

University of Wales Trinity Saint David

Cloud computing

By Aleksandar Peshankov

IPv4 & IPv6

Submission date: 17 - December-2020

Submission ID: 1905148

File name:

Word count:

Character count:

Aleksandar Peshankov

Bcs in Cloud Computing

Contents

Part 1:	3
1. Research report of IPv6 addressing	3
Part 2	8
Explanation and analysis	11

Part 1:

1. Research report of IPv6 addressing

IPv6 uses an address space that is far larger than could be consumed by devices in the near reason future. The for such a large address space is to attempt to make address management easier, both when numbering hosts interior subnets and when numbering networks within the Internet. The hope is that addresses and subnets can be assigned according to logical schemes rather than assigning addresses in the maximum compact way. This is in contrast to allocation of addresses for IPv4; inside the CIDR world it is unclear where the network address ends and the host address begins. Some deductions can be made about IPv4 addresses: we can consult IANA and whois databases to determine who addresses have been assigned to. However, unless whois/DNS information is well maintained, it will be hard to know how addresses are actually being used. In this paper, we show how to use IPv6's extra expressiveness to infer topics about how addresses are being used. Others have used active probing to measure IPv6 topology or compare performance to IPv4, focusing on the connectivity graph or performance of the network, rather than configuration details.

Address Analysis Technique2.1 Prefix analysis

The breakdown of IPv6 address space is described by several IANA registries. The overall breakdown of address space is described in the `ipv6-address-space` registry. Smaller chunks are then described in more detail by other registries. In the case of other global addresses, we can use the `ipv6-unicast-address-assignments` to identify the RIR that addresses have been assigned to. This analysis is the same sort of classification that can be performed on IPv4 addresses. However, in some cases an IPv6 address will provide details about how IPv6 has been deployed. In particular, we can identify users of 6to4 (`2002::/16`), Teredo (`2001::/32`, formerly `3ffe:831f::/32`) and 6bone allocations (`3ffe::/16`, formerly `5f00::/8`).

1.2 Host ID analysis

Just as the prefix can tell us where an address may be (al)located or if certain transition techniquis are in use, the host-identity can also give us information about how IPv6 is configured on a node. This sort of infoomation is unavailable in IPv4 or in IPv6 if studies are entirely primarily based on address block or routing table information. Perhaps the most common mechanisms for assigning host IDs are manual configuration (on routers and some servers) and autoconfiguration (based on the MAC address of a device). Auto configuration can usually be identified because of the way that MAC address are converted to host IDs. In particular, the dominance of EUI-64 based addressing and Ethernet/WiFi cards with vendor-assigned addresses leads us to expect `fffe` as the middle 16 bits of the host ID and the 7th bit of the host ID will be set. ISATAP is a way that makes use of IPv4 as a layer 2 for IPv6, and it has a method for generating an IPv6 host ID from the underlying IPv4 deal with. The creation leads us to expect the primary quad (sixteen bits) of the host ID to be `0000` or `0200` and the second quad to be `5efe`, and these can be used as a test for ISATAP addresses. ISATAP is not the simplest scheme that uses IPv4 addresses as a manner to generate host IDs. IPv6 address parsers will usually permit the last two hex quads of the host ID to be

written as a traditional IPv4 dotted decimal. We use the subsequent heuristic to perceive host IDs that have the last two quads generated from a IPv4 address: an address is v4- based if (a) it is a 6to4 cope with and the second one quad is similar to the 7th quad; or (b) the 5th and sixth quads are zero, the seventh and eighth quads are one-of-a-kind, and the resulting IPv4 address could not be in IANA reserved/multicast address area. We have primarily based this heuristic on numerous factors. One is that 6over4 uses an IPv4 address padded with zeros and, as stated in, a few 6to4 implementations do the same. Also, a few sites derive their manually configured IPv6 cope with scheme from their IPv4 scheme. This take a look at has weaknesses; we can discuss its effectiveness in Section four. Teredo additionally uses a special host ID based on two IPv4 addresses (the address of the NAT box and the address of the Teredo server). Since Teredo makes use of an easily identifiable prefix, we become aware of such host IDs based totally at the prefix. In IPv4 networks, it's far common for addresses to be assigned dynamically by using DHCP from a equal pool. This presently seems less commonplace in IPv6 networks, perhaps because of the huge availability of vehicle configuration and relatively gradual development of DHCPv6- capable servers. Concerns have been raised due to the fact a set host ID, generated from a MAC address,(thinking about the troubles told beforehand in this introduction, especially for this theme and complex) would allow the tracking of gadgets as they moved from network to network. In reaction to this, a method for randomly generating IPv6 host IDs changed into designated, that is now to be had in many IPv6 implementations. This privacy addressing makes use of a cryptographic hash to generate the host ID, and then clears the sixth bit. This offers us with a way to identify privacy addresses. A crypto photo hash have to produce 0 and 1 bits in equal proportions. For a 63-bit output the Law of Large Numbers says that most people of privacy addresses may have round 32 bits set. The real technique used to perceive privacy addresses is to first determine if the address may be recognized as a few other sort of deal with, and if no longer it is considered as a candidate privateness deal with. The deal with must then satisfy the following: the host ID ought to have the sixth bit clean; the host ID must have between 27 and 35 set bits; the primary 32 bits ought to have among nine and 21 set bits; the remaining 32 bits have to have between 10 and 22 set bits; the host ID have to now not have or greater 'phrases' in it. These standards are designed to cowl the majority of privateness addresses, at the same time as rejecting patterns which are possibly to were manually configured, which include ::ffff:ffff and feed:babe:lifeless:red meat.

1.3 IE IPv6-Enabled Nameserver

The IE t0p-stage domain is served by a number of IPv6-succesful name servers. The IEDR, Ireland's domain registry, perform this type of, which has been advertised within the root sector due to the fact that September 2004. Log files showing all queries to this name server were available for the dates 22 April 2007–20 May 2007. The log documents record the date of the DNS requests and the IPv6 deal with making the request. The server best deals with IPv6 requests, so no comparable IPv4 statistics are to be had. 3.3 Traceroute Data In this phase we consider pretty a specific dataset. The worldwide IPv6 routing table is still pretty compact, with best around 1000 prefixes gift. We can do not forget what form of IPv6 addressing is used to offer the routing infrastructure for this community. We don't forget tracrouting to the ::1 cope with of every prefix and recording the addresses discovered by way of the traceroutes. The intention is to show the addressing used to direction among prefixes, with out probing too deeply the internal shape of any prefix. Such a list of addresses must be dominated through addresses assigned to routers. The list of addresses became accrued in September 2007. A goal list of 866 prefixes changed into prepared primarily based at the IPv6 BGP table at HEAnet. Three specific source addresses had been used: one 6to4 address, one in a business ISP's PA area and one in HEAnet's PA area. We anticipate to peer slightly distinctive lists of addresses for every supply address, due to each variability in routes and supply address selection. For every supply address, a list of intermediate router addresses turned into produced using traceroute. The three special source addresses produced 1558, 1687 and 1698 addresses respectively

1.4 IE IPv6-Enabled Nameserver

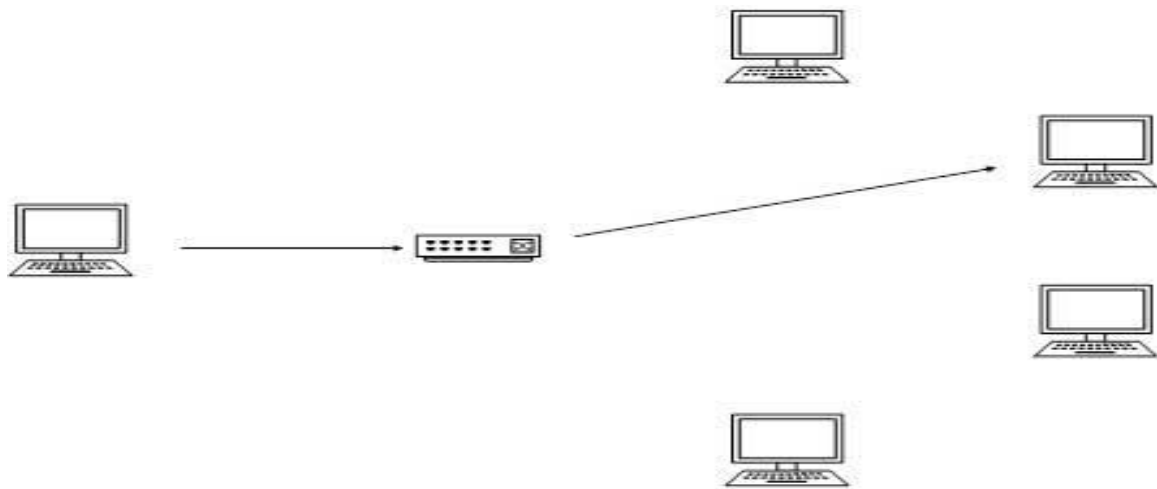
Activity is quite regular over the two months. It is crucial to note that for a DNS question to be logged, there is no want for a TCP handshake to complete, and so there may be no check for return routability. Thus, about zero.5% of queries come from 6one prefixes and a handful of requests come from unassigned (2000:1::1), ULA and documentation addresses. For comparison, Fig. 7 shows the corresponding results for ftp.Heanet.Ie. We expect a contrast between the consumer populations of these servers, because clients of reflect servers need to now not have tons in not unusual with recursive DNS servers. Indeed, when compared to ftp.Heanet.Ie, ns6.Iedr.Ie sees fewer requests from privacy, Teredo and ISATAP addresses. Even the proportion of 6to4 addresses is lower. The geographic distribution of the addresses also seems more even. We also see an increase in wordy and low addressing. This suggests that administrators shy away from transition mechanisms for recursive resolvers and opt for manually-assigned 2addresses.

2. Addressing models

In computer networking, addressing mode refers to the mechanism how we address a host on the network. IPv6 offers several types of modes by which a single host can be addressed, more than one host can be addressed at once or the host at closest distance can be addressed.

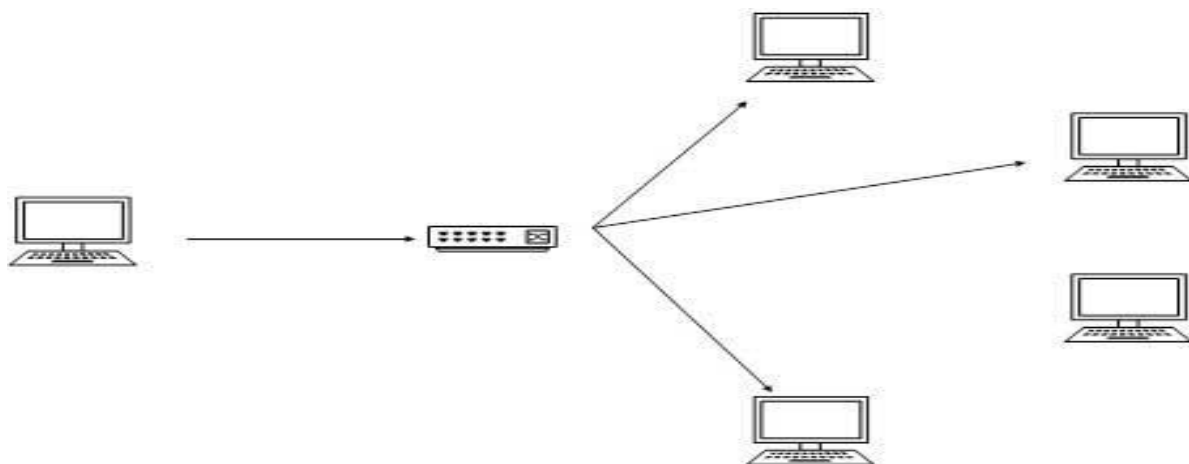
Unicast

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment. A network switch or router when receives a unicast IP packet, destined to single host, sends out to one of its outgoing interface which connects to that particular host.



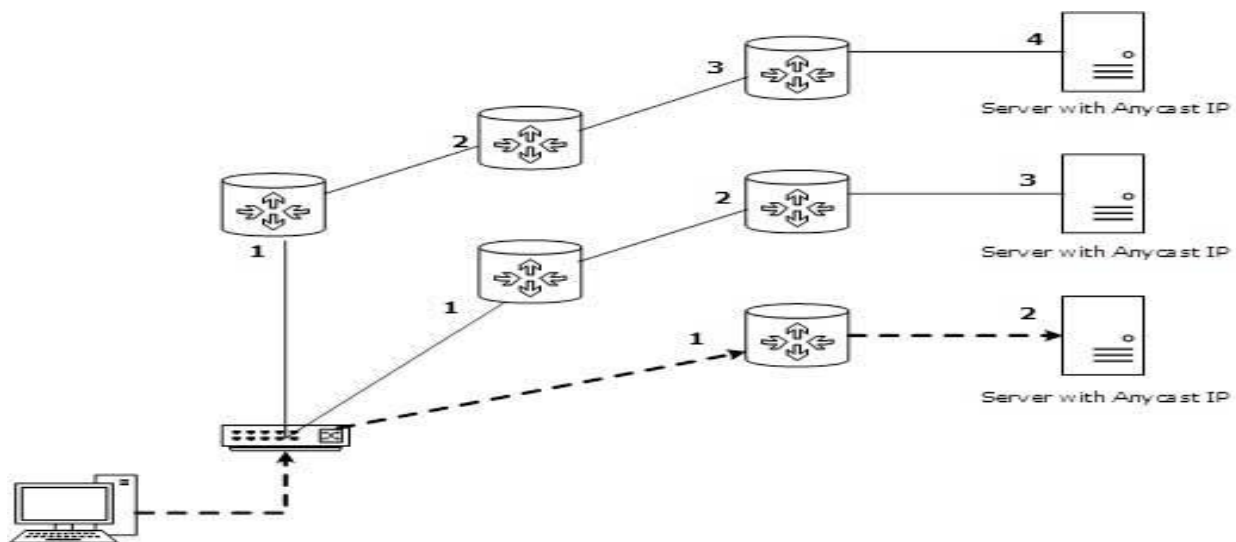
Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All hosts interested in that multicast information, need to join that multicast group first. All interfaces which have joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender, in terms of Routing cost.



Address Types

Hexadecimal Number System

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is positional number system which uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F symbol to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Part 2

School of Applied Computing – 711 hosts					
Hosts location	NetworkID/CIDR	First host	Last host	Mask	Broadcast
Open access 250 hosts	172.16.0.0/23	172.16.0.1	172.16.1.254	255.255.254.0	172.16.1.255
Lab 308 140 hosts	172.16.2.0/24	172.16.2.1	172.16.2.254	255.255.255.0	172.16.2.255
Lab 301 60 hosts	172.16.3.0/25	172.16.3.1	172.16.3.126	255.255.255.128	172.16.3.127
Lab 309 50 hosts	172.16.3.128/26	172.16.3.129	172.16.3.190	255.255.255.192	172.16.3.191
Lab 304 45 hosts	172.16.3.192/26	172.16.3.193	172.16.3.254	255.255.255.192	172.16.3.255
Lab 306 40 hosts	172.16.4.0/26	172.16.4.1	172.16.4.62	255.255.255.192	172.16.4.63
Lab 303 36 hosts	172.16.4.64/26	172.16.4.65	172.16.4.126	255.255.255.192	172.16.4.127
Lab 302 30 hosts	172.16.4.128/26	172.16.4.129	172.16.4.190	255.255.255.192	172.16.4.191
Test centre 22 hosts	172.16.4.192/27	172.16.4.193	172.16.4.222	255.255.255.224	172.16.4.223
Staff 20 hosts	172.16.4.224/27	172.16.4.225	172.16.4.254	255.255.255.224	172.16.4.255
Lab 310 18 hosts	172.16.5.0/27	172.16.5.1	172.16.5.30	255.255.255.224	172.16.5.31

School of Engineering – 406 hosts					
Host location	NetworkID/CIDR	First host	Last host	Mask	Broadcast
Lab 202 80 hosts	172.16.6.0/25	172.16.6.1	172.16.6.126	255.255.255.128	172.16.6.127
Lab 409 80 hosts	172.16.6.128/25	172.16.6.129	172.16.6.254	255.255.255.128	172.16.6.255
Lab 203 65 hosts	172.16.7.0/25	172.16.7.1	172.16.7.126	255.255.255.128	172.16.7.127
Lab 404 45 hosts	172.16.7.128/26	172.16.7.129	172.16.7.190	255.255.255.192	172.16.7.191
Lab 410 45 hosts	172.16.7.192/26	172.16.7.193	172.16.7.254	255.255.255.192	172.16.7.255
Lab 408 28 hosts	172.16.8.0/27	172.16.8.1	172.16.8.30	255.255.255.224	172.16.8.31
Lab 205 25 hosts	172.16.8.32/27	172.16.8.33	172.16.8.62	255.255.255.224	172.16.8.63
Lab 201 20 hosts	172.16.8.64/27	172.16.8.65	172.16.8.94	255.255.255.224	172.16.8.95
Staff 18 hosts	172.16.8.96/27	172.16.8.97	172.16.8.126	255.255.255.224	172.16.8.127

School of Automotive Engineering – 283 hosts					
Host location	NetworkID/CIDR	First host	Last host	Mask	Broadcast
Lab 301 50 hosts	172.16.9.0/26	172.16.9.1	172.16.9.62	255.255.255.192	172.16.9.63
Lab 206 48 hosts	172.16.9.64/26	172.16.9.65	172.16.9.126	255.255.255.192	172.16.9.127
Lab 101 40 hosts	172.16.9.128/26	172.16.9.129	172.16.9.190	255.255.255.192	172.16.9.191
Lab 205 40 hosts	172.16.9.192/26	172.16.9.193	172.16.9.254	255.255.255.192	172.16.9.255
Lab 103 35 hosts	172.16.10.0/26	172.16.10.1	172.16.10.62	255.255.255.192	172.16.10.63
Lab 102 25 hosts	172.16.10.64/27	172.16.10.65	172.16.10.94	255.255.255.224	172.16.10.95
Staff 25 hosts	172.16.10.96/27	172.16.10.97	172.16.10.126	255.255.255.224	172.16.10.127
Lab CAD 20 hosts	172.16.10.128/27	172.16.10.129	172.16.10.190	255.255.255.224	172.16.10.191

Server name	IPv6 address
MP	0:0:0:0:ffff:ac10:b01
DNS	0:0:0:0:ffff:ac10:c01
Email	0:0:0:0:ffff:ac10:d01
Finance	0:0:0:0:ffff:ac10:e01
Registry	0:0:0:0:ffff:ac10:f01
File server	0:0:0:0:ffff:ac10:1001
Print server	0:0:0:0:ffff:ac10:1101

Explanation and analysis

School of Applied Computing: 20 staff, lab301 – 60 pcs, Lab302 – 30 pcs, Lab303 – 36 pcs, Lab 304 – 45 pcs, Lab306 – 40 pcs, Lab308 – 140 pcs, Lab309 – 50 pcs and Lab310 – 18 pcs

1. Open access 250 hosts – in the first room with a subnet mask /23, computers had been released 510 due to the fact with subnet masks /24 the most number is 254. If you need to hook up with greater than 4 new computer systems will need to build a new community.
2. Lab 308 – 140 host. With subnet mask /25 the maximum number Hosts/Net is 126.
3. Lab 301 – 60 host. With a subnet mask /26, maximum number Hosts/Net is 62. If you need to attach greater new computers will need to build a new network.
4. From lab 309 to lab 302 subnet mask is /26. Maximum number Hosts/Net 62.
5. Test centre, Staff and Lab 310 subnet mask is /27 with maximum number on Hosts 30

School of Automotive Engineering: 25 staff, lab101 – 40 pcs, Lab102 – 25 pcs, Lab103 – 35 pcs, Lab205 – 40 pcs, Lab206 – 48 pcs, CAD lab – 20 pcs and Lab301 – 50 pcs

1. Lab 202, lab 409 and lab 203 subnet mask is /25 because maximum number Hosts/Net is 126.
2. Lab 404 and Lab 410 subnet mask is /26 maximum number Hosts/Net is 62.
3. The rest of the rooms have a subnet mask /27.

School of Engineering: 18 staff, lab201 – 20 pcs, Lab202 – 80 pcs, Lab203 – 65 pcs, Lab205 – 25 pcs, Lab404 – 45 pcs, Lab408 – 28 pcs, Lab409 – 80 pcs, Lab410 – 45 pcs

1. Lab 301, 206, 101, 205 and 103 subnet mask is /26, maximum number Hosts/Net is 62
2. The rest of the rooms have a subnet mask /27 with maximum number on Hosts 30.