Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: November 09, 2013

Z. Chen
China Telecom
C. Zhou
Huawei Technologies
T. Tsou
Huawei Technologies (USA)
T. Taylor
Huawei Technologies

May 08, 2013

Syslog Format for NAT Logging
draft-ietf-behave-syslog-nat-logging-01

Abstract

With the wide deployment of Carrier Grade NAT (CGN) devices, the logging of NAT-related events has become very important for legal purposes. The logs may be required to identify a host that was used to launch malicious attacks or engage in illegal behaviour, and/or may be required for accounting purposes. This document identifies the events that need to be logged and the parameters that are required in the logs depending on the context in which the NAT is being used. It goes on to standardize formats for reporting these events and parameters using SYSLOG (RFC 5424). A companion document specifies formats for reporting the same events and parameters using IPFIX (RFC 5101). Applicability statements are provided in this document and its companion to guide operators and implementors in their choice of which technology to use for logging.

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 November 09, 2013.

Table of Contents

1. Introduction

Operators already need to record the addresses assigned to subscribers at any point in time, for operational and regulatory reasons. When operators introduce NAT devices which support address sharing (e.g., Carrier Grade NATs (CGNs)) into their network, additional information has to be logged. This document and [I-D.behave-ipfix-nat-logging] are provided in order to standardize the events and parameters to be recorded at the NAT, using SYSLOG [RFC5424] and IPFIX [RFC5101] respectively. The content proposed to be logged by the two documents is exactly the same, but as will be seen, the choice of which to use in a given scenario is an engineering issue.

Detailed logging requirements will vary depending on the context in which they are used. For example, different methods for transition from IPv4 to IPv6 require different events and different parameters to be logged. Section 2 covers this topic. That same section also

has a brief discussion of possible architectural arrangements under which log generation is carried out.

Section 3 provides a more detailed description of the events that need logging and the parameters that may be required in the logs.

The use of SYSLOG [RFC5424] has advantages and disadvantages compared with the use of IPFIX [RFC5101]. Section 4 provides a statement of applicability for the SYSLOG approach.

Section 5 specifies SYSLOG record formats for logging of the events and parameters described in Section 3. The definitions provide the flexibility to vary actual log contents based on the requirements of the particular deployment.

Despite the discussion of IPv6 transition technologies, this document is limited to logging of events observed at NAT devices only. Logging of other events associated with IPv6 transition is out of scope.

1.1. Terminology

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 "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

This document uses the term "Session" as it is defined in Section 2.3 of [RFC2663] and the term Binding Information Base (BIB) as it is defined in Section 2 of [RFC6146].

2. Deployment Considerations

This section deals with two major topics. The first is a review of the major IPv4 to IPv6 transition methods and what they imply for NAT logging. This flows into the second topic, which is the different architectural contexts within which NAT logging may occur. Of course, not all NAT usage occurs in conjunction with IP transition, and traditional NAT usage is also considered.

2.1. NAT Logging Requirements For Different Transition Methods

A number of transition technologies have been or are being developed to aid in the transition from IPv4 to IPv6. 6rd [RFC5969] and DS-Lite [RFC6333] are at the deployment stage. Several 'stateless' technologies: Public IPv4 over IPv6 [I-D.softwire-public-4over6], MAP-E [I-D.softwire-map], and Lightweight 4over6 [I-D.softwire-lw4over6] have seen experimental deployment and are in

the process of being standardized at the time of writing of this document.

Of the technologies just listed, 6rd and Public IPv4 over IPv6 do not involve NATs and hence need not be considered further. The other techniques involve NAT at the customer edge, at the border router, or both, and hence are in scope.

A DS-Lite Address Family Transition Router (AFTR) includes a large-scale session-stateful NAT44 processing potentially millions of sessions per second. The special character of AFTR operation over that of a traditional NAT44 is that the source IPv4 addresses of the interior hosts may not be unique. As a consequence, the session tables need to include the IPv6 addresses used to encapsulate the packets outgoing from those hosts. See Section 6.6 of [RFC6333].

The DS-Lite customer edge equipment (the 'B4') may also perform NAT44 functions, but these will be similar to the functions performed by traditional NAT44 devices. This document therefore does not include any requirements specific to the B4.

To reduce the volume of potential logging at the DS-Lite AFTR, there have been proposals to assign groups of ports to the B4 at one time, assuming that the assignment can be coordinated between the B4 and the AFTR. Examples of such proposals include [I-D.tsou-behave-natx4-log-reduction] and [I-D.pcp-port-set]. If bulk port assignment is implemented, then instead of logging individual sessions the AFTR will log address binding and bulk port assignment events. Depending on the number of ports assigned at once, this could reduce the volume of logs by one or two orders of magnitude, but at the cost of reducing the average number of subscribers that can share one IPv4 address.

Lightweight 4over6 and MAP-E both require NAT44 operation at the customer equipment, with an added restriction on port number usage. The functions of the customer equipment (the "unified CPE") are specified in [I-D.softwire-unified-cpe]. A mapping between an IPv4 address (in general, shared between subscribers), an IPv6 address used for the encapsulating tunnel to the border router, and an assigned set of port numbers defined by a port set identifier is provisioned rather than established dynamically. The unified CPE may log this mapping when it receives it, but it is more likely that any such logging is performed by service provider infrastructure. This document therefore does not recognize any specific requirements for logging of sessions, address bindings, or port assignments at the unified CPE.

The unified CPE does experience one event unique to its operation. The border router, for either Lightweight 4over6 or MAP-E, is required to monitor port usage by outgoing IPv4 packets. If the ports used by a host fall outside its configured port set, the border router may return an ICMPv6 type 1, code 5 (source address failed ingress/egress policy) error message to the unified CPE. Receipt of such error messages at the unified CPE indicates inconsistency of configuration between the unified CPE and the border router. It is also possible for the same reason that the unified CPE receives incoming IPv4 packets with destination port numbers outside of its assigned range.

The log reporting this event should capture the port set configured on the unified CPE. For both Lightweight 4over6 and MAP-E, this is associated with an identifier, the port set identifier (PSID). In the case of Lightweight 4over6, the actual set of port numbers can be calculated from the combination of the PSID value and the size of the single contiguous range of ports assigned to the CPE. In the case of MAP-E, the default assignment consists of a series of equally sized and equally spaced ranges, so the calculation needs the range spacing as well as the range size. Normally, just logging the PSID should be sufficient for debugging misconfigurations.

2.2. Architectural Context

The architectural context within which logging is deployed is an important factor in the rate at which logs need to be recorded. The required logging rate in turn determines whether SYSLOG is a practical solution. See the discussion of feasible logging rates in Section 4.

The three basic contexts we can consider are logging at provisioning time, logging of NAT bindings or sessions triggered by new packet flows at the customer edge, and logging of NAT sessions at a carrier grade NAT (CGN).

Logging at provisioning time is applicable when resources such as address bindings and port blocks are allocated at provisioning time and not as new packet flows are detected. This is true of several of the transition methods discussed in Section 2.1. As mentioned in that section, the basic data from which logs are generated can be captured by DHCP servers or by AAA. The details are out of scope for this document.

The Port Control Protocol (PCP) [RFC6887] and its port set extension [I-D.pcp-port-set] can be viewed as a way to provision by other means. However, PCP can be invoked on a per-flow basis, so the volume of logs generated by PCP can be closer to the volume that has

to be recorded in the other architectural contexts mentioned above and discussed below. The volume really depends on how PCP is being used in a specific network.

Logging at the customer edge (or at the ISP edge for NATs protecting the ISP's internal networks) may be done by the customer for purposes of internal management, or by the ISP for its own administrative and regulatory purposes. Given the likelihood of a high internal community of interest, it is possible but unlikely that a NAT at the edge of a large enterprise network processes a number of new packet flows per second which is comparable to the volume handled by a carrier grade NAT. Most customer edge NATs will handle a much smaller volume of flows.

The volume of new flows per second processed by a carrier grade NAT can rise into the millions. This has a major impact on the applicability of SYSLOG to logging of CGN sessions.

3. NAT-Related Events and Parameters

The events which follow were initially gleaned, in the words of the authors of [I-D.behave-ipfix-nat-logging], from [RFC4787] and [RFC5382]. Some details were subsequently informed by the discussion in Section 2. Since the present document deals with SYSLOG rather than IPFIX, the timestamp and the event type will appear in the log header rather than as an explicit part of the structured data portion of the log. Hence they are omitted from the parameter tabulations that follow.

The listed parameters include an optional NAT identifier and an optional NAT type in each case. The NAT identifier is potentially useful only if the HOSTNAME field in the log header identifies an off-board device rather than the NAT itself. The NAT type identifies which of the NAT types listed in Table 1 is reporting the event.

Reference will be made below to a subscriber-identifying address parameter. For traditional NATs, the source IPv4 address (for NAT44) or IPv6 address (for NAT64) is sufficient. For the transition methods discussed in Section 2.1, which are all based on IPv4-in-IPv6 tunnels, the subscriber site is identified by the IPv6 tunnel endpoint address provisioned to that site. In the case of DS-Lite, as mentioned already, the source IPv4 address is not meaningful, and in the case of Lightweight 4over6 and MAP-E the IPv4 address may be shared. Table 1 summarizes this information for concise reference below.

NAT Type	Subscriber-Identifying Address

Traditional NAT44	Pre-NAT IPv4 source address
----	----
Traditional NAT64	Pre-NAT IPv6 source address
----	----
DS-Lite AFTR (Note)	Encapsulating IPv6 source address
----	----
Unified CPE	Encapsulating IPv6 source address

Note: for Gateway-Initiated DS-Lite [RFC6674], the encapsulating protocol may not be IPv6. In that case the subscriber-identifying address consists of the combination of the softwire identifier (SWID) and the context identifier (CID). See [RFC6674].

Table 1: Subscriber-Identifying Address, By NAT Type

3.1. NAT Session Creation and Deletion

NAT session creation and deletion events are recorded when a binding to a specific destination address and port is recorded in or deleted from the session database. See the discussion in Section 3 of [RFC6146]. The following specific events are defined:

- NAT Session Creation
- NAT Session Deletion

These take the same parameters for all types of NAT, aside from the variation in subscriber-identifying address noted above:

- NAT type (OPTIONAL);
- NAT identifier (OPTIONAL);
- VLAN identifier or VPN Routing and Forwarding (VRF) identifier (OPTIONAL);
- Subscriber-identifying address (see Table 1) (MANDATORY);
- Post-NAT source IPv4 address (MANDATORY);
- Protocol identifier (MANDATORY);
- Source port or ICMP identifier (MANDATORY);
- Post-NAPT source port or ICMP identifier (MANDATORY);

- Destination IPv4 (for NAT44) or IPv6 (for NAT64) address (OPTIONAL);
- Post-NAT destination IPv4 address (OPTIONAL);
- Post-NAPT destination port or ICMP identifier (OPTIONAL);
- Address realm (internal or external) of the source of the packet triggering the creation of the session (OPTIONAL).

Note that [RFC6888] recommends against destination logging because of the privacy issues it creates. The pre-NAT value of destination address will differ from the post-NAT value only in a double-NAT situation. Hence in most cases even with destination logging the pre-NAT value will not be recorded.

3.2. Binding Information Base (BIB) Entry Creation and Deletion

By definition, a BIB entry refers to a destination-independent mapping between a source transport address and a post-NAT source transport address. The parameters for the BIB entry creation and deletion events reflect this difference from NAT session creation and deletion. Moreover, BIB entry creation is always triggered by a packet from an internal source. The BIB events are:

- NAT BIB entry Creation
- NAT BIB entry Deletion

These events have the following parameters:

- NAT type (OPTIONAL);
- NAT identifier (OPTIONAL);
- VLAN identifier or VPN Routing and Forwarding (VRF) identifier (OPTIONAL);
- Subscriber-identifying address (see Table 1) (MANDATORY);
- Post-NAT source IPv4 address (MANDATORY);
- Protocol identifier (MANDATORY);
- Source port or ICMP identifier (MANDATORY);
- Post-NAPT source port or ICMP identifier (MANDATORY);

3.3. Address Binding Event

This event reports when a given source address has been bound to an external source address. An address binding occurs when the first packet in the first flow from the host in the internal realm is received at the NAT. It MAY occur under other circumstances (e.g., PCP request, or NAT policy permits assignment of a new external address due to port conflict). The event parameters are:

- NAT type (OPTIONAL);
- NAT identifier (OPTIONAL);
- Subscriber-identifying address (see Table 1) (MANDATORY);
- Post-NAT source IPv4 address (MANDATORY);

3.4. Port Block Allocation and Deallocation

This event is reported when a block of ports/ICMP identifiers is allocated or deallocated to a given address binding, rather than allocating individual ports as individual flows are recognized. The same allocation applies to each protocol supported by the NAT. The parameters for this event are:

- NAT type (OPTIONAL);
- NAT identifier (OPTIONAL);
- Subscriber-identifying address (see Table 1) (MANDATORY);
- Post-NAT source IPv4 address (MANDATORY);
- Starting port number (OPTIONAL);
- Ending port number (OPTIONAL);
- Port range size (OPTIONAL);
- Range step size (OPTIONAL).

Flexibility is provided to report a single range of ports (using starting port number and ending port number) or a series of equally spaced ranges (using starting port number, port range size, range step size, and optionally the ending port number). Where a series of ranges is being allocated, the interpretation of the parameters is as follows:

- starting port number is the first (lowest) port number in the first range;

- port range size is the number of ports in each allocated range, with a minimum value of 1;

- Range step size is the number of port numbers between corresponding values in subsequent ranges. Hence the starting port for a given range is some multiple of range step size plus the value of the starting port number parameter.

- Ending port number is the highest port value allocated (i.e., the final port number in the final range). This is needed only if that value is less than the last value defined by the other parameters that would not exceed 65535.

3.5. NAT Address Exhaustion Event

This event will be generated when a NAT device runs out of global IPv4 addresses in a given pool of addresses. Typically, this event would mean that the NAT device will not be able to create any new translations until some addresses or ports are freed. This event takes the following parameters:

- NAT type (OPTIONAL);

- NAT identifier (OPTIONAL);

- address pool identifier (MANDATORY).

3.6. Port Exhaustion Event

This event will be generated when a NAT device runs out of ports for a global IPv4 address. Port exhaustion shall be reported per protocol (UDP, TCP, etc.). The event parameters are:

- NAT type (OPTIONAL);

- NAT identifier (OPTIONAL);

- Post-NAT source IPv4 address (MANDATORY);

- Protocol identifier (MANDATORY).

3.7. Quota Exceeded Event

This event is reported when the NAT cannot allocate a new session or BIB entry because of an administratively imposed limit. The parameters of this event are:

- NAT type (OPTIONAL);
- NAT identifier (OPTIONAL);
- quota limit type (MANDATORY);
- VLAN identifier or VPN Routing and Forwarding (VRF) identifier (OPTIONAL);
- Subscriber-identifying address (see Table 1) (OPTIONAL);
- Protocol identifier (OPTIONAL).

The possible limit types are on the number of sessions, number of BIB entries, and global number of NAT entries. These limits may apply to an individual protocol, in which case the protocol identifier MUST be present. The limits may apply to an user, in which case a subscriber-identifying address MUST be present. Alternatively, the limits apply to a domain identified by a VLAN or VRF identifier which MUST then be present.

3.8. Invalid Port Detected

As discussed in Section 2.1, this event may be reported at a unified CPE, either through receipt of ICMP error messages or by direct observation of incoming IPv4 packets. It takes the following parameters:

- NAT identifier (OPTIONAL);
- Subscriber-identifying address. For the unified CPE, this is always the encapsulating IPv6 address. (MANDATORY);
- port set identifier provisioned to the unified CPE (MANDATORY);
- port range size (OPTIONAL);
- range step size (OPTIONAL).

Port range size is always applicable but, as shown above, is optional to record. Range step size is not applicable for Lightweight 4over6, which allocates a single contiguous range of ports to the CPE.

4. SYSLOG Applicability

The primary advantage of SYSLOG is the human readability and searchability of its contents. In addition, it has built-in priority and severity fields that allow for separate routing of reports requiring management action. Finally, it has a well-developed underpinning of transport and security protocol infrastructure.

SYSLOG presents two obstacles to scalability: the fact that the records will typically be larger than records based on a binary protocol such as IPFIX, and, depending on the architectural context, the reduced performance of a router that is forced to do text manipulation in the data plane. One has to conclude that for larger message volumes, IPFIX should be preferred as the reporting medium on the NAT itself. It is possible that SYSLOG could be used as a back-end format on an off-board device processing IPFIX records in real time, but this would give a limited boost to scalability. One concern expressed in list discussion is that when the SYSLOG formatting process gets overloaded records will be lost.

As a result, the key question is what the practical cutoff point is for the expected volume of SYSLOG records, on-board or off-board the NAT. This obviously depends on the computing power of the formatting platform, and also on the record lengths being generated.

Information has been provided to the BEHAVE list at the time of writing to the effect that one production application is generating an average of 150,000 call detail records per second, varying in length from 500 to 1500 bytes. Capacities several times this level have been reported involving shorter records, but this particular application has chosen to limit the average in order to handle peaks.

As illustrated by the examples in Section 5.3, typical record sizes for the high-volume logs are in the order of 150 to 200 bytes, so throughput capacity should be higher than in the call detail case for the same amount of computing power. In private communication, a discussant has noted a practical limit of a few hundred thousand SYSLOG records per second on a router.

5. SYSLOG Record Format For NAT Logging

This section describes the SYSLOG record format for NAT logging in terms of the field names used in [RFC5424] and specified in Section 6 of that document. In particular, this section specifies values for the APP-NAME and MSGID fields in the record header, the SD-ID identifying the STRUCTURED-DATA section, and the PARAM-NAMEs and PARAM-VALUE types for the individual possible parameters within that section. The specification is in three parts, covering the header,

encoding of the individual parameters, and encoding of the complete log record for each event type.

5.1. SYSLOG HEADER Fields

Within the HEADER portion of the SYSLOG record, the priority (PRI) level is subject to local policy, but a default value of 8x is suggested, representing a Facility value of 10 (security/ authorization) and a Severity level varying with the event type. The suggested value by event type is shown in Table 2. Depending on where the SYSLOG record is generated, the HOSTNAME field may identify the NAT or an offline logging device. In the latter case, it may be desirable to identify the NAT using the NID field in the STRUCTURED-DATA section (see below). The value of the HOSTNAME field is subject to the preferences given in Section 6.2.4 of [RFC5424].

The values of the APP-NAME and MSGID fields in the record header determine the semantics of the record. The APP-NAME value "NAT" indicates that the record relates to an event reported by a NAT device. The MSGID values indicate the individual events. They are listed in Table 2 for each of the events defined in Section 3. The table also shows the SD-ID value used to label the event-specific STRUCTURED-DATA element.

Event	MSGID	PRI	SD-ID
NAT session creation	SessAdd	86 info	NATsess
NAT session deletion	SessDel	86 info	NATsess
NAT BIB entry creation	BIBAdd	86 info	NATBIB
NAT BIB entry deletion	BIBDel	86 info	NATBIB
Address binding event	AddrBind	86 info	NATBind
Port block allocation	PBlkAdd	86 info	NATPBlk
Port block deallocation	PBlkDel	86 info	NATPBlk
NAT address exhaustion	AddrEx	82 critical	NATAddrEx
NAT port exhaustion	PortEx	84 warning	NATPEx
Quota exceeded	Quota	85 notice	NATQEx
Invalid port detected	InvPort	83 error	NATInvP

Table 2: Recommended MSGID Encodings and Default PRI Values for the Events Defined In Section 3

5.2. Parameter Encodings

This section describes how to encode the individual parameters that can appear in NAT-related logs. These parameters are taken from the event descriptions in Section 3. Formally, as will be seen in Table 12, a parameter used with more than one event is registered as multiple separate parameters, one for each event report in which it is used. However, there is no reason to change either the PARAM-NAME or the encoding of the PARAM-VALUE between different instances of the same parameter.

For all of the parameters described below that convey IPv4 or IPv6 addresses, it is RECOMMENDED that implementations allow the operator to configure the portion of the address that will be recorded. Particularly for IPv6, this may involve omission of a specified number of trailing as well as leading octets of the address.

> *** Open issue *** The parameter "subscriber-identifying address" has multiple possible types, as shown in Table 1. One could encode this as two parameters, a type and a value which is a string restricted to decimal (for IPv4) or hexadecimal digits. That way the parameter could be shown as MANDATORY in the IANA registration. This version opts for compactness, using a different PARAM-NAME for each type, with the consequence that the individual parameters will be shown as OPTIONAL in the IANA registry but normative text in the next section will mandate the appearance of the appropriate one depending on the NAT type.
>
> *** Open issue *** Should we provide for GW-initiated DS-Lite?

The parameter specifications provided in this section are summarized in Table 3. This table also shows the PARAM-NAME value for each parameter.

PARAM-NAME	Parameter
NTyp	NAT type
NID	NAT identifier
VLANid	VLAN identifier
VRFid	VPN routing and forwarding identifier
PreS4	Pre-NAT IPv4 source address
PreS6	Pre-NAT IPv6 source address
Enc6	Encapsulating IPv6 source address
PostS4	Post-NAT source IPv4 address
Proto	Protocol identifier
PreSPt	Source port or ICMP identifier
PostSPt	Post-NAPT source port or ICMP identifier

PreD4	Destination IPv4 address
PreD6	Destination IPv6 address
PostD4	Post-NAT destination IPv4 address
PostDPt	Post-NAPT destination port or ICMP identifier
TrigR	Address realm triggering the creation of the session
PtMin	Starting port number
PtMax	Ending port number
PtRgSz	Port range size
PtRgStp	Range step size
APoolId	Address pool identifier
QTyp	Quota limit type
PSID	Port set identifier

Table 3: Parameters Used In NAT-Related Log Reports, By PARAM-NAME

5.2.1. NTyp: NAT Type

PARAM-VALUE: one of the values provided in the IANA SYSLOG NAT type registry established by this document. The initial values in that registry are:

44 NAT44;

64 NAT64;

AFTR DS-Lite AFTR [RFC6333];

UCPE unified CPE [I-D.softwire-unified-cpe].

This parameter is primarily additional information for the human reader of a log report, but could be used to provide a consistency check on the contents of a log. Instances where parameter usage depends on the NAT type of the reporting NAT are noted in Section 5.3.

5.2.2. NID: NAT Identifier

PARAM-VALUE: a UTF-8 string identifying the NAT observing the event which this record reports. Needed only if the necessary identification is not provided by the HOSTNAME parameter in the log record header.

5.2.3. VLANid: VLAN Identifier

PARAM-VALUE: a decimal integer representing the VLAN identifier associated with the subscriber site.

5.2.4. VRFid: VPN Routing and Forwarding Identifier

PARAM-VALUE: a hexadecimal number representing a VPN identifier [RFC2685] associated with the subscriber site. It is RECOMMENDED that implementations be configurable to include or not include the OUI portion of the identifier.

5.2.5. PreS4: Pre-NAT IPv4 Source Address

PARAM-VALUE: part or all of an IPv4 address, represented in dotted decimal form.

5.2.6. PreS6: Pre-NAT IPv6 Source Address

PARAM-VALUE: Part or all of an IPv6 address, represented in the form specified by [RFC5952].

5.2.7. Enc6: Encapsulating IPv6 Source Address

PARAM-VALUE: Part or all of an IPv6 address, represented in the form specified by [RFC5952].

5.2.8. PostS4: Post-NAT Source IPv4 Address

PARAM-VALUE: part or all of an IPv4 address, represented in dotted decimal form.

5.2.9. Proto: Protocol Identifier

PARAM-VALUE: an integer indicating the value of the Protocol header field (IPv4) or Next Header field (IPv6) in the incoming packet(s) (after decapsulation, for NAT type "AFTR") to which the event described by this record applies.

5.2.10. PreSPt: Pre-NAT Source Port or ICMP Identifier

PARAM-Value: integer value of the source port number or ICMP identifier before NAT processing.

5.2.11. PostSPt: Post-NAT Source Port or ICMP Identifier

PARAM-Value: integer value of the source port number or ICMP identifier after NAT processing.

5.2.12. PreD4: Pre-NAT Destination IPv4 Address

PARAM-VALUE: part or all of an IPv4 address, represented in dotted decimal form.

5.2.13. PreD6: Pre-NAT Destination IPv6 Address

PARAM-VALUE: Part or all of an IPv6 address, represented in the form specified by [RFC5952].

5.2.14. PostD4: Post-NAT Destination IPv4 Address

PARAM-VALUE: part or all of an IPv4 address, represented in dotted decimal form.

5.2.15. PostDPt: Post-NAPT Destination Port or ICMP Identifier

PARAM-Value: integer value of the destination port number or ICMP identifier after NAT processing.

5.2.16. TrigR: Realm Triggering Session Creation

PARAM-VALUE: "I" for internal, "E" for external.

5.2.17. PtMin: Starting Port Number

PARAM-Value: integer between 0 and 65535.

5.2.18. PtMax: Ending Port Number

PARAM-Value: integer between 0 and 65535. MUST be greater than or equal to PtMin if both are present.

5.2.19. PtRgSz: Port Range Size

PARAM-Value: integer between 1 and 65535. PtMin MUST also be present. PtRgSz SHOULD be less than or equal to (PtMax - PtMin + 1) if both other parameters are present, otherwise it SHOULD be less than or equal to (65535 - PtMin + 1).

5.2.20. PtRgStp: Step Size Between Port Ranges

PARAM-Value: integer between 1 and 65535. MUST be greater than or equal to PtRgSz if both parameters are present.

5.2.21. APoolId: Address Pool Identifier

PARAM-Value: integer identifying a specific address pool at the reporting NAT.

5.2.22. QTyp: Quota Limit Type

Value indicating which type of administrative quota has been exhausted. The possible values are:

SESS limit on number of session entries;

BIB limit on number of BIB entries;

ALL limit on global number of entries.

5.2.23. PSID: Port Set Identifier

PARAM-VALUE: integer between 0 and 65535 designating a port set. In practice the upper limit is likely to be two orders of magnitude smaller.

5.3. Encoding Of Complete Log Report For Each Event Type

This section describes the complete NAT-related contents of the logs used to report the events listed in Table 2.

5.3.1. NAT Session Creation and Deletion

As indicated in Table 2, the NAT session creation event is indicated by MSG-ID set to "SessAdd". Similarly, the NAT session deletion event is indicated by MSG-ID set to "SessDel". For both events, the associated SD-ELEMENT is tagged by SD-ID "NATsess". The contents of the NATsess SD-ELEMENT are shown in Table 4. The requirements for these contents are derived from the description in Section 3.1.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
VLANid	Section 5.2.3	OPTIONAL
VRFid	Section 5.2.4	OPTIONAL
PreS4	Section 5.2.5	Note 1
PreS6	Section 5.2.6	Note 1
Enc6	Section 5.2.7	Note 1
PostS4	Section 5.2.8	MANDATORY
Proto	Section 5.2.9	MANDATORY
PreSPt	Section 5.2.10	MANDATORY
PostSPt	Section 5.2.11	MANDATORY

PreD4	Section 5.2.12	OPTIONAL (Note 2)
PreD6	Section 5.2.13	OPTIONAL (Note 2)
PostD4	Section 5.2.14	OPTIONAL
PostDPt	Section 5.2.15	OPTIONAL
TrigR	Section 5.2.16	OPTIONAL

Table 4: Contents Of the SD-ELEMENT Section For Logging the Session Creation and Deletion Events

Note 1: one of PreD4, PreD6, or Enc6 MUST be present. For NAT type "44", use PreD4. For NAT type "64", use PreD6. For NAT types "AFTR" and "UCPE", use Enc6.

Note 2: use PreD4 for NAT types "44", "AFTR", and "UCPE". Use PreD6 for NAT type "64".

5.3.1.1. Examples

The first example is deliberately chosen to show how long a complete session log might be. For this first example, assume the log is formatted at an off-board device, which collects the information from an AFTR. Thus HOSTNAME and NID are both present. IPv6 addresses are reported omitting a common /16 prefix and the IID portion of the address (not to be too unrealistic!). Destination logging is enabled and all the other optional parameters are present. The AFTR does not translate the destination address, so PreD4 is not included. Note that the log could also include other SD-ELEMENTs (e.g., timeQuality), but enough is enough.

The log appears as a single record, but is wrapped between lines for purposes of presentation.

```
<86>1 2013-05-07T22:14:15.03Z record.example.net NAT 5063 SessAdd
[NATsess NTyp="AFTR" NID="bgw211.example.net"
VLANid="00201B000471E6" Enc6="A2E0:62" PostS4="198.51.100.127"
Proto="6" PreSPt="49156" PostSPt="6083" PostD4="198.51.100.16"
PostDPt="80" TrigR="I"]
```

Character count: about 260.

The next example is perhaps more typical in size. Assume an enterprise NAT44 generating its own logs. The enterprise does do destination logging as a matter of policy, but the other optional parameters are omitted. This is a session deletion event.

```
<86>1 2013-05-07T15:27:49.603-04:00 cerberus.example.com
NAT 175 SessDel [NATsess PreS4="192.0.2.5" PostS4="198.51.100.14"
```

```
   Proto="6" PreSPt="51387" PostSPt="17865" PostD4="198.51.100.86"
   PostDPt="80"]
```

The character count: about 200.

5.3.2. Binding Information Base (BIB) Entry Creation or Deletion

As indicated in Table 2, the NAT BIB entry creation event is indicated by MSG-ID set to "BIBAdd". Similarly, the NAT BIB entry deletion event is indicated by MSG-ID set to "BIBDel". For both events, the associated SD-ELEMENT is tagged by SD-ID "NATBIB". The contents of the NATBIB SD-ELEMENT are shown in Table 5. The requirements for these contents are derived from the description in Section 3.2.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
VLANid	Section 5.2.3	OPTIONAL
VRFid	Section 5.2.4	OPTIONAL
PreS4	Section 5.2.5	Note 1
PreS6	Section 5.2.6	Note 1
Enc6	Section 5.2.7	Note 1
PostS4	Section 5.2.8	MANDATORY
Proto	Section 5.2.9	MANDATORY
PreSPt	Section 5.2.10	MANDATORY
PostSPt	Section 5.2.11	MANDATORY

Table 5: Contents Of the SD-ELEMENT Section For Logging BIB Entry Creation and Deletion Events

Note 1: one of PreD4, PreD6, or Enc6 MUST be present. For NAT type "44", use PreD4. For NAT type "64", use PreD6. For NAT types "AFTR" and "UCPE", use Enc6.

As an example, consider a NAT64 where, as in the first session example above, the first /16 prefix and the final 64 bits are omitted from the IPv6 address.

```
   <86>1 2013-05-07T15:27:49.603-04:00 orpheus.example.com
   NAT 683 BIBAdd [NATBIB PreS6="F73E:7008" PostS4="198.51.100.1"
   Proto="6" PreSPt="27386" PostSPt="4809"]
```

Character count: about 160.

5.3.3. Address Binding Event

As indicated in Table 2, the NAT address binding event is indicated by MSG-ID set to "AddrBind". The associated SD-ELEMENT is tagged by SD-ID "NATBind". The contents of the NATBind SD-ELEMENT are shown in Table 6. The requirements for these contents are derived from the description in Section 3.3.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
PreS4	Section 5.2.5	Note 1
PreS6	Section 5.2.6	Note 1
Enc6	Section 5.2.7	Note 1
PostS4	Section 5.2.8	MANDATORY

Table 6: Contents Of the SD-ELEMENT Section For Logging the Address Binding Event

Note 1: one of PreD4, PreD6, or Enc6 MUST be present. For NAT type "44", use PreD4. For NAT type "64", use PreD6. For NAT types "AFTR" and "UCPE", use Enc6.

As an example, consider a managed DS-Lite B4 [RFC6333] operating as a NAT44 in coordination with the AFTR using PCP to obtain an external address binding and a port range. See Section 11 of [RFC6887] for the address binding. (The port allocation is shown in the next section's example.) The example here shows the address binding being recorded by the B4, although it could as well be recorded by the AFTR. As usual, the first /16 prefix and the final 64 bits are omitted from the encapsulating IPv6 address.

```
<86>1 2013-05-07T15:27:49.603Z yourd137mzmhow.example.net
NAT 68 AddrBind [NATBind Enc6="5A27:876E" PostS4="198.51.100.1"]
```

Character count: about 135.

5.3.4. Port Block Allocation and Deallocation

As indicated in Table 2, the port block allocation event is indicated by MSG-ID set to "PBlkAdd". The associated SD-ELEMENT is tagged by SD-ID "NATPBlk". Similarly, the port block deallocation event is indicated by MSG-ID set to "PBlkDel". For both events, the contents of the NATPBlk SD-ELEMENT are shown in Table 7. The requirements for these contents are derived from the description in Section 3.4.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
PtMin	Section 5.2.17	MANDATORY
PtMax	Section 5.2.18	OPTIONAL
PtRgSz	Section 5.2.19	OPTIONAL
PtRgStp	Section 5.2.20	OPTIONAL

Table 7: Contents Of the SD-ELEMENT Section For Logging the Port Block Allocation or Deallocation Event

As in the example in the previous section example, consider a managed DS-Lite B4 [RFC6333] operating as a NAT44 in coordination with the AFTR using PCP to obtain an external address binding and a port range. See [I-D.pcp-port-set] for the port set part of this operation. The example here shows the port set allocation being recorded by the B4, although it could as well be recorded by the AFTR.

Strictly for purposes of illustration, assume that the B4 is allocated two ranges of 64 consecutive values each, with the first beginning at 2048 and the second at 4096. Thus the port range step size is 2048 and the last port is 4159.

```
<86>1 2013-05-07T15:27:49.751Z yourd137mzmhow.example.net
NAT 68 PBlkAdd [NATPBlk PtMin="2048" PtMax="4159" PtRgSz="64"
PtRgStp="2048"]
```

Character count: about 135.

5.3.5. Address Exhaustion Event

As indicated in Table 2, the address exhaustion event is indicated by MSG-ID set to "AddrEx". The associated SD-ELEMENT is tagged by SD-ID "NATAddrEx". The contents of the NATAddrEx SD-ELEMENT are shown in Table 8. The requirements for these contents are derived from the description in Section 3.5.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
APoolId	Section 5.2.21	MANDATORY

Table 8: Contents Of the SD-ELEMENT Section For Logging the Address Exhaustion Event

The example shows this event being reported by a DS-Lite AFTR. Note the critical priority indication at the beginning of the log. As with the session example, we assume off-board log generation.

```
<82>1 2013-05-07T22:14:15.03Z record.example.net NAT 5063
AddrEx [NATAddrEx NID="bgw211.example.net" APoolId="2"]
```

Character count: about 120.

5.3.6. NAT Port Exhaustion

As indicated in Table 2, the port exhaustion event is indicated by MSG-ID set to "PortEx". The associated SD-ELEMENT is tagged by SD-ID "NATPEx". The contents of the NATPEx SD-ELEMENT are shown in Table 9. The requirements for these contents are derived from the description in Section 3.6.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
PostS4	Section 5.2.8	MANDATORY
Proto	Section 5.2.9	MANDATORY

Table 9: Contents Of the SD-ELEMENT Section For Logging the Port Exhaustion Event

The example is straightforward. Note the warning priority indication at the beginning of the log.

```
<84>1 2013-05-07T22:14:15.03Z cerberus.example.com NAT 5063
PortEx [NATPEx PostS4="198.51.100.1" Proto="6"]
```

Character count: about 110.

5.3.7. Quota Exceeded

As indicated in Table 2, the quota exceeded event is indicated by MSG-ID set to "Quota". The associated SD-ELEMENT is tagged by SD-ID "NATQEx". The contents of the NATQEx SD-ELEMENT are shown in Table 10. The requirements for these contents are derived from the description in Section 3.7.

PARAM-NAME	Description	Requirement
NTyp	Section 5.2.1	OPTIONAL
NID	Section 5.2.2	OPTIONAL
QTyp	Section 5.2.22	MANDATORY
VLANid	Section 5.2.3	OPTIONAL
VRFid	Section 5.2.4	OPTIONAL
PreS4	Section 5.2.5	OPTIONAL (Note 1)
PreS6	Section 5.2.6	OPTIONAL (Note 1)
Enc6	Section 5.2.7	OPTIONAL (Note 1)
Proto	Section 5.2.9	OPTIONAL

Table 10: Contents Of the SD-ELEMENT Section For Logging the Quota Exceeded Event

Note 1: if the quota applies to a specific user site, one of PreS4, PreS6, or Enc6 MUST be present. Use PreS4 for NAT44, PreS6 for NAT64, and Enc6 for AFTR or UCPE.

Example 1: limit on TCP sessions for a specific user site reached at an AFTR with off-board log generation.

```
<85>1 2013-05-07T22:14:15.03Z record.example.net NAT 5063
Quota [NATQEx NID="bgw211.example.net" QTyp="SESS"
Enc6="A2E0:62" Proto="6"]
```

Character count: about 130.

Example 2: global limit on number of entries for all subscribers served by the same VPN.

```
<85>1 2013-05-07T15:27:49.603-04:00 cerberus.example.com
NAT 175 Quota [NATQEx QTyp="ALL" VRFid="1246"]
```

Character count: about 105.

Example 3: limit on total number of BIB entries for TCP.

```
<85>1 2013-05-07T15:27:49.603-04:00 cerberus.example.com
NAT 175 Quota [NATQEx QTyp="BIB" Proto="6"]
```

Character count: about 95.

5.3.8. Invalid Port Detected

As indicated in Table 2, the invalid port detected event is indicated by MSG-ID set to "InvPort". The associated SD-ELEMENT is tagged by SD-ID "NATInvP". The contents of the NATInvP SD-ELEMENT are shown in Table 11. The requirements for these contents are derived from the description in Section 3.8.

PARAM-NAME	Description	Requirement
NID	Section 5.2.2	OPTIONAL
Enc6	Section 5.2.7	MANDATORY
PSID	Section 5.2.23	MANDATORY
PtRgSz	Section 5.2.19	OPTIONAL
PtRgStp	Section 5.2.20	OPTIONAL

Table 11: Contents Of the SD-ELEMENT Section For Logging the Invalid Port detected Event

Example: managed unified CPE running Lightweight 4over6 and configured to report the port range size.

```
<83>1 2013-05-07T15:27:49.603Z yourd137mzmhow.example.net
NAT 68 InvPort [NATInvP Enc6="5A27:876E" PSID="15" PtRgSz="512"]
```

Character count: about 120.

6. IANA Considerations

This document requests IANA to make the following assignments to the SYSLOG Structured Data ID Values registry. RFCxxxx refers to the present document when approved.

Structured Data ID	Structured Data Parameter	Required or Optional	Reference
NATsess		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	VLANid	OPTIONAL	RFCxxxx
	VRFid	OPTIONAL	RFCxxxx
	PreS4	OPTIONAL	RFCxxxx
	PreS6	OPTIONAL	RFCxxxx
	Enc6	OPTIONAL	RFCxxxx
	PostS4	MANDATORY	RFCxxxx
	Proto	MANDATORY	RFCxxxx
	PreSPt	MANDATORY	RFCxxxx

	PostPt	MANDATORY	RFCxxxx
	PreD4	OPTIONAL	RFCxxxx
	PreD6	OPTIONAL	RFCxxxx
	PostD4	OPTIONAL	RFCxxxx
	PostDPt	OPTIONAL	RFCxxxx
	TrigR	OPTIONAL	RFCxxxx
----	----	----	----
NATBIB		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	VLANid	OPTIONAL	RFCxxxx
	VRFid	OPTIONAL	RFCxxxx
	PreS4	OPTIONAL	RFCxxxx
	PreS6	OPTIONAL	RFCxxxx
	Enc6	OPTIONAL	RFCxxxx
	PostS4	MANDATORY	RFCxxxx
	Proto	MANDATORY	RFCxxxx
	PreSPt	MANDATORY	RFCxxxx
	PostPt	MANDATORY	RFCxxxx
----	----	----	----
NATBind		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	PreS4	OPTIONAL	RFCxxxx
	PreS6	OPTIONAL	RFCxxxx
	Enc6	OPTIONAL	RFCxxxx
	PostS4	MANDATORY	RFCxxxx
----	----	----	----
NATPBlk		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	PtMin	MANDATORY	RFCxxxx
	PtMax	OPTIONAL	RFCxxxx
	PtRgSz	OPTIONAL	RFCxxxx
	PtRgStp	OPTIONAL	RFCxxxx
----	----	----	----
NATAddrEx		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	APoolId	MANDATORY	RFCxxxx
----	----	----	----
NATPEx		OPTIONAL	RFCxxxx
	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	PostS4	MANDATORY	RFCxxxx
	Proto	MANDATORY	RFCxxxx
----	----	----	----
NATQEx		OPTIONAL	RFCxxxx

	NTyp	OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	QTyp	MANDATORY	RFCxxxx
	VLANid	OPTIONAL	RFCxxxx
	VRFid	OPTIONAL	RFCxxxx
	PreS4	OPTIONAL	RFCxxxx
	PreS6	OPTIONAL	RFCxxxx
	Enc6	OPTIONAL	RFCxxxx
	Proto	OPTIONAL	RFCxxxx
----	----	----	----
NATInvP		OPTIONAL	RFCxxxx
	NID	OPTIONAL	RFCxxxx
	Enc6	MANDATORY	RFCxxxx
	PSID	MANDATORY	RFCxxxx
	PtRgSz	OPTIONAL	RFCxxxx
	PtRgStp	OPTIONAL	RFCxxxx

Table 12: NAT-Related STRUCTERED-DATA Registrations

IANA is further requested to establish a new registry entitled "syslog NAT Types" within the "syslog Parameters" registry. The initial values for this registry are shown in Table 13. New values may be added following the criterion of IETF Review.

Value	Description	Reference
44	NAT44	RFCxxxx
64	NAT64	RFCxxxx
AFTR	DS-Lite AFTR [RFC6333]	RFCxxxx
UCPE	Unified CPE [I-D.softwire-unified-cpe]	RFCxxxx

Table 13: syslog NAT Type Values

The reference [I-D.softwire-unified-cpe] is given below in the Informative References section.

7. Security Considerations

When logs are being recorded for regulatory reasons, preservation of their integrity and authentication of their origin is essential. To achieve this result, it is RECOMMENDED that the operator deploy [RFC5848].

Access to the logs defined here while the reported assignments are in force could improve an attacker's chance of hijacking a session

through port-guessing. Even after an assignment has expired, the information in the logs SHOULD be treated as confidential, since, if revealed, it could help an attacker trace sessions back to a particular subscriber or subscriber location. It is therefore RECOMMENDED that these logs be transported securely, using [RFC5425], for example, and that they be stored securely at the collector.

8. References

8.1. Normative References

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

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC2685] Fox, B. and B. Gleeson, "Virtual Private Networks Identifier", RFC 2685, September 1999.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

[RFC5425] Miao, F., Ma, Y., and J. Salowey, "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5848] Kelsey, J., Callas, J., and A. Clemm, "Signed Syslog Messages", RFC 5848, May 2010.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

8.2. Informative References

[I-D.behave-ipfix-nat-logging] Sivakumar, S. and R. Penno, "IPFIX Information Elements for logging NAT Events (Work in progress)", March 2013.

[I-D.pcp-port-set] Sun, Q., Boucadair, M., Sivakumar, S., Zhou, C., Tsou, T., and S. Perreault, "Port Control Protocol (PCP) Extension for Port Set Allocation (Work in progress)", March 2013.

[I-D.softwire-lw4over6]
Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I. Farrer, "Lightweight 4over6: An Extension to the DS-Lite Architecture (Work in progress)", April 2013.

[I-D.softwire-map]
Troan, O., Dec, W., Li, X., Bao, C., Matsushima, S., and T. Murakami, "Mapping of Address and Port with Encapsulation (MAP) (Work in progress)", March 2013.

[I-D.softwire-public-4over6]
Cui, Y., Wu, J., Wu, P., Vautrin, O., and Y. Lee, "Public IPv4 over IPv6 Access Network (Work in progress)", February 2013.

[I-D.softwire-unified-cpe]
Boucadair, M. and I. Farrer, "Unified IPv4-in-IPv6 Softwire CPE (Work in progress)", March 2013.

[I-D.tsou-behave-natx4-log-reduction]
Tsou, T., Li, W., and T. Taylor, "Port Management To Reduce Logging In Large-Scale NATs (Work in progress)", May 2013.

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

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5382] Guha, S., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, "NAT Behavioral Requirements for TCP", BCP 142, RFC 5382, October 2008.

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[RFC6674] Brockners, F., Gundavelli, S., Speicher, S., and D. Ward, "Gateway-Initiated Dual-Stack Lite Deployment", RFC 6674, July 2012.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

[RFC6888] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, April 2013.

Authors' Addresses

Zhonghua Chen
China Telecom
P.R. China

Email: 18918588897@189.cn

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: cathy.zhou@huawei.com

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

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

T. Taylor
Huawei Technologies
Ottawa
Canada

Email: tom.taylor.stds@gmail.com