Network Working Group   B. Liu
Internet Draft   S. Jiang
Intended status: Best Current Practice   Huawei Technologies Co., Ltd
Expires: September 12, 2012   C. Byrne
                                                            T-Mobile USA
                                                          March 12, 2012

Analysis and recommendation for the ULA usage
draft-liu-v6ops-ula-usage-analysis-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes use cases where ULA address may be beneficially used.

Table of Contents

1. Introduction 2
2. The features of ULA 2
2.1. Globally unique..... 2
2.2. Independent address space 3
2.3. Well known prefix 3
3. ULA usage analysis 3
3.1. ULA-only deployment..... 4
3.2. ULA with PA 5
3.3. Special routing/prefix..... 6
3.4. Used as identifier 7
4. Security Considerations 7
5. IANA Considerations 8
6. Conclusions 8
7. References 8
7.1. Normative References 8
7.2. Informative References 8
8. Acknowledgments 9

1. Introduction

Unique Local Addresses (ULAs) are defined in RFC 4193 [RFC4193] as provider-independent prefixes that can be used on isolated networks, internal networks, and VPNs. Although ULAs may be treated like global scope by applications, normally they are not used on the publicly routable internet.

However, the ULAs haven't been widely used since IPv6 hasn't been widely deployed yet.

The use of ULA addresses in various types of networks has been confused for network operators. Some network operators believe ULAs are not useful at all while other network operators run their entire networks on ULA address space. This document attempts to clarify the advantages and disadvantages of ULAs and how they can be most appropriately used.

(Editor's note: This draft welcomes any existing practice of deploying ULA to be discussed.)

2. The features of ULA

2.1. Globally unique

ULA is intended to be globally unique to avoid collision. Since the hosts assigned with ULA may occasionally be merged into one network,

this uniqueness is necessary. The prefix uniqueness is based on randomization of 40 bits and is considered random enough to ensure a high degree of uniqueness and make merging of networks simple and without the need to renumbering overlapping IP address space. Overlapping is cited as a deficiency with how [RFC1918] addresses were deployed, and ULA was designed to overcome this deficiency.

Notice that, as described in [RFC4864], in practice, applications may treat ULAs like global-scope addresses, but address selection algorithms may need to distinguish between ULAs and ordinary global-scope unicast addresses to ensure bidirectional communications.

2.2. Independent address space

ULA provides an internal address independence capability in IPv6 that is similar to how RFC 1918 is commonly used. ULA allows administrators to configure the internal network of each platform the same way it is configured in IPv4. Many organizations have security policies and architectures based around the local-only routing of RFC1918 addresses and those policies may directly map to ULA. ULA can be used for internal communications without having any permanent or only intermittent Internet connectivity. And it needs no registration so that it can support on-demand usage and does not carry any RIR documentation burden or disclosures.

2.3. Well known prefix

The prefixes of ULAs are well known and they are easy to be identified and easy to be filtered.

This feature may be convenient to management of security policies and troubleshooting. For example, the administrators can decide what parameters have to be assembled or transmitted globally, by a separate function, through an appropriate gateway/firewall, to the Internet or to the telecom network.

3. ULA usage analysis

In this section, we try to cover plausible possible ULA use case. Some of them have been discussed in other documents which are briefly reviewed as well as other potential valid usage is discussed.

3.1. ULA-only deployment

This section talks about use cases that hosts in a network are only assigned with ULAs.

IP is used ubiquitously. Some situations like RS-485, or other type of industrial control bus, or even non-networked digital interface like MIL-STD-1397 began to use IP protocol.

If one is in a network that does not have service from someone that will allocate it a prefix and wants to either use addresses that are not link-local or addresses that will allow for routing, a ULA provides a way to generate a prefix for the purpose.

- Isolated network

In some situations, the network is isolated or it has not been connected to the outside yet. ULA is a straightforward way to assign the IP addresses in the network with minimal administrative cost or burden.

ULA is a good solution for networks that are explicitly designed to not connect to the internet. These networks may include machine-to-machine, sensor networks, or other types of SCADA networks which may include very large numbers of addresses and explicitly prohibited from connect to the global internet (electricity meters...). Just like many implementation of RFC1918 address space, the ULA address space is one layer of a multilayer security design.

- Connected network

In some situations, hosts/interfaces are assigned with ULA-only, but the networks need to communicate with the outside. The use case may include the following two models.

o Using NAT

With some a kind of NAT which provides a simple one to one mapping for a subset of the internal addresses could fit the requirement.

Generally, this draft doesn't consider the ULA+NAT a good model of IPv6 deployment in normal cases. When thinking about ULA, we should eliminate the misunderstanding that ULA means the IPv6 version of rfc1918 deployment model.

But this draft doesn't intend to deny the requirement of ULA+NAT for some special cases. In some very constrained situations(for example,

in the sensors), the network needs ULA as the on-demand and stable addressing which doesn't need much code to support address assignment mechanisms like DHCP or ND. And the network also needs to connect to the outside, then there can be a gateway to be the NAT which may not be so sensitive to the constrained resource. This behavior could refer NPTv6 [RFC6296].

- Using application-layer proxies

The proxies terminate the network-layer connectivity of the hosts and delegate the outgoing/incoming connections.

This draft also doesn't recommend this use case as a good deployment model. However, there may be some scenarios that need this kind of deployment for some special purpose(strict application access control, content monitoring, e.g.).

3.2. ULA with PA

There are two classes of network probably to use ULA with PA addresses:

- Home network. Home networks are normally assigned with PA addresses to connect to the uplink of some an ISP. And besides, they may need internal routed networking even when the ISP link is down. Then ULA is a proper tool to fit the requirement. And in [RFC6204], it requires the CPE to support ULA.

- Enterprise network. An enterprise network is usually a managed network with a fixed PA space. The ULA could be used for internal connectivity redundancy and better internal connectivity or isolation of certain functions like OAM of servers.

For either home networks or enterprise networks, the main purpose of using ULA along with PA is to provide a logically local routing plane separated from the globally routing plane. The benefit is to ensure stable and specific local communication regardless of the ISP uplink failure. This benefit is especially meaningful for the home network or private OAM function in an enterprise.

In some special cases such as renumbering, enterprise administrators may want to avoid the need to renumber their internal-only, private nodes when they have to renumber the PA addresses of the whole network because of changing ISPs, ISPs restructure their address allocations, or whatever reasons. In these situations, ULA is an effective tool for the internal-only nodes.

Besides the internal-only nodes, the public nodes can also benefit from ULA for renumbering. When renumbering, as RFC4192 suggested, it has a period to keep using the old prefix(es) before the new prefix(es) is(are) stable. In the process of adding new prefix(es) and deprecating old prefix(es), it is not easy to keep the local communication immune of global routing plane change. If we use ULA for the local communication, the separated local routing plane can isolate the affecting by global routing change.

But for the separated local routing plane, there always be some argument that in practice the ULA+PA makes terrible operational complexity. But it is not a ULA-specific problem, the multiple-addresses-per-interface is an important feature of IPv6 protocol. So it is ambiguous that the argument is just about just ULA+PA only, or about the common running multiple addresses per-interface. [Editor's note: this issue has not achieved consensus yet]

Another issue is mentioned in [RFC5220], there is a possibility that the longest matching rule will not be able to choose the correct address between ULAs and global unicast addresses for correct intra-site and extra-site communication. In [draft-ietf-6man-rfc3484bis] , it claimed that a site-specific policy entry can be used to cause ULAs within a site to be preferred over global addresses.

3.3. Special routing/prefix

- Special routing

If you have a special routing scenario, of which [draft-baker-v6ops-b2b-private-routing] is an example, for various reasons you might want to have routing that you control and is separate from other routing. In the b2b case, even though two companies each have at least one ISP, they might choose to also use direct connectivity that only connects stated machines, such as a silicon foundry with client engineers that use it. A ULA provides a simple way to obtain such a prefix that would be used in accordance with an agreement between the parties.

- Used as NAT64 prefix

Since the NAT64 pref64 is just a group of local fake addresses for the DNS64 to point traffic to a NAT64, the pref64 is a very good use of ULA. It ensures that only local systems can use the translation resources of the NAT64 system since the ULA is not globally routable and helps clearly identify traffic that is locally contained and destine to a NAT64. Using ULA for Pref64 is deployed and it is an operational model.

But there's an issue should be noticed. The NAT64 standard (RFC6146) mentioned the pref64 should align with RFC6052, in which the IPv4-Embedded IPv6 Address format was specified. If we pick a /48 for NAT64, it happened to be a standard 48/ part of ULA (7bit ULA famous prefix+ 1 "L" bit + 40bit Global ID). Then the 40bit of ULA is not violated to be filled with part of the 32bit IPv4 address. This is important, because the 40bit assures the uniqueness of ULA, if the prefix is shorter than /48, the 40bit would be violated, and this may cause conformance issue. But it is considered that the most common use case will be a /96 PREF64, or even /64 will be used. So it seems this issue is not common in current practice.

It is most common that ULA Pref64 will be deployed on a single internal network, where the clients and the NAT64 share a common internal network. ULA will not be effective as Pref64 when the access network must use an Internet transit to receive the translation service of a NAT64 since the ULA will not route across the internet.

3.4. Used as identifier

In [RFC6281], the protocol BTMM (Back To My Mac) needs to assign a topology-independent identifier to each client host according to the following considerations:

- TCP connections between two end hosts wish to survive in network changes.

- Sometimes one needs a constant identifier to be associated with a key so that the Security Association can survive the location changes[RFC6281].

ULA can fit the requirements, and besides, ULA can be used directly because it belongs to the existing IPv6 code and it can be created by the ends themselves at boot time. As ULA would not cause any problem to the routing system, it can be considered as an ID/Locator split solution in this case.

But there is a problem of ULAs being identifiers, that in theory it has the possibility of collision. However, the probability is desirable small enough.

4. Security Considerations

Security considerations regarding ULAs, in general, please refer to the ULA specification RFC 4193 [RFC4193].

5. IANA Considerations

None.

6. Conclusions

- ULAs have been successfully deployed in a diverse set of circumstances including large private machine-to-machine type networks, enterprise networks with private systems, and within service providers to limit Internet communication with non-public services such as caching DNS servers and NAT64 translation resources.

- ULAs do not provide any intrinsic security benefit, but the characteristic that they cannot be routed on the internet may be leveraged as part of a multilayer security policy to limit the communication with the internet.

- ULAs are self-assigned and unique. Self-assigned allows for network deployments independent of RIR policy or documentation requirements. The fact that ULA require randomization within the prefix ensures that ULA is an improvement over RFC1918 deployments which were likely to collide when internal networks merged.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP14, March 1997.

[RFC4193] Hinden, R., B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

7.2. Informative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets",BCP 5, RFC 1918, February 1996.

[RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.

[RFC5220] Matsumoto, A., Fujisaki, T., Hiromi, R., and K. Kanayama, "Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules", RFC 5220, July 2008.

[RFC6281] Cheshire, S., Zhu, Z., Wakikawa, R., and L. Zhang, "Understanding Apple's Back to My Mac (BTMM) Service", RFC 6281, June 2011.

[RFC6296] Wasserman, M., and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.

[draft-ietf-6man-rfc3484bis] Thaler, D., Draves, R., Matsumoto, A., and Tim Chown, "Default Address Selection for Internet Protocol version 6 (IPv6)", Working in progress.

[draft-baker-v6ops-b2b-private-routing] F. Baker, "Business to Business Private Routing", Expired

8. Acknowledgments

Many valuable comments were received in the mail list, especially from Fred Baker, Brian Carpenter, Anders Brandt and Wesley George.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Bing Liu
Huawei Technologies Co., Ltd
Huawei Q14 Building, No.156 Beiqing Rd.,
Zhong-Guan-Cun Environmental Protection Park, Beijing
P.R. China

Email: leo.liubing@huawei.com

Sheng Jiang
Huawei Technologies Co., Ltd
Huawei Q14 Building, No.156 Beiqing Rd.,
Zhong-Guan-Cun Environmental Protection Park, Beijing
P.R. China

Email: jiangsheng@huawei.com

Cameron Byrne
T-Mobile USA
Bellevue, Washington 98006
USA

EMail: brian.e.carpenter@gmail.com