIDCOM implementations, offering a MIDCOM protocol option for operators with an operational environment that is Diameter focused that desire the use of 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 (CLI), SNMP, NETCONF, or Port Control Protocol (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 3.2 to 8 cover DNCA specifics, with Section 3.2 describing session management, Section 5 the use of the Diameter base protocol, Section 6 new commands, Section 8 Attribute Value Pairs (AVPs) used, and Section 9 accounting aspects. Section 10 presents AVP occurrence tables. IANA and security considerations are addressed in Sections 11 and 12, respectively.

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 and terminology 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: 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 endpoints, 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 NAPT, 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 through a NAS, which facilitates the authentication of the endpoint and configures the endpoint'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 an 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 1:1:1 relationship between an endpoint, the access-session it represents, and the associated DNCA session.

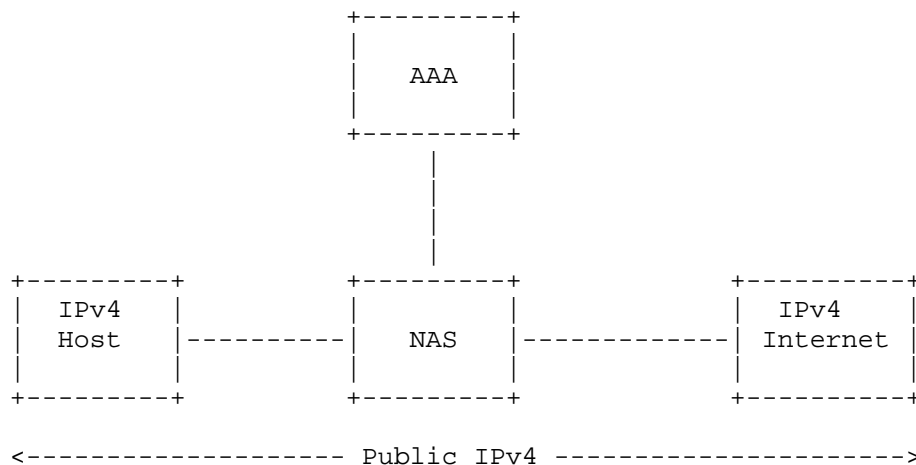
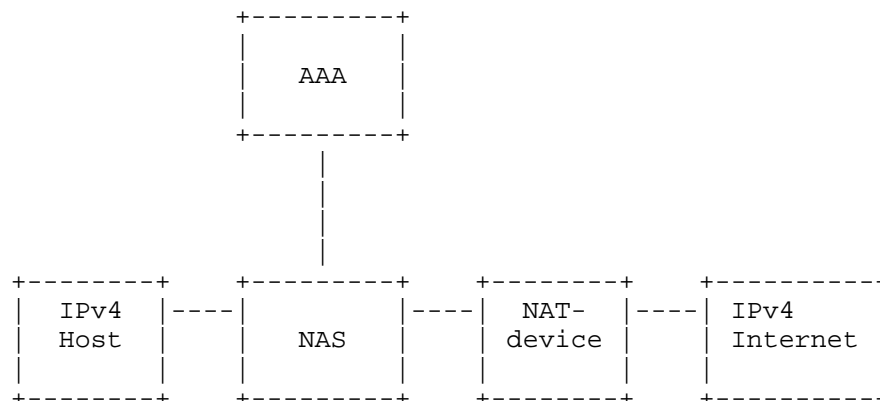


Figure 1: Typical Network Deployment for Internet Access

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 [CGN-REQS]. This includes cases like the following:

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



For NAT44 deployments (IPv4 host):

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

For NAT64 deployments (IPv6 host):

<----- Public IPv6 -----><---- Public IPv4 ---->

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:

- o 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.
- o Per-endpoint reporting of the allocated NAT-bindings.

- o Unique identification of an endpoint on a 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 using either accounting mechanisms or an explicit session query to the NAT.

3.3. Deployment Scenarios for DNCA

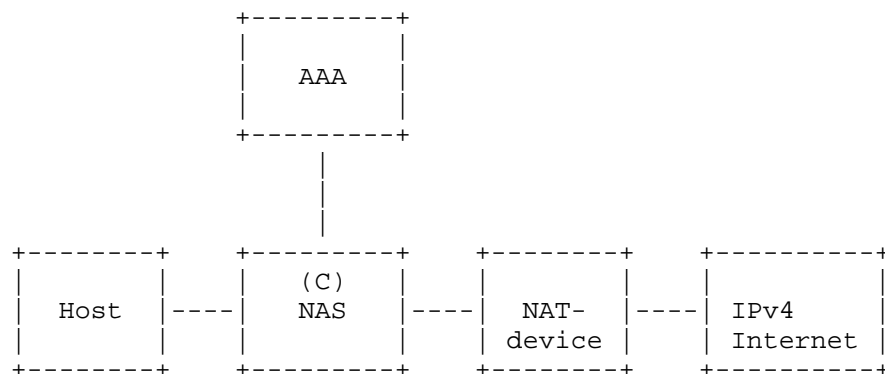
DNCA can be deployed in different ways. DNCA supports deployments with "n" NAT controllers and "m" NAT devices, with n and m equal to or greater than 1. From a DNCA perspective, an operator should ensure that the session representing a particular endpoint is atomic. Any deployment MUST ensure that, for 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 that they would not be unclear about to which NAT controller to send accounting information. Operational considerations MAY require an operator to use alternate control mechanisms or protocols such as SNMP or manual configuration via a CLI to apply per-endpoint NAT-specific configuration, for example, static NAT-bindings. For these cases, the NAT device MUST allow the operator to configure a policy on how configuration conflicts are resolved. Such a policy could specify, for example, that manually configured NAT-bindings using the CLI 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 --->

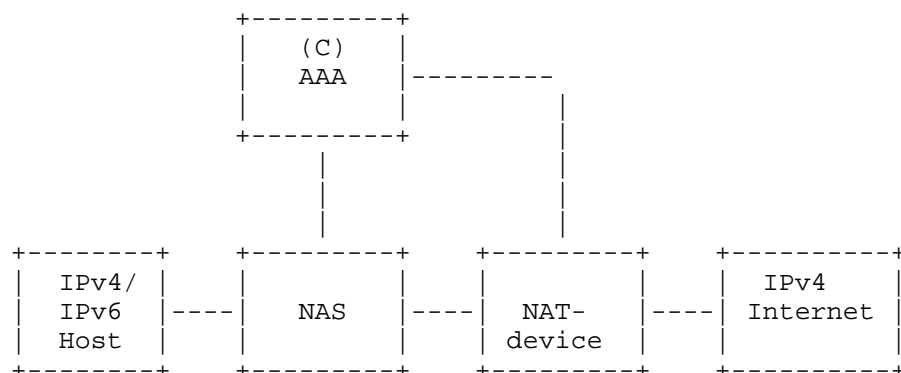
For NAT64 deployments (IPv6 host):

<----- Public IPv6 -----><--- Public IPv4 --->

Figure 3: NAT Control Deployment: Integrated Deployment

Figure 3 shows examples of integrated deployments. It illustrates two scenarios: one where an IPv4 host (with a private IPv4 address) accesses the IPv4 Internet and another 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 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. It illustrates two scenarios: one where an IPv4 host (with a private IPv4 address) accesses the IPv4 Internet and another where an IPv6 host accesses the IPv4 Internet.

4. DNCA Session Establishment and Management

Note that from this section on, there are references to some of the commands and AVPs defined for DNCA. Please refer to Sections 6 and 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 be due to, for example, 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 the 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 predefined NAT-bindings to be established for this endpoint, or a description of the address pool, from which external addresses are to be allocated.

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 the NC-Request-Type AVP set to INITIAL_REQUEST to initiate a Diameter NAT control session. On receipt of an 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 the 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:

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

- o A description of the external IP address pool(s) to be used for the session.
- o 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 from which external IP addresses should be allocated, 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:

- o If a DNCA Diameter peer within the NAT device receives an NCR from a DNCA Diameter peer within a NAT controller with the NC-Request-Type AVP set to INITIAL_REQUEST that identifies an already existing session, that is, the endpoint identifier matches an already existing session, the DNCA Diameter peer within the NAT device MUST return an NCA with the Result-Code set to SESSION_EXISTS and provide the Session-Id of the existing session in the Duplicate-Session-Id AVP.
- o If a DNCA Diameter peer within the NAT device receives an NCR from a DNCA Diameter peer within a NAT controller with the NC-Request-Type AVP set to INITIAL_REQUEST that matches more than one of the already existing sessions, that is, the DNCA Diameter peer and endpoint identifier match already existing sessions, the DNCA Diameter peer within the NAT device MUST return an NCA with the Result-Code set to INSUFFICIENT_CLASSIFIERS. In case a DNCA Diameter peer receives an NCA that reports Insufficient-Classifiers, it MAY choose to retry establishing a new session using additional or more specific classifiers.
- o 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 the Result-Code AVP set to UNKNOWN_BINDING_TEMPLATE_NAME.
- o 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 the Result-Code set to BINDING_FAILURE. A DNCA Diameter peer within a NAT device MUST treat an NCR as an atomic operation; hence, none of the requested bindings will be established by the NAT device. Either all requested actions within an NCR MUST be completed successfully or the entire request fails.

- o 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 the 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.
- o If a NAT device does not have sufficient resources to process a request, the DNCA Diameter peer MUST return an NCA with the Result-Code set to RESOURCE_FAILURE.
- o In the case where Max-NAT-Bindings, NAT-Control-Definition, and 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 that NAT-Control-Binding-Template references, Max-NAT-Bindings and NAT-Control-Definition MUST override the values specified in the template to which NAT-Control-Binding-Template refers.

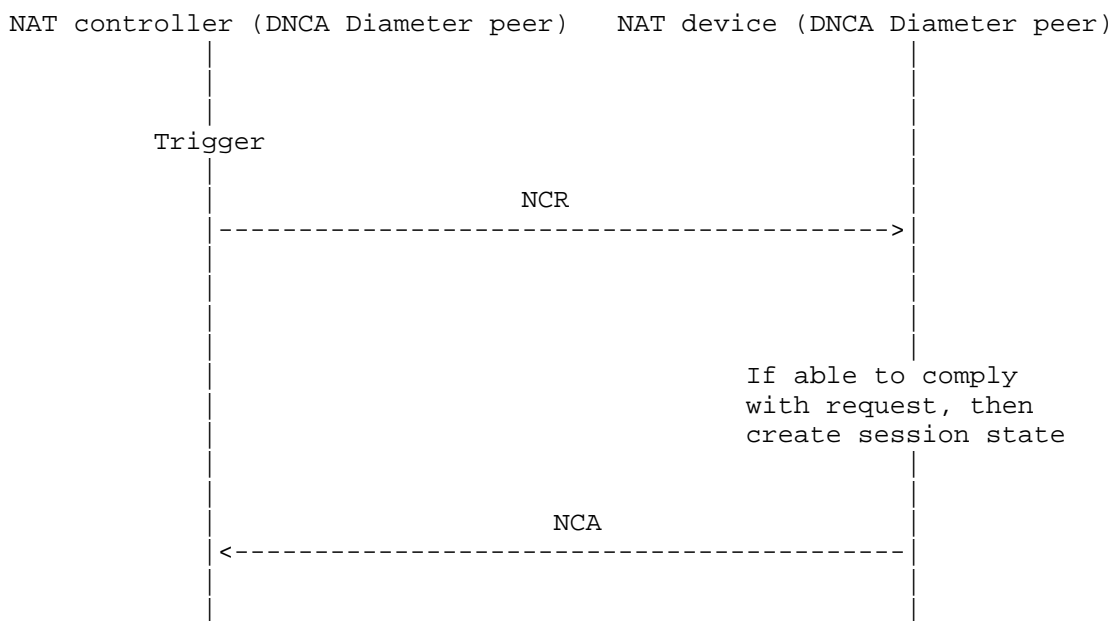


Figure 5: Initial NAT-Control-Request and Session Establishment

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 the Result-Code set to DIAMETER_SUCCESS.

4.2. Session Update

A session update is performed if the NAT controller desires to change the behavior of the NAT device for an existing session. A session update could be used, for example, to change the number of allowed bindings for a particular session or establish or remove a predefined binding.

The DNCA Diameter peer within the NAT controller generates an NCR message to the DNCA Diameter peer within the NAT device with the 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 the 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:

- o If a DNCA Diameter peer within a NAT device receives an NCR update or query request for a non-existent session, it MUST set the Result-Code in the answer to `DIAMETER_UNKNOWN_SESSION_ID`.
- o If the NCR contains a NAT-binding Predefined template not defined on the NAT device, an NCA with the Result-Code AVP set to `UNKNOWN_BINDING_TEMPLATE_NAME` MUST be returned.
- o 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 the Result-Code AVP set to `MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT` MUST be returned to the DNCA Diameter peer.
- o 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 the 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 an NCR are either all successful or all fail.
- o 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 the Result-Code AVP set to `MAX_BINDINGS_SET_FAILURE`.

- o If the NAT device does not have sufficient resources to process a request, an NCA with the Result-Code set to RESOURCE_FAILURE MUST be returned.
- o 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 the 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 the 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.
- o 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.
- o In case Max-NAT-Bindings, NAT-Control-Definition, and 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 that NAT-Control-Binding-Template references, Max-NAT-Bindings and NAT-Control-Definition MUST override the values specified in the template to which the NAT-Control-Binding-Template refers.

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

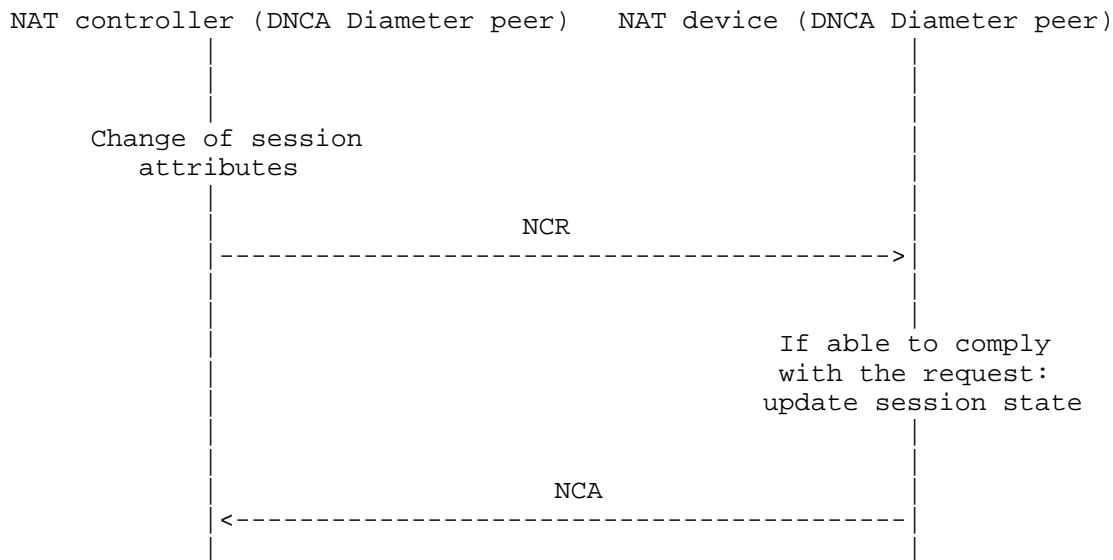


Figure 6: NAT-Control-Request for Session Update

4.3. Session and Binding Query

A session and NAT-binding query MAY be used by the DNCA Diameter peer within the NAT controller either to retrieve information on the current bindings for a particular session at the NAT device or to 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 an 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 the 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 the 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 an internal IP address or one or multiple external IP address/port pairs, it MUST include the internal IP address as part of the Framed-IP-Address AVP 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 known in advance by 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.

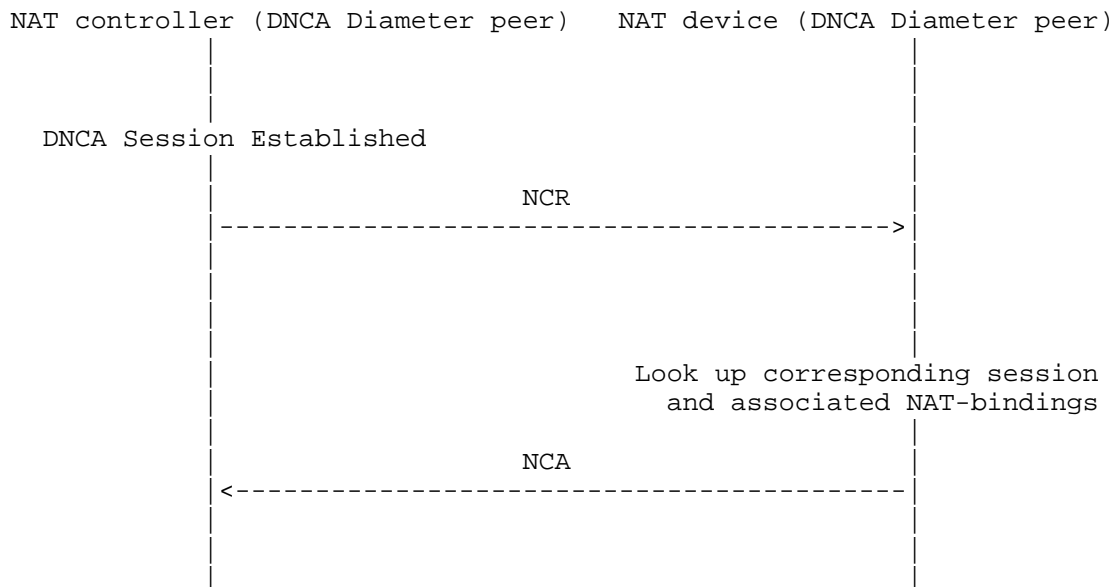


Figure 7: Session Query

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-Termination-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-Termination-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 an STR and fails to find a matching session, the DNCA Diameter peer **MUST** return an STA with the Result-Code set to `DIAMETER_UNKNOWN_SESSION_ID`.

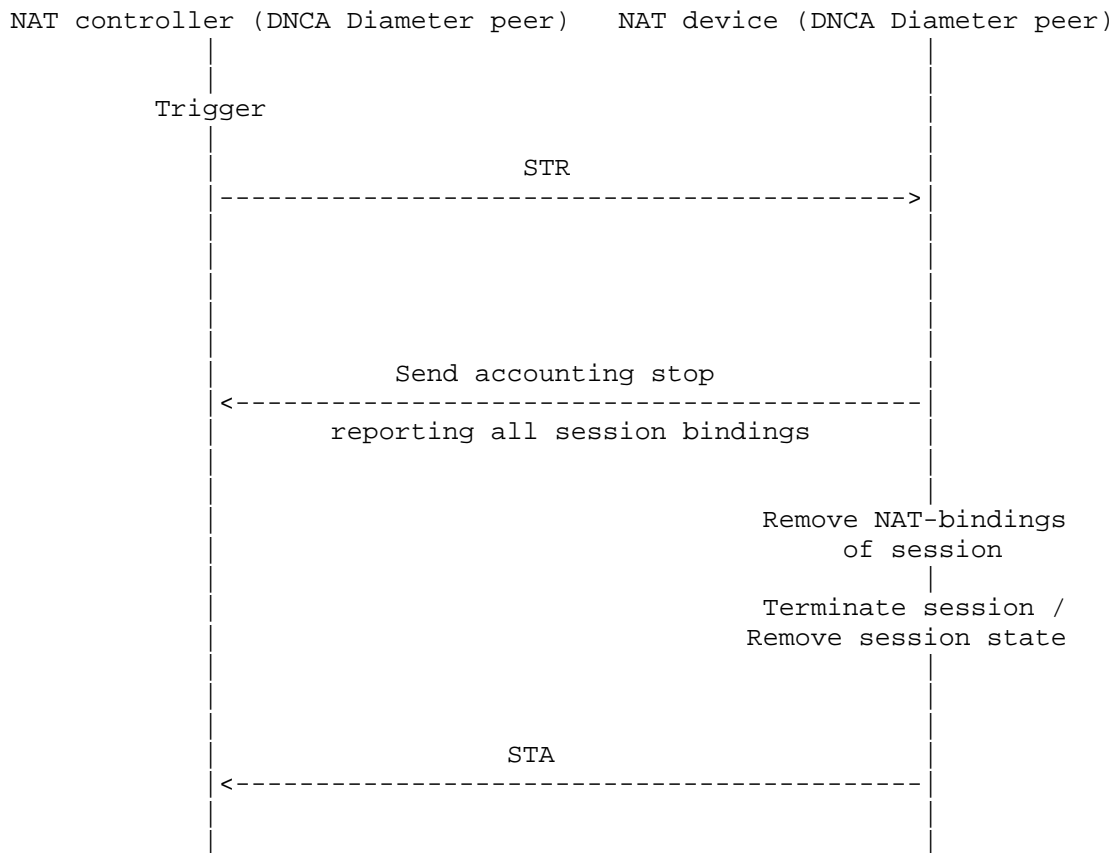


Figure 8: Terminate NAT Control Session

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 a successful session abort using an Abort-Session-Answer (ASA) message with the 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 the 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 the 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 the Result-Code set to `DIAMETER_UNABLE_TO_COMPLY` MUST be returned.

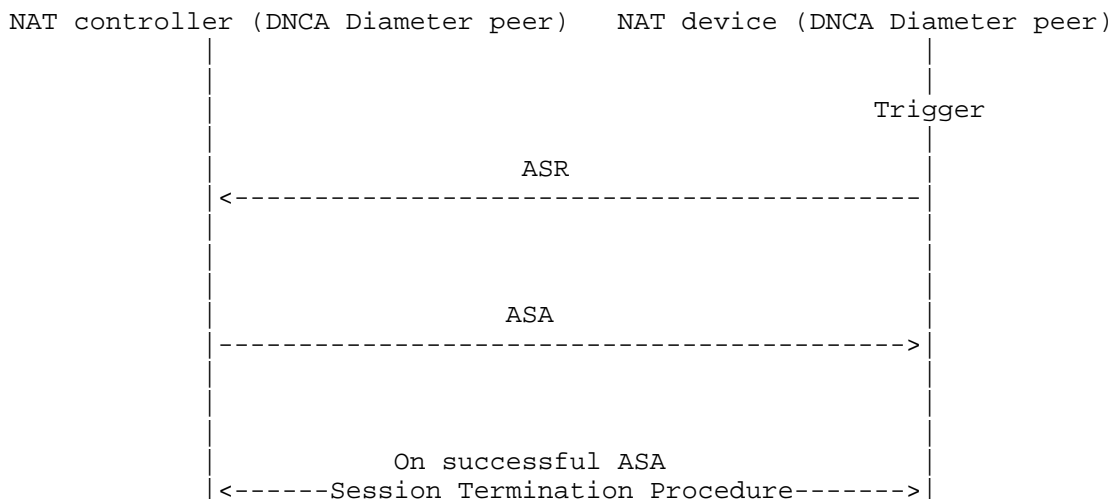


Figure 9: Abort NAT Control Session

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 the 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 a Result-Code that contains a 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-Termination-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 the 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 The NAT device and the DNCA Diameter peer within NAT device lose state. In such a case, the DNCA Diameter peer MAY receive an NCR with the NC-Request-Type AVP set to UPDATE_REQUEST for a non-existent session. The DNCA Diameter peer MUST return an NCA with the Result-Code set to DIAMETER_UNKNOWN_SESSION_ID. When a DNCA application within a NAT controller receives this NCA with the Result-Code set to DIAMETER_UNKNOWN_SESSION_ID, it MAY try to re-establish DNCA session or disconnect corresponding access session.
- o The DNCA Diameter peer within the NAT controller is unreachable, for example, it is detected by Diameter device watchdog messages (as defined in Section 5.5 of [RFC6733]) 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 the 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 used for a NAT device to clean 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 that require periodic refresh, or time out otherwise, operating system watchdogs for applications, etc.

5. Use of the Diameter Base Protocol

The Diameter base protocol [RFC6733] applies with the clarifications listed in the present specification.

5.1. Securing Diameter Messages

For secure transport of Diameter messages, the recommendations in [RFC6733] 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 an NCR command is allowed to do so based on:

- o The identity of the DNCA Diameter peer
- o The type of NCR Command
- o The content of the NCR Command
- o Any combination of the above

5.2. Accounting Functionality

Accounting functionality (the accounting session state machine, related Command Codes and AVPs) is defined in Section 9.

5.3. Use of Sessions

Each DNCA session MUST have a globally unique Session-Id, as defined in [RFC6733], which MUST NOT be changed during the lifetime of the 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 time. A DNCA Diameter peer sends an Abort-Session-Request as defined in [RFC6733] 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 12 in the Auth-Application-Id of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [RFC6733].

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 330 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, and Calling-Station-ID AVPs serve as identifiers for the endpoint.

Message format:

```
< NC-Request > ::= < Diameter Header: 330, 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 330 and the 'R' bit cleared in the Command Flags field, is sent by the DNCA Diameter peer within the NAT device in response to the NAT-Control-Request command.

Message format:

```
<NC-Answer> ::= < Diameter Header: 330, 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 [RFC6733]. 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 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 or 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.

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 = <code>UNKNOWN_SESSION_ID</code>	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 update required	Send NCR update request	Open
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 the Diameter base protocol [RFC6733]; their AVP Code values, types, and possible flag values and whether the AVP MAY be encrypted. [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in [RFC6733], Section 4.

			+-----+		
			AVP Flag rules		
+-----+			+-----+		
Attribute Name	AVP Code	Data Type	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 from the Diameter Base Protocol

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 12. Please refer to [RFC6733] 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 (4014)

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 (5042)

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, which refers to a predefined policy template in the NAT device, is unknown.

BINDING_FAILURE (5043)

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 (5044)

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 that takes precedence over DNCA.

MAXIMUM_BINDINGS_REACHED_FOR_ENDPOINT (5045)

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 (5046)

The DNCA Diameter peer within the NAT device denies a 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 (5047)

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 [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in the [RFC6733], Section 4.

Attribute Name	AVP Code	Value Type	AVP Flag Rules				Encr
			MUST	MAY	SHLD NOT	MUST NOT	
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 [RFC6733] 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" [RFC4675]; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted. [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in [RFC6733], Section 4.

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

Table 3: Reused attributes from [RFC4675]. Please refer to [RFC6733] 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. [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in [RFC6733], Section 4.

			AVP Flag Rules		
Attribute Name	AVP Code	Data Type	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 [RFC6733] 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. [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in [RFC6733], 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 the Diameter e4 application. Please refer to [RFC6733] 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. [RFC6733] specifies the AVP Flag rules for AVPs in Section 4.5. The Diameter AVP rules are defined in [RFC6733], Section 4. The AVPs defined here MUST NOT have the 'V' bit in the AVP Flags field set.

					+-----+		
					AVP Flag Rules		
+-----+					+-----+		
Attribute Name	AVP Code	Sect.	Data Type		MUST	MAY	Encr
+-----+					+-----+		
NC-Request-Type	595	8.7.1	Enumerated		M	P	Y
NAT-Control-Install	596	8.7.2	Grouped		M	P	Y
NAT-Control-Remove	597	8.7.3	Grouped		M	P	Y
NAT-Control-Definition	598	8.7.4	Grouped		M	P	Y
NAT-Internal-Address	599	8.7.5	Grouped		M	P	Y
NAT-External-Address	600	8.7.6	Grouped		M	P	Y
Max-NAT-Bindings	601	8.7.7	Unsigned32		M	P	Y
NAT-Control- Binding-Template	602	8.7.8	OctetString		M	P	Y
Duplicate- Session-Id	603	8.7.9	UTF8String		M	P	Y
NAT-External-Port- Style	604	8.7.10	Enumerated		M	P	Y
NAT-Control-Record	605	9.2.1	Grouped		M	P	Y
NAT-Control- Binding-Status	606	9.2.2	Enumerated		M	P	Y
Current-NAT-Bindings	607	9.2.3	Unsigned32		M	P	Y
+-----+					+-----+		

Table 6: New Diameter AVPs. Please refer to [RFC6733] 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 595) 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-Install AVP (AVP code 596) 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, 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: 596 >
    * [ 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 597) 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 or NAT-Control-Binding-Template AVP) SHOULD be present in the NAT-Control-Remove AVP.

AVP format:

```
NAT-Control-Remove ::= < AVP Header: 597 >
                        * [ NAT-Control-Definition ]
                        [ NAT-Control-Binding-Template ]
                        * [ AVP ]
```

8.7.4. NAT-Control-Definition AVP

The NAT-Control-Definition AVP (AVP code 598) 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 predefined 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 addresses 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: 598 >
                        { 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 599) 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: 599 >
                        [ Framed-IP-Address ]
                        [ Framed-IPv6-Prefix ]
                        [ Port ]
                        * [ AVP ]
```

8.7.6. NAT-External-Address AVP

The NAT-External-Address AVP (AVP code 600) 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 an external port as per the NAT-External-Port-Style AVP.

AVP format:

```
NAT-External-Address ::= < AVP Header: 600 >
                        [ Framed-IP-Address ]
                        [ Port ]
                        * [ AVP ]
```

8.7.7. Max-NAT-Bindings

The Max-NAT-Bindings AVP (AVP code 601) 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 602) 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 may contain NAT-bindings, an IP address pool for allocating the external IP address of a NAT-binding, and a maximum number of allowed NAT-bindings. Such a 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 603) 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 604) 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 oddity 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 [RFC6733] to report the bindings per endpoint. This reporting is achieved by sending Diameter Accounting-Request (ACR) commands [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 an 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 an NCR with NC-Request-Type AVP set to UPDATE_REQUEST, 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 an STR message.

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 [RFC6733] for exchanging endpoint NAT-binding details between the DNCA Diameter peers. The DNCA Application ID is used in the accounting commands. The 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 [RFC6733], 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 605) 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: 605 >
                        { NAT-Control-Definition }
                        { NAT-Control-Binding-Status }
                        [ Event-Timestamp ]
```

9.2.2. NAT-Control-Binding-Status

The NAT-Control-Binding-Status AVP (AVP code 606) 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 607) is of type Unsigned32. It indicates the number of NAT-bindings active on the NAT device.

10. AVP Occurrence Tables

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 the 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 the NAT-Control-Install AVP nor the NAT-Control-Remove AVP is 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 Requests

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

Attribute Name	Command Code	
	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 Messages

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

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

11. IANA Considerations

This section contains either the namespaces that have 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 [RFC5226], 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 12, 'Diameter NAT Control Application', to the Application Identifier namespace defined in [RFC6733]. See Section 4 for more information.

11.2. Command Codes

This specification uses the value 330 from the Command code namespace defined in [RFC6733] for the NAT-Control-Request (NCR) and 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 595-607 from the AVP Code namespace defined in [RFC6733]. See Section 8.7 for the assignment of the namespace in this specification.

11.4. Result-Code AVP Values

This specification assigns the values 4014 and 5042-5047 from the Result-Code AVP value namespace defined in [RFC6733]. 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 a 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 DoS attack by setting the maximum number of bindings for a session on the NAT device to zero; provisioning bindings on a NAT device that includes IP addresses already in use in other parts of the network; or requesting session termination of the Diameter session and hampering 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, a NAT-binding Predefined template on the NAT device could be configured differently than expected by the NAT controller. If either of the two DNCA Diameter peers fail to provide the required credentials, the failure should be subject to logging. The corresponding logging infrastructure of the operator SHOULD be

built in a way that it can mitigate potential DoS 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 request 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 DoS.

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 [RFC6733], 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 mechanism 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 happen due to, e.g., 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 misuse or misconfiguration 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 that 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 does the following:

- a. requests a maximum of 100 NAT-bindings for the endpoint.
- b. defines a static binding for a TCP connection that 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.

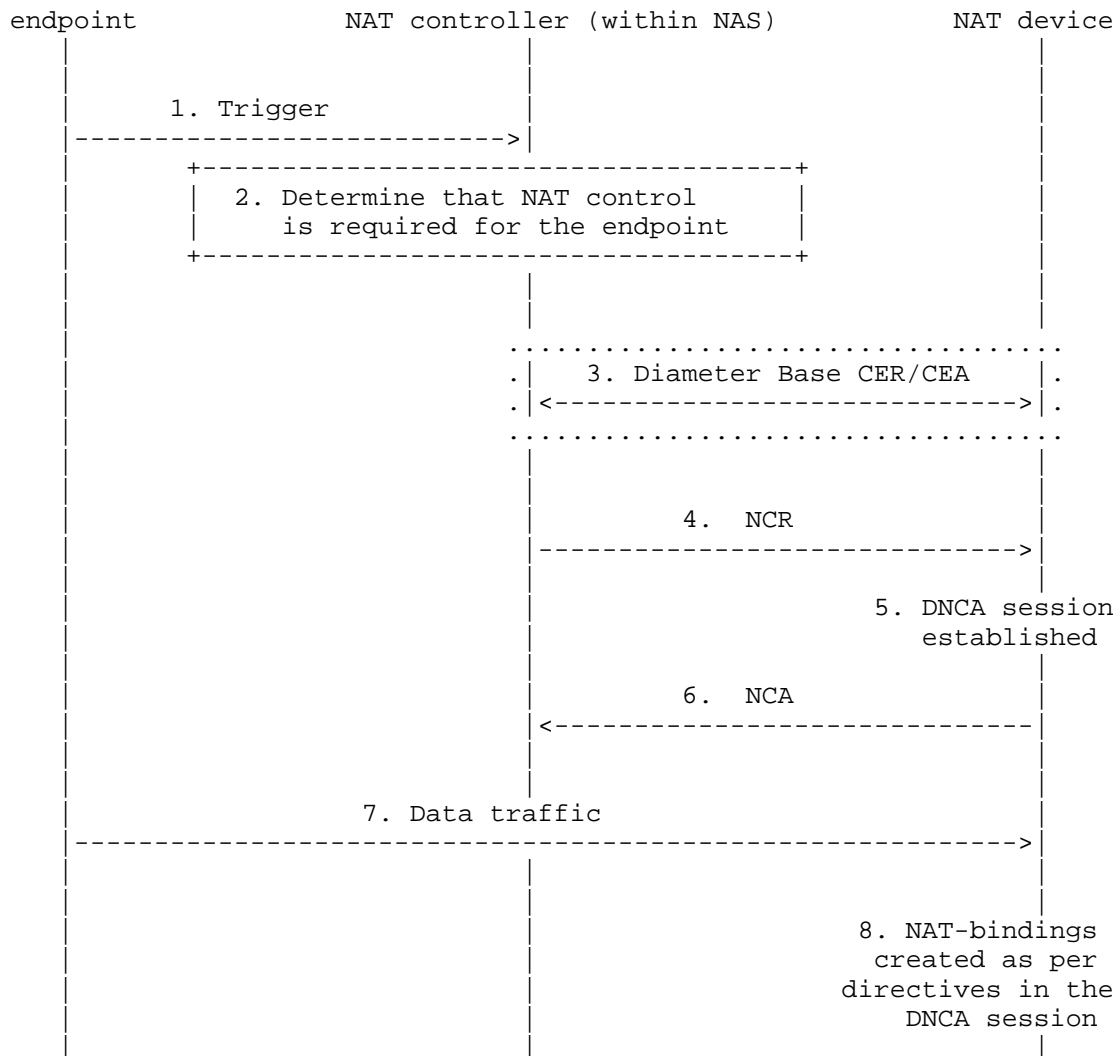


Figure 15: Initial NAT-Control-Request and Session Establishment Example

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: 330, 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: 330, 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: 330, 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: 330, 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: 330, 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 having been torn down.

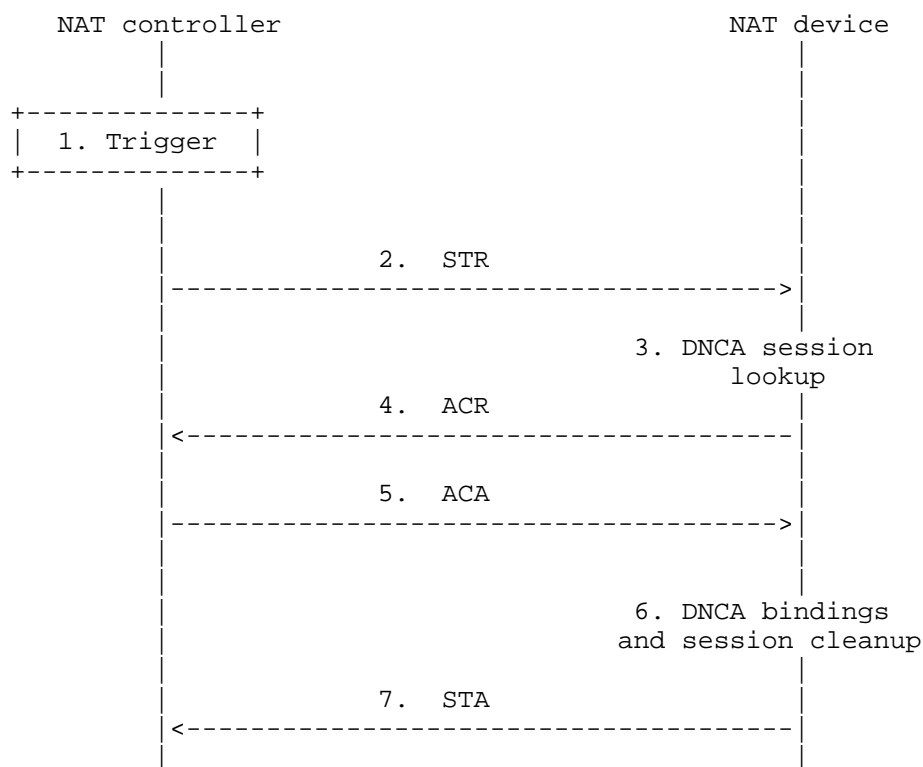


Figure 20: NAT Control Session Termination Example

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 to tear down 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. References

15.1. 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.
- [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.
- [RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.

15.2. Informative References

- [CGN-REQS] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", Work in Progress, September 2012.
- [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

