Network Working Group
Internet-Draft
Updates: 5735 (if approved)
Intended status: BCP
Expires: June 21, 2012

J. Weil
Time Warner Cable
V. Kuarsingh
Rogers Communications
C. Donley
CableLabs
C. Liljenstolpe
Telstra Corp
M. Azinger
Frontier Communications

December 19, 2011

IANA Reserved IPv4 Prefix for Shared CGN Space
draft-weil-shared-transition-space-request-12

Abstract

This document requests the allocation of an IPv4 /10 address block to be used as Shared Carrier Grade Network Address Translation (CGN) Space. Service Providers will use Shared CGN Space to number the interfaces that connect CGN devices to Customer Premise Equipment (CPE).

Shared CGN Space is distinct from RFC1918 private address space because it is intended for use on Service Provider networks. However, it may be used as RFC 1918 private address space in certain circumstances. Details are provided in the text of this document.

As this document proposes the allocation of an additional special-use IPv4 address block, it updates RFC 5735.

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 http://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 June 21, 2012.

Table of Contents

1. Introduction

IPv4 address space is nearly exhausted. However, ISPs must continue to support IPv4 growth until IPv6 is fully deployed. To that end, many ISPs will deploy Carrier Grade NAT (CGN) such as that described in [RFC6264]. In order to effectively deploy CGN, ISPs require a new IPv4 /10 address block. This address block will be called the Shared CGN Space and will be used to number the interfaces that connect CGN devices to CPE.

Shared CGN Space is distinct from [RFC1918] private address space because it is intended for use on Service Provider networks. However, it may be used as [RFC1918] private address space when at least one of the following conditions is true:

- Shared CGN Space is not also used on the Service Provider side of the CPE.

- CPE routers behave correctly when using the same address block on both the internal and external interfaces.

This document requests the allocation of an IPv4 /10 address block to be used as Shared Carrier Grade Network (CGN) Space. In conversations with many ISPs, a /10 is the smallest block that will allow them to deploy CGNs on a regional basis without requiring nested CGNs. For Instance, as described in [I-D.shirasaki-isp-shared-addr], a /10 is sufficient to service Points of Presence in the Tokyo area.

As this document proposes the allocation of an additional special-use IPv4 address block, it updates [RFC5735].

2. 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].

3. Alternatives to Shared CGN Space

The interfaces that connect CGN devices to CPE might conceivably be numbered from any of the following address spaces:

- legitimately assigned globally unique address space
- usurped globally unique address space (i.e., squat space)
- [RFC1918] space
- Shared CGN Space

A Service Provider can number the interfaces in question from legitimately assigned globally unique address space. While this solution poses the fewest problems, it is impractical because globally unique IPv4 address space is in short supply. While the Regional Internet Registries (RIR) have enough address space to allocate a single /10 to be shared by all Service Providers, they do not have enough address space to make a unique assignment to each Service Provider.

Service Providers MUST NOT number the interfaces in question from usurped globally unique address space (i.e., squat space). If a Service Provider leaks advertisements for squat space into the global Internet, the legitimate holders of that address space may be adversely impacted, as would those wishing to communicate with them. Even if the Service Provider did not leak advertisements for squat space, the Service Provider and its subscribers might lose connectivity to the legitimate holders of that address space.

A Service Provider can number the interfaces in question from [RFC1918] space if either of the following conditions are true:

- The Service Provider knows that the CPE/NAT works correctly when the same [RFC1918] address block is used both on its inside and outside interfaces.
- The Service Provider knows that the [RFC1918] address block that it uses to number interfaces between the CGN and CPE is not used on the subscriber side of the CPE.

Unless at least one of the conditions above is true, the Service Provider cannot safely use [RFC1918] address space and must resort to Shared CGN Space. This is typically the case in an unmanaged service, where subscribers provide their own CPE and number their own internal network.

4. Use of Shared CGN Space

Shared CGN Space is IPv4 address space reserved for Service Provider use with the purpose of facilitating CGN deployment. Also, Shared CGN Space can be used as additional [RFC1918] space when at least one of the following conditions is true:

- Shared CGN Space is not also used on the Service Provider side of the CPE.
- CPE routers behave correctly when using the same address block on both the internal and external interfaces.

Shared CGN Space MUST NOT be used for any purpose other than those stated above.

Because Shared CGN Space addresses have no meaning outside of the Service Provider, routing information about Shared CGN Space networks MUST NOT be propagated across Service Provider boundaries. Service Providers MUST filter incoming advertisements regarding Shared CGN Space. One exception to the above proscription against exchanging routes for Shared CGN Space is in the case of a defined business relationship between two Service Providers (e.g., for hosted CGN service).

Packets with Shared CGN Space source or destination addresses MUST NOT be forwarded across Service Provider boundaries. Service Providers MUST filter such packets on ingress links. As above, one exception to the above proscriptions is in the case of business relationships such as hosted CGN service.

When running a single DNS infrastructure, Service Providers MUST NOT include Shared CGN Space in zone files. When running a split DNS infrastructure, Service Providers MUST NOT include Shared CGN Space in external-facing zone files.

Reverse DNS queries for Shared CGN Space addresses MUST NOT be forwarded to the global DNS infrastructure. DNS Providers SHOULD filter requests for Shared CGN Space reverse DNS queries on recursive nameservers. This is done to avoid having to set up something similar to AS112.net for RFC 1918 private address space that a host has incorrectly sent for a DNS reverse-mapping queries on the public Internet [RFC6304].

Because CGN service requires non-overlapping address space on each side of the home NAT and CGN, entities misusing Shared CGN Space for purposes other than for CGN service, as described in this document, are likely to experience problems implementing or connecting to CGN

service at such time as they exhaust their supply of public IPv4 addresses.

5. Risk

5.1. Analysis

Some existing applications discover the outside address of their local CPE, determine whether the address is reserved for special-use, and behave differently based on that determination. If a new IPv4 address block is reserved for special-use and that block is used to number CPE outside interfaces, some of the above-mentioned applications may fail.

For example, assume that an application requires its peer (or some other device) to initiate an incoming connection directly with its CPE outside address. That application discovers the outside address of its CPE and determines whether that address is reserved for special-use. If the address is reserved for special-use, the application rightly concludes the that address is not reachable from the global Internet and behaves in one manner. If the address is not reserved for special-use, the application assumes that the address is reachable from the global Internet and behaves in another manner.

While the assumption that a non-special-use address is reachable from the global Internet is generally safe, it is not always true (e.g., when the CPE outside interface is numbered from globally unique address space but that address is not advertised to the global Internet as when it is behind a CGN). Such an assumption could cause certain applications to behave incorrectly in those cases.

5.2. Empirical Data

As described in [RFC6269] and [I-D.donley-nat444-impacts], CGNs offer a reasonable quality of experience for many basic services including web, email, and Instant Messaging. This is true regardless of whether the address range between the CGN and CPE is globally unique, Shared CGN Space, or [RFC1918] space. However, CGNs do adversely impact some advanced services, in particular:

1. Console gaming - some games fail when two subscribers using the same outside public IPv4 address try to connect to each other.

2. Video streaming - performance is impacted when using one of several popular video streaming technologies to deliver multiple video streams to users behind particular CPE routers.

3. Peer-to-peer - some peer-to-peer applications cannot seed content due to the inability to open incoming ports through the CGN. Likewise, some SIP client implementations cannot receive incoming calls unless they first initiate outgoing traffic or open an

incoming port through the CGN using [I-D.ietf-pcp-base] or similar mechanism.

4. Geo-location - geo-location systems identify the location of the CGN server, not the end host.

5. Simultaneous logins - some websites (particularly banking and social networking websites) restrict the number of simultaneous logins per outside public IPv4 address.

6. 6to4 - 6to4 requires globally reachable addresses, and will not work in networks that employ addresses with limited topological span such as those employing CGNs.

Based on testing documented in [I-D.donley-nat444-impacts], the CGN impacts on 1-5 are comparable regardless of whether globally unique, Shared CGN Space, or [RFC1918] addresses are used. There is, however, a difference between the three alternatives in the treatment of 6to4.

As described in [RFC6343], CPE routers do not attempt to initialize 6to4 tunnels when they are configured with [RFC1918] or [RFC5735] WAN addresses. When configured with globally unique or Shared CGN Space addresses, such devices may attempt to initiate 6to4, which would fail. Service Providers can mitigate this issue using 6to4-PMT [I-D.kuarsingh-v6ops-6to4-provider-managed-tunnel] or blocking the route to 192.88.99.1 and generating an IPv4 'destination unreachable' message [RFC6343]. When the address range is well-defined, as with Shared CGN Space, CPE router vendors can include Shared CGN Space in their list of special-use addresses (e.g., [RFC5735]) and treat Shared CGN Space similarly to [RFC1918] space. When the CGN-CPE address range is not well-defined, as in the case of globally unique space, it will be more difficult for CPE router vendors to mitigate against this issue.

Thus, when comparing the use of [RFC1918] and Shared CGN Space, Shared CGN Space poses an additional impact on 6to4 connectivity, which can be mitigated by Service Provider or CPE router vendor action. On the other hand, the use of [RFC1918] address space poses more of a challenge vis-a-vis Shared CGN Space when the subscriber and Service Provider use overlapping [RFC1918] space, which will be outside the Service Provider's control in the case of unmanaged service. Service Providers have indicated that it is more challenging to mitigate the possibility of overlapping [RFC1918] address space on both sides of the CPE router than it is to mitigate the 6to4 impacts of Shared CGN Space.

6. Security Considerations

Similar to other [RFC5735] special use IPv4 addresses, Shared CGN Space does not directly raise security issues. However, the Internet does not inherently protect against abuse of these addresses. Attacks have been mounted that depend on the unexpected use of similar special-use addresses. Network operators are encouraged to review this document and determine what security policies should be associated with this address block within their specific operating environments and should consider including Shared CGN Space in Ingress Filter lists [RFC3704] unless their Internet service incorporates a CGN.

To mitigate against potential misuse of Shared CGN Space, except where required for hosted CGN service or similar business relationship,

- Routing information about Shared CGN Space networks MUST NOT be propagated across Service Provider boundaries. Service Providers MUST filter incoming advertisements regarding Shared CGN Space.

- Packets with Shared CGN Space source or destination addresses MUST NOT be forwarded across Service Provider boundaries. Service Providers MUST filter such packets on ingress links.

- Service Providers MUST NOT include Shared CGN Space in external-facing DNS zone files.

- Reverse DNS queries for Shared CGN Space addresses MUST NOT be forwarded to the global DNS infrastructure.

- DNS Providers SHOULD filter requests for Shared CGN Space reverse DNS queries on recursive nameservers.

7. IANA Considerations

IANA is asked to record the allocation of an IPv4 /10 for use as Shared CGN Space.

The Shared CGN Space address range is: x.x.0.0/10. [Note to RFC Editor: this address range to be added before publication]

8. References

8.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

8.2. Informative References

[I-D.donley-nat444-impacts]
Donley, C., Howard, L., Kuarsingh, V., Berg, J., and U. Colorado, "Assessing the Impact of Carrier-Grade NAT on Network Applications", draft-donley-nat444-impacts-03 (work in progress), November 2011.

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", draft-ietf-pcp-base-13 (work in progress), July 2011.

[I-D.kuarsingh-v6ops-6to4-provider-managed-tunnel]
Kuarsingh, V., Lee, Y., and O. Vautrin, "6to4 Provider Managed Tunnels", draft-kuarsingh-v6ops-6to4-provider-managed-tunnel-03 (work in progress), September 2011.

[I-D.shirasaki-isp-shared-addr]
Yamagata, I., Miyakawa, S., Nakagawa, A., Yamaguchi, J., and H. Ashida, "ISP Shared Address", draft-shirasaki-isp-shared-addr-06 (work in progress), July 2011.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC6264] Jiang, S., Guo, D., and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition", RFC 6264, June 2011.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269,

June 2011.

[RFC6304] Abley, J. and W. Maton, "AS112 Nameserver Operations", RFC 6304, July 2011.

[RFC6343] Carpenter, B., "Advisory Guidelines for 6to4 Deployment", RFC 6343, August 2011.

Appendix A. Acknowledgments

Thanks to the following people (in alphabetical order) for their guidance and feedback:

Stan Barber

John Brzozowski

Isaiah Connell

Greg Davies

Owen DeLong

Kirk Erichsen

Wes George

Chris Grundemann

Tony Hain

Philip Matthews

John Pomeroy

Barbara Stark

Jean-Francois Tremblay

Leo Vegoda

Steven Wright

Ikuhei Yamagata

Authors' Addresses

Jason Weil
Time Warner Cable
13820 Sunrise Valley Drive
Herndon, VA 20171
USA

Email: jason.weil@twcable.com

Victor Kuarsingh
Rogers Communications
8200 Dixie Road
Brampton, ON L6T 0C1
Canada

Email: victor.kuarsingh@gmail.com

Chris Donley
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: c.donley@cablelabs.com

Christopher Liljenstolpe
Telstra Corp
7/242 Exhibition Street
Melbourne, VIC 316
Australia

Phone: +61 3 8647 6389
Email: cdl@asgaard.org

Marla Azinger
Frontier Communications
Vancouver, WA
USA

Phone: +1.360.513.2293
Email: marla.azinger@frontiercorp.com