DOTS
Internet-Draft
Intended status: Informational
Expires: January 18, 2019

R. Dobbins
Arbor Networks
D. Migault
Ericsson
S. Fouant

R. Moskowitz
HTT Consulting
N. Teague
Verisign
L. Xia
Huawei
K. Nishizuka
NTT Communications
July 17, 2018

Use cases for DDoS Open Threat Signaling
draft-ietf-dots-use-cases-14

Abstract

The DDoS Open Threat Signaling (DOTS) effort is intended to provide protocols to facilitate interoperability across disparate DDoS mitigation solutions. This document presents use cases which describe the interactions expected between the DOTS components as well as DOTS messaging exchanges. These use cases are meant to identify the interacting DOTS components, how they collaborate and what are the typical information to be exchanged.

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 https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 18, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Terminology and Acronyms 3
3. Use Cases 3
3.1. Upstream DDoS Mitigation by an Upstream Internet Transit Provider 3
3.2. DDoS Mitigation by a Third Party DDoS Mitigation Service Provider 7
3.3. DDoS Orchestration 9
4. Security Considerations 12
5. IANA Considerations 12
6. Acknowledgments 12
7. Informative References 13
Authors' Addresses 13

1. Introduction

At the time of writing, distributed denial-of-service (DDoS) attack mitigation solutions are largely based upon siloed, proprietary communications schemes with vendor lock-in as a side-effect. This can result in the configuration, provisioning, operation, and activation of these solutions being a highly manual and often time-consuming process. Additionally, coordinating multiple DDoS mitigation solutions simultaneously is fraught with both technical and process-related hurdles. This greatly increases operational complexity which, in turn, can degrade the efficacy of mitigations.

The DDoS Open Threat Signaling (DOTS) effort is intended to specify protocols that facilitate interoperability between diverse DDoS mitigation solutions and ensure greater integration in term of mitigation requests and attack characterization patterns. As DDoS solutions are broadly heterogeneous among vendors, the primary goal

of DOTS is to provide high-level interaction amongst differing DDoS solutions, such as initiating, terminating DDoS mitigation assistance or requesting the status of a DDoS mitigation.

This document provides use cases to provide inputs for the design of the DOTS protocol(s). The use cases are not exhaustive and future use cases are expected to emerge as DOTS is adopted and evolves.

2. Terminology and Acronyms

This document makes use of the same terminology and definitions as [I-D.ietf-dots-requirements]. In addition it uses the terms defined below:

- DDoS Mitigation Service Provider: designates the administrative entity providing the DDoS Mitigation Service.

- DDoS Mitigation System (DMS): A system that performs DDoS mitigation. The DDoS Mitigation System may be composed by a cluster of hardware and/or software resources, but could also involve an orchestrator that may take decisions such as outsourcing partial or more of the mitigation to another DDoS Mitigation System.

- DDoS Mitigation Service: designates a DDoS mitigation service provided to a customer and which is scoped to mitigate DDoS attacks. Services usually involve Service Level Agreement (SLA) that have to be met. It is the responsibility of the service provider to instantiate the DDoS Mitigation System to meet these SLAs.

- DDoS Mitigation: The action performed by the DDoS Mitigation System.

- Internet Transit Provider (ITP): designates the entity that delivers the traffic to the network. It can be an Internet Service Provider (ISP), or an upstream entity delivering the traffic to the ISP.

3. Use Cases

3.1. Upstream DDoS Mitigation by an Upstream Internet Transit Provider

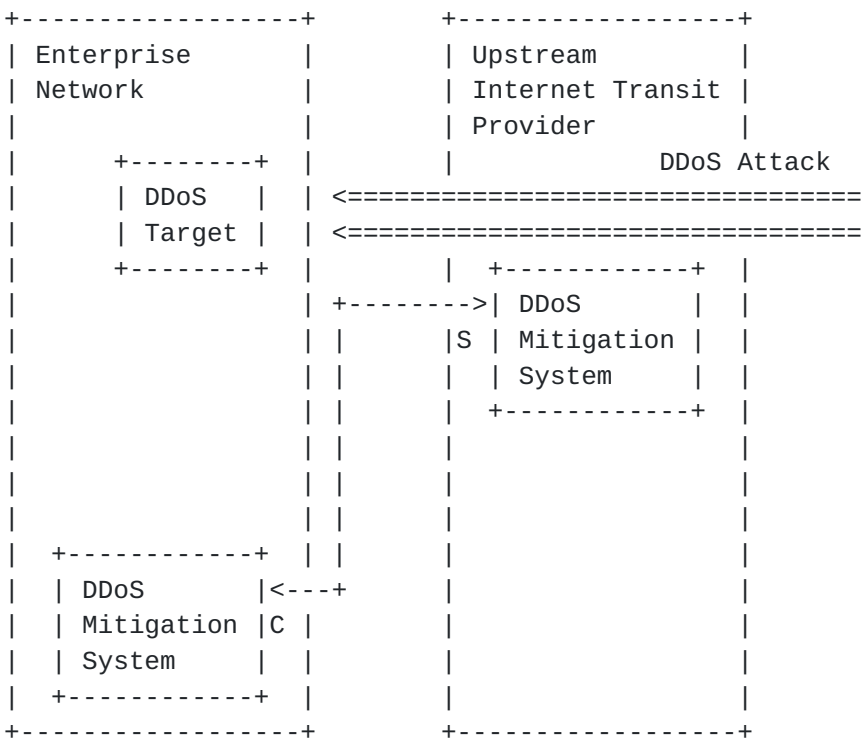
This use case describes how an enterprise or a residential customer network may take advantage of a pre-existing relation with its Internet Transit Provider (ITP) in order to mitigate a DDoS attack targeting its network. To improve the clarity of our purpose, the targeted network will be designated as enterprise network, but the

same scenario applies to any downstream network, including residential network and cloud hosting network. As the ITP provides connectivity to the enterprise network, it is already on the path of the inbound or outbound traffic of the enterprise network and well aware of the networking parameters associated to the enterprise network connectivity. This eases both the configuration and the instantiation of a DDoS Mitigation Service. This section considers two kind of DDoS Mitigation Service between an enterprise network and an ITP:

- The upstream ITP may instantiate a DDoS Mitigation System (DMS) upon receiving a request from the enterprise network. This typically corresponds to the case when the enterprise network is under attack.

- On the other hand, the ITP may identify an enterprise network as the source of an attack and send a mitigation request to the enterprise DMS to mitigate this at the source.

In the first scenario, as depicted in Figure 1, an enterprise network with self-hosted Internet-facing properties such as Web servers, authoritative DNS servers, and VoIP servers has a DMS deployed to protect those servers and applications from DDoS attacks. In addition to on-premise DDoS defense capability, enterprises have contracted with their ITP for DDoS Mitigation Services which threaten to overwhelm their WAN link(s) bandwidth.



* C is for DOTS client functionality
* S is for DOTS server functionality

Figure 1: Upstream Internet Transit Provider DDoS Mitigation

The enterprise DMS is configured such that if the incoming Internet traffic volume exceeds 50% of the provisioned upstream Internet WAN link capacity, the DMS will request DDoS mitigation assistance from the upstream transit provider.

The requests to trigger, manage, and finalize a DDoS Mitigation between the enterprise DMS and the ITP is performed using DOTS. The enterprise DMS implements a DOTS client while the ITP implements a DOTS server which is integrated with their DMS.

When the enterprise DMS detects an inbound DDoS attack targeting its resources (e.g. servers, hosts or applications), it immediately begins a DDoS Mitigation.

During the course of the attack, the inbound traffic volume exceeds the 50% threshold; the DMS DOTS client signals the DOTS server on the upstream ITP to initiate DDoS Mitigation. The DOTS server signals the DOTS client that it can serve this request, and mitigation is initiated on the ITP network by the ITP DMS.

Over the course of the attack, the DOTS server of the ITP periodically informs the DOTS client on the enterprise DMS mitigation status, statistics related to DDoS attack traffic mitigation, and related information. Once the DDoS attack has ended, or decreased to the certain level that the DOTS client can handle by itself, the DOTS server signals the enterprise DMS DOTS client that the attack has subsided.

The enterprise DMS then requests the ITP to terminate the DDoS Mitigation. The DOTS server on the ITP receives this request and once the mitigation has ended, confirms the end of upstream DDoS Mitigation to the enterprise DMS DOTS client.

The following is an overview of the DOTS communication model for this use-case:

- (a) A DDoS attack is initiated against resources of a network organization which has deployed a DOTS-capable DMS - typically a DOTS client.

- (b) The enterprise DMS detects, classifies, and begins the DDoS Mitigation.

- (c) The enterprise DMS determines that its capacity and/or capability to mitigate the DDoS attack is insufficient, and sends via its DOTS client a DOTS DDoS Mitigation request to one or more DOTS servers residing on the upstream ITP.

- (d) The DOTS server which receives the DOTS Mitigation request determines that it has been configured to honor requests from the requesting DOTS client, and honored its DDoS Mitigation by orchestrating its DMS.

- (e) While the DDoS Mitigation is active, DOTS server regularly transmits DOTS DDoS Mitigation status updates to the DOTS client.

- (f) Informed by the DOTS server status update that the attack has ended or subsided, the DOTS client transmits a DOTS DDoS Mitigation termination request to the DOTS server.

- (g) The DOTS server terminates DDoS Mitigation, and sends the notification to the DOTS client.

Note that communications between the enterprise DOTS client and the upstream ITP DOTS Server may take place in-band within the main Internet WAN link between the enterprise and the ITP; out-of-band via a separate, dedicated wireline network link utilized solely for DOTS

signaling; or out-of-band via some other form of network connectivity such as a third-party wireless 4G network connectivity.

Note also that a DOTS client that sends a DOTS Mitigation request may be also triggered by a network admin that manually confirms the request to the upstream ITP, in which case the request may be sent from an application such as a web browser or a dedicated mobile application.

Note also that when the enterprise is multihomed and connected to multiple upstream ITPs, each ITP is only able to provide a DDoS Mitigation Service for the traffic it transits. As a result, the enterprise network may require to coordinate the various DDoS Mitigation Services associated to each link. More multi-homing considerations are discussed in [I-D.boucadair-dots-multihoming].

3.2. DDoS Mitigation by a Third Party DDoS Mitigation Service Provider

This use case differs from the previous use case described in Section 3.1 in that the DDoS Mitigation Service is not provided by an upstream ITP. In other words, as represented in Figure 2, the traffic is not forwarded through the DDoS Mitigation Service Provider by default. In order to steer the traffic to the DDoS Mitigation Service Provider, some network configuration changes are required. As such, this use case likely to match large enterprises or large data centers, but not exclusively. Another typical scenario for this use case is the relation between DDoS Mitigation Service Providers forming an overlay of DMS. When a DDoS Mitigation Service Provider mitigating a DDoS attack reaches it resources capacities, it may chose to delegate the DDoS Mitigation to another DDoS Mitigation Service Provider.

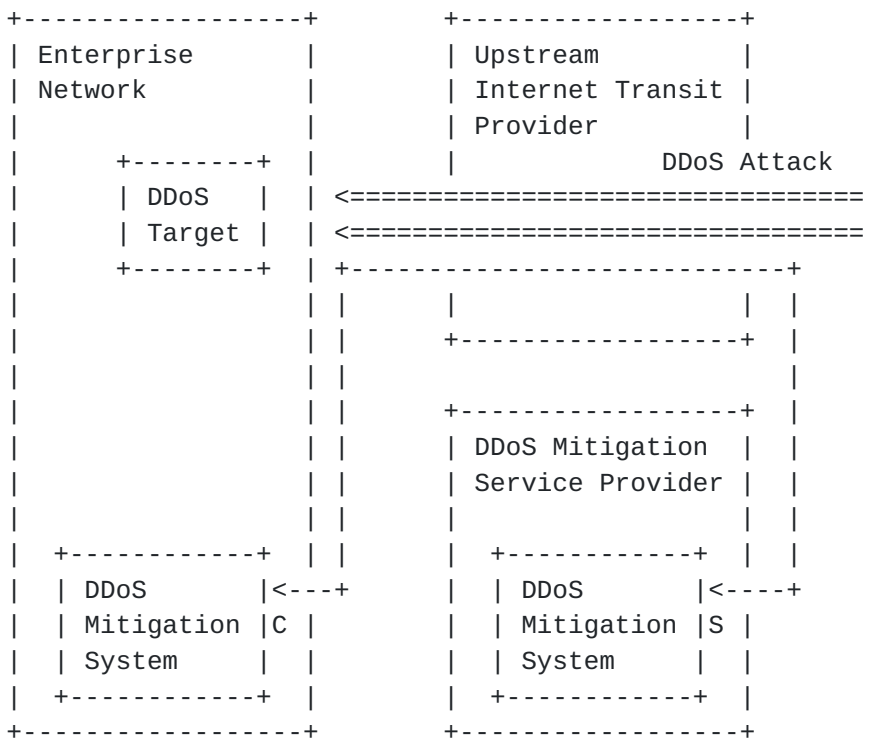


Figure 2: DDoS Mitigation between an Enterprise Network and Third Party DDoS Mitigation Service Provider

In this scenario, an Enterprise Network has entered into a pre-arranged DDoS mitigation assistance agreement with one or more other DDoS Mitigation Service Providers in order to ensure that sufficient DDoS mitigation capacity and/or capabilities may be activated in the event that a given DDoS attack threatens to overwhelm the ability of a given DMS to mitigate the attack on its own.

The pre-arrangement typically includes the agreement on the mechanisms used to redirect the traffic to the DDoS Mitigation Service Provider, as well as the mechanism to re-inject the traffic back to the Enterprise Network. Redirection to the DDoS Mitigation Service Provider typically involves BGP prefix announcement or DNS redirection, while re-injection of the scrubbed traffic to the enterprise network may be performed via tunneling mechanisms such as GRE for example. These exact mechanisms used for traffic steering are out of scope.

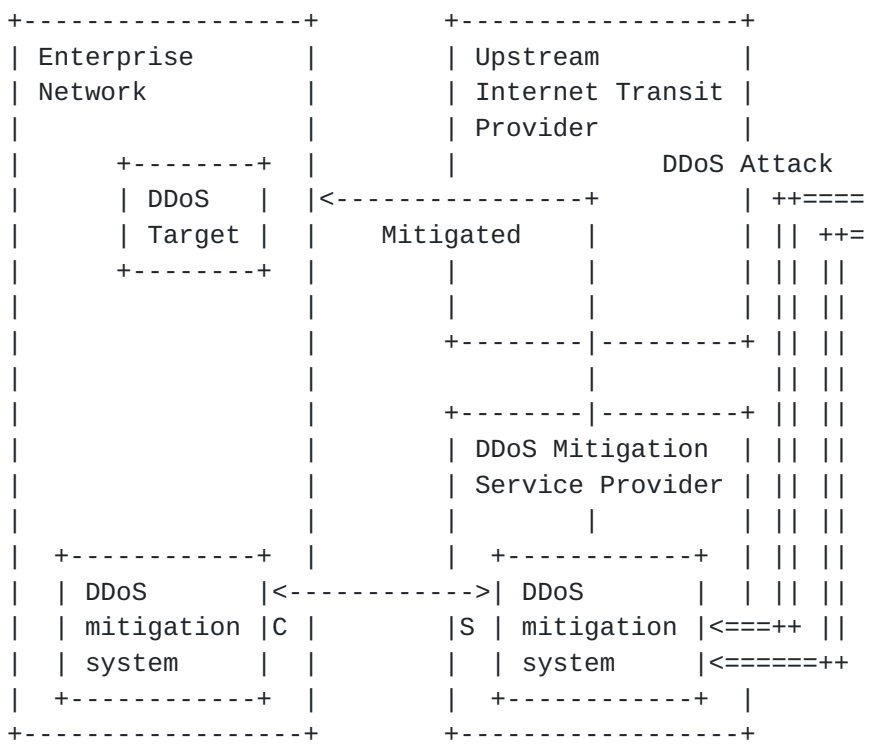


Figure 3: Redirection to a DDoS Mitigation Service Provider

When the Enterprise Network is under attack or at least is reaching its capacity or ability to mitigate a given DDoS attack traffic, the DOTS client sends a DOTS request to the DDoS Mitigation Service Provider to initiate network traffic diversion - as represented in Figure 3 - and DDoS mitigation activities. Ongoing attack and mitigation status messages may be passed between the Enterprise Network and the DDoS Mitigation Service Provider. If the DDoS attack has stopped or the severity of the attack has subsided, the DOTS client can request the DDoS Mitigation Service Provider to stop the DDoS Mitigation.

3.3. DDoS Orchestration

In this use case, one or more DDoS telemetry systems or monitoring devices monitor a network - typically an ISP network, an Enterprise network, or a data center. Upon detection of a DDoS attack, these DDoS telemetry systems alert an orchestrator in charge of coordinating the various DMS within the domain. The DDoS telemetry systems may be configured to provide required information, such as a preliminary analysis of the observation to the orchestrator.

The orchestrator analyses the various information it receives from DDoS telemetry system, and elaborates one or multiple DDoS mitigation strategies. In some case, a manual confirmation or selection may also be required to choose a proposed strategy or to initiate a DDoS Mitigation. The DDoS Mitigation may consist of multiple steps such as configuring the network, or updating already instantiated DDoS mitigation functions. In some cases, some specific DDoS mitigation functions must be instantiated and properly ordered. Eventually, the coordination of the mitigation may involve external DDoS resources such as a transit provider or a DDoS Mitigation Service Provider.

The communication used to trigger a DDoS Mitigation between the DDoS telemetry and monitoring systems and the orchestrator is performed using DOTS. The DDoS telemetry system implements a DOTS client while the orchestrator implements a DOTS server.

The communication between a network administrator and the orchestrator is also performed using DOTS. The network administrator via its web interfaces implements a DOTS client, while the Orchestrator implements a DOTS server.

The communication between the orchestrator and the DDoS mitigation systems is performed using DOTS. The orchestrator implements a DOTS Client while the DDoS mitigation systems implement a DOTS Server.

The configuration aspects of each DDoS mitigation system, as well as the instantiations of DDoS mitigation functions or network configuration is not part of DOTS. Similarly, the discovery of available DDoS mitigation functions is not part of DOTS; and as such is out of scope.

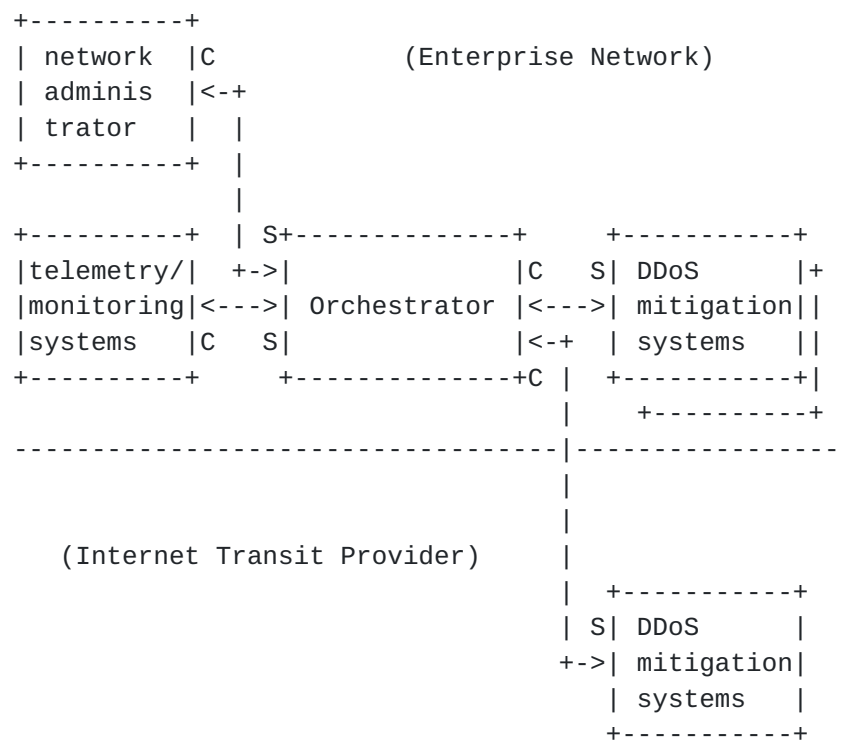


Figure 4: DDoS Orchestration

The DDoS telemetry systems monitor various network traffic and perform some measurement tasks.

These systems are configured so that when an event or some measurement indicators reach a predefined level to send DOTS mitigation request to the orchestrator. The DOTS mitigation request may be associated with some optional mitigation hints to let the orchestrator know what has triggered the request.

Upon receipt of the DOTS mitigation request from the DDoS telemetry system, the orchestrator responds with an acknowledgment, to avoid retransmission of the request for mitigation. The orchestrator may begin collecting additional fined grain and specific information from various DDoS telemetry systems in order to correlate the measurements and provide an analysis of the event. Eventually, the orchestrator may ask additional information to the DDoS telemetry system, however, the collection of these information is out of scope.

The orchestrator may be configured to start a DDoS Mitigation upon approval from a network administrator. The analysis from the orchestrator is reported to the network administrator via a web interface. If the network administrator decides to start the

mitigation, the network administrator triggers the DDoS mitigation request using the web interface of a DOTS client. This request is expected to be associated with a context that provides sufficient information to the orchestrator to infer the DDoS Mitigation to elaborate and coordinate.

Upon receiving a request to mitigate a DDoS attack performed over a target, the orchestrator, may evaluate the volumetry of the attack as well as the value that represent the target. The orchestrator may select the DDoS Mitigation Service Provider based on the attack severity. It may also coordinate the DDoS Mitigation performed by the DDoS Mitigation Service Provider with some other tasks such as for example, moving the target to another network so new sessions will not be impacted. When DDoS Mitigation is requested, the status indicates the DDoS Mitigation is starting while not effective. The DOTS client of the orchestrator will later be notified that the DDoS Mitigation is effective.

Orchestration of the DDoS mitigation systems works similarly as described in Section 3.1. The orchestrator indicates with its status whether the DDoS Mitigation is effective.

When the DDoS attack has stopped, the orchestrator indicates to the DDoS telemetry systems as well as to the network administrator the end of the DDoS Mitigation.

4. Security Considerations

The document does not describe any protocol.

DOTS is at risk from three primary attacks: DOTS agent impersonation, traffic injection, and signaling blocking.

Impersonation and traffic injection mitigation can be mitigated through current secure communications best practices.

Additional details of DOTS security requirements can be found in [I-D.ietf-dots-requirements].

5. IANA Considerations

No IANA considerations exist for this document at this time.

6. Acknowledgments

The authors would like to thank among others Tirumaleswar Reddy; Andrew Mortensen; Mohamed Boucadaire; Artyom Gavrichenkov; Jon

Shallow and the DOTS WG chairs, Roman Danyliw and Tobias Gondrom, for their valuable feedback.

7. Informative References

[I-D.boucadair-dots-multihoming]
Boucadair, M. and T. Reddy, "Multi-homing Deployment Considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS)", draft-boucadair-dots-multihoming-03 (work in progress), April 2018.

[I-D.ietf-dots-requirements]
Mortensen, A., Moskowitz, R., and T. Reddy, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-14 (work in progress), February 2018.

Authors' Addresses

Roland Dobbins
Arbor Networks
Singapore

EMail: rdobbins@arbor.net

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC 4S 0B6
Canada

EMail: daniel.migault@ericsson.com

Stefan Fouant
USA

EMail: stefan.fouant@copperriverit.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
USA

EMail: rgm@labs.htt-consult.com

Nik Teague
Verisign
12061 Bluemont Way
Reston, VA 20190

EMail: nteague@verisign.com

Liang Xia
Huawei
No. 101, Software Avenue, Yuhuatai District
Nanjing
China

EMail: Frank.xialiang@huawei.com

Kaname Nishizuka
NTT Communications
GranPark 16F 3-4-1 Shibaura, Minato-ku
Tokyo 108-8118
Japan

EMail: kaname@nttv6.jp