Workgroup: Network Working Group
Internet-Draft: draft-yu-v6ops-split6-02
Published: 21 December 2021
Intended Status: Informational
Expires: 24 June 2022
Authors:
H. Yu
Guangzhou Root Chain International Network Research Institute Co., Ltd.
H. Zhang
Guangzhou Root Chain International Network Research Institute Co., Ltd.

Separation Protocol of Locator and Identifier Towards IPv6

Abstract

In the current TCP/IP architecture, the IPv6 address has a dual meaning in semantics. It not only represents the topological location of the network node, but also the identity of the node, which is usually referred to as the semantic overload problem of the IP address. The semantically overloaded IP address represents the topological position of the network, and the topological position of the network generally does not move, so the device entering the new network environment needs to replace the new identity IP to adapt to the change of the topological position. The semantic overload of IP addresses is not conducive to supporting mobility and user identity authentication, resulting in tight storage space for routing equipment, lack of unified communication identification for network equipment, and difficulties in network traceability and management. In order to solve the problem of IP address semantic overload, this draft focuses on the separation technology SPLIT6 (Separation Protocol of Locator and Identifier Towards IPv6) of IP address identity and location.

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 24 June 2022.

Table of Contents

1. Introduction

In the current Internet architecture, the IPv6 address carries too much semantics. The network layer protocol uses the IPv6 address as the location identifier of the user terminal, and the transport layer protocol uses the IPv6 address as the identity identifier of the user terminal. This dual identity of the IPv6 address cannot satisfy the Internet's increasing mobility and security requirements.

In order to solve these problems caused by the semantic overload of IPv6 addresses, separating the location information and identity

information of IPv6 addresses has become an important research direction.

2. IPv6 address semantics problem

In the current TCP/IP architecture, the IPv6 address has a dual meaning in semantics at the same time. It not only represents the topological location of the network node, but also the identity of the node, which is usually referred to as IP address semantic overload. The semantically overloaded IP address represents the topological location, and the topological location cannot be moved, so the IP address representing the identity of the node cannot move with the movement of the user or device. The equipment entering the new network environment needs to be replaced with a new identity IP to adapt to the change of topological location. The semantic overload problem of IP addresses is not conducive to supporting mobility, affecting the scalability of core routing, reducing the effectiveness of existing security mechanisms, and restricting the development of several new technologies.

3. exist network problem

Due to the semantic overload problem of IP addresses, the following problems exist in TCP/IP in actual operation:

The storage space of routing equipment is tight. In order to improve and ensure the performance of the Internet, the routing table entries of the routing devices in the Internet should not be too many. If a large number of IP address prefixes that have not been aggregated are advertised to the core route, it will cause the expansion of the core routing table entry DFZ (default-free zone), the increase in the frequency of route updates and the increase in communication volume, and the slower route convergence, which will cause serious problems. Affect the performance and scalability of routing.

The network equipment lacks a unified communication identification. With the development of IOT (Internet Of Things) in the current Internet, the number of devices connected to the network has increased exponentially. These devices need to communicate with other devices, so a unique communication identifier that can represent this device must have. Currently, the industry does not agree to use IPv6 address as a universal communication identifier for devices. There are two reasons. One is because IP addresses have dual meanings. As the network environment changes, the device IP address will also change. Therefore, the difference between the device and the IPv6 address A one-to-one correspondence cannot be established between them; the second reason is that considering the performance and security of IOT devices, IOT devices are generally

simple in design and only use the physical layer, link layer, and network layer of the network instead of the transport layer. And application layer to reduce overhead. Therefore, the IP address is generally used to identify the device, but many IOT devices are highly mobile. How to ensure that the IOT device can still use a fixed IP address to identify it when it is moving is an important problem that needs to be solved. In view of the above problems, if the coupling problem between the identification location and the identification identity can be solved, the development of IOT and the Internet of Things can be greatly promoted.

Network security control is difficult. The most important way of network security management and control is to trace the location and identity information of the IP address of the initiator of the network behavior. However, in the current TCP/IP architecture, the IPv6 address has a dual meaning, which is not only fixed network location information, but also unbound identity information. It is not possible to locate a specific device through the IP address, and then locate a certain person. Because with the switching of the network environment, the same IP address may correspond to different users and different devices, and the devices of the same user will also be assigned to different IP addresses as the network switches. All these have caused great troubles to the supervision of network security. Because the current network is insecure, an important reason for frequent network attacks is that the attacker's address cannot be traced to the source or it is difficult to trace the source. If each user can be assigned a fixed identity-IPv6 address in the network, then network attackers will have nowhere to hide, and network supervision will become simple. Therefore, IP semantic overload is the frequent occurrence of network attacks, and the source of the attack cannot be traced back to the root cause.

User identity is difficult to authenticate. Due to the dual meaning of IP, users cannot always log in to the network using a fixed IP address. Because once the user switches the network environment, he needs to change his device's IP address and network configuration to log in to the network again. The reason for this phenomenon is that the IP address assigned by the user has location attributes, so this IP address is bound to the network environment where it is located, and the IP address cannot move with the user's location. Frequent switching of IP address and network environment will bring a lot of inconvenience to users. For example, the ongoing network conference will be interrupted, the video being watched will be suspended, and the sending and receiving of emails will need to be re-authenticated with the IP address.

The mobile performance of the device is poor. In the current TCP/IP architecture, because the IPv6 address has a dual meaning, it represents the network topology location of the device, and it is

also the identity of the device. This leads to poor mobility of the device, and a device carrying a specific IP address cannot log in to the network after switching to another network environment. These devices need to reconfigure the network and change the IP address to log in to the network again.

In the current Internet architecture, the IP address carries too much semantics. The network layer protocol uses the IP address as the location identifier of the user terminal, and the transport layer protocol uses the IP address as the identity identifier of the user terminal. This double identity of the IP address cannot Meet the increasing mobility and security needs of the Internet.

4. research status

In order to solve these problems caused by the semantic overload of IP addresses, it has become an urgent need for academia and industry to separate the location information and identity information of the IP address. In recent years, countries around the world have successively initiated a number of research projects on the separation of IP address location information and identity information. The MobilityFirst project started in 2010 and was funded by the Future Internet Architecture (FIA) program of the National Science Foundation. The first phase of the FIA project started in 2010-14 and produced a new mobility-centric architecture called MobilityFirst (MF), and a prototype implementation of the protocol stack. IETF established a corresponding working group to study the separation of identity and location identification. Among them, the HIP working group advocated by Ericsson mainly studied the host identity protocol HIP (Host Identity Protocol), and proposed rfc7401 and rfc8002. The Shim6 working group advocated by Sun company mainly researched on the IPv6 Multihoming Shim Protocol for IPv6 (Multihoming Shim Protocol for IPv6) and proposed RFC5533. The RRG (Routing Research Group) working group advocated by Cisco mainly researches the Locator/Identifier Separation Protocl (Locator/ Identifier Separation Protocl), and proposes RFC6830 and RFC8113. In addition, there are TIDR (Tunneled Inter-Domain Routing) and IVI programs. In these researches on network systems, it is generally believed that the semantic overload of IP addresses has affected the development of network system structures. Therefore, breaking the semantic overload of IP addresses and establishing a network that separates location and identity has become an important issue to be solved in the construction of next-generation IP networks.

5. SPLIT6

In view of the mobility requirements and semantic overload of IP addresses, this draft uses the idea ofseparation of location and identity to carry out research on network naming and addressing

architecture. We propose a new type of naming and addressing architecture: SPLIT6 to meet node mobility requirements and establish end-to-end secure transmission based on identity. Using SPLIT6 can not destroy the aggregation of the original IP addresses, and at the same time facilitate the supervision of IP addresses.

Under the TCP/IP architecture, the IP address confuses the functional boundaries of Locator and Identifier. Locator is a PA (Provider Allocated) address, which should be allocated according to the topology of the network to ensure the aggregation characteristics of the address and support global routing; Identifier is a PI (Provider Independent) address, which is usually allocated according to the organizational structure of the organization, and it is generally difficult to aggregate. It cannot be routed globally. Therefore, unless there is a breakthrough in flat identification routing, it is difficult to use a unified address to achieve the above two functions.

This draft proposes an architecture based on the separation of network-based Locator and Identifier: SPLIT6. SPLIT6 distinguishes the core network and the edge network. The core network uses the Locator name space, and the edge network uses the Identifier name space. The use of structured location identification in the core network ensures the aggregation characteristics of the core routing identification (Locator) and improves the scalability of the core network. A fixed identifier (Identifier) in the edge network represents a network node, and a communication session is established based on the identifier. The identity is not restricted by the site topology and can better support mobility. In addition, Identifier can be expressed as a name space with a specific meaning without restriction.

SPLIT6 needs to use a fixed network IP address to realize the roaming function of computers across different network segments, and to ensure that the network authority based on the network IP does not change during the roaming process. Just like the mobile phone used now. First of all, a proxy router needs to be deployed in each network. Every local terminal device will be registered on this proxy router (as if each mobile phone number is registered at the home location), and the terminal device will get an IP address belonging to this network. , All data packets can reach this terminal device with the terminal IP address as the destination address. This proxy router is called the Home Agent (HA). Secondly, a foreign proxy server needs to be deployed. When a terminal device roams to a foreign network, the terminal device needs to notify the home agent and the agent router of the network where it is located. This agent router is called a foreign agent (FA). A handshake will be established between the home agent and the foreign agent (as if the mobile phone is registered in the roaming place, and the roaming

network informs the home network of the mobile phone number). After the handshake, the foreign agent assigns a Locator, which is the PA address, to the terminal. In the communication process, the data packet still uses the original address (Identifier, PI address) of the terminal device as the destination address, and first reaches the foreign agent. The foreign agent replaces the Identifier with the Locator address for transmission according to the mapping table it owns, and adds the Identifier to the TLV field of the hop-by-hop option header for identification.

6. SPLIT6 Rules

SPLIT6 architecture shall follow the following two principles:

1.Identifier address should only be used in the identifier space, without entering the locator space, unless: identifier address equals naming address

2.Locator address is only used in the locator space and does not enter the identifier space, unless: identifier address equals naming address

Therefore, the end to end communication of SPLIT6 can be categorized into following four conditions depend on whether the device has moved or not.

7. Security Considerations

8. IANA Considerations

This document does not include an IANA request.

9. Acknowledgements

The authors would like to acknowledge XXX for their valuable review and comments.

10. References

10.1. 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>.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, DOI 10.17487/RFC5533, June 2009, <https://www.rfc-editor.org/info/rfc5533>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[RFC8002] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 8002, DOI 10.17487/RFC8002, October 2016, <https://www.rfc-editor.org/info/rfc8002>.

[RFC8113] Boucadair, M. and C. Jacquenet, "Locator/ID Separation Protocol (LISP): Shared Extension Message & IANA Registry for Packet Type Allocations", RFC 8113, DOI 10.17487/RFC8113, March 2017, <https://www.rfc-editor.org/info/rfc8113>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

10.2. Informative References

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <https://www.rfc-editor.org/info/rfc6052>.

Authors' Addresses

Haisheng Yu
Guangzhou Root Chain International Network Research Institute Co., Ltd.
Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: hsyu@biigroup.cn

Hanzhuo Zhang

Guangzhou Root Chain International Network Research Institute Co., Ltd.
Xiangjiang International Technology Innovation Center, 41 Jinlong Road, Nansha District, Guangzhou
Guangzhou
China

Email: hzzhang@biigroup.cn