Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 13, 2012

S. Perreault
Viagenie
T. Tsou
Huawei Technologies (USA)
S. Sivakumar
Cisco Systems

April 11, 2012

Additional Definitions of Managed Objects for Network Address Translators (NAT)
draft-perreault-behave-new-nat-mib-00

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 October 13, 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 3
4. Security Considerations 15
5. IANA Considerations 15
6. References 16
6.1. Normative References 16
6.2. Informative References 16
Authors' Addresses 16

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.

Note: "CGN" features are currently left out of this MIB. Such features include anything related to "subscribers": per-subscriber counters, limits, etc. They will either be added to this draft or will be specified in a separate draft. Stay tuned.

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.

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

    TEXTUAL-CONVENTION
        FROM SNMPv2-TC

    InetAddressType, InetAddress, 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 }
newNatConformance       OBJECT IDENTIFIER ::= { newNatMIB 2 }
    newNatGroups        OBJECT IDENTIFIER ::= { newNatConformance 1 }
    newNatCompliance    OBJECT IDENTIFIER ::= { newNatConformance 2 }
-- TODO: We need to be able to manage multiple NATs (with possible
-- overlapping address space) with a single SNMP agent.


-- 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 }

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

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


-- 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."
    ::= { 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 exceeded quotas. 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 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?

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 2 }
```

```
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 3 }


-- 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,
            newNatPoolRangeEnd }
    ::= { newNatPoolRangeTable 1 }

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

newNatPoolRangeType OBJECT-TYPE
    SYNTAX InetAddressType
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "The address type of newNatPoolRangeBegin and
         newNatPoolRangeEnd."
    ::= { newNatPoolRangeEntry 1 }

newNatPoolRangeBegin OBJECT-TYPE
    SYNTAX InetAddress (SIZE (4|16))
    MAX-ACCESS not-accessible
    STATUS current
```

```
    DESCRIPTION
        "Lowest address included in this range."
    ::= { newNatPoolRangeEntry 2 }

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

newNatPoolRangeAllocatedPorts OBJECT-TYPE
    SYNTAX Gauge32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Number of ports currently allocated on the addresses in this
         range."
    ::= { newNatPoolRangeEntry 4 }


-- address mappings

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 }


-- conformance groups

-- TBD

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.

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