Workgroup: Network Working Group
Internet-Draft:
draft-jia-scenarios-flexible-address-
structure-00
Published: 31 October 2020
Intended Status: Informational
Expires: 4 May 2021
Authors: Y. Jia Huawei
G. Li Huawei
S. Jiang Huawei

Scenarios for Flexible Address Structure

Abstract

Along as the adoption of TCP/IP in increasingly emerging scenarios, challenges emerge as well due to the ossified address structure. To still enable TCP/IP for networks that previously using exclusive protocols, a flexible address structure would be highly preferred for their particular properties. This document describes well-recognized scenarios that typically require a flexible address structure, and states the requirements of such flexible address structure.

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

As the unified protocol of the network layer, Internet Protocol (IP) constantly promotes the prosperity of the entire Internet. With the success of TCP/IP protocol stack, IP is gradually replacing exclusive protocols and becomes the core protocol of the entire communication system.

Along as the popularization of TCP/IP, increasingly scenarios long for a flexible address structure. To fulfill the reachability, IP address is designed to hold the topology semantic only [RFC0791]. While within limited domains (ref. [RFC8799]), a multi-semantic address could be increasingly preferred in implementing complex actions and capabilities for particular scenarios. Under such circumstances, a flexible address structure can unleash more possibilities in serving new scenarios.

This document describes well-recognized scenarios that typically require a flexible address structure, and states the requirements of such flexible address structure.

2. Flexibility: Potential Orientation

Since a flexible address is expected be adaptive with different scenarios and routing abilities,
potentially orientations of a flexible address structure should include multiple semantics. According to the definition of IP structure [RFC1180], cyberspace topology location serves as the only semantic of IP address. While for emerging scenarios in reality, several semantics are expected for reachability, e.g., contents [CONTENT-NET] or names [ndn]. To accommodate growing requirements of futuristic scenarios, address with multi-semantic embedding should compose the core of the flexibility. With the dynamic semantic embedding, the length of the address should accordingly adaptive.

3. Scenarios

Although new scenarios are ever changing, they principally belong to a fixed scene, i.e., limited domain [RFC8799]. Limited domain, which first defined in [RFC8799], refers to a single physical network attached to or running in parallel with the Internet, or a defined set of users and nodes distributed over a much wider area, but drawn together by a single virtual network over the Internet. Within the limited domains, requirements, behaviors, and semantics could be noticeable local and network specific.

As the dominant status of IP in networking coverage, more networks attempt to adopt TCP/IP in their local networks. Instead of building proprietary network, a TCP/IP stack network facilitates convenient reachability via global Internet and reduces operating expense for exclusive protocols. According to the location that the retrofit of address structure taking effect, targeted scenes perfectly match the demarcation of limited domain, i.e., a edge network attaching to Internet. Thus for networks that seeking for IP convenience but enhanced capabilities, limited domains are scenarios that flexible address structure taking effect.

3.1. Internet of Things (IoTs)

In many IoT scenarios, a simple, low-cost communication network is required, and there are limitations for network devices in computational power, memory, and energy availability. In addition to [IEEE.802.15.4], it can be seen that networks using link layer technologies such as Z-Wave, BLE [BLE], DECT_ULE, MS/TP, NFC, and PLC require end-to-end IPv6 protocols [RFC8200] to run on constrained node networks. The IP protocol allows IoT devices with multiple connection types to connect to each other or to other nodes on the Internet. Generally, a group of IoT network devices form a constrained node network at the edge, and IoT terminals connect to these network devices for data transmission. Devices located on the edge of this network and the Internet can act as gateway devices. To ensure security and reliability, multiple gateways must be deployed. IoT devices on the network can easily select one of gateways for traffic to pass through. This type of network and IoT devices in the network require as little computational power as possible, smaller memory requirements, and better energy availability to reduce the total cost of ownership of the network.

3.2. Satellite Network

In the future, the space-based Internet will provide global Internet connections through satellite and station on the ground interconnection. The low cost of satellite launch and the reduction of the cost of network equipment will promote the development of high-density satellite networks. With the convergence of space-based networks and terrestrial networks, users can experience seamless broadband access. Whatever on cruise ships, flights, and cars, users can switch data communication services over Wi-Fi, cellular, or

satellite networks at any time. The network service provider will plan the transmission path of user traffic based on the network coverage, satellite orbit, route, and link load. The advantage of long-distance transmission but shorter delay of space-based networks is fully used to provide high-quality Internet connections for users in areas not covered by terrestrial networks. There is a significant difference between the high dynamics of satellite network and the statics of terrestrial network topology. The traditional satellite network cannot meet the preceding requirements through the networking of the dedicated station on the ground.

3.3. Dynamic Service and Resource

In the future, the network will integrate services and resources from various aspects such as life, production, and learning. Digitalized services and resources are divided into multiple data blocks on the network and multiple copies of data blocks exist, which will become the basic mode. Access to services and resources through URIs has been discussed by many researches, such as NDN [ndn] and ICN [RFC7476]. In practice, the dynamic services and resource management and access mechanisms of integrating ID and address technologies will be more suited to user needs. Providers of services and resources can publish online services and resources through unified identifiers without additional planning of identifiers and locations for data and their replicas. Users can access required services and resources in the nearest and on-demand mode. Further, users can make a request based on the type of service and resource and get a response to the service or a copy of the data.

3.4. Policy-based Traffic Control

Policy-based traffic control is constantly far from flexible. To restrict traffics for specific objects, e.g., devices, users, or group of them, a current solution is subnet partition. Representative technique for subnet partition includes VLAN [RFC5517] and VxLAN [RFC7348]. However, such mechanism usually involve numerous manual configuration, and even small changes in reality could also result in a repartition or manual efforts.

According to the semantic of IP address forwarding, any inconvenience of traffic control stems from the decoupling of address semantic and policy objects. Since address content only present topology location in IPv6, extra out-of-band effort is needed to partition network or recognize traffic from target objects.

For address with objects identifier encoded, policy-based traffic control could be almost automatic. For every node forwarding traffic, object identity could be first extracted from both source and destination address once packets arrive. Then by matching objects and policy-based rules, nodes on the path could trigger particular actions that dynamically assigned by administrators. For

examples, action permit, action deny, and action permit but low priority. Particular, such action could also be applied from security restriction.

3.5. Robust Trust and Security

A flexible semantic could be significate in constructing a trust and secure communication. For example, Cryptographically Generated Addresses (CGA) [RFC3972] embeds a truncated public key in the last 57-bit of IPv6 address. Even with a truncated key, authentication and security is greatly enhanced within a IP network via asymmetric cryptography and IPsec [RFC4301]. Similarly, Host Identity Protocol (HIP) [RFC7401] refers such methodology and constructs a enhanced TCP/IP stack.

Within a flexible address structure, any secure-related keys could be intactly included in address structure without any information loss. Under such condition, connection provided by such address could be considered as absolute secure only if the cryptography involved is secure.

4. Requirements

According to the capabilities for scenarios above, this section extracts basic requirements for a flexible address structure. Points below details the basal requirements.

*Multi-Semantics: Since semantics are the core of network routing, multi-semantics compose the main capability of the flexible address.

*Variable Address Length: As for networks with constrained devices, short address becomes necessary for protocol adoption. While on other hand, address space should be adequate enough to accommodate numerous devices.

*IPv6 Interoperability: Without global reachability, a flexible address would be the same as an exclusive protocol. In other words, a flexible address should be valuable only it is inter-operable with IPv6.

5. Security Considerations

This document introduces no new security considerations.

6. IANA Considerations

This document does not include an IANA request.

7. Informative References

[BLE] Bluetooth SIG Working Groups, "Bluetooth Specification", <https://www.bluetooth.com/specifications/>.

[CONTENT-NET] Choi, J., Han, J., and E. Cho, "A survey on content-oriented networking for efficient content delivery", IEEE Communications Magazine 2011, 49(3): 121-127, May 2011.

[IEEE.802.15.4] IEEE 802.15 WPAN Task Group 4, "IEEE 802.15.4 - IEEE Standard for Low-Rate Wireless Networks", May 2020, <https://standards.ieee.org/standard/802_15_4-2020.html>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC1180] Socolofsky, T. and C. Kale, "TCP/IP tutorial", RFC 1180, DOI 10.17487/RFC1180, January 1991, <https://www.rfc-editor.org/info/rfc1180>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC5517] HomChaudhuri, S. and M. Foschiano, "Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment", RFC 5517, DOI 10.17487/RFC5517, February 2010, <https://www.rfc-editor.org/info/rfc5517>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[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>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <https://www.rfc-editor.org/info/rfc7476>.

[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>.

[RFC8799]
Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

[ndn] Zhang, L., Afanasyev, A., and J. Burke, "Named data networking", ACM SIGCOMM Computer Communication Review 44(3): 66-73, 2014.

Authors' Addresses

Yihao Jia
Huawei Technologies Co., Ltd
156 Beiqing Rd.
Haidian, Beijing
100095
P.R. China

Email: jiayihao@huawei.com

Guangpeng Li
Huawei Technologies Co., Ltd
156 Beiqing Rd.
Haidian, Beijing
100095
P.R. China

Email: liguangpeng@huawei.com

Sheng Jiang
Huawei Technologies Co., Ltd
156 Beiqing Rd.
Haidian, Beijing
100095
P.R. China

Email: jiangsheng@huawei.com