Abstract

This document describes a simple and efficient mechanism that can be used to detect and localize failures in P2PSIP overlay network. This document mainly consists of two parts: information carried in a P2PSIP Peer "Echo request" message and "Echo response" message for the purpose of fault detection and localization, and mechanisms for processing those messages.
Table of Contents

1.  Introduction ................................................. 3
2.  Overview of Functions ...................................... 3
3.  Terminology .................................................. 3
4.  Motivation ................................................... 4
5.  Packets Formats .............................................. 5
   5.1.  Message Header .......................................... 5
   5.2.  Message Attributes ...................................... 6
      5.2.1.  Response Attribute .................................. 6
      5.2.2.  Echo Attribute ...................................... 7
      5.2.3.  Respond Peer Info Attribute ......................... 10
6.  Message ...................................................... 11
   6.1.  Echo request ............................................ 11
   6.2.  Echo response ........................................... 11
      6.2.1.  Echo response from the terminator peer .............. 12
      6.2.2.  Echo response from the intermediate peer .......... 13
7.  Security Considerations ...................................... 14
8.  IANA Considerations .......................................... 14
9.  Examples ..................................................... 15
   9.1.  P2PSIP Ping .............................................. 15
   9.2.  P2PSIP Traceroute ....................................... 16
10. Acknowledgments .............................................. 17
11. References ................................................... 17
   11.1.  Normative References .................................. 17
   11.2.  Informative References ................................. 18
Authors’ Addresses ............................................... 19
Intellectual Property and Copyright Statements .................. 21
1. Introduction

Service is provisioned by more than one peers collectively in the P2PSIP overlay network, this mode avoids "a single point of failure" introduced by the traditional Client/Server mode. "Collectivity" means that the failure occurred in one peer can not impact service provided by the overlay network, i.e., most peers can continuously and normally be served by the overlay network, but some peers or peers are impacted. The quality of service provided by the overlay network will degrade or even be interrupted due to the failure. Considering the complexity of service provisioning in the overlay network, a diagnostics system is more desirable for the overlay network than the usual network adopting Client/Server mode.

This document describes a simple and efficient mechanism that can be used to detect and localize failures in P2PSIP overlay network, i.e., this document describes a P2PSIP diagnostics protocol. This document mainly consists of two parts: information carried in a P2PSIP Peer "Echo request" message and "Echo response" message for the purpose of fault detection and localization, and mechanisms for processing those messages. An important consideration in this design is that P2PSIP Peer Echo requests follow the same data path that normal P2PSIP peer protocol packets would traverse.

2. Overview of Functions

As one diagnostics protocol, P2PSIP diagnostics protocol is mainly used to detect and localize failures in P2PSIP overlay network. It provides mechanisms to detect and localize malfunctioning or badly behaving peers including disabled peers, congested peer and misrouting peers. It provides a mechanism to detect connectivity to the specified peer, a mechanism to detect availabilities of specified resource record and a mechanism to discover P2PSIP overlay topology and responding underlay topology.

P2PSIP diagnostics protocol reuses P2PSIP peer protocol [I-D.jiang-p2psip-sep]; essentially it reuses P2PSIP peer protocol specification and then introduces one new type of message (i.e., Echo message). P2PSIP diagnostics protocol strictly follows the P2PSIP peer protocol specification on the messages routing, transporting and NAT traversal etc.

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
The other concepts used in this document are compatible with "Concepts and Terminology for Peer to Peer SIP" [I-D.ietf-p2psip-concepts] and the P2PSIP peer protocol SEP [I-D.jiang-p2psip-sep].

4. Motivation

In the last few years, overlay networks have rapidly evolved and emerged as a promising platform to deploy new applications and services in the Internet. One of the reasons overlay networks are seen as an excellent platform for large scale distributed systems is their resilience in the presence of failures. This resilience has three aspects: data replication, routing recovery, and static resilience. Routing recovery algorithms are used to repopulate the routing table with live nodes when failures are detected. Static resilience measures the extent to which an overlay can route around failures even before the recovery algorithm repairs the routing table. Both routing recovery and static resilience relies on accurate and timely detection of failures.

As descriptions in the "P2PSIP Security Analysis and Evaluation" [I-D.song-p2psip-security-eval], "Security requirements in P2PSIP" [I-D.matuszewski-p2psip-security-requirement] and "Security Mechanisms for Peer to Peer SIP" [I-D.jennings-p2psip-security-mechanisms], there are some malfunctioning or badly behaving peers in the P2PSIP overlay, those peers may be disabled peers, congested peers or peers behaving with misrouting, and the impact of those peers in the overlay network is degradation of quality of service provided collectively by the peers in the overlay network or interruption of those services. It is desirable to identify malfunctioning or badly behaving peers through some diagnostics tools, and exclude or reject them from the P2PSIP system. Besides those faults, node failures may caused by underlying failures, for example, when the IP layer routing failover speed after link failures is very slow, then the recovery from the incorrect overlay topology may also be slow. Moreover, if a backbone link fails and the failover is slow, the network may be partitioned, which may lead to partitions of overlay topologies and inconsistent routing results between different partitioned components.

Some keep-alive algorithms based on periodically probe and acknowledge enable accurate and timely detection of failures of one peer’s neighbors [Overlay-Failure-Detection], but those algorithms only can detect the disabled neighbors using the periodical method, it is evidently not enough for overlay network.
One general P2PSIP overlay diagnostics protocol supporting periodical method and on-demand method for node failures and network failures is desirable, especially for P2PSIP overlay network operators. This document describe one general P2PSIP overlay diagnostics protocol based on P2PSIP peer protocol, at some degree, it is a good complementation for some keep-alive algorithms in the P2PSIP peer protocol implementation.

In this document, we mainly describe how to detect and localize those failures including disabled peers, congested peers, misrouting behaviors and underlying network faults in P2PSIP overlay network through a simple and efficient mechanism. This mechanism is modeled after the ping/traceroute paradigm: ping (ICMP echo request [RFC792]) is used for connectivity checks, and traceroute is used for hop-by-hop fault localization as well as path tracing. This document specifies a "ping" mode and a "traceroute" mode for diagnose P2PSIP overlay network.

The basic idea is to transmit a P2PSIP peer protocol request message (Echo request message) along the same path which all other P2PSIP peer protocol request messages would traverse. In "Ping" mode, an Echo request message are forwarded by the intermediate peers along the path and then terminated by the responsible peer, and after local diagnostics, the responsible peer returns an Echo response message. In "Traceroute" mode, an Echo request message is received and disposed by each peer along the routing path, each peer along the path returns an Echo response message with local diagnostics information including the result and causes if existing.

One approach these tools can be used is to detect the connectivity to the specified peer or the availability of the specified resource-record through P2PSIP Ping operation once the overlay network receives some alarms about overlay service degradation or interruption, if the ping fails, one can then initiate a P2PSIP Traceroute to determine where the fault lies.

5. Packets Formats

This document reuses P2PSIP peer protocol to carry diagnostics information. Considering special usage due to diagnostics, this document extends P2PSIP peer protocol by introducing one new type of message and some attributes.

5.1. Message Header

The mechanism defined in this document follows P2PSIP peer protocol specification, the introduced message whatever requests or responses
adopt the same message format with existing P2PSIP peer protocol messages. Different types of messages convey different TLV objects following by the common message header according to the protocol design. Those objects are called "Attributes". Please refer to P2PSIP peer protocol [I-D.jiang-p2psip-sep] for the detailed format of Message Header.

This document introduces one new type of message as below:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Echo</td>
</tr>
</tbody>
</table>

5.2. Message Attributes

As P2PSIP peer protocol, a P2PSIP diagnostics protocol message contains zero, one or multiple Attributes which describe the specified contents. All attributes follow P2PSIP peer protocol specification and adopt TLV style. Please refer to P2PSIP peer protocol [I-D.jiang-p2psip-sep] for the detailed format of Message Attributes.

This document introduces two new types of attributes as below:

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Echo</td>
</tr>
<tr>
<td>16</td>
<td>Respond Peer Info</td>
</tr>
</tbody>
</table>

In addition to the newly introduced Echo attribute, this document extends the Response attribute defined in P2PSIP peer protocol specification.

5.2.1. Response Attribute

This document extends the Response attribute defined in the P2PSIP peer protocol specification to describe the result of diagnostics as Figure 1.
Figure 1 Response Attribute Format

M-flag: the value is set;

Reserved (7 bits): those bits are reserved and ignored;

Attribute Type (8 bits): the value is 7 (0x07) for Response Attribute;

Length (16 bits): the length in bytes of this attribute;

Response Code (16 bits): response code is determined by the responder, this field is necessary for any response attribute;

Response Sub-Code (16 bits): response sub-code is determined by the responder, this field is optional.

This document introduces new response codes as below:

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>414</td>
<td>Underlay Destination Unreachable</td>
</tr>
<tr>
<td>415</td>
<td>Underlay Time exceeded</td>
</tr>
<tr>
<td>416</td>
<td>Upstream Misrouting</td>
</tr>
<tr>
<td>417</td>
<td>Loop detected</td>
</tr>
<tr>
<td>419</td>
<td>TTL hops exceeded</td>
</tr>
</tbody>
</table>

This document introduces response sub-codes for response code 414 as below:

<table>
<thead>
<tr>
<th>Response Sub-Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>net unreachable</td>
</tr>
<tr>
<td>1</td>
<td>host unreachable</td>
</tr>
<tr>
<td>2</td>
<td>protocol unreachable</td>
</tr>
<tr>
<td>3</td>
<td>port unreachable</td>
</tr>
<tr>
<td>4</td>
<td>fragmentation needed</td>
</tr>
<tr>
<td>5</td>
<td>source route failed</td>
</tr>
</tbody>
</table>

5.2.2. Echo Attribute

This document introduces Echo attribute to describe diagnostics control information, including but not limited to: the routing mode.
of the Echo message, the number of hops that the Echo message traverses, the reply rule to generate the Echo response message, the timestamp of initiating the Echo request message, the timestamp of receiving the Echo request message, and the expiration time of the Echo request message.

The Echo attribute format is shown as Figure 2:

```
+-----------------+-----------------+-----------------+-----------------+
| M | U | P | Reserved | Attribute Type | Length          |
+-----------------+-----------------+-----------------+-----------------+
| Routing Mode   | Hop Counter    | Reply rule      | Underlay TTL    |
+-----------------+-----------------+-----------------+-----------------+
| TimeStamp Initiated (seconds) |
+-----------------+-----------------+-----------------+-----------------+
| TimeStamp Initiated (microseconds) |
+-----------------+-----------------+-----------------+-----------------+
| TimeStamp Received (seconds) |
+-----------------+-----------------+-----------------+-----------------+
| TimeStamp Received (microseconds) |
+-----------------+-----------------+-----------------+-----------------+
| Expiration time (seconds) |
+-----------------+-----------------+-----------------+-----------------+
| Expiration time (microseconds) |
```

**Figure 2 Echo Attribute Format**

M-flag: the flag is set;

U-flag: indicate whether the receiver of Echo request message needs to carry immediate upstream peer information in the following Echo response message. If set (U=1), the Echo response message must carry its immediate upstream peer information such as Peer-ID;

P-flag: indicate whether the intermediate peer continues to forward the Echo request message when it detects misrouting behavior of its immediate upstream peer for this Echo request message. If set (P=1), the intermediate peer continues to forward the Echo request message upon detecting misrouting behavior of its immediate upstream peer; otherwise the intermediate peer stops forwarding. Certainly the intermediate peer should stop forwarding any received Echo request message once detecting looping even when P-flag is set;

Reserved (5 bits): those bits are reserved and ignored;
Attribute Type (8 bits): the value is 15 (0x0F);

Length (16 bits): the length in bytes of this attribute;

Routing Mode (8 bits): indicate the routing mode of the Echo message in the overlay.

Hop Counter (8 bits): This field is ignored by Echo requests. In Echo responses, this field must be exactly copied from the TTL field of the message header in the received Echo request. Then this information is sent back to the request initiator to compute the hops that the message traverses in the overlay.

Reply rule (8 bits): indicate the process policy to the Echo request specified by the initiator;

Underlay TTL (8 bits): indicate the underlay TTL which the intermediate peer must adopt when forwarding the Echo requests, it is specified by the initiator;

Timestamp Initiated (64 bits): the time-of-day (in seconds and microseconds, according to the sender’s clock) in NTP format [RFC2030] when the P2PSIP Overlay Echo request is sent; It can be carried in the Echo response message from the receiver; certainly it first appears in the Echo request message;

Timestamp Received (64 bits): it is in an Echo response message and the time-of-day (according to the receiver’s clock) in NTP format [RFC2030] that the corresponding the P2PSIP Overlay Echo request was received;

Expiration time (64 bits): the expiration time of Echo request message, it is the time-of-day in NTP format [RFC2030].

This document defines those routing modes as below:

<table>
<thead>
<tr>
<th>Forward mode</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Recursive</td>
</tr>
<tr>
<td>1</td>
<td>Iterative</td>
</tr>
<tr>
<td>2</td>
<td>Semi-recursive</td>
</tr>
<tr>
<td>3</td>
<td>Overlay native</td>
</tr>
</tbody>
</table>

This document defines those reply rules as below:
Reply rule | Meaning
---|---
1 | Do not reply except destination peer
2 | Immediately reply

5.2.3. Respond Peer Info Attribute

This document introduces Respond Peer attribute to describe Peer information such as Peer-ID.

Respond Peer Info attribute is also a composite attribute. Like the Source Peer Info attribute and Destination Peer Info attribute, it may be also comprised of Peer-ID attribute, Peer Service Capability attribute and several Peer Address Info attributes, the Peer-ID attribute and at least one Peer Address Info attribute are necessary among them.

The Respond Peer Info attribute format is shown as Figure 3.

```
0                   1                   2                   3
+-------------------+-------------------+-------------------+-------------------+
| M | U | D | Reserved | Attribute Type | Length |
|-------------------|-------------------|-------------------|-------------------|
| Peer-ID           | Peer service capability |
| Peer Address Info - 1 |
| Peer Address Info - N |
| Peer Address Info - N |
| Peer Address Info - N |
```

Figure 3 Respond Peer Info attribute format

M-flag: the value is 1;

U-flag: indicate whether this attribute describe the immediate upstream peer of the initiator generating this attribute. If set (U=1), the attribute is used to describe the immediate upstream peer on the path;

D-flag: indicate whether this attribute describe the immediate downstream peer of the initiator generating this attribute (e.g. next-hop peer in the overlay forwarding path). If set (D=1), the attribute is used to describe the immediate downstream peer on the path. If U=0 and D=0, the attribute is used to describe the peer
itself (i.e. the attribute generator);

Reserved (5 bits): those bits are reserved and ignored;

Attribute Type (8 bits): the value is 16 (0x10);

Length (16 bits): the length in bytes of this attribute.

6. Message

All P2PSIP peer protocol requests and responses use the common message header after which zero, one or more TLV-style attributes follow.

This document introduces the new Echo message to detect and localize failures in P2PSIP overlay network.

6.1. Echo request

An Echo request message is used to detect possible failures in the specified path of P2PSIP overlay network, including disabled peers, congested peers, misrouting behavior and underlying network faults. An Echo request message is also used to discover the topology of the specified path and check the reachability to the specified peer or the availability of the specified resource-record.

An Echo request is normal P2PSIP peer protocol message; it can be initiated by any peer supporting P2PSIP peer protocol specification in the P2PSIP overlay network.

An Echo request must contain a message header and an Echo attribute.

Echo request =
  Message Header
  Echo Attribute
  Source Peer Info

6.2. Echo response

An Echo response message is used to convey local diagnostics information including result, causes and possible other assistant information.

An Echo response message must contain a message header, a Response attribute, an Echo attribute and one or more Respond Peer Info attributes. It may contain a Resource Info attribute and a Status attribute. If the peer is one intermediate peer, the Echo response
message must contain three Respond Peer Info attributes to describe the response peer itself, immediate upstream peer and next-hop peer individually. If the peer is the last peer terminating the Echo request message, the Echo message must contain two Respond Peer Info attributes to describe self and immediate upstream peer. The TTL in the received Echo request must be copied to the Hop Counter field in the Echo response. In the following section, the last peer terminating the Echo request message is called as the "terminator peer", in comparison with "intermediate peer" and "initiator peer" or "initiator".

One implementation to estimate whether one peer is disabled is that the initiator uses local timer to determine whether the expected Echo response message is expired, i.e., the peer thinks that the specified peer is disabled if it does not receive the Echo response message before the local timer expires which starts when issuing an Echo request message to the specified peer in the P2PSIP overlay network. This local timer can be updated in the specified interval by the Echo response message from the intermediate peers in the "Traceroute" mode.

Echo response =
Message Header
Response Attribute
Echo Attribute
Respond Peer Info Attribute
[Resource Info Attribute]
[Status Attribute]

6.2.1. Echo response from the terminator peer

When an Echo request message arrived at a peer, if the peer’s responsible ID space covers the destination ID of the Echo request message or the peer finds that the destination ID is unreachable in the P2PSIP overlay (e.g., detecting loop), then the peer constructs and returns an Echo response message using the specified Routing Mode indicated by the Echo request message when the Reply rule field of the received Echo attribute is not Zero, and the peer does not give any response when the Reply rule field is Zero.

The Echo response must carry a Response attribute, a Respond Peer Info attribute describing the receiver of the Echo request message, an Echo attribute containing TimeStamp Received field and TimeStamp Initiated field copied from the received Echo request message.

The returning Echo response message further must carry a Resource attribute when the responsible resource-record exists in the peer. If the Echo response message does not carry any Resource attribute,
it means that the resource-record whose Resource-ID is equal to the destination ID of the Echo request message does not exist in the peer.

If the peer finds that it is bush or congested, the returning Echo response message must carry a Status attribute.

If the peer finds that its immediate upstream peer behaves with misrouting, the returning Echo response message must carry a Response attribute with the response code 416 "Upstream Misrouting" and a Respond Peer Info attribute describing information of its immediate upstream peer.

6.2.2. Echo response from the intermediate peer

When an Echo request arrived at a peer, if the peer’s responsible ID space does not cover the destination ID of the Echo request, then the peer continues to forward this Echo request according to the specified Routing Mode field in the received Echo request.

The peer should return an Echo response carrying a Response attribute with the response code 414 "Underlay Destination Unreachable" when it receives an ICMP message with "Destination Unreachable" information after forwarding the received Echo request.

The peer should return an Echo response carrying a Response attribute with the response code 415 "Underlay Time Exceeded" when it receives an ICMP message with "Time Exceeded" information after forwarding the received Echo request.

When an Echo request arrived at a peer, if the peer’s responsible ID space does not cover the destination ID of the Echo request message and the value of received Reply rule field is 2, then the peer must construct and return an Echo response and continue to forward the Echo request.

The Echo response must carry a Response attribute, a Respond Peer Info attribute describing the receiver of the Echo request message, a Respond Peer Info attribute describing the immediate downstream peer (i.e. next hop to forward the Echo request message in the P2PSIP overlay network), an Echo attribute containing TimeStamp Received field and TimeStamp Initiated field copied from the received Echo request.

The returning Echo response must carry a Resource attribute when the responsible resource-record exists in the peer. If the Echo response does not carry any Resource attribute, it means that the resource-record whose Resource-ID is equal with the destination ID of the Echo
request message does not exist in the peer.

If the peer finds that it is bush or congested, the returning Echo response message must carry a Status attribute.

If the peer finds that its immediate upstream peer behaves with misrouting, the returning Echo response must carry a Response attribute with the response code 416 "Upstream Misrouting" and Respond Peer Info attribute describing information of its immediate upstream peer.

7. Security Considerations

One feasible P2PSIP Traceroute implementation based on the value of "Reply Rule" field 2 "Immediately reply" (Section 9.2) may cause DoS attack to the initiator, though this implementation is more efficient than traditional Traceroute operation of Internet using pacing ICMP message.

An advice is to use the efficient Traceroute operation in administrated P2PSIP overlay and use the pacing-style Traceroute operation in the untrustworthy P2PSIP overlay network, certainly, the probability of this type of DoS attack is very low because the overlay is distributed and the it is very hard for the attacker to know the accurate Peer-IDs and attack most of all peers simultaneously.

8. IANA Considerations

Message Type: this document introduces a new type of message as below:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Echo</td>
</tr>
</tbody>
</table>

Attribute Type: this document introduces two new types of attributes as below:

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Echo</td>
</tr>
<tr>
<td>16</td>
<td>Respond Peer Info</td>
</tr>
</tbody>
</table>

Response Code: this document introduces some new response definitions as below:
Result Code       Name
414               Underlay Destination Unreachable
415               Underlay Time exceeded
416               Upstream Misrouting
417               Loop detected
419               TTL hops exceeded

Response Sub-Code: this document defines response sub-codes for the response code 414 "Underlay Destination Unreachable" as below:

Response Sub-Code Meaning
0              net unreachable
1              host unreachable
2              protocol unreachable
3              port unreachable
4              fragmentation needed
5              source route failed

9. Examples

9.1. P2PSIP Ping

Any peer supporting P2PSIP diagnostics protocol can use P2PSIP Ping operation to check the reachability to the specified peer in the overlay or the availability of the specified resource-record.

In the normal P2PSIP Ping operation, a peer constructs and issues an Echo request message to the specified destination ID. The destination ID of the Echo request message is the specified Peer-ID or Resource-ID, the source ID of the Echo request message is the Peer-ID of the initiator. The "Reply Rule" value must be 1 "Do not reply except last peer", and the initiator determines the "Routing Mode", and "Underlay TTL" of the Echo request message by itself. Any intermediate peer does only simply forward this message to its next hop in the overlay and not disposes this Echo request message until the message arrives at the terminator peer who may be the responsible peer or one peer who finds that the destination ID is unreachable, eventually the terminator peer returns an Echo response message.

Here is an example of a P2PSIP Ping operation; it is shown as Figure 4:
The overlay network operator may use P2PSIP Ping operation to measure the message transmission delay and jitter between two specified peers.

9.2. P2PSIP Traceroute

Any peer supporting P2PSIP diagnostics protocol can use P2PSIP traceroute operation to detect and localize malfunctioning or badly behaving peers including disabled peers, congested peers and misrouting peers, or detect and localize network failure, or to discover the topology of the specified path in the overlay network.

In one possible P2PSIP Traceroute operation, a peer constructs and issues an Echo request message to the specified destination ID. The destination ID in the Echo request message is the specified Peer-ID or Resource-ID, the source ID in the Echo request message is the Peer-ID of the initiator. The value of "Reply Rule" field must be 2 "Immediately reply", and the initiator determines the "Routing mode"and "Underlay TTL" of the Echo request message by itself. Any intermediate peer does dispose this Echo request message, i.e., forwards this message to its next hop in the overlay and then returns an Echo response message. The terminator peer for the Echo request message is the destination peer or one peer who finds that the destination ID is unreachable; eventually the terminator peer returns an Echo response message.

Here is an example of a P2PSIP Traceroute operation; it is shown as Figure 5:
10. Acknowledgments

Thanks to Jiang Haifeng for his valued comments.

11. References

11.1. Normative References


11.2. Informative References


Authors’ Addresses

Song Yongchao
Huawei
Baixia Road No.91
Nanjing, Jiangsu Province 210001
PRC

Phone: +86-25-84565081
Fax: +86-25-84565070
Email: melodysong@huawei.com

Zheng Hewen
Huawei
Baixia Road No. 91
Nanjing, Jiangsu Province 210001
PRC

Email: hwzheng@huawei.com
Jiang Xingfeng
Huawei
Baixia Road No.91
Nanjing, Jiangsu Province  210001
PRC

Phone:  +86-25-84565079
Fax:  +86-25-84565070
Email:  jiang.x.f@huawei.com