

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: July 4, 2022

Z. Du  
P. Liu  
China Mobile  
December 31, 2021

Gateway Based Trust Relationship Between the Endpoint and the  
Intermediate Node  
draft-du-panrg-gateway-based-trust-relationship-01

## Abstract

This document describes a mechanism about establishing trust relationship between the endpoint and the intermediate node along the path based on the gateway of the endpoint.

## 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 2119](#) [[RFC2119](#)].

## 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 July 4, 2022.

## Copyright Notice

Copyright (c) 2021 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

Internet-Draft

Gateway-based Trust Relationship

December 2021

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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Proposed Mechanism for the Trust Problem . . . . .	<a href="#">3</a>
<a href="#">3.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">6.</a>	References . . . . .	<a href="#">4</a>
<a href="#">6.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">6.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">5</a>

## [1.](#) Introduction

In future, many new services would emerge in the network, such as the 5G URLLC (Ultra Reliable Low Latency Communication) service, and the holographic type communications. Many of the new services need a higher QoS (Quality of Service) level than the current Internet services, and some of them have a critical SLA (Service-Level Agreement) requirement. The SLA differences between the new services and traditional services would become larger and lager. However, current networks can only provide the Best Effort bearing, in which all the traffic are treated as the same kind. In summary, current networks are short of negotiation abilities between the network and the applications. PANRG in the IRTF has proposed a research direction to enable the path aware networking. A lot of analyses have been done in the [[RFC9049](#)], which explains reasons why various Path Aware techniques have seen limited or no deployment.

One of the reasons is that it is hard to establish a trust relationship between the Endpoint and Intermediate Node. In the current network structure, the Endpoints only needs to be aware of the each other, and assume that the network can provide a good connection service for them. On the other hand, traditionally, Intermediate Nodes only need to support IP forwarding and do not need to be aware of up-layer information. In addition, the network nodes work in a per-packet model, not a per-flow model. Also in the

[RFC9049], it is said that "per-connection state in intermediate nodes has been an impediment to adoption and deployment".

However, we can find that the gateway of the Endpoint is able to maintain a per-connection state and a trust-relationship for each

user. For example, the users in the fixed network need to be authorized by the BNG (Broadband Network Gateway), and the BNG also needs to do the accounting for each user. It is hard and unnecessary to make every intermediate node along the path has the same ability as the BNG; however, if they can have some communication with the BNG, perhaps they can make a better path choice for the user. Following this direction, this document proposes a mechanism about how to enable the communication between the BNG and the Head-End node in the network, because the Head-End node is the main node to select the path for a flow in the network. If any future work on the trust relationship between the Endpoint and the Intermediate Node is considered, the mechanism in this document can be a reference.

## 2. Proposed Mechanism for the Trust Problem

As shown in the Figure 1, in the fixed network, the BNG works as the gateway for the Client, and provides the Internet connection service for the Applications. The Client and Server are the EndPoints, and the BNG, Head-End, Mid-Node, End-Node are the nodes along the path from the Client to the Server. There are three paths, i.e., A, B, C, with different properties such as high bandwidth or low latency, between the Head-End and the End-Node in the network.

By default, all the traffic from the APPs are forwarded from the Head-End to the End-Node with the same treatment in the network. In the Head-end, perhaps a load balance mechanism can be enabled, but normally without any per-flow mechanism, because the Head-End does not know the requirements of each flow. If the Applications need different treatments in the network, and the Head-End can schedule the traffic to a proper path, the user can have a better experience and the network resource can be used more efficiently.

```
Client                                     Server
+-----+                               +-----+
|App x|-\                               /->|App x|
+-----+ | +-----+ +-----+ +-----+ +-----+ | +-----+
```

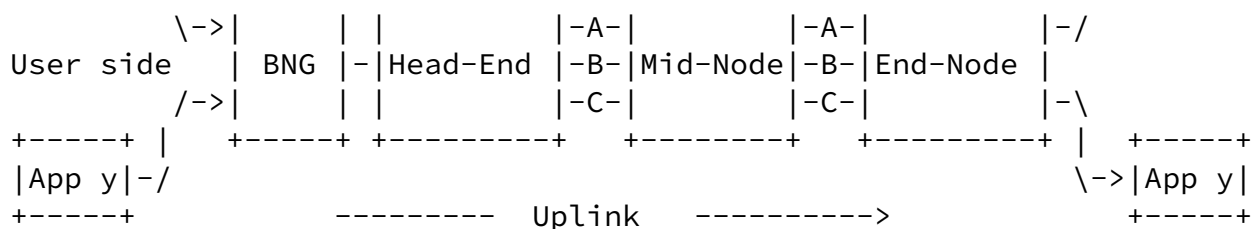


Figure 1: Path-aware Mechanism in the Fixed Network

The following paragraphs are about the trust problems and the potential solutions for them.

The first problem is the path information collection for the Endpoints. The Endpoints should be able to trust the path information that the Intermediate Nodes signal. As a first step, we only consider the situation that information is limited and does not need to be updated frequently. In this case, if the Head-End needs to inform the Endpoints something, it can send the information with its signature generated by using a private key. The Endpoints can check the information using the corresponding public key. For example, the public key can be obtained by the Endpoint in the authentication procedure.

The second problem is the Head-End should trust the Endpoints if it receives some path selection suggestions from the Endpoints. In this case, we think that the BNG has authenticated the Endpoints, so that the BNG can send some information to the Head-End indicating that the Endpoint is not a fake one. For example, the BNG and the Head-End can using an IPSec to transfer the traffic that needs specific treatment. Another option is that the BNG can forward the traffic that needs specific treatment with its signature generated by using a private key. The Head-End can check the information using the corresponding public key of the BNG.

The reason that we do not suggest that the Endpoints make the signature is because their number is much larger than the number of BNGs. We do not think the Head-End can handle a large number of keys. Meanwhile, in this mechanism, the Intermediate Node does not need to maintain per-connection state.

### [3.](#) IANA Considerations

TBD.

#### [4.](#) Security Considerations

TBD.

#### [5.](#) Acknowledgements

TBD.

#### [6.](#) References

##### [6.1.](#) Normative References

[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>>.

Du & Liu

Expires July 4, 2022

[Page 4]

---

Internet-Draft

Gateway-based Trust Relationship

December 2021

##### [6.2.](#) Informative References

[RFC9049] Dawkins, S., Ed., "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", [RFC 9049](#), DOI 10.17487/RFC9049, June 2021, <<https://www.rfc-editor.org/info/rfc9049>>.

#### Authors' Addresses

Zongpeng Du  
China Mobile  
No.32 XuanWuMen West Street  
Beijing 100053  
China

Email: [duzongpeng@foxmail.com](mailto:duzongpeng@foxmail.com)

Peng Liu  
China Mobile  
No.32 XuanWuMen West Street  
Beijing 100053

China

Email: liupengyjy@chinamobile.com