Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 20, 2012

S. Perreault
Viagenie
T. Tsou
Huawei Technologies (USA)
S. Sivakumar
Cisco Systems
June 18, 2012

Additional Managed Objects for Network Address Translators (NAT)
draft-ietf-behave-nat-mib-01

Abstract

This memo defines a portion of the Management Information Base (MIB) for devices implementing Network Address Translator (NAT) function. This MIB module may be used for monitoring of a device capable of NAT function.

Status of this Memo

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

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

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

This Internet-Draft will expire on December 20, 2012.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
2. Overview 3
3. Definitions 4
4. Security Considerations 26
5. IANA Considerations 26
6. References 26
6.1. Normative References 26
6.2. Informative References 27
Appendix A. Change Log (to be removed by RFC Editor prior to publication) 27
A.1. Changed in -01 27
Authors' Addresses 27

1. Introduction

[RFC4008] defines some objects for managing network address translators (NATs). Current operational practice often requires additional objects, in particular for enterprise and Internet service provider (ISP) deployments. This document defines those additional objects.

This module is designed to be completely independent from [RFC4008]. A NAT implementation could be managed using this module, the one from [RFC4008], or both.

2. Overview

New features in this module are as follows:

Counters: Many new counters are introduced. Most of them are available in two variants: global and per-transport protocol.

Limits: A few limits on the quantity of state data stored by the NAT device. Some of them can trigger notifications.

Address+Port Pools: Pools of external addresses and ports are often used in enterprise and ISP settings. Pools are listed in a table, each with its range of addresses and ports. It is possible to inspect each pool's usage, to set limits, and to receive notifications when thresholds are crossed.

Address Mappings: NATs that have an "IP address pooling" behavior of "Paired" [RFC4787] maintain a mapping from internal address to external address. This module allows inspection of this mapping table.

Mapping table indexed by external 3-tuple: It is often necessary to determine the internal address that is mapped to a given external address and port. This MIB provides this table with an index to accomplish this efficiently, without having to iterate over all mappings.

Per-subscriber counters, limits, and notifications: Carrier-Grade NATs operate with a notion of "subscriber", to which are associated a set of counters, limits, and notifications. The subscriber identifier may not necessarily be an internal address, as in the case of DS-Lite, where the identifier is the IPv6 address of the tunnel endpoint and the internal addresses are the same for each subscriber.

3. Definitions

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

```
NEW-NAT-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Counter64, Gauge32,
    Integer32, Unsigned32, mib-2
        FROM SNMPv2-SMI

    OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
        FROM SNMPv2-CONF

    TEXTUAL-CONVENTION
        FROM SNMPv2-TC

    InetAddressType, InetAddress, InetAddressPrefixLength,
    InetPortNumber
        FROM INET-ADDRESS-MIB;

newNatMIB MODULE-IDENTITY
    LAST-UPDATED "200001010000Z"
    ORGANIZATION "TBD"
    CONTACT-INFO "TBD"
    DESCRIPTION
        "This MIB module defines generic managed objects for NAT."

    REVISION "200001010000Z"
    DESCRIPTION
        "Dummy version. RFC Editor must replace this."

    ::= { mib-2 9999 }


-- table of contents

newNatNotifications     OBJECT IDENTIFIER ::= { newNatMIB 0 }
newNatObjects           OBJECT IDENTIFIER ::= { newNatMIB 1 }
    newNatCounters      OBJECT IDENTIFIER ::= { newNatObjects 1 }
    newNatLimits        OBJECT IDENTIFIER ::= { newNatObjects 2 }
    newNatPoolObjects   OBJECT IDENTIFIER ::= { newNatObjects 3 }
    newNatMapObjects    OBJECT IDENTIFIER ::= { newNatObjects 4 }
    newNatSubscribers   OBJECT IDENTIFIER ::= { newNatObjects 5 }
newNatConformance       OBJECT IDENTIFIER ::= { newNatMIB 2 }
    newNatGroups        OBJECT IDENTIFIER ::= { newNatConformance 1 }
    newNatCompliance    OBJECT IDENTIFIER ::= { newNatConformance 2 }
```

```
-- textual conventions

ProtocolNumber ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "A transport protocol number, from the 'protocol-numbers' IANA
         registry."
    SYNTAX Unsigned32 (0..255)

NatPoolIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
        "A unique ID that is assigned to each pool."
    SYNTAX Unsigned32 (1..4294967295)


-- notifications

newNatNotifPoolWatermarkLow NOTIFICATION-TYPE
    OBJECTS { newNatPoolIndex }
    STATUS current
    DESCRIPTION
        "This notification is generated when the specified pool's number
         of free addresses becomes lower than or equal to the specified
         threshold. The threshold is specified by the
         newNatPoolWatermarkLow object"
    ::= { newNatNotifications 1 }

newNatNotifPoolWatermarkHigh NOTIFICATION-TYPE
    OBJECTS { newNatPoolIndex }
    STATUS current
    DESCRIPTION
        "This notification is generated when the specified pool's number
         of free addresses becomes greater than or equal to the
         specified threshold. The threshold is specified by the
         newNatPoolWatermarkHigh object"
    ::= { newNatNotifications 2 }

newNatNotifMappings NOTIFICATION-TYPE
    OBJECTS { newNatCntMappings }
    STATUS current
    DESCRIPTION
        "This notification is generated when newNatCntMappings exceeds
         the value of newNatMappingsNotifyThreshold."
    ::= { newNatNotifications 3 }
```

```
newNatNotifAddrMappings NOTIFICATION-TYPE
    OBJECTS { newNatCntAddressMappings }
    STATUS current
    DESCRIPTION
        "This notification is generated when newNatCntAddressMappings
         exceeds the value of newNatAddrMapNotifyThreshold."
    ::= { newNatNotifications 4 }

newNatNotifSubscriberMappings NOTIFICATION-TYPE
    OBJECTS { newNatSubscriberCntMappings }
    STATUS current
    DESCRIPTION
        "This notification is generated when newNatSubscriberCntMappings
         exceeds the value of newNatSubscriberMapNotifyThresh, unless
         newNatSubscriberMapNotifyThresh is zero.."
    ::= { newNatNotifications 5 }


-- counters

newNatCntTranslates OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT has been applied."
    ::= { newNatCounters 1 }

newNatCntOOP OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         no external port was available, excluding quota limitations."
    ::= { newNatCounters 2 }

newNatCntResource OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         of resource constraints (excluding out-of-ports condition)."
    ::= { newNatCounters 3 }

newNatCntStateMismatch OBJECT-TYPE
    SYNTAX Counter64
```

```
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         of mapping state mismatch. For example, a TCP packet that
         matches an existing mapping but is dropped because its flags
         are incompatible with the current state of the mapping would
         cause this counter to be incremented."
    ::= { newNatCounters 4 }

newNatCntQuota OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         of quota limitations. Quotas include absolute limits as well as
         limits on rate of allocation."
    ::= { newNatCounters 5 }

newNatCntMappings OBJECT-TYPE
    SYNTAX Gauge32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of currently active mappings.

         Equal to newNatCntMapRemovals - newNatCntMapCreations."
    ::= { newNatCounters 6 }

newNatCntMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mapping creations. This includes static mappings."
    ::= { newNatCounters 7 }

newNatCntMapRemovals OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mapping removals. This includes static mappings."
    ::= { newNatCounters 8 }

newNatCntAddressMappings OBJECT-TYPE
    SYNTAX Gauge32
```

```
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of active address mappings.

         Equal to newNatCntAddrMapRemovals - newNatCntAddrMapCreations."
    ::= { newNatCounters 9 }

newNatCntAddrMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of address mapping creations. This includes static
         mappings."
    ::= { newNatCounters 10 }

newNatCntAddrMapRemovals OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of address mapping removals. This includes static
         mappings."
    ::= { newNatCounters 11 }

newNatCntProtocolTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatCntProtocolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of protocols with per-protocol counters."
    ::= { newNatCounters 128 }

newNatCntProtocolEntry OBJECT-TYPE
    SYNTAX NewNatCntProtocolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Per-protocol counters."
    INDEX { newNatCntProtocolNumber }
    ::= { newNatCntProtocolTable 1 }

NewNatCntProtocolEntry ::=
    SEQUENCE {
        newNatCntProtocolNumber         ProtocolNumber,
        newNatCntProtocolTranslates     Counter64,
        newNatCntProtocolOOP            Counter64,
```

```
        newNatCntProtocolResource       Counter64,
        newNatCntProtocolStateMismatch  Counter64,
        newNatCntProtocolQuota          Counter64,
        newNatCntProtocolMappings       Gauge32,
        newNatCntProtocolMapCreations   Counter64,
        newNatCntProtocolMapRemovals    Counter64
    }

newNatCntProtocolNumber OBJECT-TYPE
    SYNTAX ProtocolNumber
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Counters in this conceptual row apply to packets using the
         transport protocol identified by this object's value."
    ::= { newNatCntProtocolEntry 1 }

newNatCntProtocolTranslates OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT has been applied."
    ::= { newNatCntProtocolEntry 2 }

newNatCntProtocolOOP OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         no external port was available."
    ::= { newNatCntProtocolEntry 3 }

newNatCntProtocolResource OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         of resource constraints (excluding out-of-ports condition)."
    ::= { newNatCntProtocolEntry 4 }

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

```
        "The number of packets to which NAT could not be applied because
         of state table mismatch. For example, a TCP packet that matches
         an existing mapping but is dropped because its flags are
         incompatible with the current state of the mapping would cause
         this counter to be incremented."
    ::= { newNatCntProtocolEntry 5 }

newNatCntProtocolQuota OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets to which NAT could not be applied because
         of exceeded quotas. Quotas include absolute limits as well as
         limits on rate of allocation."
    ::= { newNatCntProtocolEntry 6 }

newNatCntProtocolMappings OBJECT-TYPE
    SYNTAX Gauge32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of active mappings.

         Equal to newNatCntMapRemovals - newNatCntMapCreations."
    ::= { newNatCntProtocolEntry 7 }

newNatCntProtocolMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mapping creations. This includes static mappings."
    ::= { newNatCntProtocolEntry 8 }

newNatCntProtocolMapRemovals OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mapping removals. This includes statis mappings."
    ::= { newNatCntProtocolEntry 9 }


-- limits

newNatLimitMappings OBJECT-TYPE
    SYNTAX Unsigned32
```

```
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Global limit on the total number of mappings. Zero means
         unlimited."
    ::= { newNatLimits 1 }
-- TODO: How does that work with bulk port allocation?

newNatMappingsNotifyThreshold OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "See newNatNotifMappings."
    ::= { newNatLimits 2 }

newNatLimitAddressMappings OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Global limit on the total number of internal-to-external
         address mappings.  Zero means unlimited.

         This limit is only applicable to NATs that have an 'IP address
         pooling' behavior of 'Paired' [RFC4787]."
    ::= { newNatLimits 3 }

newNatAddrMapNotifyThreshold OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "See newNatNotifAddrMappings."
    ::= { newNatLimits 4 }

newNatLimitFragments OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Global limit on the total number of fragments pending
         reassembly.  Zero means unlimited.

         This limit is only applicable to NATs having 'Receive
         Fragments Out of Order' behavior [RFC4787]."
    ::= { newNatLimits 5 }
```

```
newNatLimitSubscribers OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Global limit on the number of subscribers with active mappings.
         Zero means unlimited."
    ::= { newNatLimits 6 }


-- pools

newNatPoolTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatPoolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of pools."
    ::= { newNatPoolObjects 1 }

newNatPoolEntry OBJECT-TYPE
    SYNTAX NewNatPoolEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Entry in the table of pools."
    INDEX { newNatPoolIndex }
    ::= { newNatPoolTable 1 }

NewNatPoolEntry ::=
    SEQUENCE {
        newNatPoolIndex         NatPoolIndex,
        newNatPoolUsage         Integer32,
        newNatPoolWatermarkLow  Integer32,
        newNatPoolWatermarkHigh Integer32,
        newNatPoolPortMin       InetPortNumber,
        newNatPoolPortMax       InetPortNumber
        -- TODO: virtual router ID, status, ref count, etc.
    }

newNatPoolIndex OBJECT-TYPE
    SYNTAX NatPoolIndex
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Index of an address pool."
    ::= { newNatPoolEntry 1 }
```

```
newNatPoolUsage OBJECT-TYPE
    SYNTAX Integer32 (0..100)
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Percentage of the pool's total number of external ports
         currently mapped."
    ::= { newNatPoolEntry 2 }

newNatPoolWatermarkLow OBJECT-TYPE
    SYNTAX Integer32 (-1|0..100)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Low watermark on a pool's usage, in percentage of the total
         number of ports available. If set to -1, the watermark is
         disabled. Otherwise when newNatPoolUsage becomes lower than or
         equal to newNatPoolWatermarkLow, a notification is sent. The
         NAT may also start behaving in low usage mode (this is
         implementation-defined)."
    ::= { newNatPoolEntry 3 }

newNatPoolWatermarkHigh OBJECT-TYPE
    SYNTAX Integer32 (-1|0..100)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "High watermark on a pool's usage, in percentage of the total
         number of ports available. If set to -1, the watermark is
         disabled. Otherwise, when newNatPoolUsage becomes higher than
         or equal to newNatPoolWatermarkHigh, a notification is sent.
         The NAT may also start behaving in high usage mode (this is
         implementation-defined)."
    ::= { newNatPoolEntry 4 }

newNatPoolPortMin OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Minimal port number to be allocated in this pool."
    ::= { newNatPoolEntry 5 }

newNatPoolPortMax OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
```

```
        "Maximal port number to be allocated in this pool."
    ::= { newNatPoolEntry 6 }


newNatPoolRangeTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatPoolRangeEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "This table contains address ranges used by pool entries."
    ::= { newNatPoolObjects 2 }

newNatPoolRangeEntry OBJECT-TYPE
    SYNTAX NewNatPoolRangeEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "NAT pool address range."
    INDEX { newNatPoolRangeType,
            newNatPoolRangeBegin }
    ::= { newNatPoolRangeTable 1 }

NewNatPoolRangeEntry ::=
    SEQUENCE {
        newNatPoolRangePoolIndex        NatPoolIndex,
        newNatPoolRangeType             InetAddressType,
        newNatPoolRangeBegin            InetAddress,
        newNatPoolRangeEnd              InetAddress,
        newNatPoolRangeAllocatedPorts   Gauge32
        -- TODO: the usual bookkeeping things
    }

newNatPoolRangePoolIndex OBJECT-TYPE
    SYNTAX NatPoolIndex
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Index of the address pool to which this address range belongs.
         See newNatPoolIndex."
    ::= { newNatPoolRangeEntry 1 }

newNatPoolRangeType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The address type of newNatPoolRangeBegin and
         newNatPoolRangeEnd."
```

```
    ::= { newNatPoolRangeEntry 2 }

newNatPoolRangeBegin OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Lowest address included in this range."
    ::= { newNatPoolRangeEntry 3 }

newNatPoolRangeEnd OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Highest address included in this range."
    ::= { newNatPoolRangeEntry 4 }

newNatPoolRangeAllocatedPorts OBJECT-TYPE
    SYNTAX Gauge32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of ports currently allocated on the addresses in this
         range."
    ::= { newNatPoolRangeEntry 5 }


-- indexed mapping tables

newNatMapIntAddrTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatMapIntAddrEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of mappings from internal to external address.

         This table is only applicable to NATs that have an 'IP address
         pooling' behavior of 'Paired' [RFC4787]."
    ::= { newNatMapObjects 1 }

newNatMapIntAddrEntry OBJECT-TYPE
    SYNTAX NewNatMapIntAddrEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Mapping from internal to external address."
    INDEX { newNatMapIntAddrType,
```

```
            newNatMapIntAddrInt }
    ::= { newNatMapIntAddrTable 1 }

NewNatMapIntAddrEntry ::=
    SEQUENCE {
        newNatMapIntAddrType    InetAddressType,
        newNatMapIntAddrInt     InetAddress,
        newNatMapIntAddrExt     InetAddress
    }

newNatMapIntAddrType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Address type for newNatMapIntAddrInt and newNatMapIntAddrExt."
    ::= { newNatMapIntAddrEntry 1 }

newNatMapIntAddrInt OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Internal address."
    ::= { newNatMapIntAddrEntry 2 }

newNatMapIntAddrExt OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "External address."
    ::= { newNatMapIntAddrEntry 3 }

newNatMappingTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatMappingTableEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table of mappings indexed by external 3-tuple."
    ::= { newNatMapObjects 2 }

newNatMappingTableEntry OBJECT-TYPE
    SYNTAX NewNatMappingTableEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "A single NAT mapping."
```

```
    INDEX { newNatMappingProto,
            newNatMappingExtAddressType,
            newNatMappingExtAddress,
            newNatMappingExtPort }
    ::= { newNatMappingTable 1 }

NewNatMappingTableEntry ::=
    SEQUENCE {
        newNatMappingProto          ProtocolNumber,
        newNatMappingExtAddressType InetAddressType,
        newNatMappingExtAddress     InetAddress,
        newNatMappingExtPort        InetPortNumber,
        newNatMappingIntAddressType InetAddressType,
        newNatMappingIntAddress     InetAddress,
        newNatMappingIntPort        InetPortNumber,
        newNatMappingPool           NatPoolIndex
    }

newNatMappingProto OBJECT-TYPE
    SYNTAX ProtocolNumber
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The mapping's transport protocol number."
    ::= { newNatMappingTableEntry 1 }

newNatMappingExtAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Type of the mapping's external address."
    ::= { newNatMappingTableEntry 2 }

newNatMappingExtAddress OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The mapping's external address. If this is the undefined
         address, all external addresses are mapped to the internal
         address."
    ::= { newNatMappingTableEntry 3 }

newNatMappingExtPort OBJECT-TYPE
    SYNTAX InetPortNumber
    MAX-ACCESS not-accessible
    STATUS current
```

```
    DESCRIPTION
        "The mapping's external port number. If this is zero, all
         external ports are mapped to the internal port."
    ::= { newNatMappingTableEntry 4 }

newNatMappingIntAddressType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Type of the mapping's internal address."
    ::= { newNatMappingTableEntry 5 }

newNatMappingIntAddress OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The mapping's internal address. If this is the undefined
         address, addresses are not translated."
    ::= { newNatMappingTableEntry 6 }

newNatMappingIntPort 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."
    ::= { newNatMappingTableEntry 7 }

newNatMappingPool OBJECT-TYPE
    SYNTAX NatPoolIndex (0|1..4294967295)
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Index of the pool that contains this mapping's external address
         and port. If zero, no pool is associated with this mapping."
    ::= { newNatMappingTableEntry 8 }


-- subscribers

newNatSubscribersTable OBJECT-TYPE
    SYNTAX SEQUENCE OF NewNatSubscribersTableEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
```

```
        "Table of CGN subscribers."
    ::= { newNatSubscribers 1 }

newNatSubscribersTableEntry OBJECT-TYPE
    SYNTAX NewNatSubscribersTableEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Each entry describes a single CGN subscriber."
    INDEX { newNatSubscriberIdentifierType,
            newNatSubscriberIdentifier }
    ::= { newNatSubscribersTable 1 }

NewNatSubscribersTableEntry ::=
    SEQUENCE {
        newNatSubscriberIdentifierType      InetAddressType,
        newNatSubscriberIdentifier          InetAddress,
        newNatSubscriberIntPrefixType       InetAddressType,
        newNatSubscriberIntPrefix           InetAddress,
        newNatSubscriberIntPrefixLength     InetAddressPrefixLength,
        newNatSubscriberPool                NatPoolIndex,
        newNatSubscriberCntTranslates       Counter64,
        newNatSubscriberCntOOP              Counter64,
        newNatSubscriberCntResource         Counter64,
        newNatSubscriberCntStateMismatch    Counter64,
        newNatSubscriberCntQuota            Counter64,
        newNatSubscriberCntMappings         Gauge32,
        newNatSubscriberCntMapCreations     Counter64,
        newNatSubscriberCntMapRemovals      Counter64,
        newNatSubscriberLimitMappings       Unsigned32,
        newNatSubscriberMapNotifyThresh     Unsigned32
    }

newNatSubscriberIdentifierType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Address type of the subscriber identifier."
    ::= { newNatSubscribersTableEntry 1 }

newNatSubscriberIdentifier OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Address used for uniquely identifying the subscriber.
```

```
         In traditional NAT, this is the internal address assigned to
         the CPE. In case an address range is assigned to a subscriber,
         the first address in the range is used as identifier. For
         tunnelled connectivity (e.g., DS-Lite [RFC6333]), the outer
         address is used as identifier (i.e., the IPv6 address in the
         case of DS-Lite)."
    ::= { newNatSubscribersTableEntry 2 }

newNatSubscriberIntPrefixType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Subscriber's internal prefix type."
    ::= { newNatSubscribersTableEntry 3 }

newNatSubscriberIntPrefix OBJECT-TYPE
    SYNTAX InetAddress
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Prefix assigned to a subscriber's CPE."
    ::= { newNatSubscribersTableEntry 4 }

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

newNatSubscriberPool OBJECT-TYPE
    SYNTAX NatPoolIndex
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "External address pool to which this subscriber belongs."
    ::= { newNatSubscribersTableEntry 6 }

newNatSubscriberCntTranslates OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets received from or sent to this subscriber
```

```
         and to which NAT has been applied."
    ::= { newNatSubscribersTableEntry 7 }

newNatSubscriberCntOOP OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets received from this subscriber to which
         NAT could not be applied because no external port was
         available, excluding quota limitations."
    ::= { newNatSubscribersTableEntry 8 }

newNatSubscriberCntResource OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets received from this subscriber to which
         NAT could not be applied because of resource constraints
         (excluding out-of-ports condition)."
    ::= { newNatSubscribersTableEntry 9 }

newNatSubscriberCntStateMismatch OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets received from or destined to this
         subscriber to which NAT could not be applied because of mapping
         state mismatch. For example, a TCP packet that matches an
         existing mapping but is dropped because its flags are
         incompatible with the current state of the mapping would cause
         this counter to be incremented."
    ::= { newNatSubscribersTableEntry 10 }

newNatSubscriberCntQuota OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The number of packets received from or destined to this
         subscriber to which NAT could not be applied because of quota
         limitations. Quotas include absolute limits as well as limits
         on the rate of allocation."
    ::= { newNatSubscribersTableEntry 11 }

newNatSubscriberCntMappings OBJECT-TYPE
```

```
    SYNTAX Gauge32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of currently active mappings created by or for this
         subscriber.

         Equal to newNatSubscriberCntMapRemovals -
         newNatSubscriberCntMapCreations."
    ::= { newNatSubscribersTableEntry 12 }

newNatSubscriberCntMapCreations OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mappings created by or for this subscriber."
    ::= { newNatSubscribersTableEntry 13 }

newNatSubscriberCntMapRemovals OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of mappings removed by or for this subscriber."
    ::= { newNatSubscribersTableEntry 14 }

newNatSubscriberLimitMappings OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Limit on the number of active mappings created by or for this
         subscriber. Zero means unlimited."
    ::= { newNatSubscribersTableEntry 15 }

newNatSubscriberMapNotifyThresh OBJECT-TYPE
    SYNTAX Unsigned32
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "See newNatNotifSubscriberMappings."
    ::= { newNatSubscribersTableEntry 16 }


-- conformance groups

newNatGroupBasicObjects OBJECT-GROUP
```

```
    OBJECTS { newNatCntTranslates,
              newNatCntOOP,
              newNatCntResource,
              newNatCntStateMismatch,
              newNatCntQuota,
              newNatCntMappings,
              newNatCntMapCreations,
              newNatCntMapRemovals,
              newNatCntProtocolTranslates,
              newNatCntProtocolOOP,
              newNatCntProtocolResource,
              newNatCntProtocolStateMismatch,
              newNatCntProtocolQuota,
              newNatCntProtocolMappings,
              newNatCntProtocolMapCreations,
              newNatCntProtocolMapRemovals,
              newNatLimitMappings,
              newNatMappingsNotifyThreshold,
              newNatPoolIndex,
              newNatPoolUsage,
              newNatPoolWatermarkLow,
              newNatPoolWatermarkHigh,
              newNatPoolPortMin,
              newNatPoolPortMax,
              newNatPoolRangePoolIndex,
              newNatPoolRangeEnd,
              newNatPoolRangeAllocatedPorts,
              newNatMappingIntAddressType,
              newNatMappingIntAddress,
              newNatMappingIntPort,
              newNatMappingPool }
    STATUS current
    DESCRIPTION
        "Basic counters, limits, and thresholds."
    ::= { newNatGroups 1 }

newNatGroupAddrMapObjects OBJECT-GROUP
    OBJECTS { newNatCntAddressMappings,
              newNatCntAddrMapCreations,
              newNatCntAddrMapRemovals,
              newNatLimitAddressMappings,
              newNatAddrMapNotifyThreshold,
              newNatMapIntAddrExt }
    STATUS current
    DESCRIPTION
        "Objects that require 'Paired IP address pooling' behavior
         [RFC4787]."
    ::= { newNatGroups 2 }
```

```
newNatGroupFragmentObjects OBJECT-GROUP
    OBJECTS { newNatLimitFragments }
    STATUS current
    DESCRIPTION
        "Objects that require 'Receive Fragments Out of Order' behavior
         [RFC4787]."
    ::= { newNatGroups 3 }

newNatGroupSubscriberObjects OBJECT-GROUP
    OBJECTS { newNatSubscriberIntPrefixType,
              newNatSubscriberIntPrefix,
              newNatSubscriberIntPrefixLength,
              newNatSubscriberPool,
              newNatSubscriberCntTranslates,
              newNatSubscriberCntOOP,
              newNatSubscriberCntResource,
              newNatSubscriberCntStateMismatch,
              newNatSubscriberCntQuota,
              newNatSubscriberCntMappings,
              newNatSubscriberCntMapCreations,
              newNatSubscriberCntMapRemovals,
              newNatSubscriberLimitMappings,
              newNatSubscriberMapNotifyThresh,
              newNatLimitSubscribers }
    STATUS current
    DESCRIPTION
        "Per-subscriber counters, limits, and thresholds."
    ::= { newNatGroups 4 }

newNatGroupBasicNotifications NOTIFICATION-GROUP
    NOTIFICATIONS { newNatNotifPoolWatermarkLow,
                    newNatNotifPoolWatermarkHigh,
                    newNatNotifMappings }
    STATUS current
    DESCRIPTION
        "Basic notifications."
    ::= { newNatGroups 5 }

newNatGroupAddrMapNotifications NOTIFICATION-GROUP
    NOTIFICATIONS { newNatNotifAddrMappings }
    STATUS current
    DESCRIPTION
        "Notifications about address mappings."
    ::= { newNatGroups 6 }

newNatGroupSubscriberNotifs NOTIFICATION-GROUP
    NOTIFICATIONS { newNatNotifSubscriberMappings }
    STATUS current
```

```
    DESCRIPTION
        "Notifications about subscribers."
    ::= { newNatGroups 7 }


-- compliance statements

newNatBasicCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "Basic compliance with this MIB is attained when the objects
         contained in the mandatory groups are implemented."
    MODULE  -- this module
        MANDATORY-GROUPS { newNatGroupBasicObjects,
                           newNatGroupBasicNotifications }
    ::= { newNatCompliance 1 }

newNatAddrMapCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "NATs that have 'Paired IP address pooling' behavior [RFC4787]
         and implement the objects in this group can claim this level of
         compliance."
    MODULE  -- this module
        MANDATORY-GROUPS { newNatGroupBasicObjects,
                           newNatGroupBasicNotifications,
                           newNatGroupAddrMapObjects,
                           newNatGroupAddrMapNotifications }
    ::= { newNatCompliance 2 }

newNatFragmentsCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "NATs that have 'Receive Fragments Out of Order' behavior
         [RFC4787] and implement the objects in this group can claim
         this level of compliance."
    MODULE  -- this module
        MANDATORY-GROUPS { newNatGroupBasicObjects,
                           newNatGroupBasicNotifications,
                           newNatGroupFragmentObjects }
    ::= { newNatCompliance 3 }

newNatCGNCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "NATs that have 'Paired IP address pooling' and 'Receive
         Fragments Out of Order' behavior [RFC4787] and implement the
         objects in this group can claim this level of compliance.
```

```
         This level of compliance is to be expected of a CGN compliant
         with [I-D.ietf-behave-lsn-requiremnents]."
    MODULE  -- this module
        MANDATORY-GROUPS { newNatGroupBasicObjects,
                           newNatGroupBasicNotifications,
                           newNatGroupAddrMapObjects,
                           newNatGroupAddrMapNotifications,
                           newNatGroupFragmentObjects,
                           newNatGroupSubscriberObjects,
                           newNatGroupSubscriberNotifs }
    ::= { newNatCompliance 4 }


END
```

4. Security Considerations

TBD

5. IANA Considerations

TBD

6. References

6.1. Normative References

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

6.2. Informative References

[RFC4008] Rohit, R., Srisuresh, P., Raghunarayan, R., Pai, N., and C. Wang, "Definitions of Managed Objects for Network Address Translators (NAT)", RFC 4008, March 2005.

Appendix A. Change Log (to be removed by RFC Editor prior to publication)

A.1. Changed in -01

- Added CGN stuff (per-subscriber quotas, counters, notifications).
- Added conformance groups and compliance statements.
- Added mapping table indexed by external 3-tuple.

Authors' Addresses

Simon Perreault
Viagenie
246 Aberdeen
Quebec, QC G1R 2E1
Canada

Phone: +1 418 656 9254
Email: simon.perreault@viagenie.ca
URI: http://viagenie.ca

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com

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

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