IPv4 Header Option For User Identification In CGN Scenario
draft-chen-intarea-v4-uid-header-option-00

Abstract

   In some application scenarios, it is necessary to be able to identify
   an user when CGN is deployed. This document defines a new IPv4
   header option for host identification, which contains NAT mapping
   information, e.g. the internal source IP address before translation.
   Each time a NAT device performs translation on an IP packet, NAT
   mapping information will be added in the IP header. With the NAT
   mapping information, it will be easy to identify a host.

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 September 8, 2011.

Copyright Notice

Table of Contents

1. Introduction

   Some existing applications, e.g. web server, FTP server, etc, may
   need to perform operations based on the user's IP address, e.g.,
   controlling the number of sessions, anti-virus filtering, traffic
   control against malicious attack, account security assistance, etc.

   In the initial phase of IPv6 transition, CGNs are deployed to resolve
   the IPv4 public address depletion problem. Due to dynamic address
   mapping, some services and applications which require the knowledge
   of the source address will have problems. It is possible to query
   NAT log server or CGN to find out a user's source address
   [ID.draft-zhang-v6ops-cgn-source-trace], but this will impose high
   performance requirements on the NAT log server or CGN, and usually
   this kind of service is only available for law enforcement department
   of the operators themselves.

   If the address mapping information is carried as an IPv4 header
   option, it will help those services and applications work, with
   minimum impact to the network.

   An alternative solution is proposed by draft-wing-nat-reveal-option
   [draft-wing-nat-reveal-option]. The solution is based on TCP option;
   although quite some interesting applications are based on TCP, but
   there are still some scenarios it cannot cover, e.g., user traffic
   monitoring and analysis, and some UDP based applications.

1.1. Requirements Language

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Terminology

   The following terms are used in this document:

   BNG: Broadband Network Gateway

   CPE: Customer Premises Equipment

   CGN: Carrier Grade NAT

   UID: User Identification

   UE: User Equipment

2. Motivating Scenarios

```
   +--------------+                    +--------------+     +---------+
   |              |                    |              |     |         |
 +------+    +-----+  +---------+  +-----+      +-----+   | Public  |
 | CUST |____| CPE |__| Accesss |__| BNG |_____| CGN |___|  IPv4   |
 | UE   |    | NAT |  | Network |  |     |      |     |   | Network |
 +------+    +-----+  +---------+  +-----+      +-----+   |         |
   | Customer LAN |                    | Provider LAN |     +---------+
   +--------------+                    +--------------+
```

Figure 1: NAT444 Deployment

Dynamic IP address mapping in CGN will cause problems for services
and applications which require knowledge of the source IP address.
This section describes some typical scenarios where normal operations
cannot be carried out without some mitigating measures such as those
proposed in this document.

2.1. Limit The Number Of Sessions From An IP Address

Some download services need to limit the number of concurrent
sessions from a same IP address. But if CGN is deployed, multiple
users may be sharing the same IP address, so that such a mechanism
will prevent some users from accessing services properly.

2.2. Anti-virus Filtering And Limiting Malicious Attack Traffic

Some existing traffic monitoring and analysis devices gather
statistics and perform analysis, to enable anti-virus filtering based
on the source IP address of packets. Some servers apply security
policies based on source IP address to prevent malicious attacks
[RFC4732]. For example, servers can refuse malicious users according
to their source IP address to prevent drunk mail, malicious
registration, etc. Deployment of CGN will impact the correct
operation of traffic monitoring and analysis.

2.3. Account Security Assistance

Some existing services provide user account security guarantees by
combining authentication and the user's IP address. For example, the
server can log the user's IP address each time the user logs in, and
if the user logs in with an IP address different from the last one or
the most often used one, the server can inform the user, and may ask
the user for extra authentication information. The deployment of CGN
will stop this kind of assistance from working.

3. User Identification (UID) IPv4 Header Option

3.1. Option Format

   The UID option consists of an option header and one or more instances
   of the NAT Mapping sub-option. The NAT Mapping sub-option is
   described in the next section. The UID option is illustrated in
   Figure 2.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |     Num       |   Reserved    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    :                                                               :
    :                         NAT Mapping(s)                        :
    :                                                               :
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                 Figure 2: UID IPv4 Header Option Format

   The fields of the option header are defined as follows:

   Type:

      The option type, which has the format specified in [RFC0791] and
      the following specific sub-field values:

      Copied flag: 1 (copy into fragments)

      Option class: 2 (debugging and measurement)

      Option number: TBD.

   Length:

      Total length of the option in octets. As specified in [RFC0791],
      the length value includes the Type and Length octets in its count.
      Also as specified in [RFC0791], the maximum value of Length is 40
      octets minus the length of any other IPv4 header options that are
      present.

   Num:

      The number of appended NAT Mapping sub-option instances.

   Reserved: always 0.

3.2. NAT Mapping Sub-option

   Each instance of the NAT Mapping sub-option records the source of the
   packet from the point of view of the NAT adding that instance.
   Depending on the scenario, that source can be identified by an IPv4
   address, IPv6 address, or one of several types of tunnel plus host or
   context identifier, depending on whether DS Lite or Gateway-Initiated
   DS Lite is used. The format of the NAT Mapping sub-option is shown
   in Figure 3.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| IdTyp |TIdTyp |    Sequence   |   TId Length  |    Pointer    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Context/Host Identifier (depending on IdTyp)         :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Tunnel Identifier (depending on TIdTyp)               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                              |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
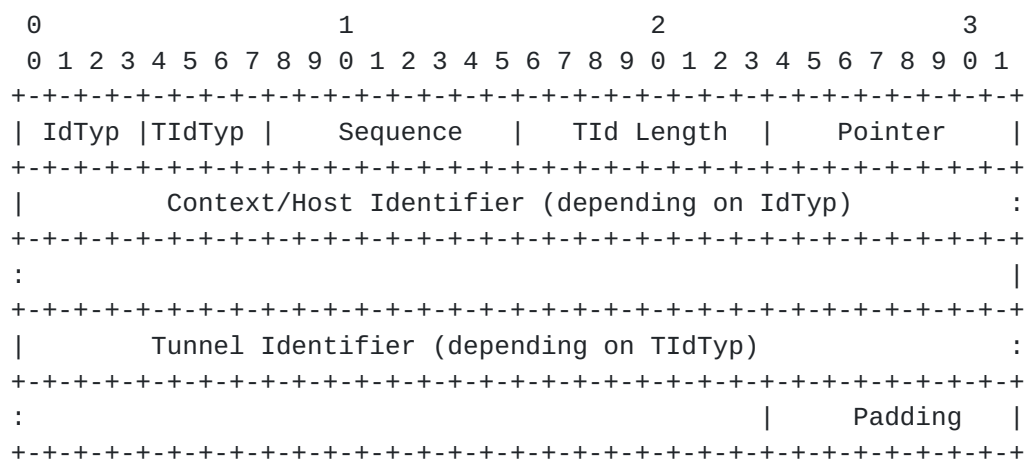
                  Figure 3: NAT Mapping Sub-option Format

   The fields of the NAT Mapping sub-option are as follows:

   IdTyp:

      Type of context or host identifier. For native transport, this is
      either IPv4 address or IPv6 address. For DS Lite [ID.DS-Lite], it
      is always IPv4 address. For Gateway-Initiated DS Lite
      [ID.GI-DS-Lite], it is the type of the context identifier. This
      document specifies the following values for IdTyp:

         00: reserved;

         01: IPv4 address;

         02: IPv6 address;

         03: GRE key;

         04: IPv6 Flow Label.

All other values are reserved.

TIdTyp:

   Type of tunnel identifier. For native IP transport, this is NULL.
   For DS Lite, it is IPv6 address. For Gateway-Initiated DS Lite,
   it can be IPv4 or IPv6 address or MPLS VPN ID. Hence this
   document specifies the following values for TIdTyp:

      00: NULL;

      01: IPv4 address;

      02: IPv6 address;

      03: MPLS VPN ID.

   All other values are reserved.

Sequence:

   Sequence number of the NAT Mapping sub-option instance, indicating
   the order in which it was added to the option. The sequence
   number is assigned to the instance when it is created, and never
   changes after that. As a result, downstream entities can know if
   instances have been deleted because of lack of space if the first
   instance present in the option does not have a sequence number
   equal to 1.

TId Length:

   Length of the tunnel identifier. This is equal to 0 if the TIdTyp
   is NULL, 4 if the TIdTyp is IPv4 address, 16 if the TIdTyp is IPv6
   address, and 7 if the TIdTyp is MPLS VPN ID.

Pointer:

   The sum of the lengths of the Context/Host Identifier field, the
   Tunnel Identifier field, and the Padding field, effectively
   pointing to the end of the sub-option instance.

Context/Host Identifier:

   The source address of the incoming packet, for native transport.
   The source address of the decapsulated packet, for DS Lite. The
   context identifier value, for Gateway-Initiated DS Lite. The
   length of this field is 16 for an IPv6 address and 4 for all other
   types. A context identifier of type Flow Label MUST be

constructed by placing the Flow Label in the least significant
bits of the word in network byte order and setting the most
significant bits to zeroes.

Tunnel Identifier:

For native transport, this field is empty. For tunneled
transport, it is the IPv4 or IPv6 source address in the outer
header or the MPLS VPN ID of the tunnel.

Padding:

Always 0. Present only when needed to extend the Tunnel
Identifier to a four-octet boundary (i.e., when the identifier is
an MPLS VPN ID).

3.3. Procedures

3.3.1. Procedures At a NAT

If a NAT conforming to this specification receives a packet that it
will forward as an IPv4 packet, then:

o if the incoming packet (after decapsulation if applicable) was an
   IPv6 packet, or if it was an IPv4 packet but contained no UID
   header option, and if sufficient space exists in the IPv4 header
   to permit it, the NAT MUST add the UID option containing a single
   instance of the NAT Mapping sub-option. The sequence number of
   the instance MUST be 1.

o if the incoming packet (after decapsulation if applicable) is an
   IPv4 packet containing the UID header option, the NAT MUST append
   an instance of the NAT Mapping sub-option to the existing sequence
   of instances. The sequence number of the new instance MUST be the
   sequence number of the preceding instance incremented by 1. For
   the settings of the remaining fields of the instance, see below.
   If the result is to cause the IPv4 header to exceed its limit of
   60 octets [RFC0791], the NAT MUST delete the NAT Mapping sub-
   option with the lowest sequence number from the UID option. The
   NAT MUST repeat this action until the IPv4 header length does not
   exceed 60 octets. If as a result, no more sub-option instances
   remain in the UID option, the NAT MUST delete the option itself.

In either case, the remaining fields are set according to the
particular transport mechanism in use.

3.3.2. Procedures At an Edge Device Or Firewall

   Depending on local policy, edge routers or firewalls conforming to
   this specification MAY strip off the UID option on the outgoing
   interfaces if necessary, e.g., because the application server or end
   user may not be able to recognize the UID option, or because there
   may be potential interoperability issues in the communication between
   ISPs due to this option. In this case, the UID option is still
   useful for user traffic monitoring and analysis in the operator's
   network.

3.3.3. Procedures At Other Routers

   Other routers along the packet path should pass the option along
   unchanged and copy it to fragments when fragmentation occurs, simply
   in conformity to [RFC0791]. For greater certainty, routers
   conforming to this specification MUST behave as just described.

4. Maximum Transmission Unit

   Because IPv4 header options are inserted into packets, which will
   change the length of an IP packet, a NAT Device MUST modify the MTU
   value in an ICMP message accordingly when receiving or generating a
   ICMP Packet Too Big error message.

5. NAT configuration

   There SHOULD be a configurable parameter on the NAT for the
   administrator to enable/disable use of the UID option.

6. Impact To Existing Devices

   The UID option is in the IP header, and complies with the format
   defined in [RFC0791]. As mentioned in Section 3.3.3, any network
   devices that fully support [RFC0791] should handle the UID option
   without any change. User terminal devices do not have to support
   this option.

   Resolving the user identification problem via the UID option protects
   the existing investment and does not require extra cost while being
   compatible with existing user and network devices. Obviously the
   consuming applications such as download services, traffic monitoring
   and analysis, and enhanced identification need to be modified to make
   use of the information provided by the UID option.

7. Security Considerations

   TBD.

8. IANA Considerations

   This document defines a new IPv4 option type, which shall be
   allocated by IANA. This requires IANA to set up a new registry for
   IPv4 options. The initial population of this registry consists of
   the options defined in [RFC0791], plus the new option added by this
   specification. [Need to determine if any other options have been
   defined. Registry format to be added later.]

9. Acknowledgements

   To be completed.

10. References

10.1. Informative References

   [RFC4732]   Handley, M., Rescorla, E., and IAB, "Internet Denial-of-
               Service Considerations", RFC 4732, December 2006.

   [draft-wing-nat-reveal-option]
               Yourtchenko, A. and D. Wing, "Revealing hosts sharing an
               IP address using TCP option(work in progress)",
               August 2010.

10.2. Normative References

   [ID.DS-Lite]
               Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
               Stack Lite Broadband Deployments Following IPv4 Exhaustion
               (Work in progress)", March 2011.

   [ID.GI-DS-Lite]
               Brockners, F., Gundavelli, S., Speicher, S., and D. Ward,
               "Gateway Initiated Dual-Stack Lite Deployment(work in
               progress)", Oct 2010.

   [ID.draft-zhang-v6ops-cgn-source-trace]
               zhang, D., "Solution Model of Source Address Tracing for
               Carrier Grade NAT (CGN)(work in progress)",
               February 2011.

   [RFC0791]   Postel, J., "Internet Protocol", STD 5, RFC 791,
               September 1981.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

   Youming Wu
   China Telecom
   109, Zhongshan Ave. West, Tianhe District
   Guangzhou 510630
   P.R. China

   Phone:
   Email: wuym@gsta.com

   Hui Ji
   China Telecom
   NO19.North Street,CHAOYANGMEN,DONGCHENG District
   Beijing
   P.R. China

   Phone:
   Email: jihui@chinatelecom.com.cn

   Qi Chen (editor)
   China Telecom
   109, Zhongshan Ave. West, Tianhe District
   Guangzhou 510630
   P.R. China

   Phone:
   Email: chenqi.0819@gmail.com

   Tina Tsou (editor)
   Huawei Technologies
   Bantian, Longgang District
   Shenzhen 518129
   P.R. China

   Phone:
   Email: tena@huawei.com