

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 10, 2013

S. Perreault
Viagenie
T. Tsou
Huawei Technologies (USA)
S. Sivakumar
Cisco Systems
July 9, 2012

Managed Objects for Carrier Grade NAT (CGN)
draft-perreault-sunset4-cgn-mib-00

Abstract

This memo defines a portion of the Management Information Base (MIB) that may be used for monitoring of a device capable of Carrier Grade 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 January 10, 2013.

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. Terminology	3
3. Overview	3
4. Definitions	3
5. Security Considerations	9
6. IANA Considerations	9
7. Normative References	9
Authors' Addresses	9

1. Introduction

[I-D.ietf-behave-nat-mib] defines objects for managing network address translators (NATs). This document builds on top of it, defining objects specifically for Carrier Grade NATs (CGN).

2. Terminology

The "CGN" term is defined in [I-D.ietf-behave-lsn-requirements].

3. Overview

New features in this module are as follows:

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.

4. Definitions

The following objects are added to the MIB module defined in [I-D.ietf-behave-nat-mib].

-- notifications

```
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 }
```

-- limits

```
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 }

-- subscribers

newNatSubscribers OBJECT IDENTIFIER ::= { newNatObjects 5 }

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

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 }

-- compliance statements

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-requirements]."
    MODULE -- this module
    MANDATORY-GROUPS { newNatGroupBasicObjects,
```



```
newNatGroupBasicNotifications,  
newNatGroupAddrMapObjects,  
newNatGroupAddrMapNotifications,  
newNatGroupFragmentObjects,  
newNatGroupSubscriberObjects,  
newNatGroupSubscriberNotifs }  
 ::= { newNatCompliance 4 }
```

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Normative References

[I-D.ietf-behave-lsn-requirements]
Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A.,
and H. Ashida, "Common requirements for Carrier Grade NATs
(CGNs)", draft-ietf-behave-lsn-requirements-07 (work in
progress), June 2012.

[I-D.ietf-behave-nat-mib]
Perreault, S., Tsou, T., and S. Sivakumar, "Additional
Managed Objects for Network Address Translators (NAT)",
draft-ietf-behave-nat-mib-01 (work in progress),
June 2012.

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

