**Comments from Sriram**

Network Working Group J. Wu

Internet-Draft D. Li

Intended status: Informational L. Qin

Expires: 30 March 2023 Tsinghua University

M. Huang

N. Geng

Huawei

26 September 2022

Source Address Validation in Inter-domain Networks (Inter-domain SAVNET)

Gap Analysis, Problem Statement, and Requirements

draft-wu-savnet-inter-domain-problem-statement-01

Abstract

Source Address Validation in Inter-domain Networks (Inter-domain

SAVNET) WG efforts focus on narrowing the technical gaps of existing source

address validation (SAV) mechanisms in inter-domain scenarios. This

document provides a gap analysis of existing SAV mechanisms, describes

the problem statement based on the analysis results, and concludes

the requirements for improving inter-domain SAV.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in RFC 8174 [RFC8174].

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 30 March 2023.

Wu, et al. Expires 30 March 2023 [Page 1]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as

described in Section 4.e of the Trust Legal Provisions and are

provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2

2. Terminology . . . . . . . . . . . . . . . . . . . . . . . . . 3

3. Gap Analysis . . . . . . . . . . . . . . . . . . . . . . . . 4

3.1. Improper Permit . . . . . . . . . . . . . . . . . . . . . 4

3.1.1. Reflection Attack Scenario . . . . . . . . . . . . . 4

3.1.2. Spoofing within a Customer Cone . . . . . . . . . . . 5

3.2. Improper Block . . . . . . . . . . . . . . . . . . . . . 5

3.2.1. NO\_EXPORT in BGP Advertisement . . . . . . . . . . . 6

3.2.2. Direct Server Return (DSR) Scenario . . . . . . . . . 7

3.3. Misaligned Incentive . . . . . . . . . . . . . . . . . . 8

4. Problem Statement . . . . . . . . . . . . . . . . . . . . . . 9

4.1. Inaccurate Validation . . . . . . . . . . . . . . . . . . 9

4.2. Misaligned Incentive . . . . . . . . . . . . . . . . . . 9

5. Requirements . . . . . . . . . . . . . . . . . . . . . . . . 10

5.1. Accurate SAV . . . . . . . . . . . . . . . . . . . . . . 10

5.2. Direct Incentive . . . . . . . . . . . . . . . . . . . . 10

5.3. Working in Partial Deployment . . . . . . . . . . . . . . 10

5.4. Acceptable Overhead . . . . . . . . . . . . . . . . . . . 11

6. Inter-domain SAVNET Scope . . . . . . . . . . . . . . . . . . 11

7. Security Considerations . . . . . . . . . . . . . . . . . . . 11

8. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 11

9. Normative References . . . . . . . . . . . . . . . . . . . . 11

Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 12

1. Introduction

Source address validation in inter-domain networks (Inter-domain

SAVNET) is vital to mitigate source address spoofing between ASes.

Inter-domain SAV is essential to the Internet security [RFC5210].

Many efforts have been taken on the tasks of inter-domain SAV.

Wu, et al. Expires 30 March 2023 [Page 2]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

Ingress filtering [RFC2827] [RFC3704] is a typical method of inter-

domain SAV. Strict uRPF [RFC3704] reversely looks up the FIB table

and requires that the valid incoming interface must be the same

interface which would be used to forward traffic to the source

address in the FIB table. Feasible-path uRPF (FP-uRPF) [RFC3704],

taking a looser SAV than strict uRPF, is designed to add more

alternative valid incoming interfaces for the source address. To be

more flexible about directionality, BCP 84 [RFC3704][RFC8704]

recommends that i) the loose uRPF method which loses directionality

completely SHOULD be applied on lateral peer and transit provider

interfaces, and that ii) the Enhanced FP-uRPF (EFP-uRPF) method with

Algorithm B, looser than strict uRPF, FP-uRPF, and EFP-uRPF with

Algorithm A, SHOULD be applied on customer interfaces. Routers

deploying EFP-uRPF accept a data packet from customer interfaces only

when the source address of the packet is contained in that of the

customer cone.

Despite the diversity of inter-domain SAV mechanisms, there are still

some points that are under considered but important for enhancing

Internet security. Moreover, in the currently focused SAV work

scope, these mechanisms may lead to improper permit or improper block

problems in some scenarios.

This document does an analysis of the existing inter-domain SAV

mechanisms and answers: i) what are the technical gaps, ii) what are

the major problems needing to be solved, and iii) what are the

potential directions for further enhancing inter-domain SAV.

2. Terminology

SAV: Source Address Validation, i.e., validating the authenticity of

a packet's source IP address.

SAV rule: The filtering rule generated by inter-domain SAV mechanisms

that determines valid incoming interfaces for a specific source

prefix.

SAV table: The data structure that stores SAV rules on the data

plane. The router queries its local SAV table to validate the

authenticity of source addresses.

Improper block: Cases when packets with legitimate source addresses

are improperly blocked.

Improper permit: Cases when packets with spoofed source addresses are

improperly permitted.

Wu, et al. Expires 30 March 2023 [Page 3]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

3. Gap Analysis

BCP 84 recommends loose uRPF at provider/peer interfaces and EFP-uRPF

at customer interfaces. The followings are the gap analysis of these

SAV mechanisms.

3.1. Improper Permit

Existing SAV mechanisms may have improper permit problems that the

packets with spoofed source addresses are considered as legal. Here

are two cases where improper permit will appear.

3.1.1. Reflection Attack Scenario

The first case is at provider or peer interfaces where loose uRPF is

deployed. Loose uPRF almost accepts any source address, which fails

to protect ASes in the customer cone from externally injected

attacks.

+----------+

Attacker(P4') +-+ AS3(P3) |

+----------+

|

(P2C) |

|

+----v-----+

| AS4(P4) |-+Victim

+/\+----+/\+

/ \

/ \

(C2P) / \ (C2P)

+----------+ +----------+

| AS1(P1) | | AS2(P2) +-+Server

+----------+ +----------+

P4' is the spoofed source prefix P4 by the attacker

which is attached to AS3

Figure 1: A reflection attack scenario

Figure 1 shows a reflection attack scenario. AS 3 is the provider of

AS 4. AS 4 is the provider of AS 1 and AS 2. EFP-uRPF is deployed

at AS 4's customer interfaces, and loose uRPF is implemented at AS

4's provider interface. Assume a reflection attacker is attached to

AS 3. It sends packets spoofing P4 to the server located in AS 2 for

attacking the victim in AS 4. However, this attack cannot be

successfully blocked though AS 4 has deployed inter-domain SAV.

[#Sriram] AS4 can have a filtering rule that says it will not accept externally received data packets with SA in its (AS4’s) own prefix (P4). So, you should modify the example to show spoofed packet has SA in P1 (instead of P4).

Wu, et al. Expires 30 March 2023 [Page 4]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

3.1.2. Spoofing within a Customer Cone

The second case is at customer interfaces where EFP-uRPF with

algorithm B is deployed. It allows packets with source addresses of

the customer cone to enter from any customer interfaces to avoid

potential improper block problems that EFP-uRPF with algorithm A may

have. However, vulnerability is imported. Although EFP-uRPF with

algorithm B can prevent ASes inside the customer cone from using

source addresses of ASes outside the customer cone, it sacrifices the

directionality of traffic from different customers, which will lead

to improper permit problems.

+----------+

+ AS 3(P3) |

+----------+

|

(P2C) |

|

+----v-----+

| AS 4(P4) |

+/\+----+/\+

/ \

/ \

(C2P) / \ (C2P)

+----------+ +----------+

Victim+-+ AS 1(P1) | | AS 2(P2) +-+Attacker

+----------+ +----------+

P1' is the spoofed source prefix P1 by the attacker

which is attached to AS3

[#Sriram] P1’ is not shown in the Figure.

[#Sriram] If AS2 performs SAV, the attack will not be successful. It appears that zero improper admits can be achieved in a customer cone as whole only if there is complete adoption (i.e., at all ASes) within the customer cone.

Figure 2: Spoofing within a customer cone

In Figure 2, assume AS 4 implements EFP-uRPF with algorithm B at

customer interfaces. Under EFP-uRPF with algorithm B, AS 4 will

generate SAV rules with legitimate P1 and P2 at both customer

interfaces. When the attacker in AS 2 spoofs source address of AS 1,

AS 4 will improperly permit these packets with spoofed source

addresses of prefix P1. The same also applies when the attacker in

AS 1 forges prefix P2. That is to say, EFP-uRPF algorithm B cannot

prevent source address spoofing between ASes of the customer cone.

3.2. Improper Block

In some cases, existing SAV mechanisms may improperly block the

packets with legitimate source addresses. Here are two cases where

improper permit will appear.

Wu, et al. Expires 30 March 2023 [Page 5]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

3.2.1. NO\_EXPORT in BGP Advertisement

Figure 3 presents a NO\_EXPORT scenario. AS 1 is the common customer

of AS 2 and AS 3. AS 4 is the provider of AS 2. The relationship

between AS 3 and AS 4 is customer-to-provider (C2P) or peer-to-peer

(P2P). All arrows in Figure 2 represent BGP advertisements. AS 2

owns prefix P2 and advertises it to AS 4 through BGP. AS 3 also

advertises its own prefix P3 to AS 4. AS 1 has prefix P1 and

advertises the prefix to the providers, i.e., AS 2 and AS 3. After

receiving the route for prefix P1 from AS 1, AS 3 propagates this

route to AS 4. Differently, AS 2 does not propagate the route for

prefix P1 to AS 4, since AS 1 adds the NO\_EXPORT community attribute

in the BGP advertisement destined to AS 2. In the end, AS 4 only

learns the route for prefix P1 from AS 3.

Assume that AS 3 is the customer of AS 4. If AS 4 runs EFP-uRPF with

algorithm A at customer interfaces, the packets with source addresses

of P1 are required to arrive only from AS 3. When AS 1 sends the

packets with legitimate source addresses of prefix P1 to AS 4 through

AS 2, AS 4 will improperly block these packets. EFP-uRPF with

algorithm B works well in this case.

Assume that AS 3 is the peer of AS 4. AS 4 will never learn the

route of P1 from its customer interfaces. So, no matter EFP-uRPF

with algorithm A or that with algorithm B are used by AS 4, there

will be improper block problems.

Besides the NO\_EXPORT case above, there are also many route filtering

policies that can result in interruption of BGP advertisement.

Improper block may be induced by existing inter-domain SAV mechanisms

in such cases, and it is hard to prevent networks from taking these

configurations.

Wu, et al. Expires 30 March 2023 [Page 6]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

+-----------------+

| AS 4 |

+-+/\+-------+/\+-+

/ \

/ \

P3[AS 3]/(P2P/C2P) (C2P)\ P2[AS 2]

P1[AS 3, AS 1] / \

/ \

+----------------+ +----------------+

P3---+ AS 3 | | AS 2 +---P2

+--------/\------+ +-------/\-------+

\ /

P1[AS 1]\(C2P) (C2P)/P1[AS 1]

\ / NO\_EXPORT

+-----------------+

| AS 1 +---P1

+-----------------+

Figure 3: Interrupted BGP advertisement caused by NO\_EXPORT

[#Sriram] Improper block problem can be solved if there are more ways to uncover hidden prefixes in the customer cone. EFP-uRPF is a step in the right direction.

[#Sriram] BAR-SAV (draft-sriram-sidrops-bar-sav-01) is an improvement over EFP-uRPF (RFC 8704). BAR-SAV solves the above problem and overcomes some other gaps identified in this analysis with the help of ROA and ASPA data. ROA adoption seems to be progressing well, and ASPA adoption is expected to gain traction since it solves two important and critical problems with BGP: route leaks (RFC 7908)and forged-origin hijacks (draft-ietf-sidrops-rpkimaxlen-15; to be RFC 9319 soon). ASPA also offers a basic way of BGP AS path verification, not as secure as BGPsec but something reasonable without cryptographic signatures in the UPDATE.

[#Sriram] I realize BAR-SAV is still an individual draft (not an RFC or WG draft).

3.2.2. Direct Server Return (DSR) Scenario

Anycast is a network addressing and routing methodology. An anycast

IP address is shared by devices in multiple locations, and incoming

requests are routed to the location closest to the sender.

Therefore, anycast is widely used in Content Delivery Network (CDN)

to improve the quality of service by bringing the content to the user

as soon as possible. In practice, anycast IP addresses are usually

announced only from some locations with a lot of connectivity. Upon

receiving incoming requests from users, requests are then tunneled to

the edge locations where the content is. Subsequently, the edge

locations do direct server return (DSR), i.e., directly sending the

content to the users. To ensure that DSR works, servers in edge

locations must send response packets with anycast IP address as the

source address. However, since edge locations never advertise the

anycast prefixes through BGP, an intermediate AS with EFP-uRPF may

improperly block these response packets.

Wu, et al. Expires 30 March 2023 [Page 7]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

+----------+

Anycast Server+-+ AS3(P3) |

+----------+

|

(P2C) | P3[AS3]

|

+----v-----+

| AS4 |

+/\+----+/\+

/ \

P1[AS1] / \ P2[AS2]

(C2P) / \ (C2P)

+----------+ +----------+

User+-+ AS1(P1) | | AS2(P2) +-+Edge Server

+----------+ +----------+

P3 is the anycast prefix and is only advertised from AS3

Figure 4: A Direct Server Return (DSR) scenario

Figure 4 shows a specific DSR scenario. The anycast IP prefix (i.e.,

prefix P3) is only advertised from AS 3 through BGP. Assume AS 3 is

the provider of AS 4. AS 4 is the provider of AS 1 and AS 2. When

users in AS 1 send requests to the anycast destination IP, the

forwarding path from users to anycast servers is AS 1 -> AS 4 -> AS

3. Anycast servers in AS 3 receive the requests and then tunnel them

to the edge servers in AS 2. Finally, the edge servers send the

content to the users with source addresses of prefix P3. The reverse

forwarding path is AS 2 -> AS 4 -> AS 1. Since AS 4 never receives

routing information for prefix P3 from AS 2, EFP-uRPF algorithm A/

EFP-uRPF algorithm B or other existing uRPF-like mechanisms at AS 4

will improperly block the response packets from AS 2.

[#Sriram] BAR-SAV does fill this gap (see Section 5.1 of draft-sriram-sidrops-bar-sav-01).

3.3. Misaligned Incentive

Existing SAV mechanisms validate upstream (i.e., the packets from

customers to providers) strictly but take a loose validation for

downstream (i.e., the packets from providers/peers to customers).

Even an AS as well as its provider deploy BCP 84, the AS may still

suffer source address spoofing attacks.

The reflection attack scenario in Figure 1 shows a misaligned

incentive case. The attacker connected to AS 3 spoofs the prefix P4

owned by AS 4 and sends attack packets to the server attached to AS

2. The reflection attack succeeds even AS 4 has enabled SAV.

Wu, et al. Expires 30 March 2023 [Page 8]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

The scenario in Figure 2 is another example. AS 4 deploying EFP-uRPF

with algorithm B cannot prevent source address spoofing within an

customer cone. Technical limitations induce inaccurate SAV

(particularly improper permit) and further degrade the incentive of

deployers.

A detailed discussion about incentive can be found in

[draft-qin-savnet-incentive-00].

4. Problem Statement

4.1. Inaccurate Validation

High accuracy, i.e., avoiding improper block problems while trying

best to reduce improper permit problems, is the basic and key problem

of an SAV mechanism. Existing inter-domain SAV mechanisms have

accuracy gaps in some scenarios like routing asymmetry induced by BGP

route policies or configurations. Particularly, EFP-uRPF takes the

RPF list in data-plane, which means the packets from customer

interfaces with unknown source prefixes (not appear in the RPF list)

will be discarded directly. Improper block issues will arise when

legitimate source prefixes are not accurately learned by EFP-uRPF.

The root cause is that these mechanisms leverage local RIB table of

routers to learn the source addresses and determine the valid

incoming interface, which may not match the real data-plane

forwarding path from the source. It may mistakenly consider a valid

incoming interface as invalid, resulting in improper block problems;

or consider an invalid incoming interface as valid, resulting in

improper permit problems. Essentially, it is impossible to generate

an accurate SAV table solely based on the router's local information

due to the existence of asymmetric routes.

[#Sriram] Just a note to myself. BAR-SAV goes the extra mile to make use of authorized registry data (ROA, ASPA) in addition to BGP data to fill the gap.

4.2. Misaligned Incentive

Existing inter-domain SAV mechanisms pay more attention to upstream

(traffic from customer to provider/peer), resulting in weak source

address checking of downstream (traffic from provider/peer to

customer). The deployed network is still vulnerable to reflection

attack, which is considered the most harmful source address spoofing

attack, from other networks. "Strict upstream but weak downstream

checking" makes the benefits of deploying SAV flow to the rest of the

Internet, but not to the deployed network itself. This will harm the

incentive of ASes deploying SAV. Misaligned incentive will undermine

the motivation of the deployment.

[#Sriram] If AS3 in Figure 1 implements SAV on its customer facing interfaces, then the spoofing attack by AS4 would be blocked at the source or close to it. SAV is mostly meant to be widely deployed on customer facing interfaces and block spoofed traffic closer to the source. That is how it works best. The loose uRPF on provider facing interfaces is OK but that is not the most effective way.

Wu, et al. Expires 30 March 2023 [Page 9]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

5. Requirements

Inter-domain SAVNET WG efforts focus on narrowing the technical gaps of

existing inter-domain SAV mechanisms. The architecture of inter-

domain SAVNET should satisfy the following requirements.

5.1. Accurate SAV

SAV rules SHOULD match plausible data plane paths. Generating SAV rules

solely depending on control plane route information (e.g., RIB)

results in inaccurate SAV due to the mismatch of control plane path

and data plane path. To achieve high accuracy of SAV, an AS SHOULD

learn the real incoming direction of each source following the data

plane forwarding path. To this end, extra information out of routing

information (e.g., RIB or FIB) is needed as a supplement. According

to extra information, additional valid incoming interface may be

discovered for avoiding improper block, and some interfaces may be

removed for reducing improper permit.

Besides, it is desired that downstream are under the same SAV

criteria as upstream and that local SAV-enabled AS/cone are also

protected well (e.g., protected from reflection attacks). It would

be easy to achieve perfect all-round protection supposing SAV is

fully deployed, but, unfortunately, it is improbable in the

future. Even so, efforts are needed to narrow the gaps as much as possible.

5.2. Direct Incentive

SAV mechanisms SHOULD provide direct incentives. It would be

attractive if the networks deployed with SAV mechanisms are protected

from source address spoofing attacks instead of only providing

protection to others. The traffic forging these source prefixes

SHOULD be blocked as close to the traffic source as possible. To

make direct incentive, the accuracy of both upstream SAV and

downstream SAV SHOULD be improved.

5.3. Working in Partial Deployment

SAV mechanisms MUST provide protection for source addresses even the

mechanisms are partially deployed. It is impractical to assume that

all the ASes or most of the ASes enable SAV simultaneously. Partial

deployment or incremental deployment have to be considered during the

work of SAV.

Wu, et al. Expires 30 March 2023 [Page 10]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

5.4. Acceptable Overhead

The overhead of SAV SHOULD be controlled. Any improvement designs

for SAV mechanisms SHOULD not overload control plane. Besides, data

plane SHOULD not modify packets for simplifying the process of data

plane, which keeps same as existing SAV mechanisms.

6. Inter-domain SAVNET Scope

This document focuses on the same scope corresponding to existing

inter-domain SAV mechanisms. Generally, it includes all IP

encapsulated scenarios:

\* Native IP forwarding: including both global routing table

forwarding and CE site forwarding of VPN;

\* IP-in-IP Tunnel (IPsec, GRE, SRv6, etc.): focusing on the

validation of the outer layer IP address;

\* Both IPv4 and IPv6 addresses

Scope does not include:

\* Non-IP encapsulation: including MPLS label-based forwarding and

other non-IP-based forwarding.

7. Security Considerations

SAV rules can be generated based on route information (FIB/RIB) or

non-route information. If the information is poisoned by attackers,

the SAV rules will be false. Lots of legal packets may be dropped

improperly or malicious traffic with spoofed source addresses may be

permitted improperly. Route security should be considered by routing

protocols. Non-route information should also be protected by

corresponding mechanisms or infrastructure. If SAV mechanisms or

protocols require information exchange, there should be some

considerations on the avoidance of message alteration or message

injection.

The SAV procedure referred in this document modifies no field of

packets. So, security considerations on data-plane is not in the

scope of this document.

8. IANA Considerations

This document does not request any IANA allocations.

9. Normative References

Wu, et al. Expires 30 March 2023 [Page 11]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

[draft-qin-savnet-incentive-00]

Qin, L., Li, D., and J. Wu, "The Incentive Consideration

for Source Address Validation in Intra-domain and Inter-

domain Networks (SAVNET)", 15 September 2022.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering:

Defeating Denial of Service Attacks which employ IP Source

Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827,

May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed

Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March

2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams,

"A Source Address Validation Architecture (SAVA) Testbed

and Deployment Experience", RFC 5210,

DOI 10.17487/RFC5210, June 2008,

<https://www.rfc-editor.org/info/rfc5210>.

[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>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced

Feasible-Path Unicast Reverse Path Forwarding", BCP 84,

RFC 8704, DOI 10.17487/RFC8704, February 2020,

<https://www.rfc-editor.org/info/rfc8704>.

Authors' Addresses

Jianping Wu

Tsinghua University

Beijing

China

Email: jianping@cernet.edu.cn

Dan Li

Tsinghua University

Beijing

China

Email: tolidan@tsinghua.edu.cn

Wu, et al. Expires 30 March 2023 [Page 12]

Internet-Draft Inter-domain SAVNET Problem Statement September 2022

Lancheng Qin

Tsinghua University

Beijing

China

Email: qlc19@mails.tsinghua.edu.cn

Mingqing Huang

Huawei

Beijing

China

Email: huangmingqing@huawei.com

Nan Geng

Huawei

Beijing

China

Email: gengnan@huawei.com

Wu, et al. Expires 30 March 2023 [Page 13]