Internet Engineering Task Force (IETF)
Request for Comments: 7659
Category: Standards Track
ISSN: 2070-1721

S. Perreault
Jive Communications
T. Tsou
Huawei Technologies
S. Sivakumar
Cisco Systems
T. Taylor
PT Taylor Consulting

October 2015

Definitions of Managed Objects for Network Address Translators (NATs)

Abstract

This memo defines a portion of the Management Information Base (MIB) for devices implementing the Network Address Translator (NAT) function. The new MIB module defined in this document, NATV2-MIB, is intended to replace module NAT-MIB (RFC 4008). NATV2-MIB is not backwards compatible with NAT-MIB, for reasons given in the text of this document. A companion document deprecates all objects in NAT-MIB. NATV2-MIB can be used for the monitoring of NAT instances on a device capable of NAT function. Compliance levels are defined for three application scenarios: basic NAT, pooled NAT, and carrier-grade NAT (CGN).

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/rfc7659.

Table of Contents

1. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

2. Introduction

This memo defines a portion of the Management Information Base (MIB) for devices implementing NAT functions. This MIB module, NATV2-MIB, may be used for the monitoring of such devices. NATV2-MIB supersedes NAT-MIB [RFC4008], which did not fit well with existing NAT implementations, and hence was not itself much implemented. [RFC7658] provides a detailed analysis of the deficiencies of NAT-MIB.

Relative to [RFC4008] and based on the analysis just mentioned, the present document introduces the following changes:

- removed all writable configuration except that related to control of the generation of notifications and the setting of quotas on the use of NAT resources;
- minimized the read-only exposure of configuration to what is needed to provide context for the state and statistical information presented by the MIB module;
- removed the association between mapping and interfaces, retaining only the mapping aspect;
- replaced references to NAT types with references to NAT behaviors as specified in [RFC4787];
- replaced a module-specific enumeration of protocols with the standard protocol numbers provided by the IANA Protocol Numbers registry.

This MIB module adds the following features not present in [RFC4008]:

- additional writable protective limits on NAT state data;
- additional objects to report state, statistics, and notifications;
- support for the carrier-grade NAT (CGN) application, including subscriber-awareness, support for an arbitrary number of address realms, and support for multiple NAT instances running on a single device;
- expanded support for address pools;
- revised indexing of port map entries to simplify traceback from externally observable packet parameters to the corresponding internal endpoint.

These features are described in more detail below.

The remainder of this document is organized as follows:

- Section 3 provides a verbal description of the content and organization of the MIB module.
- Section 4 provides the MIB module definition.
- Section 5 discusses operational and management issues relating to the deployment of NATV2-MIB. One of these issues is NAT management when both NAT-MIB [RFC4008] and NATV2-MIB are deployed.
- Sections 6 and 7 provide a security discussion and a request to IANA for allocation of an object identifier for the module in the mib-2 tree, respectively.

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

This document uses the following terminology:

Upper-layer protocol: The protocol following the outer IP header of a packet. This follows the terminology of [RFC2460], but as that document points out, "upper" is not necessarily a correct description of the protocol relationships (e.g., where IP is encapsulated in IP). The abbreviated term "protocol" will often be used where it is unambiguous.

Trigger: With respect to notifications, the logical recognition of the event that the notification is intended to report.

Report: The actual production of a notification message. Reporting can happen later than triggering, or may never happen for a given notification instance, because of the operation of notification rate controls.

Address realm: A network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them. (Definition taken from [RFC2663], Section 2.1.) The abbreviated term "realm" will often be used.

3. Overview

This section provides a prose description of the contents and organization of the NATV2-MIB module.

3.1. Content Provided by the NATV2-MIB Module

The content provided by the NATV2-MIB module can be classed under four headings: configuration data, notifications, state information, and statistics.

3.1.1. Configuration Data

As mentioned above, the intent in designing the NATV2-MIB module was to minimize the amount of configuration data presented to that needed to give a context for interpreting the other types of information provided. Detailed descriptions of the configuration data are included with the descriptions of the individual tables. In general, that data is limited to what is needed for indexing and cross-referencing between tables. The two exceptions are the objects describing NAT instance behavior in the NAT instance table and the detailed enumeration of resources allocated to each address pool in the pool table and its extension.

The NATV2-MIB module provides three sets of read-write objects, specifically related to other aspects of the module content. The first set controls the rate at which specific notifications are generated. The second set provides thresholds used to trigger the notifications. These objects are listed in Section 3.1.2.

A third set of read-write objects sets limits on resource consumption per NAT instance and per subscriber. When these limits are reached, packets requiring further consumption of the given resource are

dropped rather than translated. Statistics described in Section 3.1.4 record the numbers of packets dropped. Limits are provided for:

- total number of address map entries over the NAT instance. Limit is set by object natv2InstanceLimitAddressMapEntries in table natv2InstanceTable. Dropped packets are counted in natv2InstanceAddressMapEntryLimitDrops in that table.

- total number of port map entries over the NAT instance. Limit is set by object natv2InstanceLimitPortMapEntries in table natv2InstanceTable. Dropped packets are counted in natv2InstancePortMapEntryLimitDrops in that table.

- total number of held fragments (applicable only when the NAT instance can receive fragments out of order; see [RFC4787], Section 11). Limit is set by object natv2InstanceLimitPendingFragments in table natv2InstanceTable. Dropped packets are counted by natv2InstanceFragmentDrops in the same table.

- total number of active subscribers (i.e., subscribers having at least one mapping table entry) over the NAT instance. Limit is set by object natv2InstanceLimitSubscriberActives in table natv2InstanceTable. Dropped packets are counted by natv2InstanceSubscriberActiveLimitDrops in the same table.

- number of port map entries for an individual subscriber. Limit is set by object natv2SubscriberLimitPortMapEntries in table natv2SubscriberTable. Dropped packets are counted by natv2SubscriberPortMapFailureDrops in the same table. Note that, unlike in the instance table, the per-subscriber count is lumped in with the count of packets dropped because of failures to allocate a port map entry for other reasons to save on storage.

3.1.2. Notifications

NATV2-MIB provides five notifications, intended to provide warning of the need to provision or reallocate NAT resources. As indicated in the previous section, each notification is associated with two read-write objects: a control on the rate at which that notification is generated and a threshold value used to trigger the notification in the first place. The default setting within the MIB module specification is that all notifications are disabled. The setting of threshold values is discussed in Section 5.

The five notifications are as follows:

- Two notifications relate to the management of address pools. One indicates that usage equals or exceeds an upper threshold and is therefore a warning that the pool may be over-utilized unless more addresses are assigned to it. The other notification indicates that usage equals or has fallen below a lower threshold, suggesting that some addresses allocated to that pool could be reallocated to other pools. Address pool usage is calculated as the percentage of the total number of ports allocated to the address pool that are already in use, for the most-mapped protocol at the time the notification is generated. The notifications identify that protocol and report the number of port map entries for that protocol in the given address pool at the moment the notification was triggered.

- Two notifications relate to the number of address and port map entries, respectively, in total over the whole NAT instance. In both cases, the threshold that triggers the notification is an upper threshold. The notifications return the number of mapping entries of the given type, plus a cumulative counter of the number of entries created in that mapping table at the moment the notification was triggered. The intent is that the notifications provide a warning that the total number of address or port map entries is approaching the configured limit.

- The final notification is generated on a per-subscriber basis when the number of port map entries for that subscriber crosses the associated threshold. The objects returned by this notification are similar to those returned for the instance-level mapping notifications. This notification is a warning that the number of port map entries for the subscriber is approaching the configured limit for that subscriber.

Here is a detailed specification of the notifications. A given notification can be disabled by setting the threshold to -1 (default).

Notification: natv2NotificationPoolUsageLow. Indicates that address pool usage for the most-mapped protocol equals or is less than the threshold value.

Compared value: natv2PoolNotifiedPortMapEntries as a percentage of total available ports in the pool.

Threshold: natv2PoolThresholdUsageLow in natv2PoolTable.

Objects returned: natv2PoolNotifiedPortMapEntries and natv2PoolNotifiedPortMapProtocol in natv2PoolTable.

Rate control: natv2PoolNotificationInterval in natv2PoolTable.

Notification: natv2NotificationPoolUsageHigh. Indicates that address pool usage for the most-mapped protocol has risen to the threshold value or more.

Compared value: natv2PoolNotifiedPortMapEntries as a percentage of total available ports in the pool.

Threshold: natv2PoolThresholdUsageHigh in natv2PoolTable.

Objects returned: natv2PoolNotifiedPortMapEntries and natv2PoolNotifiedPortMapProtocol in natv2PoolTable.

Rate control: natv2PoolNotificationInterval in natv2PoolTable.

Notification: natv2NotificationInstanceAddressMapEntriesHigh. Indicates that the total number of entries in the address map table over the whole NAT instance equals or exceeds the threshold value.

Compared value: natv2InstanceAddressMapEntries in natv2InstanceTable.

Threshold: natv2InstanceThresholdAddressMapEntriesHigh in natv2InstanceTable.

Objects returned: natv2InstanceAddressMapEntries and natv2InstanceAddressMapCreations in natv2InstanceTable.

Rate control: natv2InstanceNotificationInterval in natv2InstanceTable.

Notification: natv2NotificationInstancePortMapEntriesHigh. Indicates that the total number of entries in the port map table over the whole NAT instance equals or exceeds the threshold value.

Compared value: natv2InstancePortMapEntries in natv2InstanceTable.

Threshold: natv2InstanceThresholdPortMapEntriesHigh in natv2InstanceTable.

Objects returned: natv2InstancePortMapEntries and natv2InstancePortMapCreations in natv2InstanceTable.

Rate control: natv2InstanceNotificationInterval in natv2InstanceTable.

Notification: natv2NotificationSubscriberPortMapEntriesHigh. Indicates that the total number of entries in the port map table for the given subscriber equals or exceeds the threshold value configured for that subscriber.

Compared value: natv2SubscriberPortMapEntries in natv2SubscriberTable.

Threshold: natv2SubscriberThresholdPortMapEntriesHigh in natv2SubscriberTable.

Objects returned: natv2SubscriberPortMapEntries and natv2SubscriberPortMapCreations in natv2SubscriberTable.

Rate control: natv2SubscriberNotificationInterval in natv2SubscriberTable.

3.1.3. State Information

State information provides a snapshot of the content and extent of the NAT mapping tables at a given moment of time. The address and port mapping tables are described in detail below. In addition to these tables, two state variables are provided: current number of entries in the address mapping table, and current number of entries in the port mapping table. With one exception, these are provided at four levels of granularity: per NAT instance, per protocol, per address pool, and per subscriber. Address map entries are not tracked per protocol, since address mapping is protocol independent.

3.1.4. Statistics

NATV2-MIB provides a number of counters, intended to help with both the provisioning of the NAT and the debugging of problems. As with the state data, these counters are provided at the four levels of NAT instance, protocol, address pool, and subscriber when they make sense. Each counter is cumulative, beginning from a "last discontinuity time" recorded by an object that is usually in the table containing the counter.

The basic set of counters, as reflected in the NAT instance table, is as follows:

Translations: number of packets processed and translated (in this case, in total for the NAT instance).

Address map entry creations: cumulative number of address map entries created, including static mappings.

Port map entry creations: cumulative number of port map entries created, including static mappings.

Address map limit drops: cumulative number of packets dropped rather than translated because the packet would have triggered the creation of a new address mapping, but the configured limit on number of address map entries has already been reached.

Port map limit drops: cumulative number of packets dropped rather than translated because the packet would have triggered the creation of a new port mapping, but the configured limit on number of port map entries has already been reached.

Active subscriber limit drops: cumulative number of packets dropped rather than translated because the packet would have triggered the creation of a new address and/or port mapping for a subscriber with no existing entries in either table, but the configured limit on number of active subscribers has already been reached.

Address mapping failure drops: cumulative number of packets dropped because the packet would have triggered the creation of a new address mapping, but no address could be allocated in the external realm concerned because all addresses from the selected address pool (or the whole realm, if no address pool has been configured for that realm) have already been fully allocated.

Port mapping failure drops: cumulative number of packets dropped because the packet would have triggered the creation of a new port mapping, but no port could be allocated for the protocol concerned. The precise conditions under which these packet drops occur depend on the pooling behavior [RFC4787] configured or implemented in the NAT instance. See the DESCRIPTION clause for the natv2InstancePortMapFailureDrops object for a detailed description of the different cases. These cases were defined with care to ensure that address mapping failure could be distinguished from port mapping failure.

Fragment drops: cumulative number of packets dropped because the packet contains a fragment, and the fragment behavior [RFC4787] configured or implemented in the NAT instance indicates that the packet should be dropped. The main case is a NAT instance that meets REQ-14 of [RFC4787], hence it can receive and process out-of-order fragments. In that case, dropping occurs only when the

configured limit on pending fragments provided by NATV2-MIB has already been reached. The other cases are detailed in the DESCRIPTION clause of the natv2InstanceFragmentBehavior object.

Other resource drops: cumulative number of packets dropped because of unavailability of some other resource. The most likely case would be packets where the upper-layer protocol is not one supported by the NAT instance.

Table 1 indicates the granularities at which these statistics are reported.

Statistic	NAT Instance	Protocol	Pool	Subscriber
Translations	Yes	Yes	No	Yes
Address map entry creations	Yes	No	Yes	Yes
Port map entry creations	Yes	Yes	Yes	Yes
Address map limit drops	Yes	No	No	No
Port map limit drops	Yes	No	No	Yes
Active subscriber limit drops	Yes	No	No	No
Address mapping failure drops	Yes	No	Yes	Yes
Port mapping failure drops	Yes	Yes	Yes	Yes
Fragment drops	Yes	No	No	No
Other resource drops	Yes	No	No	No

Table 1: Statistics Provided By Level of Granularity

3.2. Outline of MIB Module Organization

Figure 1 shows how object identifiers are organized in the NATV2-MIB module. Under the general natv2MIB object identifier in the mib-2 tree, the objects are classed into four groups:

natv2MIBNotifications(0): identifies the five notifications described in Section 3.1.2.

natv2MIBDeviceObjects(1): identifies objects relating to the whole device, specifically, the subscriber table.

natv2MIBInstanceObjects(2): identifies objects relating to individual NAT instances. These include the NAT instance table, the protocol table, the address pool table and its address range expansion, the address map table, and the port map table.

natv2MIBConformance(3): identifies the group and compliance clauses, specified for the three application scenarios described in Section 3.4.

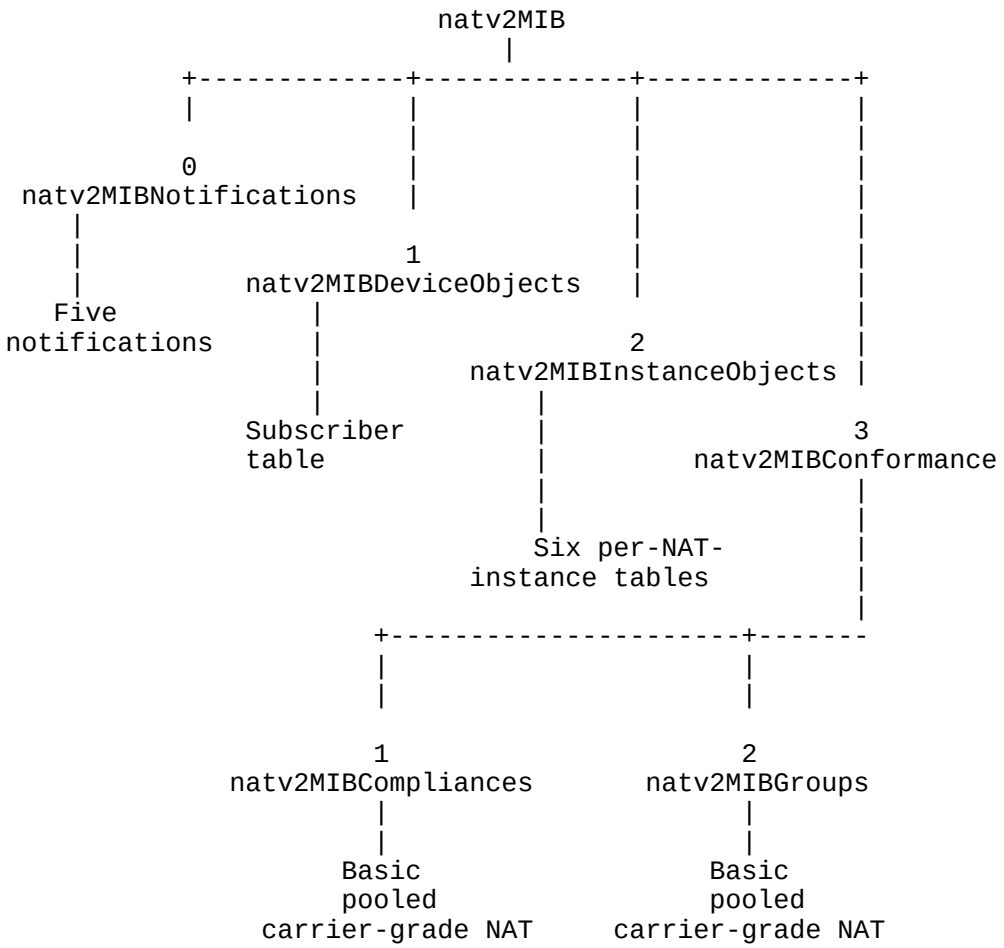

Figure 1: Organization of Object Identifiers for NATV2-MIB

3.3. Detailed MIB Module Walk-Through

This section reviews the contents of the NATV2-MIB module. The table descriptions include references to subsections of Section 3.1 where desirable to avoid repetition of that information.

3.3.1. Textual Conventions

The module defines four key textual conventions: ProtocolNumber, Natv2SubscriberIndex, Natv2InstanceIndex, and Natv2PoolIndex. ProtocolNumber is based on the IANA registry of protocol numbers and hence is potentially reusable by other MIB modules.

Objects of type Natv2SubscriberIndex identify individual subscribers served by the NAT device. The values of these identifiers are administered and, in intent, are permanently associated with their respective subscribers. Reuse of a value after a subscriber has been deleted is discouraged. The scope of the subscriber index was defined to be at the device rather than the NAT instance level to make it easier to shift subscribers between instances (e.g., for load balancing).

Objects of type Natv2InstanceIndex identify specific NAT instances on the device. Again, these are administered values intended to be permanently associated with the NAT instances to which they have been assigned.

Objects of type Natv2PoolIndex identify individual address pools in a given NAT instance. As with the subscriber and instance index objects, the pool identifiers are administered and intended to be permanently associated with their respective pools.

3.3.2. Notifications

Notifications were described in Section 3.1.2.

3.3.3. The Subscriber Table: natv2SubscriberTable

Table natv2SubscriberTable is indexed by the subscriber index. One conceptual row contains information relating to a specific subscriber: the subscriber's internal address or prefix for correlation with other management information; state and statistical information as described in Sections 3.1.3 and 3.1.4; the per-subscriber control objects described in Section 3.1.1; and natv2SubscriberDiscontinuityTime, which provides a timestamp of the latest time following, which the statistics have accumulated without discontinuity.

Turning back to the address information for a moment: this information includes the identity of the address realm in which the address is routable. That enables support of an arbitrary number of address realms on the same NAT instance. Address realm identifiers are administered values in the form of a limited-length SnmpAdminString. In the absence of configuration to the contrary, the default realm for all internal addresses as recorded in mapping entries is "internal".

> The term "address realm" is defined in [RFC2663], Section 2.1 and reused in subsequent NAT-related documents.

In the special case of Dual-Stack Lite (DS-Lite) [RFC6333], for unique matching of the subscriber data to other information in the MIB module, it is necessary that the address information should relate to the outer IPv6 header of packets going to or from the host, with the address realm being the one in which that IPv6 address is routable. The presentation of address information for other types of tunneled access to the NAT is out of scope.

3.3.4. The Instance Table: natv2InstanceTable

Table natv2InstanceTable is indexed by an object of type Natv2InstanceIndex. A conceptual row of this table provides information relating to a particular NAT instance configured on the device.

Configuration information provided by this table includes an instance name of type DisplayString that may have been configured for this instance and a set of objects indicating, respectively, the port mapping, filtering, pooling, and fragment behaviors configured or implemented in the instance. These behaviors are all defined in [RFC4787]. Their values affect the interpretation of some of the statistics provided in the instance table.

Read-write objects listed in Section 3.1.2 set the notification rate for instance-level notifications and set the thresholds that trigger them. Additional read-write objects described in Section 3.1.1 set limits on the number of address and port mapping entries, number of pending fragments, and number of active subscribers for the instance.

The state and statistical information provided by this table consists of the per-instance items described in Sections 3.1.3 and 3.1.4, respectively. natv2InstanceDiscontinuityTime is a timestamp giving the time beyond which all of the statistical counters in natv2InstanceTable are guaranteed to have accumulated continuously.

3.3.5. The Protocol Table: natv2ProtocolTable

The protocol table is indexed by the NAT instance number and an object of type ProtocolNumber as described in Section 3.3.1 (i.e., an IANA-registered protocol number). The set of protocols supported by the NAT instance is implementation dependent, but they MUST include ICMP(1), TCP(6), UDP(17), and ICMPv6(58). Depending on the application, it SHOULD include IPv4 encapsulation(4), IPv6 encapsulation(41), IPsec AH(51), and SCTP(132). Support of PIM(103) is highly desirable.

This table includes no configuration information. The state and statistical information provided by this table consists of the per-protocol items described in Sections 3.1.3 and 3.1.4, respectively. natv2InstanceDiscontinuityTime in natv2InstanceTable is reused as the timestamp giving the time beyond which all of the statistical counters in natv2ProtocolTable are guaranteed to have accumulated continuously. The reasoning is that any event affecting the continuity of per-protocol statistics will affect the continuity of NAT instance statistics, and vice versa.

3.3.6. The Address Pool Table: natv2PoolTable

The address pool table is indexed by the NAT instance identifier for the instance on which it is provisioned, plus a pool index of type Natv2PoolIndex. Configuration information provided includes the address realm for which the pool provides addresses, the type of address (IPv4 or IPv6) supported by the realm, plus the port range it makes available for allocation. The same set of port numbers (or, in the ICMP case, identifier values) is made available for every protocol supported by the NAT instance. The port range is specified in terms of minimum and maximum port number.

The state and statistical information provided by this table consists of the per-pool items described in Sections 3.1.3 and 3.1.4 respectively, plus two additional state objects described below. natv2PoolTable provides the pool-specific object natv2PoolDiscontinuityTime to indicate the time since the statistical counters have accumulated continuously.

Read-write objects to set high and low thresholds for pool usage notifications and for governing the notification rate were identified in Section 3.1.2.

> Implementation note: the thresholds are defined in terms of percentage of available port utilization. The number of available ports in a pool is equal to (max port - min port + 1) (from the natv2PoolTable configuration information) multiplied by the number of addresses provisioned in the pool (sum of number of addresses provided by each natv2PoolRangeTable conceptual row relating to that pool). At configuration time, the thresholds can be recalculated in terms of total number of port map entries corresponding to the configured percentage, so that runtime comparisons to the current number of port map entries require no further arithmetic operations.

natv2PoolTable also provides two state objects that are returned with the notifications. natv2PoolNotifiedPortMapProtocol identifies the most-mapped protocol at the time the notification was triggered.

natv2PoolNotifiedPortMapEntries provides the total number of port map entries for that protocol using addresses owned by this pool at that same time.

3.3.7. The Address Pool Address Range Table: natv2PoolRangeTable

natv2PoolRangeTable provides configuration information only. It is an expansion of natv2PoolTable giving the address ranges with which a given address pool has been configured. As such, it is indexed by the combination of NAT instance index, address pool index, and a conceptual row index, where each conceptual row conveys a different address range. The address range is specified in terms of lowest address, highest address rather than the usual prefix notation to provide maximum flexibility.

3.3.8. The Address Map Table: natv2AddressMapTable

The address map table provides a table of mappings from internal to external address at a given moment. It is indexed by the combination of NAT instance index, internal realm, internal address type (IPv4 or IPv6) in that realm, the internal address of the local host for which the map entry was created, and a conceptual row index to traverse all of the entries relating to the same internal address.

In the special case of DS-Lite [RFC6333], the internal address and realm used in the index are those of the IPv6 outer header. The IPv4 source address for the inner header, for which [RFC6333] has reserved addresses in the 192.0.0.0/29 range, is captured in two additional objects in the corresponding conceptual row: natv2AddressMapInternalMappedAddressType and natv2AddressMapInternalMappedAddress. In cases other than DS-Lite access, these objects have no meaning. (Other tunneled access is out of scope.)

The additional information provided by natv2AddressMapTable consists of the external realm, address type in that realm, and mapped external address. Depending on implementation support, the table also provides the index of the address pool from which the external address was drawn and the index of the subscriber to which the map entry belongs.

3.3.9. The Port Map Table: natv2PortMapTable

The port map table provides a table of mappings by protocol from external port, address, and realm to internal port, address, and realm. As such, it is indexed by the combination of NAT instance index, protocol number, external realm identifier, address type in that realm, external address, and external port. The mapping from

external realm, address, and port to internal realm, address, and port is unique, so no conceptual row index is needed. The indexing is designed to make it easy to trace individual sessions back to the host, based on the contents of packets observed in the external realm.

Beyond the indexing, the information provided by the port map table consists of the internal realm, address type, address, and port number, and, depending on implementation support, the index of the subscriber to which the map entry belongs.

As with the address map table, special provision is made for the case of DS-Lite [RFC6333]. The realm and outgoing source address are those for the outer header, and the address type is IPv6. Additional objects natv2PortMapInternalMappedAddressType and natv2PortMapInternalMappedAddress capture the outgoing source address in the inner header, which will be in the well-known 192.0.0.0/29 range.

3.4. Conformance: Three Application Scenarios

The conformance statements in NATV2-MIB provide for three application scenarios: basic NAT, NAT supporting address pools, and CGN.

A basic NAT MAY limit the number of NAT instances it supports to one, but it MUST support indexing by NAT instance. Similarly, a basic NAT MAY limit the number of realms it supports to two. By definition, a basic NAT is not required to support the subscriber table, the address pool table, or the address pool address range table. Some individual objects in other tables are also not relevant to basic NAT.

A NAT supporting address pools adds the address pool table and the address pool address range table to what it implements. Some individual objects in other tables also need to be implemented. A NAT supporting address pools MUST support more than two realms.

Finally, a CGN MUST support the full contents of the MIB module. That includes the subscriber table, but it also includes the special provision for DS-Lite access in the address and port map tables.

4. Definitions

This MIB module IMPORTs objects from [RFC2578], [RFC2579], [RFC2580], [RFC3411], and [RFC4001].

```
NATV2-MIB DEFINITIONS ::= BEGIN

IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
     Integer32,
     Unsigned32,
     Counter64,
     mib-2,
     NOTIFICATION-TYPE
             FROM SNMPv2-SMI          -- RFC 2578
     TEXTUAL-CONVENTION,
     DisplayString,
     TimeStamp
             FROM SNMPv2-TC           -- RFC 2579
     MODULE-COMPLIANCE,
     NOTIFICATION-GROUP,
     OBJECT-GROUP
             FROM SNMPv2-CONF         -- RFC 2580
     SnmpAdminString
             FROM SNMP-FRAMEWORK-MIB  -- RFC 3411
     InetAddressType,
     InetAddress,
     InetAddressPrefixLength,
     InetPortNumber
             FROM INET-ADDRESS-MIB;   -- RFC 4001

natv2MIB MODULE-IDENTITY
     LAST-UPDATED "201510020000Z" -- 2 October 2015

     ORGANIZATION
             "IETF Behavior Engineering for Hindrance
               Avoidance (BEHAVE) Working Group"
     CONTACT-INFO
             "Working Group Email: behave@ietf.org

              Simon Perreault
              Jive Communications
              Quebec, QC
              Canada

              Email: sperreault@jive.com
```

```
              Tina Tsou
              Huawei Technologies
              Bantian, Longgang
              Shenzhen 518129
              China

              Email: tina.tsou.zouting@huawei.com

              Senthil Sivakumar
              Cisco Systems
              7100-8 Kit Creek Road
              Research Triangle Park, North Carolina  27709
              United States

              Phone: +1 919 392 5158
              Email: ssenthil@cisco.com

              Tom Taylor
              PT Taylor Consulting
              Ottawa
              Canada

              Email: tom.taylor.stds@gmail.com"

     DESCRIPTION
             "This MIB module defines the generic managed objects
              for NAT.

              Copyright (c) 2015 IETF Trust and the persons
              identified as authors of the code.  All rights reserved.

              Redistribution and use in source and binary forms, with
              or without modification, is permitted pursuant to, and
              subject to the license terms contained in, the Simplified
              BSD License set forth in Section 4.c of the IETF Trust's
              Legal Provisions Relating to IETF Documents
              (http://trustee.ietf.org/license-info).

              This version of this MIB module is part of RFC 7659;
              see the RFC itself for full legal notices."
     REVISION     "201510020000Z" -- 2 October 2015
     DESCRIPTION
             "Complete rewrite, published as RFC 7659.
              Replaces former version published as RFC 4008."
     ::= { mib-2 234 }

-- Textual conventions
```

```
ProtocolNumber ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "A protocol number, from the IANA Protocol Numbers
         registry."
    REFERENCE
        "IANA Protocol Numbers,
         <http://www.iana.org/assignments/protocol-numbers>"
    SYNTAX Unsigned32 (0..255)

Natv2SubscriberIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "A unique value, greater than zero, for each subscriber
         in the managed system.  The value for each
         subscriber MUST remain constant at least from one
         update of the entity's natv2SubscriberDiscontinuityTime
         object until the next update of that object.  If a
         subscriber is deleted, its assigned index value MUST NOT
         be assigned to another subscriber at least until
         reinitialization of the entity's management system."
    SYNTAX Unsigned32 (1..4294967295)

Natv2SubscriberIndexOrZero ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "This textual convention is an extension of the
         Natv2SubscriberIndex convention.  The latter defines a
         greater than zero value used to identify a subscriber in
         the managed system.  This extension permits the additional
         value of zero, which serves as a placeholder when no
         subscriber is associated with the object."
    SYNTAX Unsigned32 (0|1..4294967295)

Natv2InstanceIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "A unique value, greater than zero, for each NAT instance
         in the managed system.  It is RECOMMENDED that values are
         assigned contiguously starting from 1.  The value for each
         NAT instance MUST remain constant at least from one
         update of the entity's natv2InstanceDiscontinuityTime
         object until the next update of that object.  If a NAT
         instance is deleted, its assigned index value MUST NOT
```

```
          be assigned to another NAT instance at least until
          reinitialization of the entity's management system."
    SYNTAX Unsigned32 (1..4294967295)

Natv2PoolIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
       "A unique value over the containing NAT instance, greater than
        zero, for each address pool supported by that NAT instance.
        It is RECOMMENDED that values are assigned contiguously
        starting from 1.  The value for each address pool MUST remain
        constant at least from one update of the entity's
        natv2PoolDiscontinuityTime object until the next update of
        that object.  If an address pool is deleted, its assigned
        index value MUST NOT be assigned to another address pool for
        the same NAT instance at least until reinitialization of the
        entity's management system."
    SYNTAX Unsigned32 (1..4294967295)

Natv2PoolIndexOrZero ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "This textual convention is an extension of the
         Natv2PoolIndex convention.  The latter defines a greater
         than zero value used to identify address pools in the
         managed system.  This extension permits the additional
         value of zero, which serves as a placeholder when the
         implementation does not support address pools or no address
         pool is configured in a given external realm."
    SYNTAX Unsigned32 (0|1..4294967295)

-- Notifications

natv2MIBNotifications OBJECT IDENTIFIER ::= { natv2MIB 0 }

natv2NotificationPoolUsageLow NOTIFICATION-TYPE
    OBJECTS { natv2PoolNotifiedPortMapEntries,
              natv2PoolNotifiedPortMapProtocol  }
    STATUS current
    DESCRIPTION
        "This notification is triggered when an address pool's usage
         becomes less than or equal to the value of the
         natv2PoolThresholdUsageLow object for that pool, unless the
         notification has been disabled by setting the value of the
         threshold to -1.  It is reported subject to the rate
         limitation specified by natv2PortMapNotificationInterval.
```

```
         Address pool usage is calculated as the percentage of the
         total number of ports allocated to the address pool that are
         already in use, for the most-mapped protocol at the time
         the notification is triggered.  The two returned objects are
         members of natv2PoolTable indexed by the NAT instance and
         pool indices for which the event is being reported.  They
         give the number of port map entries using external addresses
         configured on the pool for the most-mapped protocol and
         identify that protocol at the time the notification was
         triggered."
    REFERENCE
        "RFC 7659, Sections 3.1.2 and 3.3.6."
    ::= { natv2MIBNotifications 1 }

natv2NotificationPoolUsageHigh NOTIFICATION-TYPE
    OBJECTS { natv2PoolNotifiedPortMapEntries,
              natv2PoolNotifiedPortMapProtocol  }
    STATUS current
    DESCRIPTION
        "This notification is triggered when an address pool's usage
         becomes greater than or equal to the value of the
         natv2PoolThresholdUsageHigh object for that pool, unless
         the notification has been disabled by setting the value of
         the threshold to -1.  It is reported subject to the rate
         limitation specified by natv2PortMapNotificationInterval.

         Address pool usage is calculated as the percentage of the
         total number of ports allocated to the address pool that are
         already in use, for the most-mapped protocol at the time the
         notification is triggered.  The two returned objects are
         members of natv2PoolTable indexed by the NAT instance and
         pool indices for which the event is being reported.  They
         give the number of port map entries using external addresses
         configured on the pool for the most-mapped protocol and
         identify that protocol at the time the notification was
         triggered."
    REFERENCE
        "RFC 7659, Sections 3.1.2 and 3.3.6."
    ::= { natv2MIBNotifications 2 }

natv2NotificationInstanceAddressMapEntriesHigh NOTIFICATION-TYPE
    OBJECTS { natv2InstanceAddressMapEntries,
              natv2InstanceAddressMapCreations }
    STATUS current
    DESCRIPTION
        "This notification is triggered when the value of
         natv2InstanceAddressMapEntries equals or exceeds the value
         of the natv2InstanceThresholdAddressMapEntriesHigh object
```

```
         for the NAT instance, unless disabled by setting that
         threshold to -1.  Reporting is subject to the rate limitation
         given by natv2InstanceNotificationInterval.

         natv2InstanceAddressMapEntries and
         natv2InstanceAddressMapCreations are members of table
         natv2InstanceTable indexed by the identifier of the NAT
         instance for which the event is being reported.  The values
         reported are those observed at the moment the notification
         was triggered."
    REFERENCE
        "RFC 7659, Section 3.1.2."
    ::= { natv2MIBNotifications 3 }

natv2NotificationInstancePortMapEntriesHigh NOTIFICATION-TYPE
    OBJECTS { natv2InstancePortMapEntries,
              natv2InstancePortMapCreations }
    STATUS current
    DESCRIPTION
        "This notification is triggered when the value of
         natv2InstancePortMapEntries becomes greater than or equal
         to the value of natv2InstanceThresholdPortMapEntriesHigh,
         unless disabled by setting that threshold to -1.  Reporting
         is subject to the rate limitation given by
         natv2InstanceNotificationInterval.

         natv2InstancePortMapEntries and
         natv2InstancePortMapCreations are members of table
         natv2InstanceTable indexed by the identifier of the NAT
         instance for which the event is being reported.  The values
         reported are those observed at the moment the notification
         was triggered."
    ::= { natv2MIBNotifications 4 }

natv2NotificationSubscriberPortMappingEntriesHigh
NOTIFICATION-TYPE
    OBJECTS { natv2SubscriberPortMapEntries,
              natv2SubscriberPortMapCreations }
    STATUS current
    DESCRIPTION
        "This notification is triggered when the value of
         natv2SubscriberPortMapEntries for an individual subscriber
         becomes greater than or equal to the value of the
         natv2SubscriberThresholdPortMapEntriesHigh object for that
         subscriber, unless disabled by setting that threshold to -1.
         Reporting is subject to the rate limitation given by
         natv2SubscriberNotificationInterval.
```

```
         natv2SubscriberPortMapEntries and
         natv2SubscriberPortMapCreations are members of table
         natv2SubscriberTable indexed by the subscriber for
         which the event is being reported.  The values
         reported are those observed at the moment the notification
         was triggered."
    ::= { natv2MIBNotifications 5 }

-- Device-level objects

natv2MIBDeviceObjects OBJECT IDENTIFIER ::= { natv2MIB 1 }

-- Subscriber table

natv2SubscriberTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2SubscriberEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of subscribers.  As well as the subscriber index, it
         provides per-subscriber state and counter objects, a last
         discontinuity time object for the counters, and a writable
         threshold value and limit on port consumption."
    REFERENCE
        "RFC 7659, Section 3.3.3."
    ::= { natv2MIBDeviceObjects 1 }

natv2SubscriberEntry OBJECT-TYPE
    SYNTAX Natv2SubscriberEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Each entry describes a single subscriber."
    INDEX { natv2SubscriberIndex }
    ::= { natv2SubscriberTable 1 }

Natv2SubscriberEntry ::=
    SEQUENCE {
        natv2SubscriberIndex                  Natv2SubscriberIndex,
        natv2SubscriberInternalRealm              SnmpAdminString,
        natv2SubscriberInternalPrefixType         InetAddressType,
        natv2SubscriberInternalPrefix             InetAddress,
        natv2SubscriberInternalPrefixLength InetAddressPrefixLength,
-- State
        natv2SubscriberAddressMapEntries          Unsigned32,
        natv2SubscriberPortMapEntries             Unsigned32,
```

```
-- Counters and last discontinuity time
        natv2SubscriberTranslations                Counter64,
        natv2SubscriberAddressMapCreations         Counter64,
        natv2SubscriberPortMapCreations            Counter64,
        natv2SubscriberAddressMapFailureDrops      Counter64,
        natv2SubscriberPortMapFailureDrops         Counter64,
        natv2SubscriberDiscontinuityTime           TimeStamp,
-- Read-write controls
        natv2SubscriberLimitPortMapEntries         Unsigned32,
-- Disable notifications by setting threshold to -1
        natv2SubscriberThresholdPortMapEntriesHigh Integer32,
-- Disable limit by setting to 0
        natv2SubscriberNotificationInterval        Unsigned32
    }

natv2SubscriberIndex OBJECT-TYPE
    SYNTAX Natv2SubscriberIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A unique value, greater than zero, for each subscriber
         in the managed system.  The value for each
         subscriber MUST remain constant at least from one
         update of the entity's natv2SubscriberDiscontinuityTime
         object until the next update of that object.  If a
         subscriber is deleted, its assigned index value MUST NOT
         be assigned to another subscriber at least until
         reinitialization of the entity's management system."
    ::= { natv2SubscriberEntry 1 }

-- Configuration for this subscriber: realm, internal address(es)

natv2SubscriberInternalRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The address realm to which this subscriber belongs.  A realm
         defines an address space.  All NATs support at least two
         realms.

         The default realm for subscribers is 'internal'.
         Administrators can set other values for individual
         subscribers when they are configured.  The administrator MAY
         configure a new value of natv2SubscriberRealm at any time
         subsequent to initial configuration of the subscriber.  If
         this happens, it MUST be treated as a point of discontinuity
         requiring an update of natv2SubscriberDiscontinuityTime.
```

```
          When the subscriber sends a packet to the NAT through a
          DS-Lite (RFC 6333) tunnel, this is the realm of the outer
          packet header source address.  Other tunneled access is out
          of scope."
      REFERENCE
          "Address realm: RFC 2663.  DS-Lite: RFC 6333."
      DEFVAL
          { "internal" }
      ::= { natv2SubscriberEntry 2 }

natv2SubscriberInternalPrefixType OBJECT-TYPE
      SYNTAX InetAddressType
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Subscriber's internal prefix type.  Any value other than
          ipv4(1) or ipv6(2) would be unexpected.  In the case of
          DS-Lite access, this is the prefix type (IPv6(2)) used in
          the outer packet header."
      REFERENCE
          "DS-Lite: RFC 6333."
      ::= { natv2SubscriberEntry 3 }

natv2SubscriberInternalPrefix OBJECT-TYPE
      SYNTAX InetAddress
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Prefix assigned to a subscriber's Customer Premises Equipment
          (CPE).  The type of this prefix is given by
          natv2SubscriberInternalPrefixType.  Source addresses of packets
          outgoing from the subscriber will be contained within this
          prefix.  In the case of DS-Lite access, the source address
          taken from the prefix will be that of the outer header."
      REFERENCE
          "DS-Lite: RFC 6333."
      ::= { natv2SubscriberEntry 4 }

natv2SubscriberInternalPrefixLength OBJECT-TYPE
      SYNTAX InetAddressPrefixLength
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Length of the prefix assigned to a subscriber's CPE, in
          bits.  If a single address is assigned, this will be 32
          for IPv4 and 128 for IPv6."
      ::= { natv2SubscriberEntry 5 }
```

```
-- State objects

natv2SubscriberAddressMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of address map entries for the
         subscriber, including static mappings.  An address map entry
         maps from a given internal address and realm to an external
         address in a particular external realm.  This definition
         includes 'hairpin' mappings, where the external realm is the
         same as the internal one.  Address map entries are also
         tracked per instance and per address pool within the
         instance."
    REFERENCE
        "RFC 7659, Section 3.3.8."
    ::= { natv2SubscriberEntry 6 }

natv2SubscriberPortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of port map entries in the port map table
         for the subscriber, including static mappings.  A port map
         entry maps from a given external realm, address, and port
         for a given protocol to an internal realm, address, and
         port.  This definition includes 'hairpin' mappings, where the
         external realm is the same as the internal one.  Port map
         entries are also tracked per instance and per protocol and
         address pool within the instance."
    REFERENCE
        "RFC 7659, Section 3.3.9."
    ::= { natv2SubscriberEntry 7 }

-- Counters and last discontinuity time

natv2SubscriberTranslations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of translated packets received from or
         sent to this subscriber.  This value MUST be monotone
         increasing in the periods between updates of the entity's
         natv2SubscriberDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
```

```
          counter, it SHOULD NOT make use of the difference between
          the latest value of the counter and any value retrieved
          before the new value of natv2SubscriberDiscontinuityTime."
    ::= { natv2SubscriberEntry 8 }

natv2SubscriberAddressMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of address map entries created for
         this subscriber, including static mappings.  Address map
         entries are also tracked per instance and per protocol and
         address pool within the instance.

         This value MUST be monotone increasing in
         the periods between updates of the entity's
         natv2SubscriberDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2SubscriberDiscontinuityTime."
    ::= { natv2SubscriberEntry 9 }

natv2SubscriberPortMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of port map entries created for this
         subscriber, including static mappings.  Port map entries are
         also tracked per instance and per protocol and address pool
         within the instance.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2SubscriberDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2SubscriberDiscontinuityTime."
    ::= { natv2SubscriberEntry 10 }

natv2SubscriberAddressMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
        "The cumulative number of packets originated by this
         subscriber that were dropped because the packet would have
         triggered the creation of a new address map entry, but no
         address could be allocated in the selected external realm
         because all addresses from the selected address pool (or the
         whole realm, if no address pool has been configured for that
         realm) have already been fully allocated.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2SubscriberDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2SubscriberDiscontinuityTime."
    ::= { natv2SubscriberEntry 11 }

natv2SubscriberPortMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped because the
         packet would have triggered the creation of a new
         port mapping, but no port could be allocated for the
         protocol concerned.  The usual case for this will be
         for a NAT instance that supports address pooling and
         the 'Paired' pooling behavior recommended by RFC 4787,
         where the internal endpoint has used up all of the
         ports allocated to it for the address it was mapped to
         in the selected address pool in the external realm
         concerned and cannot be given more ports because
         - policy or implementation prevents it from having a
           second address in the same pool, and
         - policy or unavailability prevents it from acquiring
           more ports at its originally assigned address.

         If the NAT instance supports address pooling but its
         pooling behavior is 'Arbitrary' (meaning that
         the NAT instance can allocate a new port mapping for
         the given internal endpoint on any address in the
         selected address pool and is not bound to what it has
         already mapped for that endpoint), then this counter
         is incremented when all ports for the protocol concerned
         over the whole of the selected address pool are already
         in use.
```

```
            As a third case, if no address pools have been configured
            for the external realm concerned, then this counter is
            incremented because all ports for the protocol involved over
            the whole set of addresses available for that external realm
            are already in use.

            Finally, this counter is incremented if the packet would
            have triggered the creation of a new port mapping, but the
            current value of natv2SubscriberPortMapEntries equals or
            exceeds the value of natv2SubscriberLimitPortMapEntries
            for this subscriber (unless that limit is disabled).

            This value MUST be monotone increasing in the periods
            between updates of the entity's
            natv2SubscriberDiscontinuityTime.  If a manager detects a
            change in the latter since the last time it sampled this
            counter, it SHOULD NOT make use of the difference between
            the latest value of the counter and any value retrieved
            before the new value of natv2SubscriberDiscontinuityTime."
        REFERENCE
            "Pooling behavior: RFC 4787, end of Section 4.1."
        ::= { natv2SubscriberEntry 12 }

natv2SubscriberDiscontinuityTime OBJECT-TYPE
        SYNTAX TimeStamp
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "Snapshot of the value of the sysUpTime object at the
             beginning of the latest period of continuity of the
             statistical counters associated with this subscriber."
        ::= { natv2SubscriberEntry 14 }

-- Per-subscriber limit and threshold on port mappings
-- Disabled if set to zero
natv2SubscriberLimitPortMapEntries OBJECT-TYPE
        SYNTAX Unsigned32
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "Limit on total number of port mappings active for this
             subscriber (natv2SubscriberPortMapEntries).  Once this limit
             is reached, packets that might have triggered new port
             mappings are dropped.  The number of such packets dropped is
             counted in natv2InstancePortMapFailureDrops.

             Limit is disabled if set to zero."
```

```
    DEFVAL
         { 0 }
    ::= { natv2SubscriberEntry 15 }

natv2SubscriberThresholdPortMapEntriesHigh OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Notification threshold for total number of port mappings
         active for this subscriber.  Whenever
         natv2SubscriberPortMapEntries is updated, if it equals or
         exceeds natv2SubscriberThresholdPortMapEntriesHigh, the
         notification
         natv2NotificationSubscriberPortMappingEntriesHigh is
         triggered, unless the notification is disabled by setting
         the threshold to -1.  Reporting is subject to the minimum
         inter-notification interval given by
         natv2SubscriberNotificationInterval.  If multiple
         notifications are triggered during one interval, the agent
         MUST report only the one containing the highest value of
         natv2SubscriberPortMapEntries and discard the others."
    DEFVAL
         { -1 }
    ::= { natv2SubscriberEntry 16 }

natv2SubscriberNotificationInterval OBJECT-TYPE
    SYNTAX Unsigned32 (1..3600)
    UNITS
        "Seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Minimum number of seconds between successive
         reporting of notifications for this subscriber.  Controls
         the reporting of
         natv2NotificationSubscriberPortMappingEntriesHigh."
    DEFVAL
         { 60 }
    ::= { natv2SubscriberEntry 17 }

-- Per-NAT-instance objects

natv2MIBInstanceObjects OBJECT IDENTIFIER ::= { natv2MIB 2 }

-- Instance table
```

```
natv2InstanceTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2InstanceEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of NAT instances.  As well as state and counter
         objects, it provides the instance index, instance name, and
         the last discontinuity time object that is applicable to
         the counters.  It also contains writable thresholds for
         reporting of notifications and limits on usage of resources
         at the level of the NAT instance.

         It is assumed that NAT instances can be created and deleted
         dynamically, but this MIB module does not provide the means
         to do so.  For restrictions on assignment and maintenance of
         the NAT index instance, see the description of
         natv2InstanceIndex in the table below.  For the requirements
         on maintenance of the values of the counters in this table,
         see the description of natv2InstanceDiscontinuityTime in
         this table.

         Each NAT instance has its own resources and behavior.  The
         resources include memory as reflected in space for map
         entries, processing power as reflected in the rate of map
         creation and deletion, and mappable addresses in each realm
         that can play the role of an external realm for at least
         some mappings for that instance.  The NAT instance table
         includes limits and notification thresholds that relate to
         memory usage for mapping at the level of the whole instance.
         The limit on number of subscribers with active mappings is a
         limit to some extent on processor usage.

         The mappable 'external' addresses may or may not be
         organized into address pools.  For a definition of address
         pools, see the description of natv2PoolTable.  If the instance
         does support address pools, it also has a pooling behavior.
         Mapping, filtering, and pooling behavior are defined in the
         descriptions of the natv2InstancePortMappingBehavior,
         natv2InstanceFilteringBehavior, and
         natv2InstancePoolingBehavior objects in this table.  The
         instance also has a fragmentation behavior, defined in the
         description of the natv2InstanceFragmentBehavior object."
    REFERENCE
        "RFC 7659, Section 3.3.4.
         NAT behaviors: RFC 4787 (primary, UDP); RFC 5382 (TCP);
         RFC 5508 (ICMP); and RFC 5597 (Datagram Congestion Control
         Protocol (DCCP))."
    ::= { natv2MIBInstanceObjects 1 }
```

```
natv2InstanceEntry OBJECT-TYPE
    SYNTAX Natv2InstanceEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Objects related to a single NAT instance."
    INDEX { natv2InstanceIndex }
    ::= { natv2InstanceTable 1 }

Natv2InstanceEntry ::=
    SEQUENCE {
         natv2InstanceIndex                    Natv2InstanceIndex,
         natv2InstanceAlias                         DisplayString,
-- Configured behaviors
         natv2InstancePortMappingBehavior           INTEGER,
         natv2InstanceFilteringBehavior             INTEGER,
         natv2InstancePoolingBehavior               INTEGER,
         natv2InstanceFragmentBehavior              INTEGER,
-- State
         natv2InstanceAddressMapEntries              Unsigned32,
         natv2InstancePortMapEntries                 Unsigned32,
-- Statistics and discontinuity time
         natv2InstanceTranslations                   Counter64,
         natv2InstanceAddressMapCreations            Counter64,
         natv2InstancePortMapCreations               Counter64,
         natv2InstanceAddressMapEntryLimitDrops      Counter64,
         natv2InstancePortMapEntryLimitDrops         Counter64,
         natv2InstanceSubscriberActiveLimitDrops     Counter64,
         natv2InstanceAddressMapFailureDrops         Counter64,
         natv2InstancePortMapFailureDrops            Counter64,
         natv2InstanceFragmentDrops                  Counter64,
         natv2InstanceOtherResourceFailureDrops      Counter64,
         natv2InstanceDiscontinuityTime              TimeStamp,
-- Notification thresholds, disabled if set to -1
         natv2InstanceThresholdAddressMapEntriesHigh Integer32,
         natv2InstanceThresholdPortMapEntriesHigh    Integer32,
         natv2InstanceNotificationInterval           Unsigned32,
-- Limits, disabled if set to 0
         natv2InstanceLimitAddressMapEntries         Unsigned32,
         natv2InstanceLimitPortMapEntries            Unsigned32,
         natv2InstanceLimitPendingFragments          Unsigned32,
         natv2InstanceLimitSubscriberActives         Unsigned32
    }

natv2InstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
```

```
    DESCRIPTION
        "NAT instance index.  It is up to the implementation to
         determine which values correspond to in-service NAT
         instances.  This object is used as an index for all tables
         defined below."
    ::= { natv2InstanceEntry 1 }

natv2InstanceAlias OBJECT-TYPE
    SYNTAX DisplayString (SIZE (0..64))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "This object is an 'alias' name for the NAT instance as
         specified by a network manager and provides a non-volatile
         'handle' for the instance.

         An example of the value that a network manager might store
         in this object for a NAT instance is the name/identifier of
         the interface that brings in internal traffic for this NAT
         instance or the name of the Virtual Routing and Forwarding
         (VRF) for internal traffic."
    ::= { natv2InstanceEntry 2 }

-- Configured behaviors

natv2InstancePortMappingBehavior OBJECT-TYPE
    SYNTAX INTEGER {
           endpointIndependent (0),
           addressDependent (1),
           addressAndPortDependent (2)
        }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Port mapping behavior is the policy governing the selection
         of external address and port in a given realm for a given
         five-tuple of source address and port, destination address
         and port, and protocol.

         endpointIndependent(0), the behavior REQUIRED by RFC 4787,
         REQ-1, maps the source address and port to the same
         external address and port for all destination address and
         port combinations reached through the same external realm
         and using the given protocol.
```

```
          addressDependent(1) maps to the same external address and
          port for all destination ports at the same destination
          address reached through the same external realm and using
          the given protocol.

          addressAndPortDependent(2) maps to a separate external
          address and port combination for each different
          destination address and port combination reached through
          the same external realm."
      REFERENCE
          "RFC 4787, Section 4.1."
      ::= { natv2InstanceEntry 3 }

natv2InstanceFilteringBehavior OBJECT-TYPE
      SYNTAX INTEGER {
                endpointIndependent (0),
                addressDependent (1),
                addressAndPortDependent (2)
             }
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "Filtering behavior is the policy governing acceptance or
          the dropping of packets incoming from remote sources via a
          given external realm and destined to a specific three-tuple
          of external address, port, and protocol at the NAT instance
          that has been assigned in a port mapping.

          endpointIndependent(0) accepts for translation packets from
          all combinations of remote address and port destined to the
          mapped external address and port via the given external
          realm and using the given protocol.

          addressDependent(1) accepts for translation packets from all
          remote ports from the same remote source address destined to
          the mapped external address and port via the given external
          realm and using the given protocol.

          addressAndPortDependent(2) accepts for translation only
          those packets with the same remote source address, port, and
          protocol incoming from the same external realm as identified
          when the applicable port map entry was created.

          RFC 4787, REQ-8 recommends either endpointIndependent(0) or
          addressDependent(1) filtering behavior depending on whether
          application friendliness or security takes priority."
      REFERENCE
          "RFC 4787, Section 5."
```

```
    ::= { natv2InstanceEntry 4 }

natv2InstancePoolingBehavior OBJECT-TYPE
    SYNTAX INTEGER {
           arbitrary (0),
           paired (1)
        }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Pooling behavior is the policy used to select the address
         for a new port mapping within a given address pool to which
         the internal address has already been mapped.

         arbitrary(0) pooling behavior means that the NAT instance
         may create the new port mapping using any address in the
         pool that has a free port for the protocol concerned.

         paired(1) pooling behavior, the behavior RECOMMENDED by RFC
         4787, REQ-2, means that once a given internal address has
         been mapped to a particular address in a particular pool,
         further mappings of the same internal address to that pool
         will reuse the previously assigned pool member address."
    REFERENCE
        "RFC 4787, near the end of Section 4.1"
    ::= { natv2InstanceEntry 5 }

natv2InstanceFragmentBehavior OBJECT-TYPE
    SYNTAX INTEGER {
           fragmentNone (0),
           fragmentInOrder (1),
           fragmentOutOfOrder (2)
        }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Fragment behavior is the NAT instance's capability to
         receive and translate fragments incoming from remote
         sources.

         fragmentNone(0) implies no capability to translate incoming
         fragments, so all received fragments are dropped.  Each
         dropped fragment is counted in natv2InstanceFragmentDrops.

         fragmentInOrder(1) implies the ability to translate
         fragments only if they are received in order, so that in
         particular the header is in the first packet.  If a fragment
```

```
          is received out of order, it is dropped and counted in
          natv2InstanceFragmentDrops.

          fragmentOutOfOrder(2), the capability REQUIRED by RFC 4787,
          REQ-14, implies the capability to translate fragments even
          when they arrive out of order, subject to a protective
          limit natv2InstanceLimitPendingFragments on total number of
          fragments awaiting the first fragment of the chain.  If the
          implementation supports this capability,
          natv2InstanceFragmentDrops is incremented only when a new
          fragment arrives but is dropped because the limit on pending
          fragments has already been reached."
    REFERENCE
        "RFC 4787, Section 11."
    ::= { natv2InstanceEntry 6 }

-- State

natv2InstanceAddressMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of address map entries in total over the
         whole NAT instance, including static mappings.  An address
         map entry maps from a given internal address and realm to an
         external address in a particular external realm.  This
         definition includes 'hairpin' mappings, where the external
         realm is the same as the internal one.  Address map entries
         are also tracked per subscriber and per address pool within
         the instance."
    REFERENCE
        "RFC 7659, Section 3.3.8.
         Hairpinning: RFC 4787, Section 6."
    ::= { natv2InstanceEntry 7 }

natv2InstancePortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of entries in the port map table in total
         over the whole NAT instance, including static mappings.  A
         port map entry maps from a given external realm, address,
         and port for a given protocol to an internal realm, address,
         and port.  This definition includes 'hairpin' mappings, where
         the external realm is the same as the internal one.  Port map
```

```
          entries are also tracked per subscriber and per protocol and
          address pool within the instance."
      REFERENCE
          "RFC 7659, Section 3.3.9.
          Hairpinning: RFC 4787, Section 6."
      ::= { natv2InstanceEntry 8 }

-- Statistics

natv2InstanceTranslations OBJECT-TYPE
      SYNTAX Counter64
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "The cumulative number of translated packets passing through
          this NAT instance.  This value MUST be monotone increasing in
          the periods between updates of
          natv2InstanceDiscontinuityTime.  If a manager detects a
          change in the latter since the last time it sampled this
          counter, it SHOULD NOT make use of the difference between
          the latest value of the counter and any value retrieved
          before the new value of natv2InstanceDiscontinuityTime."
      ::= { natv2InstanceEntry 9 }

natv2InstanceAddressMapCreations OBJECT-TYPE
      SYNTAX Counter64
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "The cumulative number of address map entries created by the
          NAT instance, including static mappings.  Address map
          creations are also tracked per address pool within the
          instance and per subscriber.

          This value MUST be monotone increasing in
          the periods between updates of
          natv2InstanceDiscontinuityTime.  If a manager detects a
          change in the latter since the last time it sampled this
          counter, it SHOULD NOT make use of the difference between
          the latest value of the counter and any value retrieved
          before the new value of natv2InstanceDiscontinuityTime."
      ::= { natv2InstanceEntry 10 }

natv2InstancePortMapCreations  OBJECT-TYPE
      SYNTAX Counter64
      MAX-ACCESS read-only
      STATUS current
```

```
    DESCRIPTION
        "The cumulative number of port map entries created by the
         NAT instance, including static mappings.  Port map
         creations are also tracked per protocol and address pool
         within the instance and per subscriber.

         This value MUST be monotone increasing in
         the periods between updates of
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2InstanceEntry 11 }

natv2InstanceAddressMapEntryLimitDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped rather than
         translated because the packet would have triggered
         the creation of a new address map entry, but the limit
         on number of address map entries for the NAT instance
         given by natv2InstanceLimitAddressMapEntries has
         already been reached.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2InstanceEntry 12 }

natv2InstancePortMapEntryLimitDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped rather than
         translated because the packet would have triggered
         the creation of a new port map entry, but the limit
         on number of port map entries for the NAT instance
         given by natv2InstanceLimitPortMapEntries has
         already been reached.
```

```
          This value MUST be monotone increasing in the periods
          between updates of the entity's
          natv2InstanceDiscontinuityTime.  If a manager detects a
          change in the latter since the last time it sampled this
          counter, it SHOULD NOT make use of the difference between
          the latest value of the counter and any value retrieved
          before the new value of natv2InstanceDiscontinuityTime."
      ::= { natv2InstanceEntry 13 }

natv2InstanceSubscriberActiveLimitDrops OBJECT-TYPE
      SYNTAX Counter64
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "The cumulative number of packets dropped rather than
           translated because the packet would have triggered the
           creation of a new mapping for a subscriber with no other
           active mappings, but the limit on number of active
           subscribers for the NAT instance given by
           natv2InstanceLimitSubscriberActives has already been
           reached.

           This value MUST be monotone increasing in the periods
           between updates of the entity's
           natv2InstanceDiscontinuityTime.  If a manager detects a
           change in the latter since the last time it sampled this
           counter, it SHOULD NOT make use of the difference between
           the latest value of the counter and any value retrieved
           before the new value of natv2InstanceDiscontinuityTime."
      ::= { natv2InstanceEntry 14 }

natv2InstanceAddressMapFailureDrops OBJECT-TYPE
      SYNTAX Counter64
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
          "The cumulative number of packets dropped because the packet
           would have triggered the creation of a new address map
           entry, but no address could be allocated in the selected
           external realm because all addresses from the selected
           address pool (or the whole realm, if no address pool has
           been configured for that realm) have already been fully
           allocated.

           This value MUST be monotone increasing in the periods
           between updates of the entity's
           natv2InstanceDiscontinuityTime.  If a manager detects a
           change in the latter since the last time it sampled this
```

```
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2InstanceEntry 15 }

natv2InstancePortMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped because the
         packet would have triggered the creation of a new
         port map entry, but no port could be allocated for the
         protocol concerned.  The usual case for this will be
         for a NAT instance that supports address pooling and
         the 'Paired' pooling behavior recommended by RFC 4787,
         where the internal endpoint has used up all of the
         ports allocated to it for the address it was mapped to
         in the selected address pool in the external realm
         concerned and cannot be given more ports because
         - policy or implementation prevents it from having a
           second address in the same pool, and
         - policy or unavailability prevents it from acquiring
           more ports at its originally assigned address.

         If the NAT instance supports address pooling but its
         pooling behavior is 'Arbitrary' (meaning that
         the NAT instance can allocate a new port mapping for
         the given internal endpoint on any address in the
         selected address pool and is not bound to what it has
         already mapped for that endpoint), then this counter
         is incremented when all ports for the protocol concerned
         over the whole of the selected address pool are already
         in use.

         Finally, if no address pools have been configured for the
         external realm concerned, then this counter is incremented
         because all ports for the protocol involved over the whole
         set of addresses available for that external realm are
         already in use.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
```

```
    REFERENCE
        "Pooling behavior: RFC 4787, end of Section 4.1."
    ::= { natv2InstanceEntry 16 }

natv2InstanceFragmentDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of fragments received by the NAT
         instance but dropped rather than translated.  When the NAT
         instance supports the 'Receive Fragment Out of Order'
         capability as required by RFC 4787, this occurs because the
         fragment was received out of order and would be added to the
         queue of fragments awaiting the initial fragment of the
         chain, but the queue has already reached the limit set by
         natv2InstanceLimitsPendingFragments.  Counting in other cases
         is specified in the description of
         natv2InstanceFragmentBehavior.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    REFERENCE
        "RFC 4787, Section 11."
    ::= { natv2InstanceEntry 17 }

natv2InstanceOtherResourceFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped because of
         unavailability of a resource other than an address or port
         that would have been required to process it.  The most likely
         case is where the upper-layer protocol in the packet is not
         supported by the NAT instance.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
```

```
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2InstanceEntry 18 }

natv2InstanceDiscontinuityTime OBJECT-TYPE
    SYNTAX TimeStamp
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Snapshot of the value of the sysUpTime object at the
         beginning of the latest period of continuity of the
         statistical counters associated with this NAT instance."
    ::= { natv2InstanceEntry 19 }

-- Notification thresholds, disabled by setting to -1.

natv2InstanceThresholdAddressMapEntriesHigh OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Notification threshold for total number of address map
         entries held by this NAT instance.  Whenever
         natv2InstanceAddressMapEntries is updated, if it equals or
         exceeds natv2InstanceThresholdAddressMapEntriesHigh, then
         natv2NotificationInstanceAddressMapEntriesHigh may be
         triggered, unless the notification is disabled by setting
         the threshold to -1.  Reporting is subject to the minimum
         inter-notification interval given by
         natv2InstanceNotificationInterval.  If multiple notifications
         are triggered during one interval, the agent MUST report
         only the one containing the highest value of
         natv2InstanceAddressMapEntries and discard the others."
    DEFVAL
         { -1 }
    ::= { natv2InstanceEntry 20 }

natv2InstanceThresholdPortMapEntriesHigh OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Notification threshold for total number of port map
         entries held by this NAT instance.  Whenever
         natv2InstancePortMapEntries is updated, if it equals or
         exceeds natv2InstanceThresholdPortMapEntriesHigh, then
         natv2NotificationInstancePortMapEntriesHigh may be
         triggered, unless the notification is disabled by setting
         the threshold to -1.  Reporting is subject to the minimum
```

```
          inter-notification interval given by
          natv2InstanceNotificationInterval.  If multiple notifications
          are triggered during one interval, the agent MUST report
          only the one containing the highest value of
          natv2InstancePortMapEntries and discard the others."
      DEFVAL
          { -1 }
      ::= { natv2InstanceEntry 21 }

natv2InstanceNotificationInterval OBJECT-TYPE
      SYNTAX Unsigned32 (1..3600)
      UNITS
          "Seconds"
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
          "Minimum number of seconds between successive
           notifications for this NAT instance.  Controls the reporting
           of natv2NotificationInstanceAddressMapEntriesHigh and
           natv2NotificationInstancePortMapEntriesHigh."
      DEFVAL
          { 10 }
      ::= { natv2InstanceEntry 22 }

  -- Limits, disabled if set to 0

natv2InstanceLimitAddressMapEntries OBJECT-TYPE
      SYNTAX Unsigned32
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
          "Limit on total number of address map entries supported by
           the NAT instance.  When natv2InstanceAddressMapEntries has
           reached this limit, subsequent packets that would normally
           trigger creation of a new address map entry will be dropped
           and counted in natv2InstanceAddressMapEntryLimitDrops.
           Warning of an approach to this limit can be achieved by
           setting natv2InstanceThresholdAddressMapEntriesHigh to a
           non-zero value, for example, 80% of the limit.  The limit is
           disabled by setting its value to zero.

           For further information, please see the descriptions of
           natv2NotificationInstanceAddressMapEntriesHigh and
           natv2InstanceAddressMapEntries."
      DEFVAL
          { 0 }
      ::= { natv2InstanceEntry 23 }
```

```
natv2InstanceLimitPortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Limit on total number of port map entries supported by the
         NAT instance.  When natv2InstancePortMapEntries has reached
         this limit, subsequent packets that would normally trigger
         creation of a new port map entry will be dropped and counted
         in natv2InstancePortMapEntryLimitDrops.  Warning of an
         approach to this limit can be achieved by setting
         natv2InstanceThresholdPortMapEntriesHigh to a non-zero
         value, for example, 80% of the limit.  The limit is disabled
         by setting its value to zero.

         For further information, please see the descriptions of
         natv2NotificationInstancePortMapEntriesHigh and
         natv2InstancePortMapEntries."
    DEFVAL
        { 0 }
    ::= { natv2InstanceEntry 24 }

natv2InstanceLimitPendingFragments OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Limit on number of out-of-order fragments received by the
         NAT instance from remote sources and held until head of
         chain appears.  While the number of held fragments is at this
         limit, subsequent packets that contain fragments not
         relating to those already held will be dropped and counted
         in natv2InstancePendingFragmentLimitDrops.  The limit is
         disabled by setting the value to zero.

         Applicable only when the NAT instance supports 'Receive
         Fragments Out of Order' behavior; leave at default
         otherwise.  See the description of
         natv2InstanceFragmentBehavior."
    REFERENCE
         "RFC 4787, Section 11."
    DEFVAL { 0 }
    ::= { natv2InstanceEntry 25 }

natv2InstanceLimitSubscriberActives OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
```

```
    DESCRIPTION
        "Limit on number of total number of active subscribers
         supported by the NAT instance.  An active subscriber is
         defined as any subscriber with at least one map entry,
         including static mappings.  While the number of active
         subscribers is at this limit, subsequent packets that would
         otherwise trigger first mappings for newly active
         subscribers will be dropped and counted in
         natv2InstanceSubscriberActiveLimitDrops.  The limit is
         disabled by setting the value to zero."
    DEFVAL { 0 }
    ::= { natv2InstanceEntry 26 }

-- Table of counters per upper-layer protocol identified by the
-- packet header and supported by the NAT instance.

natv2ProtocolTable  OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2ProtocolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of protocols with per-protocol counters.  Conceptual
         rows of the table are indexed by the combination of the NAT
         instance number and the IANA-assigned upper-layer protocol
         number as given by the ProtocolNumber Textual Convention
         (TC) and contained in the packet IP header.  It is up to the
         agent implementation to determine and operate upon only
         those upper-layer protocol numbers supported by the NAT
         instance."
    REFERENCE
        "RFC 7659, Section 3.3.5."
    ::= { natv2MIBInstanceObjects 2 }

natv2ProtocolEntry OBJECT-TYPE
    SYNTAX Natv2ProtocolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Per-protocol counters."
    INDEX { natv2ProtocolInstanceIndex,
            natv2ProtocolNumber }
    ::= { natv2ProtocolTable 1 }

Natv2ProtocolEntry ::=
    SEQUENCE {
        natv2ProtocolInstanceIndex          Natv2InstanceIndex,
        natv2ProtocolNumber                     ProtocolNumber,
```

```
-- State
        natv2ProtocolPortMapEntries             Unsigned32,
-- Statistics.  Discontinuity object from instance table reused here.
        natv2ProtocolTranslations               Counter64,
        natv2ProtocolPortMapCreations           Counter64,
        natv2ProtocolPortMapFailureDrops        Counter64
    }

natv2ProtocolInstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "NAT instance index.  It is up to the implementation to
         determine and operate upon only those values that
         correspond to in-service NAT instances."
    ::= { natv2ProtocolEntry 1 }

natv2ProtocolNumber OBJECT-TYPE
    SYNTAX ProtocolNumber
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Counters in this conceptual row apply to packets indicating
         the upper-layer protocol identified by the value of
         this object.  It is up to the implementation to determine and
         operate upon only those values that correspond to protocols
         supported by the NAT instance."
    REFERENCE
        "RFC 7659, Section 3.3.5.
         IANA Protocol Numbers,
         <http://www.iana.org/assignments/protocol-numbers>"
    ::= { natv2ProtocolEntry 2 }

 -- State
natv2ProtocolPortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of entries in the port map table in total
         over the whole NAT instance for a given protocol, including
         static mappings.  A port map entry maps from a given external
         realm, address, and port for a given protocol to an internal
         realm, address, and port.  This definition includes 'hairpin'
         mappings, where the external realm is the same as the
         internal one.  Port map entries are also tracked per
         subscriber, per instance, and per address pool within the
```

```
         instance."
    REFERENCE
        "RFC 7659, Sections 3.3.5 and 3.3.9.
         Hairpinning: RFC 4787, Section 6."
    ::= { natv2ProtocolEntry 3 }

-- Statistics
natv2ProtocolTranslations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets translated by the NAT
         instance in either direction for the given protocol.

         This value MUST be monotone increasing in the periods
         between updates of the NAT instance
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2ProtocolEntry 4 }

natv2ProtocolPortMapCreations  OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of port map entries created by the NAT
         instance for the given protocol.

         This value MUST be monotone increasing in the periods
         between updates of the NAT instance
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    ::= { natv2ProtocolEntry 5 }

natv2ProtocolPortMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped because the packet
         would have triggered the creation of a new port map entry,
```

```
         but no port could be allocated for the protocol concerned.
         The usual case for this will be for a NAT instance that
         supports address pooling and the 'Paired' pooling behavior
         recommended by RFC 4787, where the internal endpoint has
         used up all of the ports allocated to it for the address it
         was mapped to in the selected address pool in the external
         realm concerned and cannot be given more ports because
         - policy or implementation prevents it from having a
           second address in the same pool, and
         - policy or unavailability prevents it from acquiring
           more ports at its originally assigned address.

         If the NAT instance supports address pooling but its
         pooling behavior is 'Arbitrary' (meaning that
         the NAT instance can allocate a new port mapping for
         the given internal endpoint on any address in the
         selected address pool and is not bound to what it has
         already mapped for that endpoint), then this counter
         is incremented when all ports for the protocol concerned
         over the whole of the selected address pool are already
         in use.

         Finally, if the NAT instance has no configured address
         pooling, then this counter is incremented because all
         ports for the protocol concerned over the whole of the
         NAT instance for the external realm concerned are already
         in use.

         This value MUST be monotone increasing in the periods
         between updates of the NAT instance
         natv2InstanceDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2InstanceDiscontinuityTime."
    REFERENCE
        "RFC 4787, end of Section 4.1."
    ::= { natv2ProtocolEntry 6 }

-- pools

natv2PoolTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2PoolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "Table of address pools, applicable only if these are
        supported by the NAT instance.  An address pool is a set of
```

```
        addresses and ports in a particular realm, available for
        assignment to the 'external' portion of a mapping.  Where more
        than one pool has been configured for the realm, policy
        determines which subscribers and/or services are mapped to
        which pool.  natv2PoolTable provides basic information, state,
        statistics, and two notification thresholds for each pool.
        natv2PoolRangeTable is an expansion table for natv2PoolTable
        that identifies particular address ranges allocated to the
        pool."
    REFERENCE
        "RFC 7659, Section 3.3.6."
    ::= { natv2MIBInstanceObjects 3 }

natv2PoolEntry OBJECT-TYPE
    SYNTAX Natv2PoolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Entry in the table of address pools."
    INDEX { natv2PoolInstanceIndex, natv2PoolIndex }
    ::= { natv2PoolTable 1 }

Natv2PoolEntry ::=
    SEQUENCE {
-- Index
         natv2PoolInstanceIndex                Natv2InstanceIndex,
         natv2PoolIndex                        Natv2PoolIndex,
-- Configuration
         natv2PoolRealm                        SnmpAdminString,
         natv2PoolAddressType                  InetAddressType,
         natv2PoolMinimumPort                  InetPortNumber,
         natv2PoolMaximumPort                  InetPortNumber,
-- State
         natv2PoolAddressMapEntries            Unsigned32,
         natv2PoolPortMapEntries               Unsigned32,
-- Statistics and discontinuity time
         natv2PoolAddressMapCreations          Counter64,
         natv2PoolPortMapCreations             Counter64,
         natv2PoolAddressMapFailureDrops       Counter64,
         natv2PoolPortMapFailureDrops          Counter64,
         natv2PoolDiscontinuityTime            TimeStamp,
-- Notification thresholds and objects returned by notifications
         natv2PoolThresholdUsageLow            Integer32,
         natv2PoolThresholdUsageHigh           Integer32,
         natv2PoolNotifiedPortMapEntries       Unsigned32,
         natv2PoolNotifiedPortMapProtocol      ProtocolNumber,
         natv2PoolNotificationInterval         Unsigned32
    }
```

```
natv2PoolInstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "NAT instance index.  It is up to the agent implementation
         to determine and operate upon only those values that
         correspond to in-service NAT instances."
    ::= { natv2PoolEntry 1 }

natv2PoolIndex OBJECT-TYPE
    SYNTAX Natv2PoolIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of an address pool that is unique for a given NAT
         instance.  It is up to the agent implementation to determine
         and operate upon only those values that correspond to
         provisioned pools."
    ::= { natv2PoolEntry 2 }

-- Configuration
natv2PoolRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE (0..32))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Address realm to which this pool's addresses belong."
    REFERENCE
        "Address realms are discussed in Section 3.3.3 of
         RFC 7659.  The primary reference is RFC 2663, Section 2.1."
    ::= { natv2PoolEntry 3 }

natv2PoolAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Address type supplied by this address pool.  This will be the
         same for all pools in a given realm (by definition of an
         address realm).  Values other than ipv4(1) or ipv6(2) would
         be unexpected."
    REFERENCE
        "InetAddressType in RFC 4001."
    ::= { natv2PoolEntry 4 }

natv2PoolMinimumPort OBJECT-TYPE
    SYNTAX InetPortNumber
```

```
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Minimum port number of the range that can be allocated in
         this pool.  Applies to all protocols supported by the NAT
         instance."
    REFERENCE
        "InetPortNumber in RFC 4001."
    ::= { natv2PoolEntry 5 }

natv2PoolMaximumPort OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Maximum port number of the range that can be allocated in
         this pool.  Applies to all protocols supported by the NAT
         instance."
    REFERENCE
        "InetPortNumber in RFC 4001."
    ::= { natv2PoolEntry 6 }

-- State
natv2PoolAddressMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of address map entries using external
         addresses drawn from this pool, including static mappings.
         This definition includes 'hairpin' mappings, where the
         external realm is the same as the internal one.  Address map
         entries are also tracked per subscriber and per instance."
    REFERENCE
        "RFC 7659, Section 3.3.8.
         Hairpinning: RFC 4787, Section 6."
    ::= { natv2PoolEntry 7 }

natv2PoolPortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The current number of entries in the port map table using
         external addresses and ports drawn from this pool, including
         static mappings.  This definition includes 'hairpin'
         mappings, where the external realm is the same as the
         internal one.  Port map entries are also tracked per
```

```
          subscriber, per instance, and per protocol within the
          instance."
    REFERENCE
        "RFC 7659, Section 3.3.9.
         Hairpinning: RFC 4787, Section 6."
    ::= { natv2PoolEntry 8 }

-- Statistics and discontinuity time
natv2PoolAddressMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of address map entries created in this
         pool, including static mappings.  Address map entries are
         also tracked per instance and per subscriber.

         This value MUST be monotone increasing in
         the periods between updates of the entity's
         natv2PoolDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2PoolDiscontinuityTime."
    ::= { natv2PoolEntry 9 }

natv2PoolPortMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of port map entries created in this
         pool, including static mappings.  Port map entries are also
         tracked per instance, per protocol, and per subscriber.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2PoolDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2PoolDiscontinuityTime."
    ::= { natv2PoolEntry 10 }

natv2PoolAddressMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
        "The cumulative number of packets originated by the
         subscriber that were dropped because the packet would have
         triggered the creation of a new address map entry, but no
         address could be allocated from this address pool because
         all addresses in the pool have already been fully allocated.
         Counters of this event are also provided per instance, per
         protocol, and per subscriber.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2PoolDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2PoolDiscontinuityTime."
    ::= { natv2PoolEntry 11 }

natv2PoolPortMapFailureDrops OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The cumulative number of packets dropped because the packet
         would have triggered the creation of a new port map entry,
         but no port could be allocated for the protocol concerned.
         The usual case for this will be for a NAT instance that
         supports the 'Paired' pooling behavior recommended by RFC
         4787, where the internal endpoint has used up all of the
         ports allocated to it for the address it was mapped to in
         this pool and cannot be given more ports because
         - policy or implementation prevents it from having a
           second address in the same pool, and
         - policy or unavailability prevents it from acquiring
           more ports at its originally assigned address.

         If the NAT instance pooling behavior is 'Arbitrary' (meaning
         that the NAT instance can allocate a new port mapping for
         the given internal endpoint on any address in the selected
         address pool and is not bound to what it has already mapped
         for that endpoint), then this counter is incremented when
         all ports for the protocol concerned over the whole of this
         address pool are already in use.

         This value MUST be monotone increasing in the periods
         between updates of the entity's
         natv2PoolDiscontinuityTime.  If a manager detects a
         change in the latter since the last time it sampled this
```

```
         counter, it SHOULD NOT make use of the difference between
         the latest value of the counter and any value retrieved
         before the new value of natv2PoolDiscontinuityTime."
    REFERENCE
        "Pooling behavior: RFC 4787, end of Section 4.1."
    ::= { natv2PoolEntry 12 }


natv2PoolDiscontinuityTime OBJECT-TYPE
    SYNTAX TimeStamp
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Snapshot of the value of the sysUpTime object at the
         beginning of the latest period of continuity of the
         statistical counters associated with this address
         pool.  This MUST be initialized when the address pool
         is configured and MUST be updated whenever the port
         or address ranges allocated to the pool change."
    ::= { natv2PoolEntry 13 }

-- Notification thresholds and objects returned by notifications
natv2PoolThresholdUsageLow OBJECT-TYPE
    SYNTAX Integer32 (-1|0..100)
    UNITS "Percent"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Threshold for reporting low utilization of the address pool.
         Utilization at a given instant is calculated as the
         percentage of ports allocated in port map entries for the
         most-used protocol at that instant.  If utilization is less
         than or equal to natv2PoolThresholdUsageLow, an instance of
         natv2NotificationPoolUsageLow may be triggered, unless
         disabled by setting it to -1.  Reporting is subject to the
         per-pool notification interval given by
         natv2PoolNotificationInterval.  If multiple notifications
         are triggered during one interval, the agent MUST report
         only the one with the lowest value of
         natv2PoolNotifiedPortMapEntries and discard the others.

         Implementation note: the percentage specified by this object
         can be converted to a number of port map entries at
         configuration time (after port and address ranges have been
         configured or reconfigured) and compared to the current
         value of natv2PoolNotifiedPortMapEntries."
    REFERENCE
        "RFC 7659, Sections 3.1.2 and 3.3.6."
```

```
    DEFVAL { -1 }
    ::= { natv2PoolEntry 14 }

natv2PoolThresholdUsageHigh OBJECT-TYPE
    SYNTAX Integer32 (-1|0..100)
    UNITS "Percent"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Threshold for reporting high utilization of the address
         pool.  Utilization at a given instant is calculated as the
         percentage of ports allocated in port map entries for the
         most-used protocol at that instant.  If utilization is
         greater than or equal to natv2PoolThresholdUsageHigh, an
         instance of natv2NotificationPoolUsageHigh may be triggered,
         unless disabled by setting it to -1.

         Reporting is subject to the per-pool notification interval
         given by natv2PoolNotificationInterval.  If multiple
         notifications are triggered during one interval, the agent
         MUST report only the one with the highest value of
         natv2PoolNotifiedPortMapEntries and discard the others.
         In the rare case where both upper and lower thresholds
         are crossed in the same interval, the agent MUST report only
         the upper-threshold notification.

         Implementation note: the percentage specified by this object
         can be converted to a number of port map entries at
         configuration time (after port and address ranges have been
         configured or reconfigured) and compared to the current
         value of natv2PoolNotifiedPortMapEntries."
    DEFVAL { -1 }
    ::= { natv2PoolEntry 15 }

natv2PoolNotifiedPortMapEntries OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION
        "Number of port map entries using addresses and ports from
         this address pool for the most-used protocol at a given
         instant.  One of the objects returned by
         natv2NotificationPoolUsageLow and
         natv2NotificationPoolUsageHigh."
    ::= { natv2PoolEntry 16 }

natv2PoolNotifiedPortMapProtocol OBJECT-TYPE
    SYNTAX ProtocolNumber
```

```
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION
        "The most-used protocol (i.e., with the largest number of
         port map entries) mapped into this address pool at a given
         instant.  One of the objects returned by
         natv2NotificationPoolUsageLow and
         natv2NotificationPoolUsageHigh."
    ::= { natv2PoolEntry 17 }

natv2PoolNotificationInterval OBJECT-TYPE
    SYNTAX Unsigned32 (1..3600)
    UNITS
        "Seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Minimum number of seconds between successive
         notifications for this address pool.  Controls the generation
         of natv2NotificationPoolUsageLow and
         natv2NotificationPoolUsageHigh."
    DEFVAL
        { 20 }
    ::= { natv2PoolEntry 18 }


natv2PoolRangeTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2PoolRangeEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "This table contains address ranges used by pool entries.
         It is an expansion of natv2PoolTable."
    REFERENCE
        "RFC 7659, Section 3.3.7."
    ::= { natv2MIBInstanceObjects 4 }

natv2PoolRangeEntry OBJECT-TYPE
    SYNTAX Natv2PoolRangeEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "NAT pool address range."
    INDEX {
         natv2PoolRangeInstanceIndex,
         natv2PoolRangePoolIndex,
         natv2PoolRangeRowIndex
    }
```

```
    ::= { natv2PoolRangeTable 1 }

Natv2PoolRangeEntry ::=
    SEQUENCE {
        natv2PoolRangeInstanceIndex    Natv2InstanceIndex,
        natv2PoolRangePoolIndex        Natv2PoolIndex,
        natv2PoolRangeRowIndex         Unsigned32,
        natv2PoolRangeBegin            InetAddress,
        natv2PoolRangeEnd              InetAddress
    }

natv2PoolRangeInstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of the NAT instance on which the address pool and this
         address range are configured.  See Natv2InstanceIndex."
    ::= { natv2PoolRangeEntry 1 }

natv2PoolRangePoolIndex OBJECT-TYPE
    SYNTAX Natv2PoolIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of the address pool to which this address range
         belongs.  See Natv2PoolIndex."
    ::= { natv2PoolRangeEntry 2 }

natv2PoolRangeRowIndex OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Row index for successive range entries for the same
         address pool."
    ::= { natv2PoolRangeEntry 3 }

natv2PoolRangeBegin OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Lowest address included in this range.  The type of address
         (IPv4 or IPv6) is given by natv2PoolAddressType
         in natv2PoolTable."
    ::= { natv2PoolRangeEntry 4 }
```

```
natv2PoolRangeEnd OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Highest address included in this range.  The type of address
         (IPv4 or IPv6) is given by natv2PoolAddressType
         in natv2PoolTable."
    ::= { natv2PoolRangeEntry 5 }

-- Indexed mapping tables

-- Address Map Table.  Mapped from the internal to external address.

natv2AddressMapTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2AddressMapEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of mappings from the internal to external address.  By
         definition, this is a snapshot of NAT instance state at a
         given moment.  Indexed by NAT instance, internal realm, and
         internal address in that realm.  Provides the mapped external
         address and, depending on implementation support, identifies
         the address pool from which the external address and port
         were taken and the index of the subscriber to which the
         mapping has been allocated.

         In the case of DS-Lite (RFC 6333), the indexing realm and
         address are those of the IPv6 encapsulation rather than the
         IPv4 inner packet."
    REFERENCE
        "RFC 7659, Section 3.3.8. DS-Lite: RFC 6333"
    ::= { natv2MIBInstanceObjects 5 }

natv2AddressMapEntry OBJECT-TYPE
    SYNTAX Natv2AddressMapEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Mapping from internal to external address."
    INDEX { natv2AddressMapInstanceIndex,
            natv2AddressMapInternalRealm,
            natv2AddressMapInternalAddressType,
            natv2AddressMapInternalAddress,
            natv2AddressMapRowIndex }
    ::= { natv2AddressMapTable 1 }
```

```
Natv2AddressMapEntry ::=
    SEQUENCE {
        natv2AddressMapInstanceIndex       Natv2InstanceIndex,
        natv2AddressMapInternalRealm       SnmpAdminString,
        natv2AddressMapInternalAddressType  InetAddressType,
        natv2AddressMapInternalAddress      InetAddress,
        natv2AddressMapRowIndex            Unsigned32,
        natv2AddressMapInternalMappedAddressType InetAddressType,
        natv2AddressMapInternalMappedAddress     InetAddress,
        natv2AddressMapExternalRealm       SnmpAdminString,
        natv2AddressMapExternalAddressType InetAddressType,
        natv2AddressMapExternalAddress     InetAddress,
        natv2AddressMapExternalPoolIndex   Natv2PoolIndexOrZero,
        natv2AddressMapSubscriberIndex     Natv2SubscriberIndexOrZero
    }

natv2AddressMapInstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of the NAT instance that generated this address map."
    ::= { natv2AddressMapEntry 1 }

natv2AddressMapInternalRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Realm to which the internal address belongs.  In most cases,
         this is the realm defining the address space of the packet
         being translated.  However, in the case of DS-Lite (RFC
         6333), this realm defines the IPv6 outer header address
         space.  It is the combination of that outer header and
         the inner IPv4 packet header that is remapped to the
         external address and realm.  The corresponding IPv4 realm is
         restricted in scope to the tunnel, so there is no point in
         identifying it.  The mapped IPv4 address will normally be the
         well-known value 192.0.0.2, or at least lie in the reserved
         192.0.0.0/29 range.

         If natv2AddressMapSubscriberIndex in this table is a valid
         subscriber index (i.e., greater than zero), then the value
         of natv2AddressMapInternalRealm MUST be identical to the
         value of natv2SubscriberRealm associated with that index."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
```

```
         the NAT mapping tables)."
    ::= { natv2AddressMapEntry 2 }

natv2AddressMapInternalAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Address type in the header of packets on the
         interior side of this mapping.  Any value other than ipv4(1)
         or ipv6(2) would be unexpected.

         In the DS-Lite case, the address type is ipv6(2)."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel source
         address in the NAT mapping tables)."
    ::= { natv2AddressMapEntry 3 }

natv2AddressMapInternalAddress OBJECT-TYPE
    SYNTAX InetAddress (SIZE (0..16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Source address of packets originating from the interior
         of the association provided by this mapping.  The address
         type is given by natv2AddressMapInternalAddressType.

         In the case of DS-Lite (RFC 6333), this is the IPv6 tunnel
         source address.  The mapping in this case is considered to
         be from the combination of the IPv6 tunnel source address
         natv2AddressMapInternalRealmAddress and the well-known IPv4
         inner source address natv2AddressMapInternalMappedAddress to
         the external address."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
         the NAT mapping tables)."
    ::= { natv2AddressMapEntry 4 }

natv2AddressMapRowIndex OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of a conceptual row corresponding to a mapping of the
         given internal realm and address to a single external realm
         and address.  Multiple rows will be present because of a
```

```
         promiscuous external address selection policy, policies
         associating the same internal address with different address
         pools, or because the same internal realm-address
         combination is communicating with multiple external address
         realms."
    ::= { natv2AddressMapEntry 5 }

natv2AddressMapInternalMappedAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Internal address type actually translated by this mapping.
         Any value other than ipv4(1) or ipv6(2) would be unexpected.
         In the general case, this is the same as given by
         natv2AddressMapInternalRealmAddressType.  In the
         tunneled case, it is the address type used in the
         encapsulated packet header.  In particular, in the DS-Lite
         case, the mapped address type is ipv4(1)."
    REFERENCE
        "DS-Lite: RFC 6333."
    ::= { natv2AddressMapEntry 6 }

natv2AddressMapInternalMappedAddress OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Internal address actually translated by this mapping.  In the
         general case, this is the same as
         natv2AddressMapInternalRealmAddress.  The address type is
         given by natv2AddressMapInternalMappedAddressType.  In the
         case of DS-Lite (RFC 6333), this is the source address of
         the encapsulated IPv4 packet, normally lying in the well-known
         range 192.0.0.0/29.  The mapping in this case is considered
         to be from the combination of the IPv6 tunnel source address
         natv2AddressMapInternalRealmAddress and the well-known IPv4
         inner source address natv2AddressMapInternalMappedAddress to
         the external address."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
         the NAT mapping tables)."
    ::= { natv2AddressMapEntry 7 }

natv2AddressMapExternalRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS read-only
```

```
    STATUS current
    DESCRIPTION
        "External address realm to which this mapping maps the
         internal address.  This can be the same as the internal realm
         in the case of a 'hairpin' connection, but otherwise will be
         different."
    ::= { natv2AddressMapEntry 8 }

natv2AddressMapExternalAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Address type for the external realm.  Any value other than
         ipv4(1) or ipv6(2) would be unexpected."
    ::= { natv2AddressMapEntry 9 }

natv2AddressMapExternalAddress OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "External address to which the internal address is mapped.
         The address type is given by
         natv2AddressMapExternalAddressType.

         In the DS-Lite case, the mapping is from the combination of
         the internal IPv6 tunnel source address as presented in this
         table and the well-known IPv4 source address of the
         encapsulated IPv4 packet."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
         the NAT mapping tables)."
    ::= { natv2AddressMapEntry 10 }

natv2AddressMapExternalPoolIndex OBJECT-TYPE
    SYNTAX Natv2PoolIndexOrZero
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Index of the address pool in the external realm from which
         the mapped external address given in
         natv2AddressMapExternalAddress was taken.  Zero if the
         implementation does not support address pools but has chosen
         to support this object or if no pool was configured for the
         given external realm."
    ::= { natv2AddressMapEntry 11 }
```

```
natv2AddressMapSubscriberIndex OBJECT-TYPE
    SYNTAX Natv2SubscriberIndexOrZero
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Index of the subscriber to which this address mapping
         applies, or zero if no subscribers are configured on
         this NAT instance."
    ::= { natv2AddressMapEntry 12 }

-- natv2PortMapTable

natv2PortMapTable OBJECT-TYPE
    SYNTAX SEQUENCE OF Natv2PortMapEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of port map entries indexed by the NAT instance,
         protocol, and external realm and address.  A port map entry
         associates an internal upper-layer protocol endpoint with an
         endpoint for the same protocol in the given external realm.
         By definition, this is a snapshot of NAT instance state at
         a given moment.  The table provides the basic mapping
         information.

         In the case of DS-Lite (RFC 6333), the table provides the
         internal IPv6 tunnel source address in
         natv2PortMapInternalRealmAddress and the IPv4 source address
         of the encapsulated packet that is actually translated in
         natv2PortMapInternalMappedAddress.  In the general (non-DS-
         Lite) case, those two objects will have the same value."
    REFERENCE
        "RFC 7659, Section 3.3.9.
         DS-Lite: RFC 6333, Sections 5.7
         (for well-known addresses) and 6.6 (on the need to have the
         IPv6 tunnel address in the NAT mapping tables)."
    ::= { natv2MIBInstanceObjects 6 }

natv2PortMapEntry OBJECT-TYPE
    SYNTAX Natv2PortMapEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A single NAT mapping."
    INDEX { natv2PortMapInstanceIndex,
            natv2PortMapProtocol,
            natv2PortMapExternalRealm,
            natv2PortMapExternalAddressType,
```

```
            natv2PortMapExternalAddress,
            natv2PortMapExternalPort }
    ::= { natv2PortMapTable 1 }

Natv2PortMapEntry ::=
    SEQUENCE {
        natv2PortMapInstanceIndex        Natv2InstanceIndex,
        natv2PortMapProtocol             ProtocolNumber,
        natv2PortMapExternalRealm        SnmpAdminString,
        natv2PortMapExternalAddressType  InetAddressType,
        natv2PortMapExternalAddress      InetAddress,
        natv2PortMapExternalPort         InetPortNumber,
        natv2PortMapInternalRealm        SnmpAdminString,
        natv2PortMapInternalAddressType  InetAddressType,
        natv2PortMapInternalAddress      InetAddress,
        natv2PortMapInternalMappedAddressType InetAddressType,
        natv2PortMapInternalMappedAddress     InetAddress,
        natv2PortMapInternalPort         InetPortNumber,
        natv2PortMapExternalPoolIndex    Natv2PoolIndexOrZero,
        natv2PortMapSubscriberIndex      Natv2SubscriberIndexOrZero
    }

natv2PortMapInstanceIndex OBJECT-TYPE
    SYNTAX Natv2InstanceIndex
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Index of the NAT instance that created this port map entry."
    ::= { natv2PortMapEntry 1 }

natv2PortMapProtocol OBJECT-TYPE
    SYNTAX ProtocolNumber
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The map entry's upper-layer protocol number."
    ::= { natv2PortMapEntry 2 }

natv2PortMapExternalRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The realm to which natv2PortMapExternalAddress belongs."
    ::= { natv2PortMapEntry 3 }

natv2PortMapExternalAddressType OBJECT-TYPE
    SYNTAX InetAddressType
```

```
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Address type for the external realm.  A value other
         than ipv4(1) or ipv6(2) would be unexpected."
    ::= { natv2PortMapEntry 4 }

natv2PortMapExternalAddress OBJECT-TYPE
    SYNTAX InetAddress (SIZE (0..16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The mapping's assigned external address.  (This address is
         taken from the address pool identified by
         natv2PortMapExternalPoolIndex, if the implementation
         supports address pools and pools are configured for the
         given external realm.)  This is the source address for
         translated outgoing packets.  The address type is given
         by natv2PortMapExternalAddressType."

    ::= { natv2PortMapEntry 5 }

natv2PortMapExternalPort OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The mapping's assigned external port number.  This is the
         source port for translated outgoing packets.  If the internal
         port number given by natv2PortMapInternalPort is zero, this
         value MUST also be zero.  Otherwise, this MUST be a non-zero
         value."
    ::= { natv2PortMapEntry 6 }

natv2PortMapInternalRealm OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The realm to which natv2PortMapInternalRealmAddress belongs.
         In the general case, this realm contains the address that is
         being translated.  In the DS-Lite (RFC 6333) case, this realm
         defines the IPv6 address space from which the tunnel source
         address is taken.  The realm of the encapsulated IPv4 address
         is restricted in scope to the tunnel, so there is no point
         in identifying it separately."
    REFERENCE
        "DS-Lite: RFC 6333."
```

```
    ::= { natv2PortMapEntry 7 }

natv2PortMapInternalAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Address type for addresses in the realm identified by
         natv2PortMapInternalRealm."
    ::= { natv2PortMapEntry 8 }

natv2PortMapInternalAddress OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Source address for packets received under this mapping on
         the internal side of the NAT instance.  In the general case,
         this address is the same as the address given in
         natv2PortMapInternalMappedAddress.  In the DS-Lite case,
         natv2PortMapInternalAddress is the IPv6 tunnel source
         address.  The address type is given
         by natv2PortMapInternalAddressType."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
         the NAT mapping tables)."
    ::= { natv2PortMapEntry 9 }

natv2PortMapInternalMappedAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Internal address type actually translated by this mapping.
         Any value other than ipv4(1) or ipv6(2) would be unexpected.
         In the general case, this is the same as given by
         natv2AddressMapInternalAddressType.  In the DS-Lite
         case, the address type is ipv4(1)."
    REFERENCE
        "DS-Lite: RFC 6333."
   ::= { natv2PortMapEntry 10 }

natv2PortMapInternalMappedAddress OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

```
        "Internal address actually translated by this mapping.  In the
         general case, this is the same as
         natv2PortMapInternalRealmAddress.  The address type is given
         by natv2PortMapInternalMappedAddressType.

         In the case of DS-Lite (RFC 6333), this is the source
         address of the encapsulated IPv4 packet, normally selected
         from the well-known range 192.0.0.0/29.  The mapping in this
         case is considered to be from the external address to the
         combination of the IPv6 tunnel source address
         natv2PortMapInternalRealmAddress and the well-known IPv4
         inner source address natv2PortMapInternalMappedAddress."
    REFERENCE
        "DS-Lite: RFC 6333, Sections 5.7 (for well-known addresses)
         and 6.6 (on the need to have the IPv6 tunnel address in
         the NAT mapping tables)."
    ::= { natv2PortMapEntry 11 }

natv2PortMapInternalPort OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The mapping's internal port number.  If this is zero, ports
         are not translated (i.e., the NAT instance is a pure NAT
         rather than a Network Address and Port Translator (NAPT))."
    ::= { natv2PortMapEntry 12 }

natv2PortMapExternalPoolIndex OBJECT-TYPE
    SYNTAX Natv2PoolIndexOrZero
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Identifies the address pool from which the external address
         in this port map entry was taken.  Zero if the implementation
         does not support address pools but has chosen to support
         this object or if no pools are configured for the given
         external realm."
    ::= { natv2PortMapEntry 13 }

natv2PortMapSubscriberIndex OBJECT-TYPE
    SYNTAX Natv2SubscriberIndexOrZero
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Subscriber using this map entry.  Zero if the implementation
         does not support subscribers but has chosen to support
         this object."
```

```
    ::= { natv2PortMapEntry 14 }

-- Conformance section.  Specifies three cumulatively more extensive
-- applications: basic NAT, pooled NAT, and carrier-grade NAT.

natv2MIBConformance OBJECT IDENTIFIER ::= { natv2MIB 3 }

natv2MIBCompliances OBJECT IDENTIFIER ::= { natv2MIBConformance 1 }
natv2MIBGroups      OBJECT IDENTIFIER ::= { natv2MIBConformance 2 }

natv2MIBBasicCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "Describes the requirements for conformance to the basic NAT
         application of NATV2-MIB."
    MODULE  -- this module
        MANDATORY-GROUPS { natv2BasicNotificationGroup,
                           natv2BasicInstanceLevelGroup
                         }
    ::= { natv2MIBCompliances 1 }

natv2MIBPooledNATCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "Describes the requirements for conformance to the pooled NAT
         application of NATV2-MIB."
    MODULE  -- this module
        MANDATORY-GROUPS { natv2BasicNotificationGroup,
                           natv2BasicInstanceLevelGroup,
                           natv2PooledNotificationGroup,
                           natv2PooledInstanceLevelGroup
                         }
    ::= { natv2MIBCompliances 2 }

natv2MIBCGNCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "Describes the requirements for conformance to the
         carrier-grade NAT application of NATV2-MIB."
    MODULE  -- this module
        MANDATORY-GROUPS { natv2BasicNotificationGroup,
                           natv2BasicInstanceLevelGroup,
                           natv2PooledNotificationGroup,
                           natv2PooledInstanceLevelGroup,
                           natv2CGNNotificationGroup,
                           natv2CGNDeviceLevelGroup,
                           natv2CGNInstanceLevelGroup
                         }
```

```
    ::= { natv2MIBCompliances 3 }

-- Groups

natv2BasicNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
         natv2NotificationInstanceAddressMapEntriesHigh,
         natv2NotificationInstancePortMapEntriesHigh
    }
    STATUS  current
    DESCRIPTION
        "Notifications that MUST be supported by all NAT
         applications."
    ::= { natv2MIBGroups 1 }

natv2BasicInstanceLevelGroup OBJECT-GROUP
    OBJECTS {
-- from natv2InstanceTable
              natv2InstanceAlias,
              natv2InstancePortMappingBehavior,
              natv2InstanceFilteringBehavior,
              natv2InstanceFragmentBehavior,
              natv2InstanceAddressMapEntries,
              natv2InstancePortMapEntries,
              natv2InstanceTranslations,
              natv2InstanceAddressMapCreations,
              natv2InstanceAddressMapEntryLimitDrops,
              natv2InstanceAddressMapFailureDrops,
              natv2InstancePortMapCreations,
              natv2InstancePortMapEntryLimitDrops,
              natv2InstancePortMapFailureDrops,
              natv2InstanceFragmentDrops,
              natv2InstanceOtherResourceFailureDrops,
              natv2InstanceDiscontinuityTime,
              natv2InstanceThresholdAddressMapEntriesHigh,
              natv2InstanceThresholdPortMapEntriesHigh,
              natv2InstanceNotificationInterval,
              natv2InstanceLimitAddressMapEntries,
              natv2InstanceLimitPortMapEntries,
              natv2InstanceLimitPendingFragments,
-- from natv2ProtocolTable
              natv2ProtocolPortMapEntries,
              natv2ProtocolTranslations,
              natv2ProtocolPortMapCreations,
              natv2ProtocolPortMapFailureDrops,
-- from natv2AddressMapTable
              natv2AddressMapExternalRealm,
              natv2AddressMapExternalAddressType,
```

```
              natv2AddressMapExternalAddress,
-- from natv2PortMapTable
              natv2PortMapInternalRealm,
              natv2PortMapInternalAddressType,
              natv2PortMapInternalAddress,
              natv2PortMapInternalPort
            }
    STATUS current
    DESCRIPTION
        "Per-instance objects that MUST be supported by
         implementations of all NAT applications."
    ::= { natv2MIBGroups 2 }

natv2PooledNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
         natv2NotificationPoolUsageLow,
         natv2NotificationPoolUsageHigh
                  }
    STATUS  current
    DESCRIPTION
        "Notifications that MUST be supported by pooled and
         carrier-grade NAT applications."
    ::= { natv2MIBGroups 3 }

natv2PooledInstanceLevelGroup OBJECT-GROUP
    OBJECTS {
-- from natv2InstanceTable
                    natv2InstancePoolingBehavior,
-- from natv2PoolTable
                    natv2PoolRealm,
                    natv2PoolAddressType,
                    natv2PoolMinimumPort,
                    natv2PoolMaximumPort,
                    natv2PoolAddressMapEntries,
                    natv2PoolPortMapEntries,
                    natv2PoolAddressMapCreations,
                    natv2PoolPortMapCreations,
                    natv2PoolAddressMapFailureDrops,
                    natv2PoolPortMapFailureDrops,
                    natv2PoolDiscontinuityTime,
                    natv2PoolThresholdUsageLow,
                    natv2PoolThresholdUsageHigh,
                    natv2PoolNotifiedPortMapEntries,
                    natv2PoolNotifiedPortMapProtocol,
                    natv2PoolNotificationInterval,
-- from natv2PoolRangeTable
                    natv2PoolRangeBegin,
                    natv2PoolRangeEnd,
```

```
-- from natv2AddressMapTable
                  natv2AddressMapExternalPoolIndex,
-- from natv2PortMapTable
                  natv2PortMapExternalPoolIndex
            }
    STATUS current
    DESCRIPTION
        "Per-instance objects that MUST be supported by
         implementations of the pooled and carrier-grade
         NAT applications."
    ::= { natv2MIBGroups 4 }

natv2CGNNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
         natv2NotificationSubscriberPortMappingEntriesHigh
    }
    STATUS  current
    DESCRIPTION
        "Notification that MUST be supported by implementations
         of the carrier-grade NAT application."
    ::= { natv2MIBGroups 5 }

natv2CGNDeviceLevelGroup OBJECT-GROUP
    OBJECTS {
-- from table natv2SubscriberTable
              natv2SubscriberInternalRealm,
              natv2SubscriberInternalPrefixType,
              natv2SubscriberInternalPrefix,
              natv2SubscriberInternalPrefixLength,
              natv2SubscriberAddressMapEntries,
              natv2SubscriberPortMapEntries,
              natv2SubscriberTranslations,
              natv2SubscriberAddressMapCreations,
              natv2SubscriberPortMapCreations,
              natv2SubscriberAddressMapFailureDrops,
              natv2SubscriberPortMapFailureDrops,
              natv2SubscriberDiscontinuityTime,
              natv2SubscriberLimitPortMapEntries,
              natv2SubscriberThresholdPortMapEntriesHigh,
              natv2SubscriberNotificationInterval
            }
    STATUS current
    DESCRIPTION
        "Device-level objects that MUST be supported by the
         carrier-grade NAT application."
    ::= { natv2MIBGroups 6 }

natv2CGNInstanceLevelGroup OBJECT-GROUP
```

```
    OBJECTS {
   -- from natv2InstanceTable
              natv2InstanceSubscriberActiveLimitDrops,
              natv2InstanceLimitSubscriberActives,
   -- from natv2AddressMapTable
              natv2AddressMapInternalMappedAddressType,
              natv2AddressMapInternalMappedAddress,
              natv2AddressMapSubscriberIndex,
   -- from natv2PortMapTable
              natv2PortMapInternalMappedAddressType,
              natv2PortMapInternalMappedAddress,
              natv2PortMapSubscriberIndex
            }
    STATUS current
    DESCRIPTION
        "Per-instance objects that MUST be supported by the
         carrier-grade NAT application."
    ::= { natv2MIBGroups 7 }

END
```

5. Operational and Management Considerations

This section covers two particular areas of operations and management: configuration requirements and transition from or coexistence with the MIB module in [RFC4008].

5.1. Configuration Requirements

This MIB module assumes that the following information is configured on the NAT device by means outside the scope of the present document or is imposed by the implementation:

- the set of address realms to which the device connects;
- for the CGN application, per-subscriber information including subscriber index, address realm, assigned prefix or address, and (possibly) policies regarding address pool selection in the various possible address realms to which the subscriber may connect. In the particular case of DS-Lite [RFC6333] access, as well as the assigned outer-layer (IPv6) prefix or address, the subscriber information will include an inner (IPv4) source address, usually 192.0.0.2;
- the set of NAT instances running on the device, identified by NAT instance index and name;

- the port mapping, filtering, pooling, and fragment behavior for each NAT instance;
- the set of protocols supported by each NAT instance;
- for the pooled NAT and CGN applications, address pool information for each NAT instance, including for each pool the pool index, address realm, address type, minimum and maximum port number, the address ranges assigned to that pool, and policies for access to that pool's resources;
- static address and port map entries.

As described in previous sections, this MIB module does provide read-write objects for control of notifications (see especially Section 3.1.2) and limiting of resource consumption (Section 3.1.1). This document is written in advance of any practical experience with the setting of these values and can thus provide only general principles for how to set them.

By default, the MIB module definition disables notifications until they are explicitly enabled by the operator, using the associated threshold value to do so. To make use of the notifications, the operator may wish to take the following considerations into account.

Except for the low address pool utilization notification, the notifications imply that some sort of administrative action is required to mitigate an impending shortage of a particular resource. The choice of value for the triggering threshold needs to take two factors into account: the volatility of usage of the given resource, and the amount of time the operator needs to mitigate the potential overload situation. That time could vary from almost immediate to several weeks required to order and install new hardware or software.

To give a numeric example, if average utilization is going up 1% per week but can vary 10% around that average in any given hour, and it takes two weeks to carry through mitigating measures, the threshold should be set to 88% of the corresponding limit (two weeks' growth plus 10% volatility margin). If mitigating measures can be carried out immediately, this can rise to 90%. For this particular example, that change is insignificant, but in other cases the difference may be large enough to matter in terms of reduced load on the management plane.

The notification rate-limit settings really depend on the operator's processes but are a tradeoff between reliably reporting the notified condition and not having it overload the management plane. Reliability rises in importance with the importance of the resource

involved. Thus, the default notification intervals defined in this MIB module range from 10 seconds (high reliability) for the address and port map entry thresholds up to 60 seconds (lower reliability) for the per-subscriber port entry thresholds. Experience may suggest better values.

The limits on number of instance-level address map and port map entries and held fragments relate directly to memory allocations for these tables. The relationship between number of map entries or number of held fragments and memory required will be implementation-specific. Hence it is up to the implementor to provide specific advice on the setting of these limits.

The limit on simultaneous number of active subscribers is indirectly related to memory consumption for map entries, but also to processor usage by the NAT instance. The best strategy for setting this limit would seem to be to leave it disabled during an initial period while observing device processor utilization, then to implement a trial setting while observing the number of blocked packets affected by the new limit. The setting may vary by NAT instance if a suitable estimator of likely load (e.g., total number of hosts served by that instance) is available.

5.2. Transition from and Coexistence with NAT-MIB (RFC 4008)

A manager may have to deal with a mixture of devices supporting the NAT-MIB module [RFC4008] and the NATV2-MIB module defined in the present document. It is even possible that both modules are supported on the same device. The following discussion brings out the limits of comparability between the two MIB modules. A first point to note is that NAT-MIB is primarily focused on configuration, while NATV2-MIB is primarily focused on measurements.

To summarize the model used by [RFC4008]:

- The basic unit of NAT configuration is the interface.
- An interface connects to a single realm, either "private" or "public". In principle that means there could be multiple instances of one type of realm or the other, but the number is physically limited by the number of interfaces on the NAT device.
- Before the NAT can operate on a given interface, an "address map" has to be configured on it. The address map in [RFC4008] is equivalent to the pool tables in the present document. Since just one "address map" is configured per interface, this is the equivalent of a single address pool per interface.

- The address binding and port binding tables are roughly equivalent to the address map and port map tables in the present document in their content, but they can be either unidirectional or bidirectional. The model in [RFC4008] shows the address binding and port binding as alternative precursors to session establishment, depending on whether the device does address translation only or address and port translation. In contrast, NATV2-MIB assumes a model where bidirectional port mappings are based on bidirectional address mappings that have conceptually been established beforehand.

- The equivalent to an [RFC4008] session in NATV2-MIB would be a pair of port map entries. The added complexity in [RFC4008] is due to the modeling of NAT service types as defined in [RFC3489] (the symmetric NAT in particular) instead of the more granular set of behaviors described in [RFC4787]. (Note: [RFC3489] has been obsoleted by [RFC5389].)

With regard to that last point, the mapping between [RFC3489] service types and [RFC4787] NAT behaviors is as follows:

- A full cone NAT exhibits endpoint-independent port mapping behavior and endpoint-independent filtering behavior.

- A restricted cone NAT exhibits endpoint-independent port mapping behavior, but address-dependent filtering behavior.

- A port restricted cone NAT exhibits endpoint-independent port mapping behavior, but address-and-port-dependent filtering behavior.

- A symmetric NAT exhibits address-and-port-dependent port mapping and filtering behaviors.

Note that these NAT types are a subset of the types that could be configured according to the [RFC4787] behavioral classification used in NATV2-MIB, but they include the two possibilities (full and restricted cone NAT) that satisfy requirements REQ-1 and REQ-8 of [RFC4787]. Note further that other behaviors defined in [RFC4787] are not considered in [RFC4008].

Having established a context for discussion, we are now in a position to compare the outputs provided to management from the [RFC4008] and NATV2-MIB modules. This comparison relates to the ability to compare results if testing with both MIBs implemented on the same device during a transition period.

[RFC4008] provides three counters: incoming translations, outgoing translations, and discarded packets, at the granularities of interface, address map, and protocol, and incoming and outgoing translations at the levels of individual address bind, address port bind, and session entries. Implementation at the protocol and address map levels is optional. NATV2-MIB provides a single total (both directions) translations counter at the instance, protocol within instance, and subscriber levels. Given the differences in granularity, it appears that the only comparable measurement of translations between the two MIB modules would be through aggregation of the [RFC4008] interface counters to give a total number of translations for the NAT instance.

NATV2-MIB has broken out the single discard counter into a number of different counters reflecting the cause of the discard in more detail, to help in troubleshooting. Again, with the differing levels of granularity, the only comparable statistic would be through aggregation to a single value of total discards per NAT instance.

Moving on to state variables, [RFC4008] offers counts of number of "address map" (i.e., address pool) entries used (excluding static entries) at the address map level and number of entries in the address bind and address and port bind tables, respectively. Finally, [RFC4008] provides a count of the number of sessions currently using each entry in the address and port bind table. None of these counts are directly comparable with the state values offered by NATV2-MIB, because of the exclusion of static entries at the address map level, and because of the differing models of the translation tables between [RFC4008] and the NATV2-MIB.

6. Security Considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection opens devices to attack. These are the tables and objects and their sensitivity/vulnerability:

Limits: An attacker setting a very low or very high limit can easily cause a denial-of-service situation.

* natv2InstanceLimitAddressMapEntries;

* natv2InstanceLimitPortMapEntries;

* natv2InstanceLimitPendingFragments;

* natv2InstanceLimitSubscriberActives;

* natv2SubscriberLimitPortMapEntries.

Notification thresholds: An attacker setting an arbitrarily low threshold can cause many useless notifications to be generated (subject to the notification interval). Setting an arbitrarily high threshold can effectively disable notifications, which could be used to hide another attack.

* natv2InstanceThresholdAddressMapEntriesHigh;

* natv2InstanceThresholdPortMapEntriesHigh;

* natv2PoolThresholdUsageLow;

* natv2PoolThresholdUsageHigh;

* natv2SubscriberThresholdPortMapEntriesHigh.

Notification intervals: An attacker setting a low notification interval in combination with a low threshold value can cause many useless notifications to be generated.

* natv2InstanceNotificationInterval;

* natv2PoolNotificationInterval;

* natv2SubscriberNotificationInterval.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

Objects that reveal host identities: Various objects can reveal the identity of private hosts that are engaged in a session with external end nodes. A curious outsider could monitor these to assess the number of private hosts being supported by the NAT device. Further, a disgruntled former employee of an enterprise could use the information to break into specific private hosts by intercepting the existing sessions or originating new sessions into the host. If nothing else, unauthorized monitoring of these objects will violate individual subscribers' privacy.

* entries in the natv2SubscriberTable;

* entries in the natv2AddressMapTable;

* entries in the natv2PortMapTable.

Other objects that reveal NAT state: Other managed objects in this MIB may contain information that may be sensitive from a business perspective, in that they may represent NAT capabilities, business policies, and state information.

* natv2SubscriberLimitPortMapEntries;

* natv2InstancePortMappingBehavior;

* natv2InstanceFilteringBehavior;

* natv2InstancePoolingBehavior;

* natv2InstanceFragmentBehavior;

* natv2InstanceAddressMapEntries;

* natv2InstancePortMapEntries.

There are no objects that are sensitive in their own right, such as passwords or monetary amounts.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

Implementations SHOULD provide the security features described by the SNMPv3 framework (see [RFC3410]), and implementations claiming compliance to the SNMPv3 standard MUST include full support for authentication and privacy via the User-based Security Model (USM) [RFC3414] with the AES cipher algorithm [RFC3826]. Implementations MAY also provide support for the Transport Security Model (TSM) [RFC5591] in combination with a secure transport such as SSH [RFC5592] or TLS/DTLS [RFC6353].

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to

the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

7. IANA Considerations

IANA has assigned an object identifier to the natv2MIB module, with prefix iso.org.dod.internet.mgmt.mib-2 in the SMI Numbers registry [SMI-NUMBERS].

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <http://www.rfc-editor.org/info/rfc2578>.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, DOI 10.17487/RFC2579, April 1999, <http://www.rfc-editor.org/info/rfc2579>.

[RFC2580] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Conformance Statements for SMIv2", STD 58, RFC 2580, DOI 10.17487/RFC2580, April 1999, <http://www.rfc-editor.org/info/rfc2580>.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <http://www.rfc-editor.org/info/rfc3411>.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, DOI 10.17487/RFC3414, December 2002, <http://www.rfc-editor.org/info/rfc3414>.

[RFC3826] Blumenthal, U., Maino, F., and K. McCloghrie, "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model", RFC 3826, DOI 10.17487/RFC3826, June 2004, <http://www.rfc-editor.org/info/rfc3826>.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, DOI 10.17487/RFC4001, February 2005, <http://www.rfc-editor.org/info/rfc4001>.

[RFC4787] Audet, F., Ed. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, DOI 10.17487/RFC4787, January 2007, <http://www.rfc-editor.org/info/rfc4787>.

[RFC5591] Harrington, D. and W. Hardaker, "Transport Security Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 5591, DOI 10.17487/RFC5591, June 2009, <http://www.rfc-editor.org/info/rfc5591>.

[RFC5592] Harrington, D., Salowey, J., and W. Hardaker, "Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5592, DOI 10.17487/RFC5592, June 2009, <http://www.rfc-editor.org/info/rfc5592>.

[RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <http://www.rfc-editor.org/info/rfc6353>.

8.2. Informative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, DOI 10.17487/RFC2663, August 1999, <http://www.rfc-editor.org/info/rfc2663>.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <http://www.rfc-editor.org/info/rfc3410>.

[RFC3489] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, DOI 10.17487/RFC3489, March 2003, <http://www.rfc-editor.org/info/rfc3489>.

[RFC4008] Rohit, R., Srisuresh, P., Raghunarayan, R., Pai, N., and C. Wang, "Definitions of Managed Objects for Network Address Translators (NAT)", RFC 4008, DOI 10.17487/RFC4008, March 2005, <http://www.rfc-editor.org/info/rfc4008>.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, DOI 10.17487/RFC5389, October 2008, <http://www.rfc-editor.org/info/rfc5389>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC7658] Perreault, S., Tsou, T., Sivakumar, S., and T. Taylor, "Deprecation of MIB Module NAT-MIB: Managed Objects for Network Address Translators (NATs)", RFC 7658, DOI 10.17487/RFC7658, October 2015, <http://www.rfc-editor.org/info/rfc7658>.

[SMI-NUMBERS] IANA, "Structure of Management Information (SMI) Numbers (MIB Module Registrations)", <http://www.iana.org/assignments/smi-number>.

Authors' Addresses

Simon Perreault
Jive Communications
Quebec, QC
Canada

Email: sperreault@jive.com

Tina Tsou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
China

Email: tina.tsou.zouting@huawei.com

Senthil Sivakumar
Cisco Systems
7100-8 Kit Creek Road
Research Triangle Park, North Carolina 27709
United States

Phone: +1 919 392 5158
Email: ssenthil@cisco.com

Tom Taylor
PT Taylor Consulting
Ottawa
Canada

Email: tom.taylor.stds@gmail.com