DOTS   T. Reddy
Internet-Draft   McAfee
Intended status: Standards Track   M. Boucadair
Expires: ~~January 31,~~ **March 9,** 2020   Orange
                                                                J. Shallow
                                                                 ~~July 30,~~
                                                          September 06, 2019

         Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal
                              Channel Call Home
                    ~~draft-ietf-dots-signal-call-home-05~~
                    draft-ietf-dots-signal-call-home-06

Abstract

    This document specifies the DOTS signal channel Call Home, which
    enables a DOTS server to initiate a secure connection to a DOTS
    client, and to receive the attack traffic information from the DOTS
    client. The DOTS server in turn uses the attack traffic information
    to identify the compromised devices launching the outgoing DDoS
    attack and takes appropriate mitigation action(s).

    The DOTS signal channel Call Home is not specific to the home
    networks; the solution targets any deployment which requires to block
    DDoS attack traffic closer to the source(s) of a DDoS attack.

Editorial Note (To be removed by RFC Editor)

    Please update these statements within the document with the RFC
    number to be assigned to this document:

    o   "This version of this YANG module is part of RFC XXXX;"

    o   "RFC XXXX: Distributed Denial-of-Service Open Threat Signaling
        (DOTS) Signal Channel Call Home";

    o   "| [RFCXXXX] |"

    o   reference: RFC XXXX

    Please update this statement with the RFC number to be assigned to
    the following documents:

    o   "RFC YYYY: Distributed Denial-of-Service Open Threat Signaling
        (DOTS) Signal Channel Specification (used to be I-D.ietf-dots-
        signal-channel)

    Please update TBD statements with the assignment made by IANA to DOTS
    Signal Channel Call Home.

    Also, please update the "revision" date of the YANG module.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. The Problem

   The DOTS signal channel protocol [I-D.ietf-dots-signal-channel] is
   used to carry information about a network resource or a network (or a
   part thereof) that is under a Distributed Denial of Service (DDoS)
   attack [RFC4732]. Such information is sent by a DOTS client to one
   or multiple DOTS servers so that appropriate mitigation actions are
   undertaken on traffic deemed suspicious. Various use cases are
   discussed in [I-D.ietf-dots-use-cases].

   Internet of Things (IoT) devices are becoming more and more prevalent
   in home networks, in particular. With compute and memory becoming
   cheaper and cheaper, various types of IoT devices become available in
   the consumer market at affordable prices. But on the downside, the
   main threat being most of these IoT devices are bought off-the-shelf
   and most manufacturers haven't considered security in the product
   design (e.g., [Sec]). IoT devices deployed in home networks can be
   easily compromised, they do not have an easy mechanism to upgrade,
   and IoT manufactures may cease manufacture and/or discontinue
   patching vulnerabilities on IoT devices (Sections 5.4 and 5.5 of
   [RFC8576]). These vulnerable and compromised devices will continue
   to be used for a long period of time in the home, and the end-user
   does not know that IoT devices in his/her home are compromised. The
   compromised IoT devices are typically used for launching DDoS attacks
   (Section 3 of [RFC8576]) on victims while the owner/administrator of
   the home network is not aware about such misbehaviors. Similar to
   other DDoS attacks, the victim in this attack can be an application
   server, a host, a router, a firewall, or an entire network. Such
   misbehaviors will have a collateral damage that affects end users and

the reputation of an Internet Service Provider (ISP).

Nowadays, network devices in a home network offer network security
(e.g., firewall [RFC4949] or Intrusion Protection System (IPS)
service [I-D.ietf-i2nsf-terminology] on a home router) to protect the
devices connected to the home network from both external and internal
attacks. Over the years several techniques have been identified to
detect DDoS attacks, some of these techniques can be enabled on home
network devices but most of them are used within the ISP's network.
The ISP offering a DDoS mitigation service can detect outgoing DDoS
attack traffic originating from its subscribers or the ISP may
receive filtering rules (e.g., using BGP Flowspec
[RFC5575][I-D.ietf-idr-flow-spec-v6]) from a downstream service
provider to filter, block, or rate-limit DDoS attack traffic
originating from the ISP's subscribers to a downstream target.

Some of the DDoS attacks like spoofed RST or FIN packets, Slowloris,
and Transport Layer Security (TLS) re-negotiation are difficult to
detect on a home network device without adversely affecting its
performance. The reason is typically home devices such as home
routers have fast path to boost the throughput. For every new TCP/
UDP flow, only the first few packets are punted through the slow
path. Hence, it is not possible to detect various DDoS attacks in
the slow path, since the attack payload is sent to the target server
after the flow is switched to fast path. The reader may refer to
Section 2 of [RFC6398] for a brief definition of slow and fast paths.

Deep Packet Inspection (DPI) of all the packets of a flow would be
able to detect some of the attacks. However, a full-fledged DPI to
detect these type of DDoS attacks is functionally or operationally
not possible for all the devices attached to the home network owing
to the memory and CPU limitations of the home routers. Furthermore,
for certain DDoS attacks the ability to distinguish legitimate
traffic from attack traffic on a per packet basis is complex. This
complexity is due to that the packet itself may look "legitimate" and
no attack signature can be identified. The anomaly can be identified
only after detailed statistical analysis.

ISPs can detect some DDoS attacks originating from a home network
(e.g., Section 2.6 of [RFC8517]), but the ISP does not have a
mechanism to detect which device in the home network is generating
the DDoS attack traffic. The primary reason being that devices in an
IPv4 home network are typically behind a Network Address Translation
(NAT) border [RFC2663]. Even in case of an IPv6 home network,
although the ISP can identify the infected device in the home network
launching the DDoS traffic by tracking its unique IPv6 address, the
infected device can easily change its IPv6 address to evade
remediation.

Existing approaches are still suffering from misused access network
resources by abusing devices; the support of means for blocking such
attacks close to the sources are missing. In particular, the DOTS
signal protocol does not discuss cooperative DDoS mitigation between
the network hosting an attack source and the ISP to the suppress the
outbound DDoS attack traffic originating from that network.

1.2. The Solution

This specification addresses the problems discussed in Section 1.1
and presents an extension to the DOTS signal channel: DOTS signal
channel Call Home.

'DOTS signal channel Call Home' (or DOTS Call Home, for short) refers
to a DOTS signal channel established at the initiative of a DOTS
server. That is, the DOTS server initiates a secure connection to a
DOTS client, and uses that connection to receive the attack traffic
information (e.g., attack sources) from the DOTS client. More
details are provided in Section 3.

DOTS agents involved in the DOTS Call Home adhere to the DOTS roles
as defined in [RFC8612]. For clarity, this document uses "Call Home
DOTS client" (or "Call Home DOTS server") to refer to a DOTS client
(or DOTS server) deployed in a Call Home scenario (Figure 1).

A high-level DOTS Call Home functional architecture is shown in
Figure 1. Attack source(s) are within the DOTS server domain.

```
                                        Scope
                             +.-.-.-.-.-.-.-.-.-.-.+
            +--------------+    :   +-------------+    :
            | Alert/DMS/   | ~~~:~~~ | Call Home  |    :
            | Peer DMS/... |    :   | DOTS client |    :
            +--------------+    :   +------+------+    :
                                :          |          :
                                :          |          :
                                :          |          :
            +--------------+    :   +------+------+    :
            |    Attack    | ~~~:~~~ | Call Home  |    :
            |   Source(s)  |    :   | DOTS server |    :
            +--------------+    :   +-------------+    :
                             +.-.-.-.-.-.-.-.-.-.-.+
```
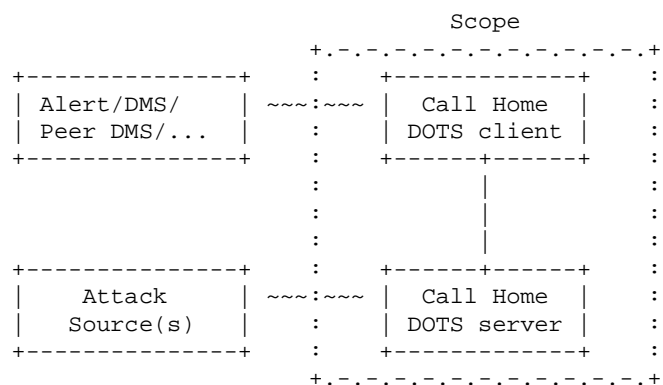
Figure 1: Basic DOTS Signal Channel Call Home Functional Architecture
A DOTS client relies upon a variety of triggers to make use of the
Call Home function (e.g., scrubbing the traffic from the attack
source, receiving an alert from an attack target, a peer DDoS
Mitigation System (DMS), or a transit provider). The definition of
these triggers is deployment-specific. It is therefore out of the
scope of this document to elaborate on how these triggers are made
available to a Call Home DOTS client.

In a typical deployment scenario, the Call Home DOTS server is
enabled on a Customer Premises Equipment (CPE), which is aligned with
recent trends to enrich the CPE with advanced security features.
Unlike classic DOTS deployments [I-D.ietf-dots-use-cases], such DOTS
server maintains a single DOTS signal channel session for each DOTS-
capable upstream provisioning domain [I-D.ietf-dots-multihoming].

For instance, the Call Home DOTS server in the home network initiates
the signal channel Call Home in 'idle' time and then subsequently the
Call Home DOTS client in the ISP environment can initiate a
mitigation request whenever the ISP detects there is an attack from a
compromised device in the DOTS server domain (i.e., from within the
home network).

The Call Home DOTS server uses the DDoS attack traffic information to
identify the compromised device in its domain that is responsible for
launching the DDoS attack, optionally notifies a network
administrator, and takes appropriate mitigation action(s). For
example, a mitigation action can be to quarantine the compromised
device or block its traffic to the attack target(s) until the
mitigation request is withdrawn.

Other motivations for introducing the Call Home function are
discussed in Section 1.1 of [RFC8071].

This document assumes that Call Home DOTS servers are provisioned
with a way to know how to reach the upstream Call Home DOTS
client(s), which could occur by a variety of means (e.g.,
[I-D.ietf-dots-server-discovery]). The specification of such means
are out of scope of this document.

More information about the applicability scope of the DOTS signal
channel Call Home is provided in Section 1.3.

1.3. Applicability Scope

The aforementioned problems may be encountered in other deployments
than those discussed in Section 1.1 (e.g., data centers, enterprise
networks). The solution specified in this document can be used for
those deployments to block DDoS attack traffic closer to the
source(s) of the attack.

An instantiation of the Call Home functional architecture is depicted
in Figure 2.

```
                         +-------------+
                         |Attack Target|
```

```
                         +-----+------+
                         | /\      Target Network
         .....................|.||.....................
                  .--------+-||-------.
                 (          ||         )-.
                .'          ||           '
               (   Internet ||            )
                (           ||          -'
                 '-(        ||          )
                   '------+-||---------'
         ......................|.||..................
                  .--------+-||-------.    Network
                 (          ||         )-. Provider
                .' Call Home ||         '  (DMS)
               ( DOTS client ||          )
                (            ||         -'
                 '-(         ||         )
                   '------+-||---------'
         ......................|.||.................
                  .--------+-||-------. Source Network
                 (          ||         )-.
                .' Call Home ||          '
               ( DOTS server || Outbound  )
                (            ||    DDoS  -'
                 '-(         ||   Attack  )
                   '------+-||---------'
                         | ||
                  +-----+-++----+
                  |Attack Source|
                  +-------------+
```
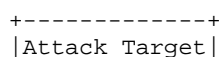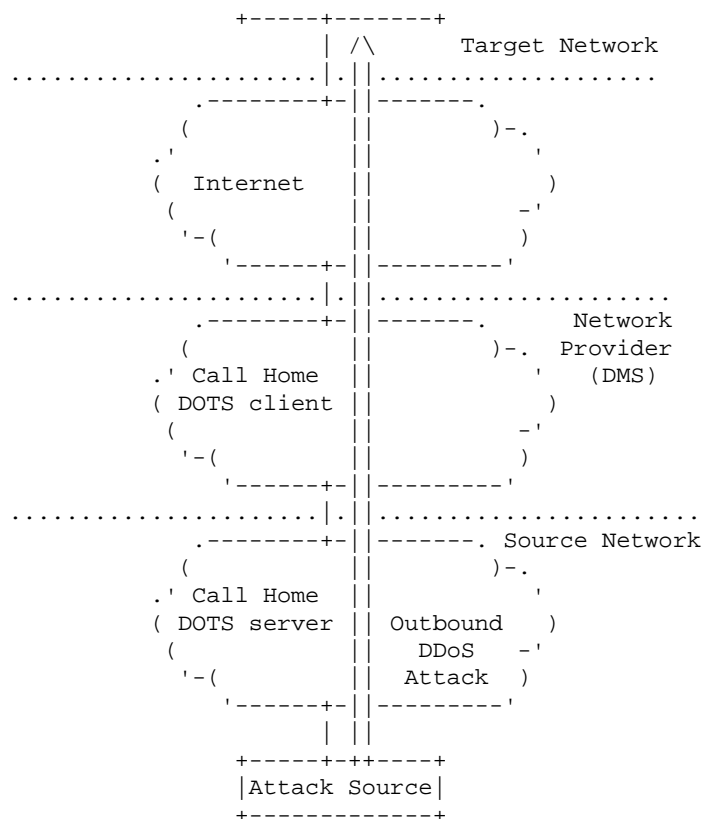
        Figure 2: DOTS Signal Channel Call Home Reference Architecture

     It is out of the scope of this document to identify an exhaustive
     list of such deployments.

   1.4.   Co-existence of Base DOTS Signal Channel & DOTS Call Home

     The DOTS signal channel Call Home does not require nor preclude the
     activation of the base DOTS signal channel
     [I-D.ietf-dots-signal-channel]. Some sample deployment schemes are
     discussed in this section for illustration purposes.

     The network that hosts an attack source may also be subject to
     inbound DDoS attacks. In that case, both the base DOTS signal
     channel and DOTS signal channel Call Home may be enabled as shown in
     Figure 3 (Same DMS provider) or Figure 4 (Distinct DMS providers).

```
                    DOTS Signal Channel      Base DOTS
                         Call Home          Signal Channel
                  +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
                  :          +------+ :: +------+          :
                  :          | DOTS | :: | DOTS |          :
                  :          |client| :: |server|          :
                  :          +--+---+ :: +---+--+          :
                  :    /\      |      ::    |              : Network
                  :    ||      |      ::    |              :Provider
                  :    ||      |      ::    |              :  (DMS)
                ...:......||.......|......::.....|...............:.......
                Outbound ||      |      ::    |          || Inbound
                 DDoS    ||      |      ::    |          ||  DDoS
                Attack   ||      |      ::    |          \/  Attack
                  :        +--+---+ :: +---+--+          :
                  :        | DOTS | :: | DOTS |          :
                  :        |server| :: |client|          :
                  :        +------+ :: +------+          :
                  +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
                              Network #A
```

     Figure 3: Activation of Base DOTS Signal Channel and Call Home (Same
                              DMS Provider)

     Note that a DMS provider may not be on the default forwarding path of
     an inbound DDoS attack traffic targeting a network (e.g., Network #B

in Figure 4). Nevertheless, the DOTS signal channel Call Home
requires the DMS provider to be on the default forwarding path of the
outbound traffic from a given network.

```
            DOTS Signal Channel       Base DOTS
                Call Home          Signal Channel
         +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
         : Network  +------+ :: +------+  Third   :
         : Provider | DOTS | :: | DOTS |  Party   :
         :  (DMS)   |client| :: |server|   DMS    :
         :          +--+---+ :: +---+--+ Provider  :
         :      /\      |     ::    |            :
         :      ||      |     ::    |            :
         :      ||      |     ::    |            :
      ...:.....||......|.....::.....|..............:........
        Outbound ||      |     ::    |         || Inbound
          DDoS   ||      |     ::    |         ||   DDoS
         Attack  ||      |     ::    |         \/  Attack
         :          +--+---+ :: +---+--+         :
         :          | DOTS | :: | DOTS |         :
         :          |server| :: |client|         :
         :          +------+ :: +------+         :
         +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
                       Network #B
```
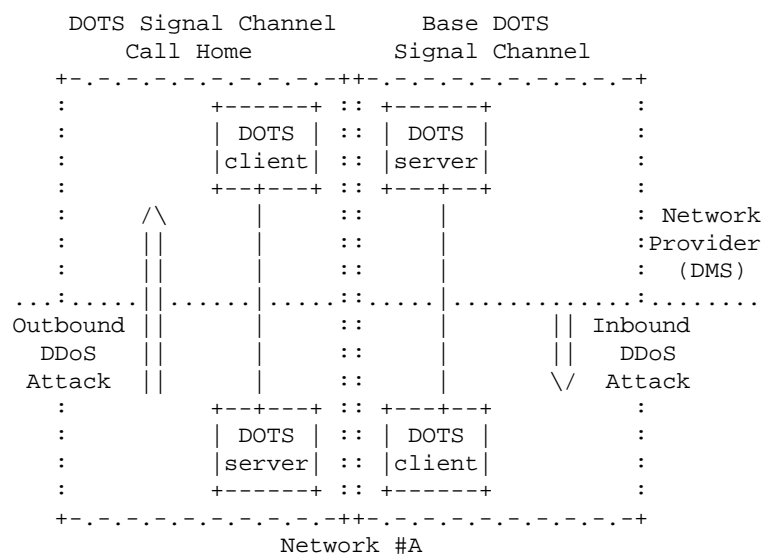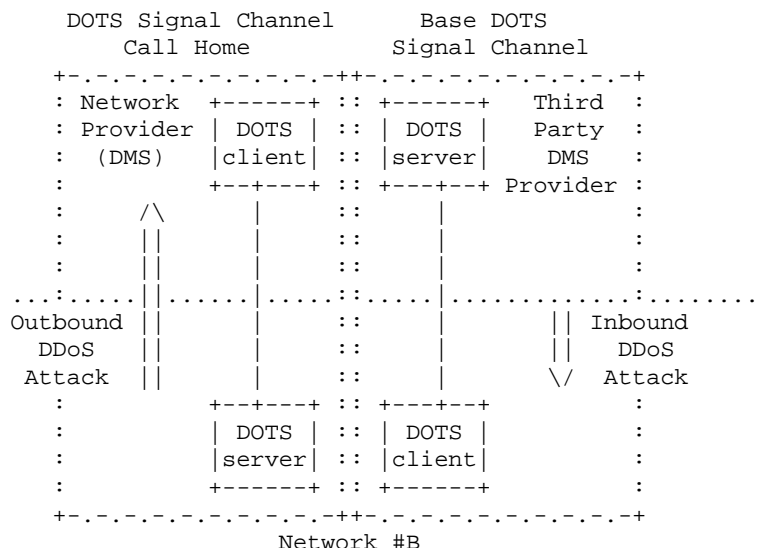
    Figure 4: Activation of Base DOTS Signal Channel and Call Home
                     (Distinct DMS Providers)

Figures 5 and 6 depict examples where the same node embeds both base
DOTS and DOTS Call Home agents. For example, a DOTS server and a
Call Home DOTS client may be enabled on the same device within the
infrastructure of a DMS provider (e.g., Node #i in Figure 5) or a
DOTS client and a Call Home DOTS server may be enabled on the same
device within a source network (e.g., Node #j with Network #D shown
in Figure 6) .

Whether the same or distinct nodes are used to host base DOTS and
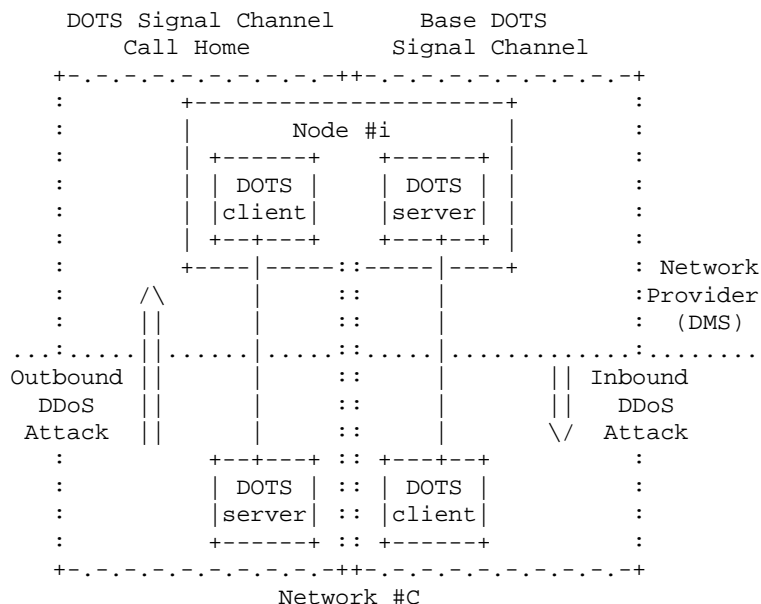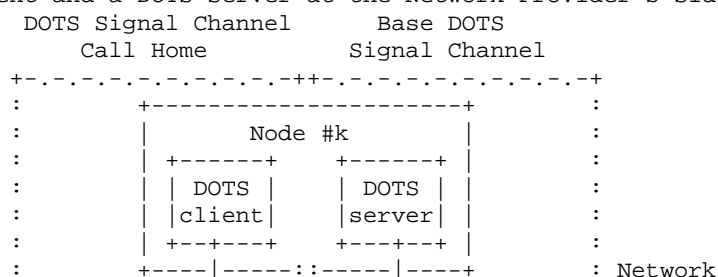DOTS Call Home agents is specific to each domain.

```
            DOTS Signal Channel       Base DOTS
                Call Home          Signal Channel
         +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
         :      +---------------------+      :
         :      |      Node #i        |      :
         :      | +------+   +------+ |      :
         :      | | DOTS |   | DOTS | |      :
         :      | |client|   |server| |      :
         :      | +--+---+   +---+--+ |      :
         :      +----|-----::-----|----+      : Network
         :      /\      |     ::    |         :Provider
         :      ||      |     ::    |         :  (DMS)
      ...:.....||......|.....::.....|..............:........
        Outbound ||      |     ::    |         || Inbound
          DDoS   ||      |     ::    |         ||   DDoS
         Attack  ||      |     ::    |         \/  Attack
         :          +--+---+ :: +---+--+         :
         :          | DOTS | :: | DOTS |         :
         :          |server| :: |client|         :
         :          +------+ :: +------+         :
         +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
                       Network #C
```

Figure 5: An Example of the Same Node Embedding both a Call Home DOTS
       Client and a DOTS Server at the Network Provider's Side
```
            DOTS Signal Channel       Base DOTS
                Call Home          Signal Channel
         +-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-+
         :      +---------------------+      :
         :      |      Node #k        |      :
         :      | +------+   +------+ |      :
         :      | | DOTS |   | DOTS | |      :
         :      | |client|   |server| |      :
         :      | +--+---+   +---+--+ |      :
         :      +----|-----::-----|----+      : Network
```

```
        :      /\    |    ::    |              :Provider
        :      ||    |    ::    |              : (DMS)
    ...:......||......|.....::.....|...............:.......
    Outbound ||    |    ::    |         || Inbound
      DDoS   ||    |    ::    |         ||  DDoS
     Attack  ||    |    ::    |         \/  Attack
        :      +----|-----::-----|----+      :
        :      | +--+---+    +---+--+ |      :
        :      | | DOTS |    | DOTS | |      :
        :      | |server|    |client| |      :
        :      | +------+    +------+ |      :
        :      |      Node #j        |      :
        :      +--------------------+      :
    +-.-.-.-.-.-.-.-.-.-++-.-.-.-.-.-.-.-.-.-+
                   Network #D
```
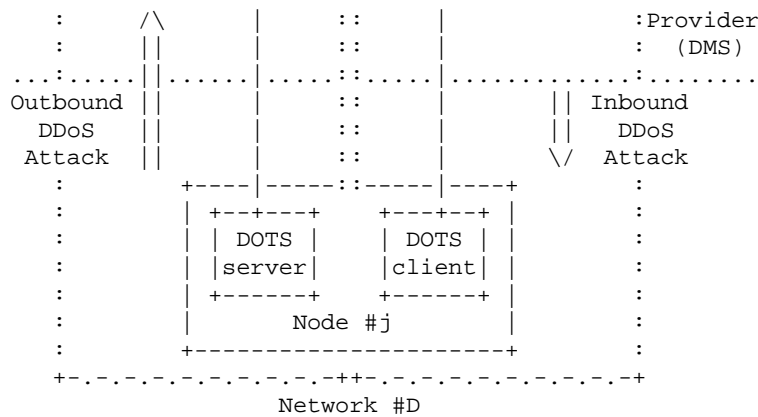
Figure 6: Another Example where the Same Node Embeds both a DOTS
Client and a Call Home DOTS Server

Appendix A elaborates on the considerations to unambiguously
distinguish DOTS messages which belong to each of these channels.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in BCP
14 [RFC2119][RFC8174] when, and only when, they appear in all
capitals, as shown here.

The reader should be familiar with the terms defined in [RFC8612].

'Base DOTS signal channel' refers to [I-D.ietf-dots-signal-channel].

The meaning of the symbols in YANG tree diagrams is defined in
[RFC8340].

(D)TLS is used for statements that apply to both Transport Layer
Security (TLS) [RFC8446] and Datagram Transport Layer Security (DTLS)
[RFC6347]. Specific terms are used for any statement that applies to
either protocol alone.

3. DOTS Signal Channel Call Home

3.1. Procedure

The DOTS signal channel Call Home preserves all but one of the DOTS
client/server roles in the DOTS protocol stack, as compared to DOTS
client-initiated DOTS signal channel protocol
[I-D.ietf-dots-signal-channel]. The role reversal that occurs is at
the (D)TLS layer; that is, (1) the Call Home DOTS server acts as a
DTLS client and the Call Home DOTS client acts as a DTLS server or
(2) the Call Home DOTS server acts as a TLS client initiating the
underlying TCP connection and the Call Home DOTS client acts as a TLS
server. The Call Home DOTS server initiates (D)TLS handshake to the
Call Home DOTS client.

For example, a home network element (e.g., home router) co-located
with a Call Home DOTS server is the (D)TLS server. However, when
calling home, the DOTS server initially assumes the role of the
(D)TLS client, but the network element's role as a DOTS server
remains the same. Furthermore, existing certificate chains and
mutual authentication mechanisms between the DOTS agents are
unaffected by the Call Home function. This Call Home function
enables the DOTS server co-located with a network element (possibly
behind NATs and firewalls) reachable by only the intended Call Home
DOTS client and hence the Call Home DOTS server cannot be subjected
to these DDoS attacks.

Figure 7 illustrates a sample DOTS Call Home flow exchange:

```
        +-----------+                      +-----------+
        | Call Home |                      | Call Home |
        |   DOTS    |                      |   DOTS    |
```

```
            |  server  |                      |  client  |
            +-----+----+                      +-----+----+
            (D)TLS client                     (D)TLS server
                 |                                  |
                 |          1. (D)TLS connection    |
                 |--------------------------------->|
                 |          2. Mitigation request   |
                 |<---------------------------------|
                 |               ...                |
```
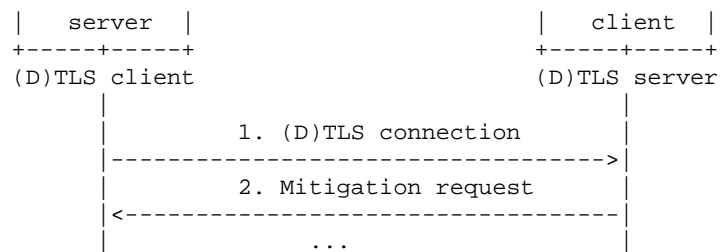
Figure 7: DOTS Signal Channel Call Home Sequence Diagram

The DOTS signal channel Call Home procedure is as follows:

1. If UDP transport is used, the Call Home DOTS server begins by
    initiating a DTLS connection to the Call Home DOTS client.

    If TCP is used, the Call Home DOTS server begins by initiating a
    TCP connection to the Call Home DOTS client. Using this TCP
    connection, the Call Home DOTS server initiates a TLS connection
    to the Call Home DOTS client.

    In some cases, peer DOTS agents may have mutual agreement to use
    a specific port number, such as by explicit configuration or
    dynamic discovery [I-D.ietf-dots-server-discovery]. Absent such
    mutual agreement, the DOTS signal channel Call Home MUST run over
    port number TBD (that is, Call Home DOTS clients must support
    accepting DTLS (or TCP) connections on TBD) as defined in
    Section 4.1, for both UDP and TCP. The interaction between the
    base DOTS signal channel and the Call Home is discussed in
    Appendix A.

    The Happy Eyeballs mechanism explained in Section 4.3 of
    [I-D.ietf-dots-signal-channel] is used for initiating (D)TLS
    connections.

2. Using this (D)TLS connection, the Call Home DOTS client may
    request, withdraw, or retrieve the status of mitigation requests.
    The Call Home DOTS client supplies the source information by
    means of new attributes defined in Section 3.3.1.

    The Heartbeat mechanism used for the DOTS Call Home deviates from
    the one defined in Section 4.7 of [I-D.ietf-dots-signal-channel].
    Section ~~3.2~~ **3.2.1** specifies the behavior to be followed by Call Home
    DOTS agents.

3.2. **DOTS Signal Channel Variations**

3.2.1. Heartbeat Mechanism

   Once the (D)TLS section is established between the DOTS agents, the
   Call Home DOTS client contacts the Call Home DOTS server to retrieve
   the session configuration parameters (Section 4.5 of
   [I-D.ietf-dots-signal-channel]). The Call Home DOTS server adjusts
   the 'heartbeat-interval' to accommodate binding timers used by on-
   path NATs and firewalls. Heartbeats will be then exchanged by the
   DOTS agents following the instructions retrieved using the signal
   channel session configuration exchange.

   It is the responsibility of Call Home DOTS servers to ensure that on-
   path translators/firewalls are maintaining a binding so that the same
   external IP address and/or port number is retained for the DOTS
   signal channel session. A Call Home DOTS client MAY trigger their
   heartbeat requests immediately after receiving heartbeat probes from
   its peer Call Home DOTS server.

   When an outgoing attack that saturates the outgoing link from the
   Call Home DOTS server is detected and reported by a Call Home DOTS
   client, the latter MUST continue to use the DOTS signal channel even
   if no traffic is received from the Call Home DOTS server.

   If the Call Home DOTS server receives traffic from the Call Home DOTS
   client, the Call Home DOTS server MUST continue to use the DOTS
   signal channel even if the missing heartbeats allowed threshold

('missing-hb-allowed') is reached.

If the Call Home DOTS server does not receive any traffic from the
peer Call Home DOTS client during the time span required to exhaust
the maximum 'missing-hb-allowed' threshold, the Call Home DOTS server
concludes the session is disconnected. Then, the Call Home DOTS
server MUST try to resume the (D)TLS session.

3.2.2. Redirected Signaling

A Call Home DOTS server MUST NOT support the Redirected Signaling
mechanism as specified in Section 4.6 of
[I-D.ietf-dots-signal-channel] (i.e., a 5.03 response that conveys an
alternate DOTS server's FQDN or alternate DOTS server's IP
address(es)). A Call Home DOTS client MUST silently discard such
message as only a Call Home DOTS server can initiate a new (D)TLS
connection.

If a Call Home DOTS client wants to redirect a Call Home DOTS server
to another Call Home DOTS client, it MUST send a PUT request to the
predefined resource ".well-known/dots/redirect" with the new Call
Home DOTS client FQDN or IP address in the body of the PUT similar to
what is described in Section 4.6 of [I-D.ietf-dots-signal-channel].
Furthermore, a new clause called 'ttl" is defined to return the Time
to live (TTL) of the alternate Call Home DOTS client.

On receipt of this PUT request, the Call Home DOTS server responds
with a 2.01 (Created), closes this connection and establishes a
connection with the new Call Home DOTS client. The processing of the
TTL is defined in Section 4.6 of [I-D.ietf-dots-signal-channel]. If
the Call Home DOTS server cannot service the PUT request, the
response is rejected with a 4.00 (bad Request).

Figure 8 shows a PUT request example to convey the alternate Call
Home DOTS client 'alt-call-home-client.example' together with its IP
addresses 2001:db8:6401::1 and 2001:db8:6401::2. The validity of
this alternate Call Home DOTS client is 10 minutes.

```
Header: PUT (Code=0.03)
Uri-Path: ".well-known"
Uri-Path: "dots"
Uri-Path: "redirect"
Uri-Path: "cuid=dz6pHjaADkaFTbjr0JGBpw"
Uri-Path: "mid=123"
Content-Format: "application/dots+cbor"

{
  "ietf-dots-signal-channel:redirected-signal": {
    "ietf-dots-call-home:alt-ch-client":
                    "alt-call-home-client.example",
    "ietf-dots-call-home:alt-ch-client-record": [
        "2001:db8:6401::1",
        "2001:db8:6401::2"
      ],
    "ietf-dots-call-home:ttl": 600
}
```

Figure 8: Example of a PUT Request for Redirected Signaling

3.3. DOTS Signal Channel Extension

3.3.1. Mitigation Request

This specification extends the mitigation request defined in
Section 4.4.1 of [I-D.ietf-dots-signal-channel] to convey the attack
source information (e.g., source prefixes, source port numbers). The
DOTS client conveys the following new parameters in the CBOR body of
the mitigation request:

source-prefix: A list of attacker prefixes used to attack the
   target. Prefixes are represented using Classless Inter-Domain
   Routing (CIDR) notation [RFC4632].

   As a reminder, the prefix length MUST be less than or equal to 32

(or 128) for IPv4 (or IPv6).

The prefix list MUST NOT include broadcast, loopback, or multicast
addresses. These addresses are considered as invalid values. In
addition, the DOTS client MUST validate that attacker prefixes are
within the scope of the DOTS server domain.

This is an optional attribute for the base DOTS signal channel
operations.

source-port-range: A list of port numbers used by the attack traffic
   flows.

   A port range is defined by two bounds, a lower port number (lower-
   port) and an upper port number (upper-port). When only 'lower-
   port' is present, it represents a single port number.

   For TCP, UDP, Stream Control Transmission Protocol (SCTP)
   [RFC4960], or Datagram Congestion Control Protocol (DCCP)
   [RFC4340], a range of ports can be any subrange of 0-65535, for
   example, 0-1023, 1024-65535, or 1024-49151.

   This is an optional attribute for the base DOTS signal channel
   operations.

source-icmp-type-range: A list of ICMP types used by the attack
   traffic flows. An ICMP type range is defined by two bounds, a
   lower ICMP type (lower-type) and an upper ICMP type (upper-type).
   When only 'lower-type' is present, it represents a single ICMP
   type.

   This is an optional attribute for the base DOTS signal channel
   operations.

The 'source-prefix' parameter is a mandatory attribute when the
attack traffic information is signaled by a Call Home DOTS client
(i.e., the Call Home scenario depicted in Figure 7). The 'target-
uri' or 'target-fqdn' parameters can be included in a mitigation
request for diagnostic purposes to notify the Call Home DOTS server
domain administrator, but SHOULD NOT be used to determine the target
IP addresses. Note that 'target-prefix' becomes a mandatory
attribute in the mitigation request signaling the attack information
because 'target-uri' and 'target-fqdn' are optional attributes and
'alias-name' will not be conveyed in a mitigation request.

In order to help attack source identification by a Call Home DOTS
server, the Call Home DOTS client SHOULD include in its mitigation
request additional information such as 'source-port-range' or
'source-icmp-type-range'. The Call Home DOTS client may not include
such information if 'source-prefix' conveys an IPv6 address/prefix.
Address sharing implications on the setting of source information
('source-prefix', 'source-port-range') are discussed in
Section 3.3.2.

Only immediate mitigation requests (i.e., 'trigger-mitigation' set to
'true') are allowed; Call Home DOTS clients MUST NOT send requests
with 'trigger-mitigation' set to 'false'. Such requests MUST be
discarded by the Call Home DOTS server with a 4.00 (Bad Request).

An example of a mitigation request sent by a Call Home DOTS client is
shown in Figure ~~8.~~ **9.**

```
  Header: PUT (Code=0.03)
  Uri-Path: ".well-known"
  Uri-Path: "dots"
  Uri-Path: "mitigate"
  Uri-Path: "cuid=dz6pHjaADkaFTbjr0JGBpw"
  Uri-Path: "mid=56"
  Content-Format: "application/dots+cbor"

  {
    "ietf-dots-signal-channel:mitigation-scope": {
      "scope": [
          {
```

```
                "target-prefix": [
                   "2001:db8:c000::/128"
                 ],
                "ietf-dots-call-home:source-prefix": [
                   "2001:db8:123::/128"
                 ],
                "lifetime": 3600
             }
           ]
         }
       }
```

      Figure 8: 9: An Example of Mitigation Request Issued by a Call Home DOTS
                                     Client

      The Call Home DOTS server MUST check that the 'source-prefix' is
      within the scope of the Call Home DOTS server domain. Note that in a
      DOTS Call Home scenario, the Call Home DOTS server considers, by
      default, that any routeable IP prefix enclosed in 'target-prefix' is
      within the scope of the Call Home DOTS client. Invalid mitigation
      requests are handled as per Section 4.4.1 of
      [I-D.ietf-dots-signal-channel].

         Note: These validation checks do not apply when the source
         information is included as a hint in the context of the base DOTS
         signal channel.

      The Call Home DOTS server domain administrator consent MAY be
      required to block the traffic from the compromised device to the
      attack target. An implementation MAY have a configuration knob to
      block the traffic from the compromised device to the attack target
      with or without DOTS server domain administrator consent. If the
      attack traffic is blocked, the Call Home DOTS server informs the Call
      Home DOTS client that the attack is being mitigated.

      If the attack traffic information is identified by the Call Home DOTS
      server or the Call Home DOTS server domain administrator as
      legitimate traffic, the mitigation request is rejected, and 4.09
      (Conflict) is returned to the Call Home DOTS client. The conflict-
      clause (defined in Section 4.4.1 of [I-D.ietf-dots-signal-channel])
      indicates the cause of the conflict. The following new value is
      defined:

      4: Mitigation request rejected. This code is returned by the DOTS
         server to indicate the attack traffic has been classified as
         legitimate traffic.

      Once the request is validated by the Call Home DOTS server,
      appropriate actions are enforced to block the attack traffic within
      the source network. The Call Home DOTS client is informed about the
      progress of the attack mitigation following the rules in
      [I-D.ietf-dots-signal-channel]. For example, if the Call Home DOTS
      server is embedded in a CPE, it can program the packet processor to
      punt all the traffic from the compromised device to the target to
      slow path. The CPE inspects the punted slow path traffic to detect
      and block the outgoing DDoS attack traffic or quarantine the device
      (e.g., using MAC level filtering) until it is remediated, and
      notifies the CPE administrator about the compromised device.

      The DOTS agents follow the same procedures specified in
      [I-D.ietf-dots-signal-channel] for managing a mitigation request.

   3.3.2. Address Sharing Considerations

      If a Carrier Grade NAT (CGN, including NAT64) is located between the
      DOTS client domain and DOTS server domain, communicating an external
      IP address in a mitigation request is likely to be discarded by the
      Call Home DOTS server because the external IP address is not visible
      locally to the Call Home DOTS server (see Figure 9). 10). The Call Home
      DOTS server is only aware of the internal IP addresses/prefixes bound
      to its domain. Thus, the Call Home DOTS client MUST NOT include the
      external IP address and/or port number identifying the suspect attack
      source, but MUST include the internal IP address and/or port number.
      To that aim, the Call Home DOTS client SHOULD rely on mechanisms,

such as [RFC8512] or [RFC8513], to retrieve the internal IP address
and port number which are mapped to an external IP address and port
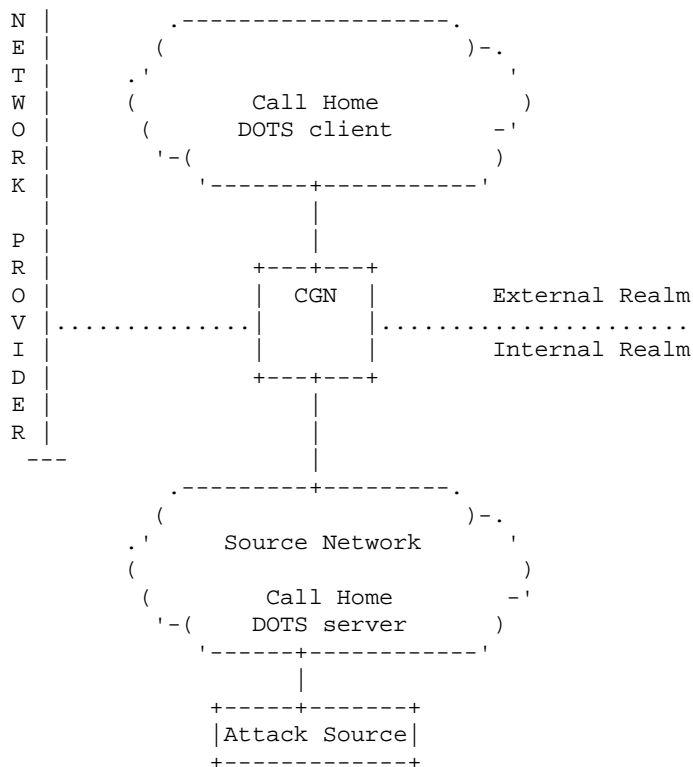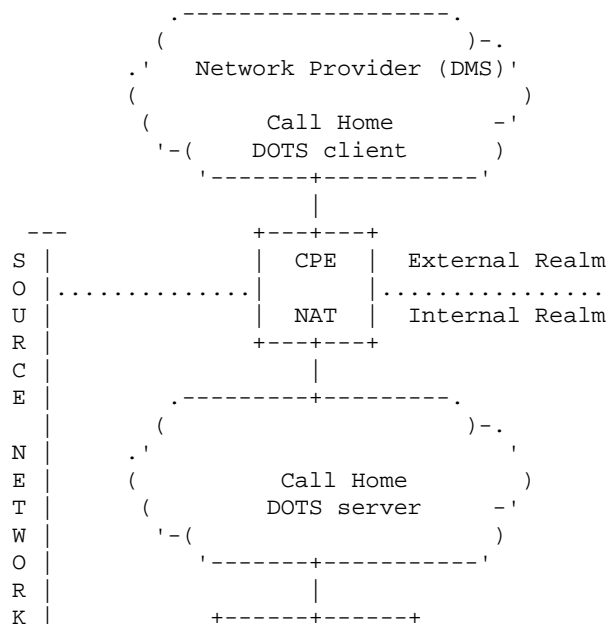number.

```
              N |  .------------------.
              E |     (                        )-.
              T |    .'                          '
              W |   (         Call Home          )
              O |    (      DOTS client       -'
              R |     '-(                      )
              K |        '-------+-----------'
                |               |
              P |               |
              R |           +---+---+
              O |           | CGN  |      External Realm
              V |...............|     |......................
              I |           |     |      Internal Realm
              D |           +---+---+
              E |               |
              R |               |
               ---              |
                    .---------+---------.
                   (                     )-.
                  .'    Source Network     '
                 (                          )
                  (        Call Home      -'
                   '-(     DOTS server    )
                      '------+-----------'
                            |
                      +-----+-------+
                      |Attack Source|
                      +------------+
```

Figure 9: **10:** Example of a CGN between DOTS Domains

If a MAP Border Relay [RFC7597] or lwAFTR [RFC7596] is enabled in the
provider's domain to service its customers, the identification of an
attack source bound to an IPv4 address/prefix MUST also rely on
source port numbers because the same IPv4 address is assigned to
multiple customers. The port information is required to
unambiguously identify the source of an attack.

If a translator is enabled on the boundaries of the domain hosting
the Call Home DOTS server (e.g., a CPE with NAT enabled as shown in
Figures 10 **11** and 11), **12),** the Call Home DOTS server uses the attack traffic
information conveyed in a mitigation request to find the internal
source IP address of the compromised device and blocks the traffic
from the compromised device traffic to the attack target until the
mitigation request is withdrawn. Doing so allows to isolate the
suspicious device while avoiding to disturb other services.

```
                   .-------------------.
                  (                     )-.
                 .'   Network Provider (DMS)'
                (                          )
                 (        Call Home      -'
                  '-(     DOTS client      )
                     '-------+-----------'
                            |
           ---           +---+---+
         S |            | CPE  | External Realm
         O |...............|     |...............
         U |            | NAT  | Internal Realm
         R |            +---+---+
         C |                |
         E |    .---------+---------.
           |   (                     )-.
         N |  .'                        '
         E |  (        Call Home        )
         T |   (       DOTS server    -'
         W |    '-(                    )
         O |       '-------+-----------'
         R |              |
         K |          +------+------+
```

```
                    |                 |Attack Source|
                                      +-------------+
```
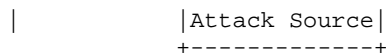
      Figure ~~10:~~ **11:** Example of a DOTS Server Domain with a NAT Embedded in a
                                  CPE

```
                         .------------------.
                        (                    )-.
                      .'  Network Provider (DMS) '
                     (                          )
                      (          Call Home     -'
                       '-(     DOTS client      )
                          '---------+---------'
                                    |
              ---                +-----+-----+
            S |                  | CPE/NAT   |  External Realm
            O |..............|   |           |................
            U |                  | Call Home |  Internal Realm
            R |                  |DOTS server|
            C |                  +-----+-----+
            E |                        |
              |         .-----------+-------.
              |        (                     )-.
            N |      .'                        '
            E |     (      Local Area Network   )
            T |      (                         -'
            W |       '-(                      )
            O |          '--------+----------'
            R |                   |
            K |            +------+------+
              |            |Attack Source|
                           +-------------+
```

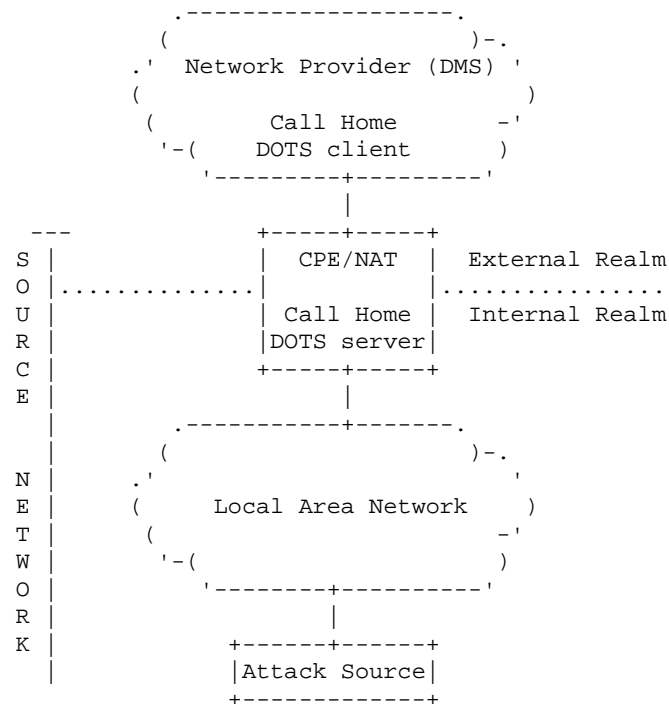   Figure ~~11:~~ **12:** Example of a Call Home DOTS Server and a NAT Embedded in a
                                  CPE

3.3.3.   DOTS Signal Call Home YANG Module

3.3.3.1.   Tree Structure

      This document augments the "ietf-dots-signal-channel" DOTS signal
      YANG module defined in [I-D.ietf-dots-signal-channel] for signaling
      the attack traffic information. This document defines the YANG
      module "ietf-dots-call-home", which has the following tree structure:

```
      module: ietf-dots-call-home
        augment /ietf-signal:dots-signal/ietf-signal:message-type
                /ietf-signal:mitigation-scope/ietf-signal:scope:
          +--rw source-prefix*      inet:ip-prefix {source-signaling}?
          +--rw source-port-range* [lower-port] {source-signaling}?
          |  +--rw lower-port    inet:port-number
          |  +--rw upper-port?   inet:port-number
          +--rw source-icmp-type-range*
          |                     [lower-type] {source-signaling}?
             +--rw lower-type    uint8
             +--rw upper-type?   uint8
        augment /ietf-signal:dots-signal/ietf-signal:message-type
                /ietf-signal:redirected-signal:
          +--rw alt-ch-client           string {call-home}?
          +--rw alt-ch-client-record*   inet:ip-address {call-home}?
          +--rw ttl     uint32 {call-home}?
```

3.3.3.2.   YANG Module

      This module uses the common YANG types defined in [RFC6991].

      <CODE BEGINS> file ~~"ietf-dots-call-home@2019-04-25.yang"~~ **"ietf-dots-call-home@2019-09-06.yang"**

```
      module ietf-dots-call-home {
        yang-version 1.1;
        namespace "urn:ietf:params:xml:ns:yang:ietf-dots-call-home";
        prefix call-home;

        import ietf-inet-types {
```

```
      prefix inet;
      reference
        "Section 4 of RFC 6991";
    }
    import ietf-dots-signal-channel {
      prefix ietf-signal;
      reference
        "RFC YYYY: Distributed Denial-of-Service Open Threat
                   Signaling (DOTS) Signal Channel Specification";
    }

    organization
      "IETF DDoS Open Threat Signaling (DOTS) Working Group";
    contact
      "WG Web:   <https://datatracker.ietf.org/wg/dots/>
       WG List:  <mailto:dots@ietf.org>

       Author:   Konda, Tirumaleswar Reddy
                 <mailto:TirumaleswarReddy_Konda@McAfee.com>;

       Author:   Mohamed Boucadair
                 <mailto:mohamed.boucadair@orange.com>;

       Author:   Jon Shallow
                 <mailto:ietf-supjps@jpshallow.com>";

    description
      "This module contains YANG definitions for the signaling
       messages exchanged between a DOTS client and a DOTS server
       for the Call Home deployment scenario.

       Copyright (c) 2019 IETF Trust and the persons identified as
       authors of the code.  All rights reserved.

       Redistribution and use in source and binary forms, with or
       without modification, is permitted pursuant to, and subject
       to the license terms contained in, the Simplified BSD License
       set forth in Section 4.c of the IETF Trust's Legal Provisions
       Relating to IETF Documents
       (http://trustee.ietf.org/license-info).

       This version of this YANG module is part of RFC XXXX; see
       the RFC itself for full legal notices.";

    revision 2019-04-25 2019-09-06 {
      description
        "Initial revision.";
      reference
        "RFC XXXX: Distributed Denial-of-Service Open Threat
                   Signaling (DOTS) Signal Channel Call Home";
    }

    feature source-signaling {
      description
        "This feature means that source-related information
         can be supplied in mitigation requests."; requests. This is
         typically applicable for DOTS Call Home.";
    }
    feature call-home {
      description
        "This feature means that Call Home functionality
         is supported.";
    }

    augment "/ietf-signal:dots-signal/ietf-signal:message-type/"
          + "ietf-signal:mitigation-scope/ietf-signal:scope" {

      if-feature source-signaling;
      description "Attacker source details.";

      leaf-list source-prefix {
        type inet:ip-prefix;
        description
          "IPv4 or IPv6 prefix identifying the attacker(s).";
```

```
        }
      list source-port-range {
        key "lower-port";
        description
          "Port range. When only lower-port is
           present, it represents a single port number.";
        leaf lower-port {
          type inet:port-number;
          mandatory true;
          description
            "Lower port number of the port range.";
        }
        leaf upper-port {
          type inet:port-number;
          must ". >= ../lower-port" {
             error-message
               "The upper port number must be greater than
                or equal to lower port number.";
          }
          description
            "Upper port number of the port range.";
        }
      }
      list source-icmp-type-range {
        key "lower-type";
        description
          "ICMP type range. When only lower-type is
           present, it represents a single ICMP type.";
        leaf lower-type {
          type uint8;
          mandatory true;
          description
            "Lower ICMP type of the ICMP type range.";
        }
        leaf upper-type {
          type uint8;
          must ". >= ../lower-type" {
             error-message
               "The upper ICMP type must be greater than
                or equal to lower ICMP type.";
          }
          description
            "Upper type of the ICMP type range.";
        }
      }
    }

    augment "/ietf-signal:dots-signal/ietf-signal:message-type/"
          + "ietf-signal:redirected-signal" {
      if-feature call-home;
      description
        "The alternate Call Home DOTS client.";

      leaf alt-ch-client {
        type string;
        description
          "FQDN of an alternate Call Home DOTS client.";
      }
      leaf-list alt-ch-client-record {
        type inet:ip-address;
        description
          "List of records for the alternate Call Home
           DOTS client.";
      }
      leaf ttl {
        type uint32;
        units "seconds";
        description
          "The Time to live (TTL) of the alternate Call Home
           DOTS client.";
      }
    }
  }
<CODE ENDS>
```

4. IANA Considerations

4.1. DOTS Signal Channel Call Home UDP and TCP Port Number

   IANA is requested to assign the port number TBD to the DOTS signal
   channel Call Home protocol for both UDP and TCP from the "Service
   Name and Transport Protocol Port Number Registry" available at:
   https://www.iana.org/assignments/service-names-port-numbers/service-
   names-port-numbers.xhtml.

      Service Name: dots-call-home
      Port Number: TBD
      Transport Protocol(s): TCP/UDP
      Description: DOTS Signal Channel Call Home
      Assignee: IESG <iesg@ietf.org>
      Contact: IETF Chair <chair@ietf.org>
      Reference: RFC XXXX

   The assignment of port number 4647 is strongly suggested (DOTS signal
   channel uses port number 4646).

4.2. DOTS Signal Channel CBOR Mappings Registry

   This specification registers the 'source-prefix', 'source-port-
   range', and 'source-icmp-type-range' parameters in the IANA "DOTS
   Signal Channel CBOR Key Values" registry established by
   [I-D.ietf-dots-signal-channel] (Figure 12). 13).

   The 'source-prefix', 'source-port-range', and 'source-icmp-type-
   range' are comprehension-optional parameters.

   o Note to the RFC Editor: Please delete (TBD1)-(TBD5) once CBOR keys
      are assigned from the 0x8000 - 0xBFFF range.

```
+------------------+-----------+--------+---------------+--------+
| Parameter Name   | YANG      | CBOR   | CBOR Major    | JSON   |
|                  | Type      | Key    | Type &        | Type   |
|                  |           |        | Information   |        |
+------------------+-----------+--------+---------------+--------+
| source-prefix    | leaf-list | 0x8000 | 4 array       | Array  |
|                  | inet:     | (TBD1) |               |        |
|                  |  ip-prefix|        | 3 text string | String |
| source-port-range| list      | 0x8001 | 4 array       | Array  |
|                  |           | (TBD2) |               |        |
| source-icmp-type-| list      | 0x8002 | 4 array       | Array  |
|  range           |           | (TBD3) |               |        |
| lower-type       | uint8     | 0x8003 | 0 unsigned    | Number |
|                  |           | (TBD4) |               |        |
| upper-type       | uint8     | 0x8004 | 0 unsigned    | Number |
|                  |           | (TBD5) |               |        |
| alt-ch-client    | string    | 0x8005 | 3 text string | String |
|                  |           | (TBD6) |               |        |
| alt-ch-client-   | leaf-list | 0x8006 | 4 array       | Array  |
|  record          | inet:     | (TBD7) |               |        |
|                  |  ip-address|       | 3 text string | String |
| ttl              | uint32    | 0x8007 | 0 unsigned    | Number |
|                  |           | (TBD8) |               |        |
+------------------+-----------+--------+---------------+--------+
```

          Figure 12: 13: Assigned DOTS Signal Channel CBOR Key Values

4.3. New DOTS Conflict Cause

   This document requests IANA to assign a new code from the "DOTS
   Signal Channel Conflict Cause Codes" registry:

```
+-----+-----------------------------------+-------------+-----------+
| Cod | Label                             | Description | Reference |
| e   |                                   |             |           |
+-----+-----------------------------------+-------------+-----------+
| 4   | request-rejected-legitimate-      | Mitigation  | [RFCXXXX] |
|     | traffic                           | request     |           |
|     |                                   | rejected.   |           |
```

```
|     |                                  | This code   |          |
|     |                                  | is returned |          |
|     |                                  | by the DOTS |          |
|     |                                  | server to   |          |
|     |                                  | indicate    |          |
|     |                                  | the attack  |          |
|     |                                  | traffic has |          |
|     |                                  | been        |          |
|     |                                  | classified  |          |
|     |                                  | as          |          |
|     |                                  | legitimate  |          |
|     |                                  | traffic.    |          |
+-----+----------------------------------+-------------+----------+
```

4.4. DOTS Signal Call Home YANG Module

   This document requests IANA to register the following URI in the "ns"
   subregistry within the "IETF XML Registry" [RFC3688]:

           URI: urn:ietf:params:xml:ns:yang:ietf-dots-call-home
           Registrant Contact: The IESG.
           XML: N/A; the requested URI is an XML namespace.

   This document requests IANA to register the following YANG module in
   the "YANG Module Names" subregistry [RFC7950] within the "YANG
   Parameters" registry:

           name: ietf-dots-call-home
           namespace: urn:ietf:params:xml:ns:yang:ietf-dots-call-home
           maintained by IANA: N
           prefix: call-home
           reference: RFC XXXX

5. Security Considerations

   This document deviates from classic DOTS signal channel usage by
   having the DOTS server initiate the (D)TLS connection. DOTS signal
   channel related security considerations discussed in Section 10 of
   [I-D.ietf-dots-signal-channel] MUST be considered. DOTS agents MUST
   authenticate each other using (D)TLS before a DOTS signal channel
   session is considered valid.

   An attacker may launch a DoS attack on the DOTS client by having it
   perform computationally expensive operations, before deducing that
   the attacker doesn't possess a valid key. For instance, in TLS 1.3
   [RFC8446], the ServerHello message contains a Key Share value based
   on an expensive asymmetric key operation for key establishment.
   Common precautions mitigating DoS attacks are recommended, such as
   temporarily blacklisting the source address after a set number of
   unsuccessful authentication attempts.

   Call Home DOTS servers may not blindly trust mitigation requests from
   Call Home DOTS clients. For example, DOTS servers can use the attack
   flow information in a mitigation request to enable full-fledged
   packet inspection function to inspect all the traffic from the
   compromised device to the target or to re-direct the traffic from the
   compromised device to the target to a DDoS mitigation system to scrub
   the suspicious traffic. Call Home DOTS servers can also seek the
   consent of DOTS server domain administrator to block the traffic from
   the compromised device to the target (see Section 3.3.1).

6. Privacy Considerations

   The considerations discussed in [RFC6973] were taken into account to
   assess whether the DOTS Call Home introduces privacy threats.

   Concretely, the protocol does not leak any new information that can
   be used to ease surveillance. In particular, the Call Home DOTS
   server is not required to share information that is local to its
   network (e.g., internal identifiers of an attack source) with the
   Call Home DOTS client.

   The DOTS Call Home does not preclude the validation of mitigation
   requests received from a Call Home DOTS client. For example, a

security service running on the CPE may require administrator's consent before the CPE acts upon the mitigation request indicated by the Call Home DOTS client. How the consent is obtained is out of scope of this document.

Note that a Call Home DOTS server can seek for an administrator's consent, validate the request by inspecting the traffic, or proceed with both.

The DOTS Call Home is only advisory in nature. Concretely, the DOTS Call Home does not impose any action to be enforced within the network hosting an attack source; it is up to the Call Home DOTS server (and/or network administrator) to decide whether and which actions are required.

Moreover, the DOTS Call Home avoids misattribution by appropriately identifying the network to which a suspect attack source belongs to (e.g., address sharing issues discussed in Section 3.3.1).

Triggers to send a DOTS mitigation request to a Call Home DOTS server are deployment-specific. For example, a Call Home DOTS client may rely on the output of some DDoS detection systems deployed within the DOTS client domain to detect potential outbound DDoS attacks or on abuse claims received from remote victim networks. Such DDoS detection and mitigation techniques are not meant to track the activity of users, but to protect the Internet and avoid altering the IP reputation of the DOTS client domain.

7. Contributors

   The following individuals have contributed to this document:

      Joshi Harsha
      McAfee, Inc.
      Embassy Golf Link Business Park
      Bangalore, Karnataka 560071
      India

      Email: harsha_joshi@mcafee.com

      Wei Pan
      Huawei Technologies
      China

      Email: william.panwei@huawei.com

8. Acknowledgements

   Thanks to Wei Pei, Xia Liang, Roman Danyliw, Dan Wing, Toema Gavrichenkov, Daniel Migault, and Valery Smyslov for the comments.

9. References

9.1. Normative References

   [I-D.ietf-dots-signal-channel]
              K, R., Boucadair, M., Patil, P., Mortensen, A., and N.
              Teague, "Distributed Denial-of-Service Open Threat
              Signaling (DOTS) Signal Channel Specification", draft-
              ietf-dots-signal-channel-35
              ietf-dots-signal-channel-37 (work in progress), July 2019.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688,
              DOI 10.17487/RFC3688, January 2004,
              <https://www.rfc-editor.org/info/rfc3688>.

   [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer
              Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347,
              January 2012, <https://www.rfc-editor.org/info/rfc6347>.

   [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types",
              RFC 6991, DOI 10.17487/RFC6991, July 2013,
              <https://www.rfc-editor.org/info/rfc6991>.

   [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language",
              RFC 7950, DOI 10.17487/RFC7950, August 2016,
              <https://www.rfc-editor.org/info/rfc7950>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol
              Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,
              <https://www.rfc-editor.org/info/rfc8446>.

9.2. Informative References

   [I-D.ietf-dots-multihoming]
              Boucadair, M., K, R., and W. Pan, "Multi-homing Deployment
              Considerations for Distributed-Denial-of-Service Open
              Threat Signaling (DOTS)", draft-ietf-dots-multihoming-02
              (work in progress), July 2019.

   [I-D.ietf-dots-server-discovery]
              Boucadair, M. and R. K, "Distributed-Denial-of-Service
              Open Threat Signaling (DOTS) ~~Server~~ **Agent** Discovery", ~~draft-
              ietf-dots-server-discovery-04~~ **draft-ietf-
              dots-server-discovery-05** (work in progress), ~~June~~ **August** 2019.

   [I-D.ietf-dots-use-cases]
              Dobbins, R., Migault, D., ~~Fouant, S.,~~ Moskowitz, R., Teague, N., Xia,
              L., and K. Nishizuka, "Use cases for DDoS Open Threat
              Signaling", ~~draft-ietf-dots-use-cases-18~~ **draft-ietf-dots-use-cases-20** (work in
              progress), ~~July~~ **September** 2019.

   [I-D.ietf-i2nsf-terminology]
              Hares, S., Strassner, J., Lopez, D., Xia, L., and H.
              Birkholz, "Interface to Network Security Functions (I2NSF)
              Terminology", draft-ietf-i2nsf-terminology-08 (work in
              progress), July 2019.

   [I-D.ietf-idr-flow-spec-v6]
              McPherson, D., Raszuk, R., Pithawala, B.,
              akarch@cisco.com, a., and S. Hares, "Dissemination of Flow
              Specification Rules for IPv6", draft-ietf-idr-flow-spec-
              v6-09 (work in progress), November 2017.

   [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address
              Translator (NAT) Terminology and Considerations",
              RFC 2663, DOI 10.17487/RFC2663, August 1999,
              <https://www.rfc-editor.org/info/rfc2663>.

   [RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram
              Congestion Control Protocol (DCCP)", RFC 4340,
              DOI 10.17487/RFC4340, March 2006,
              <https://www.rfc-editor.org/info/rfc4340>.

   [RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing
              (CIDR): The Internet Address Assignment and Aggregation
              Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August
              2006, <https://www.rfc-editor.org/info/rfc4632>.

   [RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet
              Denial-of-Service Considerations", RFC 4732,
              DOI 10.17487/RFC4732, December 2006,
              <https://www.rfc-editor.org/info/rfc4732>.

   [RFC4949] Shirey, R., "Internet Security Glossary, Version 2",
              FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007,
              <https://www.rfc-editor.org/info/rfc4949>.

   [RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol",

                     RFC 4960, DOI 10.17487/RFC4960, September 2007,
                     <https://www.rfc-editor.org/info/rfc4960>.

     [RFC5575]   Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J.,
                     and D. McPherson, "Dissemination of Flow Specification
                     Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009,
                     <https://www.rfc-editor.org/info/rfc5575>.

     [RFC6398]   Le Faucheur, F., Ed., "IP Router Alert Considerations and
                     Usage", BCP 168, RFC 6398, DOI 10.17487/RFC6398, October
                     2011, <https://www.rfc-editor.org/info/rfc6398>.

     [RFC6973]   Cooper, A., Tschofenig, H., Aboba, B., Peterson, J.,
                     Morris, J., Hansen, M., and R. Smith, "Privacy
                     Considerations for Internet Protocols", RFC 6973,
                     DOI 10.17487/RFC6973, July 2013,
                     <https://www.rfc-editor.org/info/rfc6973>.

     [RFC7596]   Cui, Y., Sun, Q., Boucadair, M., Tsou, T., Lee, Y., and I.
                     Farrer, "Lightweight 4over6: An Extension to the Dual-
                     Stack Lite Architecture", RFC 7596, DOI 10.17487/RFC7596,
                     July 2015, <https://www.rfc-editor.org/info/rfc7596>.

     [RFC7597]   Troan, O., Ed., Dec, W., Li, X., Bao, C., Matsushima, S.,
                     Murakami, T., and T. Taylor, Ed., "Mapping of Address and
                     Port with Encapsulation (MAP-E)", RFC 7597,
                     DOI 10.17487/RFC7597, July 2015,
                     <https://www.rfc-editor.org/info/rfc7597>.

     [RFC8071]   Watsen, K., "NETCONF Call Home and RESTCONF Call Home",
                     RFC 8071, DOI 10.17487/RFC8071, February 2017,
                     <https://www.rfc-editor.org/info/rfc8071>.

     [RFC8340]   Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams",
                     BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018,
                     <https://www.rfc-editor.org/info/rfc8340>.

     [RFC8512]   Boucadair, M., Ed., Sivakumar, S., Jacquenet, C.,
                     Vinapamula, S., and Q. Wu, "A YANG Module for Network
                     Address Translation (NAT) and Network Prefix Translation
                     (NPT)", RFC 8512, DOI 10.17487/RFC8512, January 2019,
                     <https://www.rfc-editor.org/info/rfc8512>.

     [RFC8513]   Boucadair, M., Jacquenet, C., and S. Sivakumar, "A YANG
                     Data Model for Dual-Stack Lite (DS-Lite)", RFC 8513,
                     DOI 10.17487/RFC8513, January 2019,
                     <https://www.rfc-editor.org/info/rfc8513>.

     [RFC8517]   Dolson, D., Ed., Snellman, J., Boucadair, M., Ed., and C.
                     Jacquenet, "An Inventory of Transport-Centric Functions
                     Provided by Middleboxes: An Operator Perspective",
                     RFC 8517, DOI 10.17487/RFC8517, February 2019,
                     <https://www.rfc-editor.org/info/rfc8517>.

     [RFC8576]   Garcia-Morchon, O., Kumar, S., and M. Sethi, "Internet of
                     Things (IoT) Security: State of the Art and Challenges",
                     RFC 8576, DOI 10.17487/RFC8576, April 2019,
                     <https://www.rfc-editor.org/info/rfc8576>.

     [RFC8612]   Mortensen, A., Reddy, T., and R. Moskowitz, "DDoS Open
                     Threat Signaling (DOTS) Requirements", RFC 8612,
                     DOI 10.17487/RFC8612, May 2019,
                     <https://www.rfc-editor.org/info/rfc8612>.

     [Sec]   UK Department for Digital Culture, Media & Sport, "Secure
                     by Design: Improving the cyber security of consumer
                     Internet of Things Report", March 2018,
                     <https://www.gov.uk/government/publications/
                     secure-by-design-report>.

Appendix A. Disambiguate Base DOTS Signal vs. DOTS Call Home

   With the DOTS signal channel Call Home, there is a chance that two
   DOTS agents can simultaneously establish two DOTS signal channels

with different directions (base DOTS signal channel and DOTS signal
channel Call Home). Here is one example drawn from the home network.
Nevertheless, the outcome of the discussion is not specific to these
networks, but applies to any DOTS Call Home scenario.

In the Call Home scenario, the DOTS server in, for example, the home
network can mitigate the DDoS attacks launched by the compromised
device in its domain by receiving the mitigation request sent by the
Call Home DOTS client in the ISP environment. In addition, the DOTS
client in the home network can initiate a mitigation request to the
DOTS server in the ISP environment to ask for help when the home
network is under a DDoS attack. Such DOTS server and DOTS client in
the home network can co-locate in the same home network element
(e.g., the Customer Premises Equipment). In this case, with the same
peer at the same time the home network element will have the base
DOTS signal channel and the DOTS signal channel Call Home defined in
this specification. Thus, these two signal channels need to be
distinguished when they are both supported. Two approaches have been
considered for distinguishing the two DOTS signal channels, but only
the one that using the dedicated port number has been chosen as the
best choice.

By using a dedicated port number for each, these two signal channels
can be separated unambiguously and easily. For example, the CPE uses
the port number 4646 allocated in [I-D.ietf-dots-signal-channel] to
initiate the basic signal channel to the ISP when it acts as the DOTS
client, and uses the port number TBD to initiate the signal channel
Call Home. Based on the different port numbers, the ISP can directly
decide which kind of procedures should follow immediately after it
receives the DOTS messages. This approach just requires two (D)TLS
sessions to be established respectively for the basic signal channel
and signal channel Call Home.

The other approach is signaling the role of each DOTS agent (e.g., by
using the DOTS data channel). For example, the DOTS agent in the
home network first initiates a DOTS data channel to the peer DOTS
agent in the ISP environment, at this time the DOTS agent in the home
network is the DOTS client and the peer DOTS agent in the ISP
environment is the DOTS server. After that, the DOTS agent in the
home network retrieves the DOTS Call Home capability of the peer DOTS
agent. If the peer supports the DOTS Call Home, the DOTS agent needs
to subscribe to the peer to use this extension. Then, the reversal
of DOTS role can be recognized as done by both DOTS agents. When the
DOTS agent in the ISP environment, which now is the DOTS client,
wants to filter the attackers' traffic, it requests the DOTS agent in
the home network, which now is the DOTS server, for help.

Signaling the role will complicate the DOTS protocol, and this
complexity is not required in context where the DOTS Call Home is not
required or only when the DOTS Call Home is needed. Besides, the
DOTS data channel may not work during attack time. Even if changing
the above example from using the DOTS data channel to the DOTS signal
channel, the more procedures will still reduce the efficiency. Using
the dedicated port number is much easier and more concise compared to
the second approach, and its cost that establishing two (D)TLS
sessions is much less. So, using a dedicated port number for the
DOTS Call Home is chosen in this specification.

Authors' Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka   560071
India

Email: kondtir@gmail.com

Mohamed Boucadair
Orange
Rennes   35000
France

Email: mohamed.boucadair@orange.com

Jon Shallow
UK

Email: supjps-ietf@jpshallow.com