SAC079
SSAC Advisory on the Changing Nature of IPv4 Address Semantics

An Advisory from the ICANN Security and Stability Advisory Committee (SSAC)
25 February 2016

Preface

This is an advisory to the ICANN Board, the ICANN community, and, more broadly, the Internet community from the ICANN Security and Stability Advisory Committee (SSAC) on the changing role of IPv4 addresses caused in no small part by the scarcity, and then exhaustion, of the supply of IPv4 addresses for the Internet.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Table of Contents

Executive Summary

In this advisory, the SSAC considers the changing role of Internet Protocol Version 4 (IPv4) addresses caused by the increasing scarcity, and subsequent exhaustion, of IPv4 addresses. The exhaustion of the IPv4 address supply has been predicted since the end of the 1980s. However, the large scale adoption of mobile devices and their associated IPv4 addressing needs accelerated the exhaustion timetable, and placed increased pressure on network operators to conserve IPv4 addresses. This pressure has resulted in a marked increase in the use of Network Address Translation (NAT) technologies, altering the attributability characteristics of IPv4 addresses, and requiring changes to their interpretation by parties wishing to use them as endpoint identifiers.

This advisory points out three implications of this development:

- Application designers need to consider the fact that an IPv4 address does not necessarily identify an endpoint.
- Law enforcement and forensic functions need to consider that an IPv4 address alone may not be sufficient to correlate Internet activity observations with an endpoint; and even an IP address and associated timestamp generally may not suffice.
- Data retention mechanisms and policies that record or reference an IP address need to refactor their actions and requirements to consider that in increasingly large parts of the Internet, an IPv4 address is merely a temporary identifier. Potentially large volumes of ancillary data are required to match an IPv4 address to an endpoint.

This advisory also issues two recommendations:

- Network operators should accelerate plans to deploy IPv6, and consider the consequences of deploying IPv4 continuation technologies, such as NAT, prior to deployment.
- Device manufacturers should accelerate plans to support IPv6 as well as, or better, than they currently support IPv4.

1. Introduction

This document discusses the changing semantics of IPv4 addresses. The pressures of scarcity and subsequent exhaustion of the supply of IPv4 addresses to support the growth of the Internet has led over time to the widespread, if not universal, reliance on address translation and other forms of middlebox IPv4 packet header manipulation technologies that allow IPv4 addresses to be shared across multiple network endpoints. Thus, in today's Internet IPv4 addresses no longer necessarily identify unique endpoints, and attribution of transactions that occur across the network to particular endpoints should no longer rely on just IPv4 addresses. This situation has a range of technical and public policy implications relating to data retention, network security, law enforcement, and data forensics.

2. Background on IPv4 Exhaustion

Version 4 of the Internet Protocol (IPv4) uses fixed address fields in the IP protocol header for the source and destination addresses of the packet. These address fields are 32 bits in length, allowing for a theoretical maximum of 4,294,967,296 addresses. In the 1980s the addressing plan used by the Internet was structured into a two level hierarchy, with a network identifier part and a host identifier part. The network identifier was one of 8, 16 or 24 bits in length, with the corresponding host identifier part being 24, 16 or 8 bits in length, respectively. One half of the address space was dedicated to addressing 8-bit networks (Class A), one quarter to 16-bit networks (Class B), and one eighth to 24-bit networks (Class C). The remaining address blocks were divided equally into a block for multicast use (Class D), and for unspecified future use (Class E).

While this structure was a relatively inefficient use of addresses, it facilitated the operation of a relatively compact routing space.

By the end of the 1980s it was apparent that this address plan would run into exhaustion problems. An analysis by Frank Solensky presented at the Internet Engineering Task Force (IETF) Meeting in August 1990 projected the Class B address pool would be exhausted by March 1994 (Figure 1).

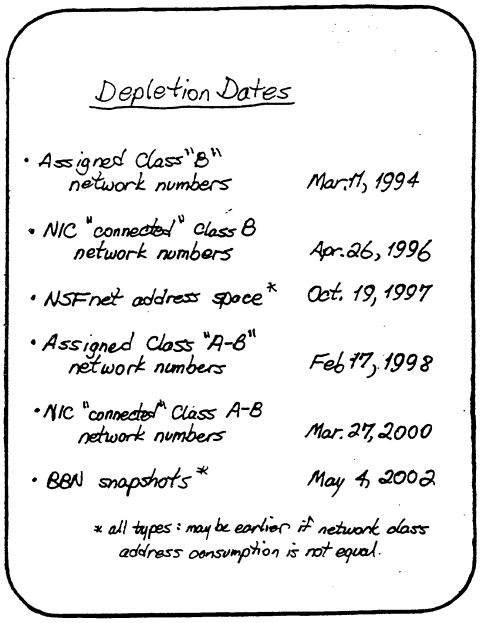

Figure 1: IPv4 Address Depletion Forecasts, August 1990 (presentation by F. Solensky, IETF 18)

The IETF responses took the form of a short-term change to the address plan that was intended to gain some additional time, and a longer term change to the protocol itself. The address plan change was, in effect, a change to the routing system that eliminated the

Class-based addresses, and allowed the length of the network part of an address to be separately specified in the route table. This change was called Classless Inter-Domain Routing (CIDR), and the major change here was a modification to the inter-domain routing protocol, the Border Gateway Protocol (BGP). This version of BGP – BGP-4 – was deployed in early 1993, and had an immediate impact on the consumption of IP addresses. The work on a new IP protocol continued, with general IETF consensus on a technical specification of the protocol (IPv6) achieved in 1997. This protocol specification expanded the address fields in the IP packet header from 32 bits to 128 bits. This was not a backward compatible change to the existing base of IPv4 hosts, so it was recognized that the transition would take some time, and that the CIDR deployment would provide that additional time.

There was one further outcome of the effort to define a new version of IP, and that was the concept of address sharing through the use of Network Address Translators (NATs).[1] The term NAT is also sometimes used to mean the mechanism of Network Address Translation. This was not the outcome of an IETF design committee per se, but a version of the approach was published as Request for Comment (RFC) 1631.

NATs proved to be very popular in the expansion of the Internet in the 1990s and 2000s. Internet Service Providers (ISPs) were able to allocate a single IPv4 address, or a small pool of addresses, to each connected customer, the customer then used a NAT on the boundary between their local network and the ISP service to share this single address across all hosts within the local network. For ISPs, this externalized the cost of address scarcity and concealed from the ISP the details of the connected network. This also added momentum to adopt a client server model of application interaction, where clients initiated connections, but were not the target of connection attempts. Clients could be located behind a NAT with minimal loss of functionality.

A further change occurred in the mid 1990s that also had an impact on the address consumption rate, namely the introduction of the Regional Internet Registry (RIR) structure. These organizations had a common focus on the address allocation function, and operated on the principle of address conservation and address utilization efficiency. A common benchmark at the time was to be able to demonstrate that the addresses already assigned to an organization were 80 percent used before further allocations would be made.

By the early 2000s predictions of address exhaustion extended into the 2030s (Figure 2)

[1] See http://www.sigcomm.org/sites/default/files/ccr/papers/2015/April/2766330-2766340.pdf.

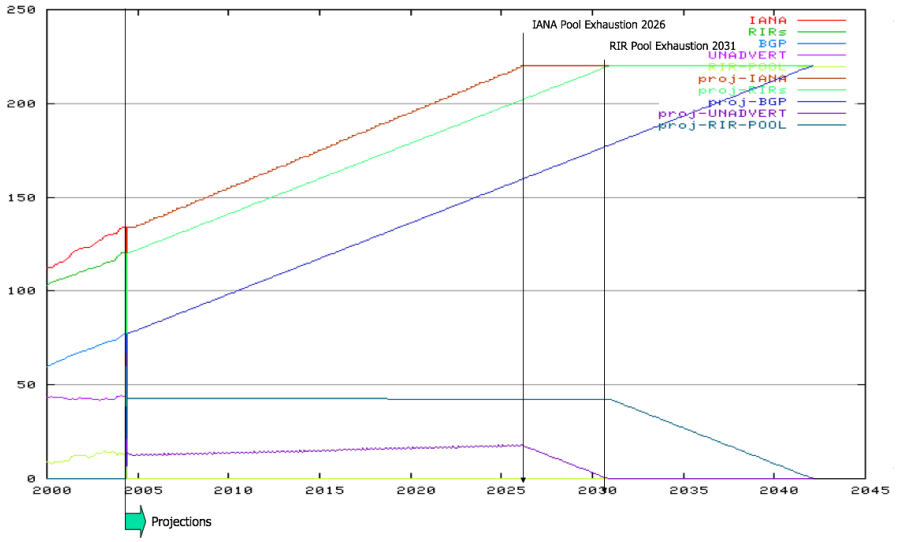

Figure 2: Address Exhaustion Projection, March 2003 (presentation to the March 2003 IEPG meeting by G. Huston)

At the same time the deployment of IPv6, which by this time had a relatively stable technical specification, was largely non-existent. To deploy IPv6 in time to avoid the exhaustion of remaining IPv4 address pools would have called for some determined action at the time.

Absent apparent economic or other incentives for existing Internet participants, IPv6 deployment simply did not happen. On the other hand, the Internet industry witnessed a dramatic expansion of the mobile IP market in the early 2000s. The specifications used within the mobile data sector, particularly Global System for Mobile Communications (GSM) and then Third Generation (3G), assumed the use of NAT functions in the carriers' networks. Thus, the large scale deployment of mobile services placed some pressure on the remaining address pools, but the use of NATs in the core of these networks alleviated the pressure on the address pools to some extent.

By 2009 it was clearly evident that some RIRs would deplete their remaining pools of IPv4 addresses long before universal adoption of IPv6 could be accomplished. An extended period of running parts of the Internet on a long-term paucity of further addresses had changed from being one of a number of possible scenarios to the most likely scenario. In February 2011, the Internet Assigned Numbers Authority (IANA), in application of the Global Policy for the Allocation of the Remaining IPv4 Address Space,[2] distributed its remaining IPv4 addresses to the RIRs, and from that point forward each RIR was working from its remaining pool.[3]

Below is the status of IPv4 address exhaustion in the five RIR regions:

[2] See https://www.icann.org/resources/pages/remaining-ipv4-2012-02-25-en.
[3] See https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt.

- Asia Pacific Network Information Centre (APNIC) consumed its general use IPv4 address pool in April 2011, and switched to a "last /8" policy for the remaining 16.7 million addresses, allocating each entity a maximum of 1,024 addresses from this pool.[4]
- The Réseaux IP Européens Network Coordination Centre (RIPE NCC) went through a similar transition in September 2012, and also switched to its "last /8" allocation policy for its remaining 16.7 million addresses.[5]
- The Latin American and Caribbean Network Information Centre (LACNIC) exhausted its remaining pool of addresses in May 2014, and as of June 10, 2015 is left with two smaller pools (two /11 address pools).[6]
- The American Registry for Internet Numbers (ARIN) exhausted its pool in September 2015, and reserved a /10 for special purpose micro allocations as part of the IPv6 transition.[7]
- As of the publication of this report, the African Network Information Centre (AFRINIC) still has some 32 million addresses in its free pool.[8] AFRINIC will switch to a "last /8" policy after half of this pool is allocated.

At its peak the RIRs allocated some 249 million addresses in a calendar year.[9] The current annual allocation rate as of the publication of this report is approximately 60 million addresses.[10] The Internet continues to grow at a far greater rate than this figure would suggest, particularly in the mobile sector and with the advent of more connected devices, and it is an inevitable consequence that this growth is being met through the use of address sharing via NATs in IPv4.

3. Network Address Translators

RFC 1631, an informational RFC, is the first specification of NATs published by the IETF, which was a memo based on a research paper by Paul Francis in January 1993.[11] This original specification operated at the IP level and performed a rewrite of the source address for outbound packets and the destination address for inbound packets by implementing a simple 1:1 address mapping. The internal translation table was based on the 32-bit IPv4 address, so this would be considered a 32-bit NAT.

While the IETF did not standardize the behavior of NATs for many years, the address utility of the NAT was dramatically increased by having the NAT look into the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) transport headers, translate both the source address and port on outbound packets, then make the

[4] See https://www.apnic.net/policy/resources.
[5] See https://www.ripe.net/publications/docs/ripe-649#51.
[6] See http://www.lacnic.net/en/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac.
[7] See https://www.arin.net/announcements/2015/20150924.html.
[8] See http://www.afrinic.net/en/services/statistics/ipv4-exhaustion.
[9] See http://www.potaroo.net/ispcol/2013-01/2012.html.
[10] See https://labs.apnic.net/?p=589.
[11] See http://www.sigcomm.org/sites/default/files/ccr/papers/2015/April/2766330-2766340.pdf.

corresponding translation upon the destination address and port for inbound packets. Here the internal translation table is based on the 32-bit IPv4 address and the 16-bit port address, so it would be considered a 48-bit NAT. Other terms such as Port Address Translation (PAT), Network Address Port Translation (NAPT),[12] Port Network Address Translation (PNAT) and IP Masquerading are also sometimes used to denote use of transport layer port information in the lookup table.

The NAT's address utility function can be further increased by using the combination of source and destination IP addresses, and ports to perform the lookup. This allows the same public-side address and port to be used by the NAT for connections established to different destinations. Here the internal translation table is based on the source and destination address and ports, so it would be considered a 96-bit NAT.

While hard evidence is not easy to come by, it appears that the most prevalent form of NAT in use in today's Internet is a 48-bit NAT. They are typically deployed with a single Internet routable IPv4 address on the NAT's external interface, and a single non-routable network from the private address (RFC 1918) pool internally.

The initial deployments of NAT occurred at the edge of the network, connecting customer networks to the public Internet. This form of deployment allowed a single IPv4 address to be assigned to each customer connection, and the edge NAT was used to share this address across the devices connected to the customer network.

Mobile networks use a slightly different architecture. The NAT is moved to the interior of the access network, and shares a pool of addresses across a set of mobile services. These NATs use larger tables and are capable of managing the state required by tens of thousands of simultaneous address translations. These often have been termed Carrier Grade NATs (CGNs).[13]

There has been a distinction between wireline access networks (that have assigned each customer connection a public IPv4 address), and mobile access networks (in which the mobile device is assigned a private address). However, this distinction is being dropped as the pressure of address scarcity increases. Access networks are now being deployed with multiple layers of NAT. Each edge customer NAT is assigned a single non-routable IPv4 address (often drawn from the RFC 6598 shared address space). A CGN within the access network then has the role of mapping each of these connections onto public addresses.

These NATs all operate in a single protocol domain, translating the address and port fields in the packet headers according to the state of the address binding table in each NAT. Some scenarios being used in networks that are supporting dual stack services involve a level of interplay between the two protocol stacks. This has led to a number of 'hybrid' NAT approaches that translate not only the addresses in an IPv4 packet, but

[12] See RFC 2663 at https://tools.ietf.org/html/rfc2663.
[13] See RFC 6888 at http://www.rfc-base.org/rfc-6888.html.

transform the IPv4 packet itself into a different protocol, such as deployments using 464XLAT.[14]

This document provides a very simplified view of what NATs are, and how they work in the real world. Often NAT functions are vastly more complex than simply performing lookups in a table. For example, a number of protocols (including File Transfer Protocol (FTP) and Session Initiation Protocol (SIP)) either embed IP address information into their protocol exchanges, and/or expect remote-end machines to initiate inbound connections after the session has already been established. This has led some NAT vendors to inspect and "fix" the addresses embedded in the protocol. In addition, NATs may need to examine traffic to know when a conversation has completed, so that they may reclaim the IPv4 table space. NATs with this type of functionality are often referred to as Application Level Gateways (ALG).[15]

There is also reason to believe that NATs are no longer as effective as they were previously at conserving IPv4 addresses. Modern applications often require many active connections at once, and "always on" applications located inside a NAT require resources to be reserved indefinitely. These application behaviors diminish a NATs' effective IPv4 address conservation.

4. Changes to IP Address Semantics

The original semantic model of an IPv4 address was that of a static identifier that uniquely distinguished one network endpoint from another. This begs the question of the definition of an 'endpoint', and the manner in which this distinguished identifier is used and negotiated in a network context.

This semantic model was adopted by many networking protocols, including IP. In this model, IP addresses are associated with endpoints in a relatively static association, such that a device that changes its address essentially changes the identity that it is presenting to the network.

The Internet was not developed in a vacuum of concepts and terminology, and perhaps one of the leading analogies that influenced the assumptions of the original semantics of an "address" was that of the telephone number. Telephone handsets were identified to the network by a unique telephone number, which had internal structure.[16] Parts of the number identified a country, and other parts identified the locality of the number, so that the number contained a codified form of routing instructions for the network to assist in call setup. In this sense a telephone number contained embedded locality information that could be used by the telephone network operator to route a call request, so that a telephone number contained both endpoint identification and locality information.

[14] See RFC 6877 at http://tools.ietf.org/html/rfc6877.
[15] See RFC 4787 at http://tools.ietf.org/html/rfc4787 and RFC 5382 at http://tools.ietf.org/html/rfc5382.
[16] See ITU specification E.164 at http://www.itu.int/rec/T-REC-E.164.

The same concepts existed with the original IP architecture, where the IPv4 address was divided into a network part and a host part. The network part allowed other networks to identify the network that contained the addressed endpoint, and the host part allowed the hosting network to identify the particular end host. Thus, the IP address contained embedded locality information that related how to reach a particular endpoint, as well as distinguishing that endpoint from all other endpoints. The introduction of CIDR in the mid-90's allowed the boundary point within an address between network and host parts to be variable, but the underlying concept of embedding locality and identification into an IP address remained.

Dynamic allocation of IPv4 addresses added a temporal aspect to the semantics of IPv4 addresses. Dial-up network access services allocated an IPv4 address for the duration of the dialed connection. Broadband access provision typically allocates an IPv4 address to an authenticated entity, reclaims it when the connection terminates and allocates it to the next user. Bootstrap Protocol/Dynamic Host Configuration Protocol (BOOTP/DHCP) usually allocates an IPv4 address to an endpoint on a Local Area Network (LAN) for a certain "lease" time. These and other dynamic address allocation schemes added a time dimension to the IPv4 address semantics: One now needs a tuple of IP Address + Time Stamp of event instantiation to identify an endpoint.

The introduction of NAT fundamentally changed the semantics of an IPv4 address. NATs create an asymmetry in the network, with an "exterior" and an "interior" defined by the NAT. The semantics of the address used on the exterior are the location and identity of the exterior interface of the NAT, rather than the identity of the endpoint host. The host part of the exterior address is interpreted by the NAT as a lookup entry into an internal, dynamically updated address translation table. The exterior address only has "meaning" in terms of utility for as long as the NAT maintains this entry in its address translation table.

Such addresses are stable, in that they consistently refer to the NAT unit, but are ephemeral in the sense that they relate only to an entry in the NAT's address translation table. Such entries are unstable, in that the values in the corresponding internal part of the translation table may change over time. The exterior address may not uniquely identify an entry in the NAT's translation table. In the case of 48-bit and 96-bit NAT, the transport protocol and the port address of the transport protocol may be used to form the lookup key of the translation table. Conventionally, the NAT uses the interior side address and port values to translate routing information into an exterior address and port on a 1:1 basis, so that a lookup with either the interior or exterior address and port pair (and interior/exterior context) will yield a unique address and port. This can be taken further and the lookup key into the translation table can also be the address and port of the remote end of the session as part of the translation table lookup key. The implication of this use of additional information in the address translation table is that the address itself is not used in a unique context, and the same exterior address may be used simultaneously in a number of concurrently active transport sessions.

The interior address has a more conventional semantic interpretation. The NAT assumes that the addresses used in the interior scope of the NAT are stable endpoint identifiers with an overlay of location information. *The critical observation here is that the semantics of an address used on the Internet vary according to where on the Internet the address is used.*

NATs may also be stacked, where multiple NATs may exist in sequence in a network path. This means that the interior of one NAT becomes the exterior of another NAT.

NATs do not announce their existence on a network path. At the level of the operation of the IP part of the protocol, commonly called layer 3, the presence of a NAT on a network path is entirely transparent. The remote side of a conversation does not change its IP level behavior if there is a NAT on the path. However, this does not necessarily apply outside of the strict purview of the IP layer. A non-NATed remote end cannot terminate a conversation with a NATed host and then re-establish contact with the same host by attempting to re-use the same IPv4 address. If the IPv4 address is a lookup into a NAT state, then the termination of the session may deallocate the NAT table entry and release the association of the exterior address with the interior address. Similarly, for 48-bit and 96-bit NATs session re-use is not readily possible. For the same reasons, embedding an IPv4 address in higher-layer protocols or the application data stream may not function in the intended manner when there are one or more NATs on the path.

The opaque nature of NATs implies changes to the traditional semantics of an IPv4 address. When a NAT is present on the data path then the addresses used in the session vary in their properties depending on where the observer is located with respect to the NATs. Observers on the exterior side of a NAT cannot assume that an address for a remote party is a stable endpoint identifier for that party. An alternative view is that this address may be part of a longer lookup vector into a NAT address translation table. The address itself will not indicate which of these two possible interpretations of the meaning of the address is the correct one. For example, in the following diagram, it is difficult for observers, without knowledge of the network topology, to disambiguate between observations at points A, B, or C. Thus, they can not assume these addresses are stable identifiers.

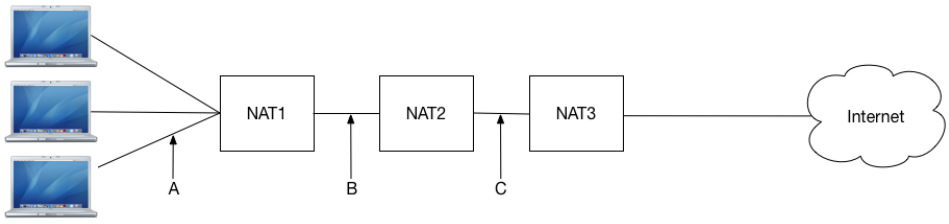

Figure 3: Potential locations of an observer relative to the NAT stack.

For example, if a member of Law Enforcement (LE) is presented with the traffic log below, and does not know the topology of the network, or where the traffic log was generated, it may not help them to identify the sender.

```
18:28:59.189949 IP 192.168.1.158.52273 >192.0.2.53.443
18:28:59.232193 IP 192.0.2.53.443 > 192.168.1.158.52273
18:28:59.279844 IP 192.168.1.158.52273 >192.0.2.53.443
18:28:59.295479 IP 192.0.2.53.443 > 192.168.1.158.52273
```

If the traffic were collected at point A in the above diagram, the source address 192.168.1.158 is one of the laptops.[17] If collected at point B or point C, the source address and port number have no meaning unless the law enforcement officer also knows the type of NATs in use, and the state of the mapping tables in the NATs at those times.

In another example, a given server on the Internet may log the source IP address and port numbers of connections, but without access to the state of the NAT tables in NAT1, NAT2, and NAT3 they will not be able to attribute the traffic to a specific endpoint.

5. Implications of Semantic Change

The increasing scarcity of IPv4 addresses has triggered some basic changes in the architecture of the Internet as it relates to the semantics of IPv4 addresses. The widespread deployment of NATs in today's Internet has resulted in a situation where addresses no longer can be assumed to be stable identification tokens that uniquely map to an endpoint. The presence of NATs implies the potential to share addresses across multiple endpoints, and the addresses used by NATs are ephemeral tokens used in a non-unique manner for individual sessions.

Because NATs do not use exterior addresses drawn from a differentiated pool, the altered semantics of an address used by a NAT are not intrinsically obvious. The logical conclusion is that an observer cannot assume that an address is a stable endpoint identifier. When used by a NAT, an address is a non-unique lookup into a translation table. In order to identify a particular NAT translation table entry it is necessary to also include an accurate timestamp. Additional data is required in this context, and depending on the nature of the NAT (e.g. 48-bit NAT, 96-bit NAT) the additional data needs to include the full set of source and destination address and port values, the type of NAT, and the set of NAT bindings that were active at this time. In the case of stacked NATs, this information needs to be available for every NAT on the path between the transacting endpoints.

This implies that those addresses still used as stable endpoint identifiers can be used in a forensic capacity to relate data logged at one part of the network to an endpoint, and potentially to a network user at that end point.

However, addresses used where there are NATs on the path lose this association with an endpoint, and the address alone is insufficient information to associate the logged data

[17] Even in this simple case, determining *which* of the pictured laptops sent the traffic may be impossible without access to DHCP logs.

with a single endpoint. Instead the address is directly associated to a NAT, and the NAT's binding logs may provide a set of potential interior endpoints. Additional data is then required in this context. Depending on the nature of the NAT (48-bit NAT vs. 96-bit NAT), the additional information needs to include: a relatively accurate time of day, the full set of source and destination address and port values, the type of NAT, and the set of NAT bindings that were active at that time. In the case of stacked NATs this information needs to be available for every NAT on the path in order to reliably associate a network layer IP address with an end system.

6. Conclusions

Today's Internet no longer uniformly associates a unique IPv4 address with each connected endpoint. Instead it uses a set of technologies that allow pools of addresses to be shared across multiple endpoints. These mechanisms enable the limited pool of available IPv4 addresses to be reused to span a network in which the number of connected endpoints vastly outnumbers the number of addresses available in the network and supported by the underlying protocol architecture.

This has three important implications for Internet technology developers, and those who depend on certain behaviors of the technology.

- Application designers need to consider the fact that an IP address does not necessarily identify an endpoint.
- Law enforcement and forensic functions need to consider that an IP address alone may not be sufficient to correlate Internet activity observations with an endpoint; and even an IP address associated timestamp generally may not suffice.
- Data retention mechanisms and policies that record or reference an IP address need to refactor their actions and requirements to consider that in increasingly large parts of the Internet, an IP address is merely a temporary identifier. Potentially large volumes of ancillary data are required to match an IP address to an endpoint.

In addition to the implications listed above. This advisory also issues two recommendations to help alleviate pressure on IPv4 address exhaustion, and eliminate the demand for NAT deployments.

- Network operators should accelerate plans to deploy IPv6, and consider the consequences of deploying IPv4 continuation technologies, such as NAT, prior to deployment.
- Device manufacturers, and application developers, should accelerate plans to support IPv6 as well as, or better, than they currently support IPv4.

7. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

7.1 Acknowledgments

The committee wishes to thank the following SSAC members and external experts for their time, contributions, and review in producing this Advisory.

SSAC members
Alain Aina
Don Blumenthal
Ben Butler
Ondrej Filip
Jim Galvin
Geoff Huston
Merike Kaeo
Warren Kumari
Xiaodong Lee
Danny McPherson
Russ Mundy
Doron Shikmoni
Suzanne Woolf

ICANN staff
Andrew McConachie (editor)
Kathy Schnitt
Steve Sheng

7.2 Disclosures of Interest

SSAC member biographical information and Disclosures of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2016-02-10-en.

7.3 Dissents

There were no dissents.

7.4 Withdrawals

KC Claffy
Mark Kosters
Carlos Martinez

Appendix A – Glossary of Terms

Application Level Gateway(ALG) – A device which combines NAT functionality with the translation of port information embedded in protocols at the session layer.

Border Gateway Protocol (BGP) – The inter-Autonomous System (AS) routing protocol for the Internet. BGP4 was deployed in 1993, and was the last major update.

Classless Inter-Domain Routing (CIDR) – The method of routing IP packets that uses a variable-length network mask. Introduced in 1993 to deal with IPv4 address exhaustion. Defined in RFC 1338 and RFC 1519.

Carrier Grade NAT (CGN) – A NAT deployed in the interior of an ISP's network, between end customers and their Autonomous System borders. Often using RFC 6598 shared address space. Defined in RFC 6888.

Global System for Mobile Communications (GSM) – The commonly accepted second family of protocols enabling mobile cellular communications. Did not include built in IP layer reachability information.

Hybrid NAT – The combination of both stateful NAT and IPv4/IPv6 protocol translation.

Network Address Translator/Network Address Translation (NAT) – A general term for the method of performing IP address translation, or the device that performs such translation..Defined in RFC 2663 and RFC 3022.

Stacked NAT – A logical topological network feature in which a packet must traverse multiple NATs from an endpoint to reach publicly routable IP space.

32-bit NAT – NAT which uses a single IPv4 address as the key in its lookup table. Referred to as Basic NAT in RFC 2663 and RFC 3022.

48-bit NAT – NAT which uses a single IPv4 address, and a single transport layer port number as the key in its lookup table. Referred to as Network Address Port Translation (NAPT) in RFC 2663 and RFC 3022. Also called Port Address Translation (PAT).

96-bit NAT – NAT which uses both destination and source IP addresses, and both destination and source transport layer port numbers as the key in its lookup table.