Internet Engineering Task Force (IETF)
Request for Comments: 6866
Category: Informational
ISSN: 2070-1721

B. Carpenter
Univ. of Auckland
S. Jiang
Huawei Technologies Co., Ltd.

February 2013

Problem Statement for Renumbering IPv6 Hosts with Static Addresses in Enterprise Networks

Abstract

This document analyses the problems of updating the IPv6 addresses of hosts in enterprise networks that, for operational reasons, require static addresses.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6866.

Table of Contents

1. Introduction

A problem that is frequently mentioned in discussions of renumbering enterprise networks [RFC5887] [RFC6879] [GAP-ANALYSIS] is that of statically assigned addresses. The scope of the present document is to analyse the problems caused for enterprise networks during renumbering by static addresses and to identify related gaps in existing technology. Some aspects also apply to small office and home networks, but these are not the intended scope of the document.

A static address can be defined as an IP address that is intended by the network manager to remain constant over a long period of time, possibly many years, regardless of system restarts or any other unpredictable events. Static addressing often implies manual address assignment, including manual preparation of configuration scripts. An implication of hosts having static addresses is that subnets must have static prefixes, which also requires analysis.

In a sense, the issue of static addresses is a result of history. As discussed in Section 3.2 of [RFC6250], various properties of IP addresses that have long been assumed by programmers and operators are no longer true today, although they were true when almost all addresses were manually assigned. In some cases, the resulting operational difficulties are avoided by static addressing.

Although static addressing is, in general, problematic for renumbering, hosts inside an enterprise may have static addresses for a number of operational reasons:

- For some reason, other hosts need to be configured with a literal numeric address for the host in question, so its address must be static.

- Even if a site has local DNS support and this is normally used to locate servers, some operators wish their servers to have static addresses so that issues of address lifetime and DNS Time to Live (TTL) cannot affect connectivity.

- Some approaches to virtual server farms require static addressing.

- On some sites, the network operations staff require hosts to have static addresses for asset management purposes and for address-based backtracking of security incidents.

- Certain software licensing mechanisms are based on IP addresses.

- Network elements, such as routers, are usually assigned static addresses, which are also configured into network monitoring and management systems.

- Access Control Lists and other security mechanisms are often configured using IP addresses.

Static addressing is not the same thing as manual addressing. Static addresses may be configured automatically, for example, by stateful DHCPv6. In that case, the database from which the static address is derived may itself have been created automatically in some fashion, or configured manually. If a host's address is configured manually by the host's administrator, it is by definition static.

This document analyses these issues in more detail and presents a problem statement. Where obvious alternatives to static addresses exist, they are mentioned.

2. Analysis

2.1. Static Addresses Imply Static Prefixes

Host addresses can only be static if subnet prefixes are also static. Static prefixes are such a long-established practice in enterprise networks that it is hard to discern the reason for them. Originally, before DHCP became available, there was simply no alternative. Thus it became accepted practice to assign subnet prefixes manually and build them into static router configurations. Today, the static nature of subnet prefixes has become a diagnostic tool in itself, at

least in the case of IPv4 where prefixes can easily be memorised. If several users sharing a subnet prefix report problems, the fault can readily be localised.

This model is being challenged for the case of unmanaged home IPv6 networks, in which it is possible to assign subnet prefixes automatically, at least in a cold start scenario [PREFIX]. For an enterprise network, the question arises whether automatic subnet prefix assignment can be made using the "without a flag day" approach to renumbering. [RFC4192] specifies that "the new prefix is added to the network infrastructure in parallel with (and without interfering with) the old prefix". Any method for automatic prefix assignment needs to support this.

2.2. Other Hosts Need Literal Address

This issue commonly arises in small networks without local DNS support, for devices such as printers, that all other hosts need to reach. In this case, not only does the host in question have a static address but that address is also configured in the other hosts. It is a long-established practice in small IPv4 enterprise networks that printers, in particular, are manually assigned a fixed address (typically, an [RFC1918] address) and that users are told to manually configure printer access using that fixed address. For a small network, the work involved in doing this is much less than the work involved in doing it "properly" by setting up DNS service, whether local or hosted by an ISP, to give the printer a name. Also, although the Service Location Protocol (SLP) [RFC2608] is widely available for tasks such as printer discovery, it is not widely used in enterprise networks. In consequence, if the printer is renumbered for any reason, the manual configuration of all users' hosts must be updated in many enterprises.

In the case of IPv6, exactly the same situation would be created by numbering the printer statically under the site's Unique Local Address (ULA) prefix [RFC4193]. Although this address would not change if the site's globally routable prefix is changed, internal renumbering for any other reason would be troublesome. Additionally, the disadvantage compared to IPv4 is that an IPv6 address is harder to communicate reliably, compared to something as simple as "10.1.1.10". The process will be significantly more error-prone for IPv6.

If such a host is numbered out of a globally routable prefix that is potentially subject to renumbering, then a renumbering event will require a configuration change in all hosts using the device in question, and such configuration data are by no means stored in the network layer.

At least two simple alternatives exist to avoid static numbering of simple devices, such as printers, by giving them local names. One is the use of Multicast DNS (mDNS) [RFC6762] in combination with DNS Service Discovery [RFC6763]. The other is the Service Location Protocol [RFC2608]. Both of these solutions are widely implemented, but seemingly not widely deployed in enterprise networks.

2.3. Static Server Addresses

On larger sites, it is safe to assume that servers of all kinds, including printers, are identified in user configurations and applications by DNS names. However, it is very widespread operational practice that servers have static IP addresses. If they did not, whenever an address assigned by stateless address autoconfiguration [RFC4862] or DHCPv6 [RFC3315] expired, and if the address actually changed for some extraneous reason, sessions in progress might fail (depending on whether the address deprecation period was long enough).

DNS aspects of renumbering are discussed in more detail in [RFC6879]. Here, we note that one reason for widespread use of static server addresses is the lack of deployment of Secure Dynamic DNS update [RFC3007], or some other method of prompt DNS updates, in enterprise networks. A separate issue is that even with such updates in place, remote users of a server would attempt to use the wrong address until the DNS TTL expired, as discussed in [RFC4192].

Server addresses can be managed centrally, even if they are static, by using DHCPv6 in stateful mode to ensure that the same address is always assigned to a given server. Consistency with DNS can be ensured by generating both DHCPv6 data and DNS data from a common configuration database using a suitable configuration tool. This does normally carry the implication that the database also contains the hardware (Media Access Control (MAC)) addresses of the relevant LAN interfaces on the servers, so that the correct IPv6 address can be delivered whenever a server requests an address. Not every operator wishes to maintain such a costly database, however, and some sites are therefore likely today to fall back on manual configuration of server addresses as a result.

In the event of renumbering the prefix covering such servers, the situation should be manageable if there is a common configuration database; the "without a flag day" procedure [RFC4192] could be followed. However, if there is no such database, a manual procedure would have to be adopted.

2.4. Static Virtual Machine Addresses

According to [PROBLEM], the placement and live migration of Virtual Machines (VMs) in a physical network requires that their IP addresses be fixed and static. Otherwise, when a VM is migrated to a different physical server, its IP address would change and transport sessions in progress would be lost. In effect, this is a special case of the previous one.

If VMs are numbered out of a prefix that is subject to renumbering, there is a direct conflict with application session continuity, unless a procedure similar to [RFC4192] is followed.

2.5. Asset Management and Security Tracing

There are some large (campus-sized) sites that not only capture the MAC addresses of servers in a configuration system, but also do so for desktop client machines with wired connections that are then given static IP addresses. Such hosts are not normally servers, so the two preceding cases do not apply. One motivation for this approach is straightforward asset management (Who has which computer?, Connected to which cable?). Another, more compelling, reason is security incident handling. If, as occurs with reasonable frequency on any large network, a particular host is found to be generating some form of unwanted traffic, it is urgent to be able to track back from its IP address to its physical location so that an appropriate intervention can be made. A static binding between the MAC address and the IPv6 address might be preferred for this purpose.

Such users will not, in most circumstances, be significantly inconvenienced by prefix renumbering, as long as it follows the [RFC4192] procedure. The address deprecation mechanism would allow for clean termination of current sessions, including those in which their machine was actually operating as a server, e.g., for a peer-to-peer application. The only users who would be seriously affected would be those running extremely long transport sessions that might outlive the address deprecation period.

Note that such large campus sites generally allocate addresses dynamically to wireless hosts, since (in an IPv4 world) addresses are scarce and allocating static addresses to intermittent users is not acceptable. Also, a wireless user may appear on different subnets at different times, so it cannot be given a single static address. These users will, in most circumstances, only be slightly inconvenienced, if at all, by prefix renumbering.

2.6. Primitive Software Licensing

Although it has many disadvantages and cannot be recommended as a solution, software licensing based on IP addresses or prefixes is still quite widely used in various forms. It is to be expected that this practice will continue for IPv6. If so, there is no alternative to informing the licensing party of the new address(es) by whatever administrative process is required. In an RFC 4192 renumbering procedure, the licenses for the old and new addresses or prefixes would have to overlap.

If acceptable to the licensing mechanism, using addresses under an enterprise's ULA prefix for software licensing would avoid this problem.

2.7. Network Elements

Each interface of a router needs an IP address, and so do other network elements, such as firewalls, proxies, and load balancers. Since these are critical infrastructures, they must be monitored and in some cases controlled by a network management system. A conventional approach to this is to assign the necessary IP addresses statically, and to configure those addresses in the monitoring and management systems. It is common practice that some such addresses will have no corresponding DNS entry. If these addresses need to be changed, there will be considerable ramifications. A restart of the network element might be needed, interrupting all user sessions in progress. Simultaneously, the monitoring and management system configurations must be updated, and in the case of a default router, its clients must be informed. To avoid such disruption, network elements must be renumbered according to an [RFC4192] procedure, like any other host.

There is a school of thought that to minimise renumbering problems for network elements and to keep the simplicity of static addressing for them, network elements should all have static ULA addresses for management and monitoring purposes, regardless of what other global addresses they may have.

2.8. Access Control Lists

Access Control Lists (ACLs) and other security mechanisms are often configured using static IP addresses. This may occur in network elements or hosts. If they are not updated promptly during a renumbering event, the result may be the opening of security loopholes, the blocking of legitimate traffic, or both. Such security loopholes may never be detected until they are successfully exploited.

2.9. Management Aspects

As noted in the Introduction, static addressing and manual address configuration are not the same thing. In terms of managing a renumbering event, static addressing derived automatically from a central database, e.g., by stateful DHCPv6, is clearly better than manual configuration by an administrator. This remains true even if the database itself requires manual changes, since, otherwise, an administrator would have to log in to every host concerned, a time-consuming and error-prone task. In cases where static addresses cannot be avoided, they could be assigned automatically from a central database using a suitable protocol, such as stateful DHCPv6. Clearly, the database needs to be supported by a suitable configuration tool, to minimise manual updates and to eliminate manual configuration of individual hosts.

3. Summary of Problem Statement

If subnet prefixes are statically assigned, various network elements and the network management system must be updated when they are renumbered. To avoid loss of existing user sessions, the old prefixes need to be removed only after a period of overlap.

If a printer or similar local server is statically addressed, and has no DNS or mDNS name and no discovery protocol, renumbering will require configuration changes in all hosts using that server. Most likely, these changes will be manual; therefore, this type of configuration should be avoided except for very small networks. Even if the server is under a ULA prefix, any subnet rearrangement that causes it to be renumbered will have the same effect.

If a server with a DNS name is statically addressed via a common configuration database that supports both DHCPv6 and DNS, then it can be renumbered "without a flag day" by following RFC 4192. However, if there is no common configuration database, then present technology requires manual intervention. Similar considerations apply to virtual servers with static addresses.

If client computers, such as desktops, are statically addressed via a common configuration database and stateful DHCPv6, they can also be renumbered "without a flag day." But other statically addressed clients will need manual intervention, so DHCPv6 should be used if possible.

If address-based software licensing is unavoidable, requiring static addresses, and ULAs cannot be used for this case, an administrative procedure during renumbering seems unavoidable.

If network elements have static addresses, the network management system and affected client hosts must be informed when they are renumbered. Even if a network element is under a ULA prefix, any subnet rearrangement that causes it to be renumbered will have the same effect.

ACLs configured with static addresses must be updated during renumbering.

It appears that the majority of the above problems can be largely mitigated if the following measures are taken:

1. The site uses a general configuration management database and an associated tool that manage all prefixes and all DHCPv6, DNS, and router and security configurations in a consistent and integrated way. Even if static addresses are used, they are always configured with this tool, and never manually. Specification of such a tool is out of scope for the present document.

2. All printers and other local servers are always accessed via a DNS or mDNS name, or via a discovery protocol. User computers are configured only with names for such servers and never with their addresses.

3. Internal traffic uses a ULA prefix, such that disturbance to such traffic is avoided if the externally used prefix changes.

4. If prefix renumbering is required, the RFC 4192 procedure is followed.

Remaining open questions are:

1. Is minor residual loss of extremely long-living transport sessions during renumbering operationally acceptable?

2. Can automatic network element renumbering be performed without interrupting any user sessions?

3. Do any software licensing systems require manual intervention?

4. Security Considerations

This document does not define a protocol, so it does not introduce any new security exposures. However, security configurations, such as ACLs, are affected by the renumbering of static addresses.

5. Acknowledgements

Valuable comments and contributions were made by Ran Atkinson, Ralph Droms, Adrian Farrel, Wes George, Brian Haberman, Bing Liu, Pete Resnick, and other participants in the 6renum WG.

6. Informative References

[GAP-ANALYSIS] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W. George, "IPv6 Site Renumbering Gap Analysis", Work in Progress, December 2012.

[PREFIX] Baker, F. and R. Droms, "IPv6 Prefix Assignment in Small Networks", Work in Progress, March 2012.

[PROBLEM] Narten, T., Ed., Gray, E., Ed., Black, D., Dutt, D., Fang, L., Kreeger, L., Napierala, M., and M. Sridharan, "Problem Statement: Overlays for Network Virtualization", Work in Progress, October 2012.

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

[RFC2608] Guttman, E., Perkins, C., Veizades, J., and M. Day, "Service Location Protocol, Version 2", RFC 2608, June 1999.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC5887] Carpenter, B., Atkinson, R., and H. Flinck, "Renumbering Still Needs Work", RFC 5887, May 2010.

[RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, May 2011.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[RFC6879] Jiang, S., Liu, B., and B. Carpenter, "IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods", RFC 6879, February 2013.

Authors' Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand

EMail: brian.e.carpenter@gmail.com

Sheng Jiang
Huawei Technologies Co., Ltd.
Q14, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

EMail: jiangsheng@huawei.com