Improving transition to IPv6-only via RFC8925 and IPv4 DNS Interventions

A case study in implementing an IPv6-only testbed which informs IPv4-only clients why internet access is unavailable

Tom Costello
Argonne National Laboratory (ANL)
tcostello@anl.gov

Nick Buraglio
Lawrence Berkeley National Laboratory (LBNL), Energy Sciences Network (ESnet)
buraglio@es.net

Andy Fleming
Argonne National Laboratory (ANL)
afleming@anl.gov

Ben Tasker
Argonne National Laboratory (ANL)
btasker@anl.gov

Brandon Siegel
Argonne National Laboratory (ANL)
bsiegel@anl.gov

***Abstract* – Nine years have passed since the American Registry for Internet Numbers exhausted its allocation of Internet Protocol version 4 (IPv4) addresses, and four years have passed since the United States Government mandated federal agencies to complete the transition to Internet Protocol version 6 (IPv6). Despite the IPv4 address shortage and IPv6 mandate, Federally Funded Research and Development Centers (FFRDCs) are still struggling to sunset IPv4. As demonstrated on SC23's SC23v6 wireless network, newer tooling such as RFC8925 allows clients to disable their IPv4 protocol stack while retaining legacy IP connectivity via the RFC6145 translation algorithm. However, SC23v6 wireless clients without RFC8925 support or a disabled IPv6 stack would continue to receive internet access via legacy IPv4. This paper introduces a method of using poisoned IPv4 Domain Name System (DNS) records to gracefully inform IPv4-only clients at SC24's SC24v6 wireless network about their inability to use the current version of internet protocol, with a goal of minimal impact to RFC8925 and dual-stack clients. When implemented as designed, this method may improve supportability and user experience of IPv6-only deployments at FFRDCs.**

***Keywords* - IPv6, Network Architecture, Network Protocol Migration, Network Traffic Engineering**

I. Introduction

Internet Protocol (IP) is the standard used to send traffic between computer networks worldwide. Internet Protocol version 4 (IPv4) was originally standardized in 1981, featuring a 32-bit address space [1]. By the early 1990's, it became clear that a new IP standard with larger address space would be necessary to avoid address exhaustion. The Internet Engineering Task Force (IETF) began accepting submissions for the next generation IP standard in 1993, leading to the first specification of Internet Protocol Version 6 (IPv6) in 1995 [2, 3]. Ratified as an IETF standard in 1998, IPv6 is now the current version of IP, featuring a 128-bit address space [4]. While the IPv4 standard allows for approximately 4.3 billion addresses, IPv6 allows for approximately 3.4×10^{38} addresses, effectively ending any address scarcity concerns.

Multiple interim solutions to the IPv4 addressing shortage also appeared in the early 1990s, such as Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) [5, 6]. Originally proposed as short-term to medium-term solutions, CIDR and NAT effectively allowed network operators to work around the IPv4 addressing shortage, in many cases deprioritizing the adoption of IPv6. By the late 2000s, explosive growth of smartphones and "Internet of Things" (IoT) device adoption resulted in a resurgence of interest in IPv6, culminating with World IPv6 Day on June 8, 2011 [7].

Running both IPv4 and IPv6 protocols on a network, a practice known as dual-stacking, has been a common deployment model for IPv6. However, dual-stacking does not address the IPv4 addressing shortage, and supporting two versions of IP can be challenging for IT support staff [31]. In 2011, IETF released two standards regarding NAT64 and DNS64, giving network operators a platform for running IPv6-only networks while maintaining reachability to IPv4 resources [8, 9]. Further improvements granting IPv6-only clients access to IPv4-only resources were achieved in 2013 with the introduction of the Customer-side Translator (CLAT) IETF standard [10]. With all these improvements and vendors such as Apple and Google rapidly adopting IETF's RFC8925 "DHCPv4 option 108" capability [11] in their respective operating systems, it is now possible to deploy IPv6-only networks to large campuses with seamless access to IPv4 resources [12] while also

979-8-3503-5554-3/24/$31.00 ©2024 IEEE
DOI 10.1109/SCW63240.2024.00112

allowing legacy IP clients to migrate at the pace of their natural life cycle.

II. IPv6 at Argonne National Laboratory

The U.S. Department of Energy's Argonne National Laboratory (Argonne) is a Federally Funded Research and Development Center (FFRDC) located in Lemont, Illinois. From the AVIDAC computer installed in 1953 to the Aurora supercomputer installed 70 years later, Argonne is no stranger to technology modernization and network protocol migrations [13]. Argonne is required to follow U.S. Office of Management and Budget (OMB) memorandums, including M-21-07's requirements to complete the transition to IPv6 [14].

Although Argonne has been the recipient of five legacy /16 IPv4 allocations (over 300,000 usable addresses), issues related to IPv4 address exhaustion are common. Many wireless networks were originally provisioned with a single /24 address space (around 250 usable addresses), which was plentiful when employees were only connecting their desktop and laptop computers. Now that employees are connecting their smartphones, wearables, and other IoT devices, it is not uncommon for certain Argonne divisions to exhaust their IPv4 addresses allocated to authenticated wireless networks. While expanding the IPv4 address pools on these networks with CIDR is possible, it requires a considerable amount of effort to change firewall rules and device configurations. NAT is also possible to resolve the IPv4 address scarcity but is avoided at Argonne on Internet-accessible networks due to the additional troubleshooting complexity and requirement of OMB memorandum M-21-31 to log every NAT translation [15].

Having achieved compliance with previous OMB memorandums on IPv6, Argonne intends on achieving M-21-07's IPv6-only requirements. Additionally, the US Federal Acquisition Rules (FAR) document 11.002 has stated "Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005)." [16]. Due to these FAR and OMB policies, researchers need to keep IPv6 in mind when performing data-intensive science at FFRDCs.

A. Argonne IPv6 Timeline

A Department of Energy Office of Science Laboratory, Argonne has connections into multiple research and education internetworks, with the highest throughput connectivity currently provided by Energy Science Network (ESnet). As the first recipient of production IPv6 address space from the American Registry for Internet Numbers in 1999, ESnet has made IPv6 available in production for Argonne since 2002 [17]. It was not until 2008 that Argonne received its own provider-independent IPv6 allocation, a /48 prefix that was quickly utilized to achieve the IPv6 requirements of OMB's September 28 2010 "Transition to IPv6" memo [18].

After the release of OMB's M-21-07 memo in 2020, Argonne began an engagement with a contractor specializing in IPv6 transition to assist with creating a plan for IPv6-only networks campus-wide. One of the initial findings was that the /48 prefix address allocation was too small, and a /32 prefix should be acquired. A /48 prefix contains around 64,000 /64 prefixes, and a /32 prefix contains around 64,000 /48 prefixes [27]. While the approximately 1.2×10^{24} addresses in a /48 would be sufficient to avoid address exhaustion, the minimum prefix length in the IPv6 internet's default-free zone is /48, and Argonne wanted at least one more provider-independent prefix to achieve a ScienceDMZ peering configuration similar to that of their IPv4 architecture. The additional /32 prefix was assigned to Argonne in October 2022 and announced to ESnet on new 400G peerings shortly afterwards [19]. Argonne is in the process of replacing its 40G enterprise edge firewall with a 100G next-generation firewall. Deploying the new /32 prefix only onto the new firewall platform resulted in smoother validation of network architecture changes. Figure 1 illustrates recent improvements to the Argonne internet edge, all of which are dual-stacked.

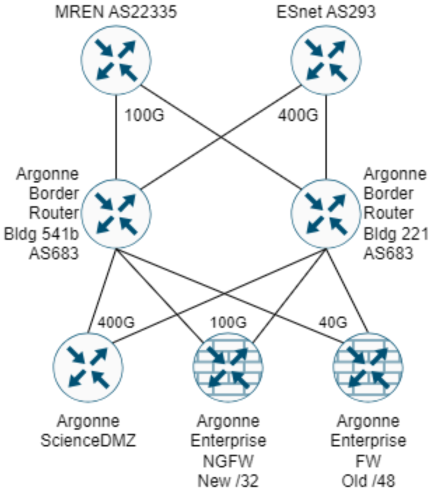


Fig. 1. Argonne IPv6 Internet Edge

B. Immediate needs for IPv6 at ANL

Although compliance with the goals written in OMB's M-21-07 IPv6 memorandum is a large motivator for completing the transition to IPv6 at Argonne, there are many other motivators for accelerating the decommissioning of IPv4 wherever possible on and off campus. The following three use-cases were specifically kept in mind when implementing the IPv6-only testbed described in section 4:

- Data-intensive science involving IoT devices, especially projects located off-campus such as Waggle and Floto. While neither projects are directly using Argonne's IPv6 resources today, the ability for direct end-to-end connectivity over networks which have implemented Carrier-Grade NAT for IPv4 makes IPv6 highly desirable [20, 21]

- Workshops and offsite meetings where IPv4 NAT results in an entire location getting blocked due to a single user entering the incorrect username and password too many times. This is particularly impactful to Argonne Leadership Computing Facility, where many students will authenticate to a single login node for the first time during their training courses. End-to-end addressing in IPv6 does not suffer from this problem.
- Environments where many computer resources are attempting to download a container from services such as Docker Hub. When behind an IPv4 proxy or NAT, all nodes will appear to the service as a single source IP, often leading to rate limits [22]. When using IPv6, each node uses its own IP address to access the service, avoiding any per-IP rate limits.

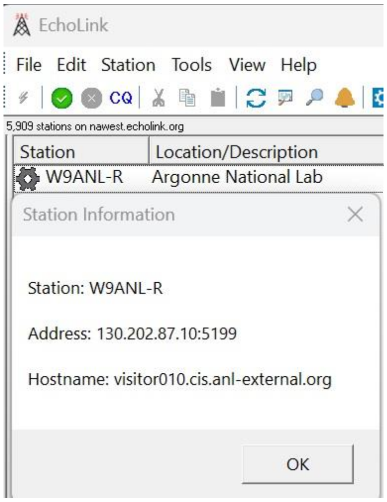
III. IPv6 at SCinet

Established as the International Conference for High Performance Computing, Networking, Storage and Analysis (aka SC Conference) in 1991, SCinet is a global collaboration of high-performance networking experts who provide a platform that connects attendees and exhibitors to the world [23]. Every year at the SC Conference, the SCinet creed of "One year to design, one month to build, one week to operate, and one day to tear down" is practiced by these volunteers [24]. As early as 2003, SCinet was embracing IPv6 on the show floor production network [25], and 20 years later SCinet made IPv6-mostly WiFi connectivity available at SC23 [12].

A. Immediate needs for IPv6 at SCinet

The SCinet SC23 IPv6 project has largely been considered to have exceeded expectations and was an excellent learning opportunity for all volunteers, however SCinet still has a large amount of IPv6 work to accomplish at SC24. DHCPv4 option 108 (commonly referred to as RFC8925, or IPv6-mostly) was utilized to disable IPv4 on clients which supported it, but no efforts to prevent IPv4-only clients from joining the SC23v6 WiFi Service Set Identifier (SSID) were made. While being able to support IPv4-only, dual-stack and IPv6-only clients on the same WiFi SSID is certainly desirable in many networks (commonly referred to as "IPv6-mostly"), it may also give a false impression to users that their IPv4-only device is successfully working in an IPv6-only environment. With many technology decision makers at FFRDCs frequenting the SC Conference show floor, SCinet wishes to provide an experience fully in compliance with the OMB's M-21-07 IPv6-only guidance, allowing these FFRDC leaders to identify room for IPv6-only improvement at their home institutions.

An example of the inadvertent IPv4 usage on SC23's IPv6-mostly WiFi would be the Argonne Amateur Radio Club's Special Event Station using Echolink software from the SC23 show floor. A SCinet volunteer successfully used a Windows 10 dual-stack host connected into the SC23v6 WiFi SSID to remotely operate a VHF amateur radio at Argonne's main campus. Echolink for Windows uses IPv4 literals to establish this connectivity instead of DNS per Figure 2. While the IPv4-only traffic worked well for the SCinet volunteer, their laptop was actively being counted towards the SC23v6 usage statistics, despite solely connecting into that SSID for an IPv4-only service [26]. For SC24, SCinet's IPv6 operational subject matter experts would like to have an accurate IPv6-only client count for future research papers.



Station: W9ANL-R

Address: 130.202.87.10:5199

Hostname: visitor010.cis.anl-external.org

Fig. 2. IPv4 literals to Argonne Amateur Radio Club present in the Echolink client application

IV. Motivation and Implementation

At both Argonne and SCinet, two of the largest hurdles when supporting IPv6-only deployments have been user experience and troubleshooting. Should a user's IPv4-only device connect into an IPv6-only WiFi network without any operational IPv4 internet access, the user may need to spend a significant amount of time determining why internet access is unavailable. For users outside of the information technology field, this may include calls to helpdesks and sizable loss of productivity while determining lack of IPv4 connectivity is the culprit. For users inside of the information technology field, this may include misguided investigations into the client operating system's network interface configuration, port-security violations, and upstream connectivity verification before determining lack of IPv4 connectivity is the culprit.

Starting at SC23, SCinet ran three WiFi SSIDs on the production show floor network: one general purpose SSID with no passwords or restrictions (e.g., "SC23"); one SSID which uses eduroam 802.1x authentication with WiFi Protected Access (WPA); and one SSID with RFC8925 support, with no passwords or restrictions (e.g., "SC23v6") [12]. For SC24, there is a strong desire to prevent IPv4-only clients from staying on the SC24v6 SSID in an effort to produce the most accurate IPv6-only client count and to allow any SC Conference attendee to experience how their devices operate on a fully OMB M-21-07 IPv6-only compliant deployment. It would be optimal for IPv4-only clients that join the SC24v6 SSID to receive a notification about their device's inability to support the current internet protocol standard and encourage them to visit the SCinet helpdesk for more information. This would be very similar to the user experience when connecting onto an airplane's in-flight entertainment WiFi, with a goal of having no noticeable impact on dual-stack or IPv6-only clients whose base operating systems comply with RFC6724 for their source address selection, noting that there may be individual applications which have their own internal address selection processes requiring further investigation.

Argonne also has three WiFi SSIDs throughout the campus: one general purpose SSID with 802.1x authentication and WPA for internal users (e.g., "Argonne-Auth"); one eduroam SSID configured in a near-identical manner to SCinet's eduroam deployment; and one SSID for guests (e.g., "Argonne-Guest") with no passwords or restrictions, but with a captive portal registration system to obtain Internet access. Other SSIDs are used in limited portions of the campus, which makes adding an additional campus-wide SSID for IPv6-only not possible as of this writing due to wireless LAN controller limitations.

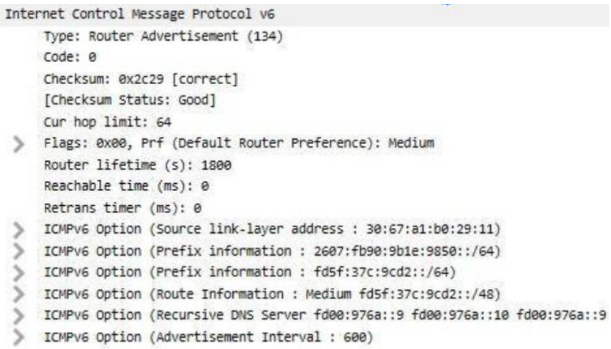
Due to the SSID count constraint, Argonne utilized their Authentication, Authorization and Accounting (AAA) server to place devices which should be complying with the OMB M-21-07 IPv6-only guidance into RFC8925-enabled networks within the Argonne-Auth SSID. Service accounts will be created and tightly controlled for devices which must retain IPv4-only support on Argonne-Auth. It would be optimal for IPv4-only clients that join Argonne-Auth without the IPv4-enabling service account to receive a notification about their device's inability to support the current internet protocol standard, and to contact Argonne ServiceDesk for more information.

A. Initial Testbed Buildout

The following criteria for a testbed was established after an IPv6 discussion at SCinet's SC24 Sprint event in April 2024, with input from the Argonne Business Information Systems Network Team to better meet IPv6 use-cases at both institutions:

- Must use a 5G mobile network internet uplink to ensure the testbed can be easily utilized at Argonne and SCinet SC24 August Planning Meeting in St, Louis, MO.
- Must demonstrate ability to redirect IPv4-only clients into a captive-portal style URL of test-ipv6.com or ip6.me, gracefully informing users that their device's lack of IPv6 support is the reason for no internet connectivity.
- Redirection of IPv4-only traffic must not interfere with IPv6-only or dual-stack client traffic.
- Full RFC8925 (DHCPv4 option 108) and RFC6146 (NAT64) support.

Upon receipt of the 5G mobile Internet gateway, it was observed to be sending a Recursive DNS Server (RDNSS) value of fd00:976a::9 and fd00:976a::10 in its Router Advertisements (RAs) per Figure 3. There were no options available to manipulate the RA on this 5G mobile internet gateway, and these Unique Local Addresses (ULA) of fd00:976a::9 and fd00:976a::10 were not alive. Every reboot, the device would obtain a different /64 prefix of IPv6 Global Unicast Addresses (GUA), with no capability to receive a larger prefix from the mobile network operator. To work around these RA limitations without needing to deploy Network Prefix Translation, a managed switch was deployed capable of sending RAs in the fd00:976a::/64 prefix with low priority. A Raspberry Pi server running BIND9 DNS64 services was deployed with an address of fd00:976a::9, allowing any clients receiving a SLAAC GUA from the 5G mobile internet gateway to perform DNS queries.



```
Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x2c29 [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
>   Flags: 0x00, Prf (Default Router Preference): Medium
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
>   ICMPv6 Option (Source link-layer address : 30:67:a1:b0:29:11)
>   ICMPv6 Option (Prefix information : 2607:fb90:9b1e:9850::/64)
>   ICMPv6 Option (Prefix information : fd5f:37c:9cd2::/64)
>   ICMPv6 Option (Route Information : Medium fd5f:37c:9cd2::/48)
>   ICMPv6 Option (Recursive DNS Server fd00:976a::9 fd00:976a::10 fd00:976a::9
>   ICMPv6 Option (Advertisement Interval : 600)
```

Fig. 3. RA from 5G mobile internet gateway with ULA RDNSS

NAT64 using the well-known prefix of 64:ff9b::/96 was functional on the 5G mobile Internet gateway, but the built-in DHCPv4 server was not capable of defining option 108, and could not be disabled. To work around these DHCPv4 limitations, DHCPv4 snooping was configured on the managed switch to block the 5G mobile Internet gateway's DHCPv4 pool, and a Raspberry Pi DHCP server was utilized to support DHCPv4 option 108 as a means of activating CLAT per RFC8925.

Originally, the testbed called for utilizing the captive-portal redirect capabilities of a wireless LAN controller to perform the redirection of IPv4-only client traffic into test-ipv6.com. Upon further testing with both controller-based and controllerless WiFi solutions, it was determined that using an additional DNS64 server which produced valid answers for IPv6 AAAA records while returning poisoned IPv4 A record answers would be a more optimal solution. Since AAAA record answers will be preferred by modern operating systems with IPv6 connectivity, the only clients relying on the A records should be clients with IPv4-only connectivity. With the DHCPv4 scope modified to have the DNS resolver pointed to the poisoned Raspberry Pi DNS64 server, figure 4 became the topology used through the testbed's deployment in July and August 2024.

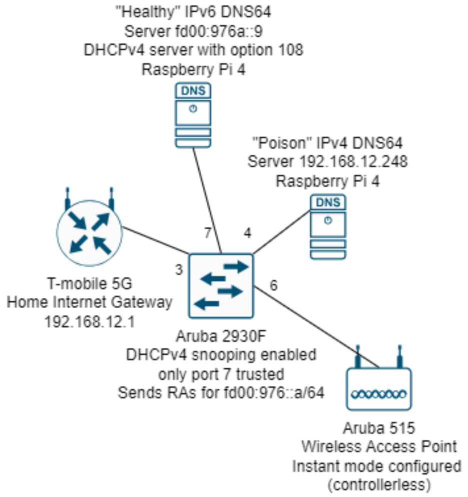
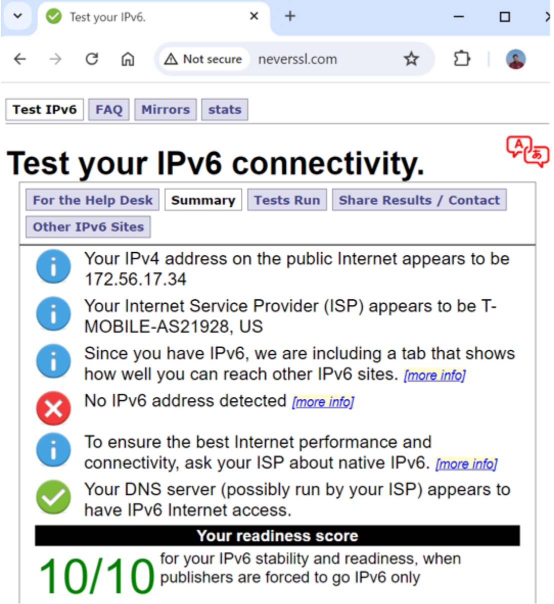


Fig. 4. Testbed Topology

V. Testbed Results

Initially, the poisoned IPv4 DNS64 server was redirecting all DNS A record queries from a Windows 10 client with IPv6 disabled into test-ipv6.com's IPv4 address with success. However, it was observed that even though the client had no GUA IPv6 address and test-ipv6.com reported no IPv6 address present, the final testing score shown in Figure 5 was erroneously reported as 10/10. To prevent misleading results from being displayed on client devices, the poisoned DNS64 server configuration was changed to redirect all A record queries towards ip6.me, where a more straightforward message about the device only supporting IPv4 is displayed.



Test your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 172.56.17.34

Your Internet Service Provider (ISP) appears to be T-MOBILE-AS21928, US

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [more info]

No IPv6 address detected [more info]

To ensure the best Internet performance and connectivity, ask your ISP about native IPv6. [more info]

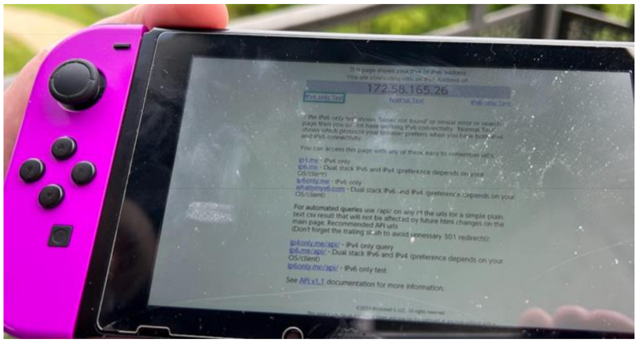
Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Fig. 5. Erroneous test-ipv6.com score via poisoned DNS on IPv4-only client

Popular consumer electronics devices such as the Nintendo Switch continue to only support legacy IPv4 connectivity. When a Nintendo Switch was connected into the testbed, its operating system reported no internet connectivity, and displayed the ip6.me redirection as designed per Figure 6. However, if the end user simply changed the DNS resolver to a known-good server, access to the IPv4 internet would be granted.



This page shows your IPv4 or IPv6 address
You are connecting with an IPv4 Address of
172.58.165.26

If the IPv6 only test shows "Server not found" or similar error or search page then you do not have working IPv6 connectivity. "Normal Test" shows which protocol your browser prefers when you have both IPv4 and IPv6 connectivity.

You can access this page with any of these easy to remember url's:

ip4.me - IPv4 only
ip6.me - Dual stack IPv6 and IPv4 (preference depends on your OS/client)
ip6only.me - IPv6 only
whatismyv6.com - Dual stack IPv6 and IPv4 (preference depends on your OS/client)

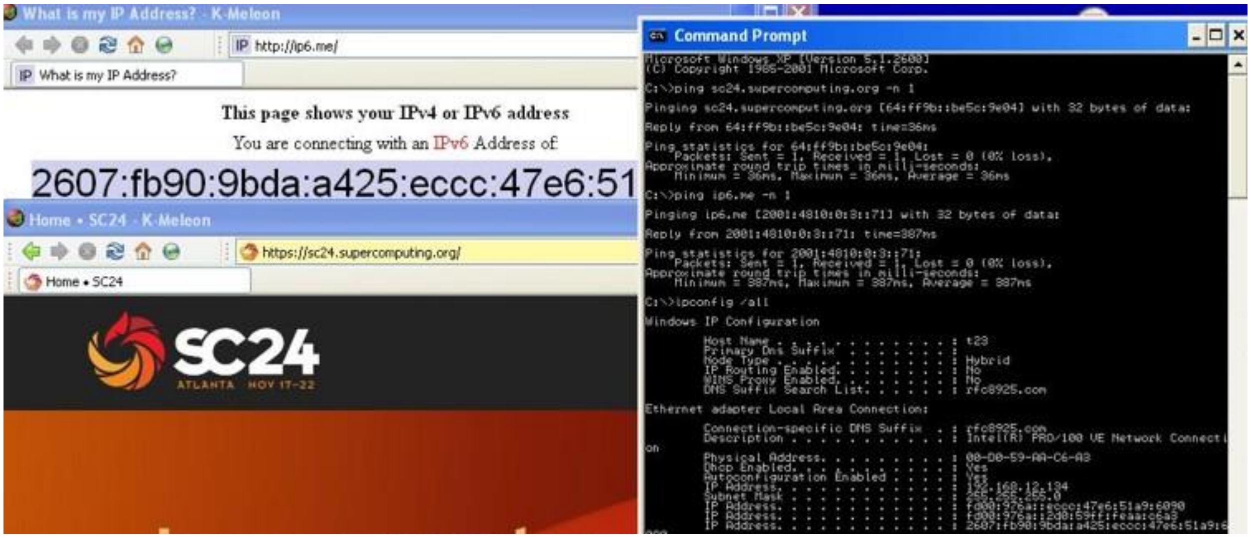
For automated queries use /api/ on any of the urls for a simple plain text csv result that will not be affected by future html changes on the main page. Recommended API urls (Dont forget the trailing slash to avoid unnessary 301 redirects):

ip4only.me/api/ - IPv4 only query
ip6.me/api/ - Dual stack IPv6 and IPv4 (preference depends on your OS/client)
ip6only.me/api/ - IPv6 only test

See API v1.1 documentation for more information.

Fig. 6. IPv4-only Nintendo Switch receiving the IPv4 DNS intervention

A wide variety of current devices supporting both RFC8925 and dual-stack connectivity were tested with successful results. Starting with Microsoft Windows Vista, IPv6 dual-stack is enabled by default, however some versions may prefer IPv4 DNS resolvers. It was observed that Windows XP, released in 2001 without support for IPv6 DNS resolvers, can work well in the testbed thanks to the poisoned IPv4 DNS64 server continuing to provide valid IPv6 AAAA DNS query answers. Figure 7 illustrates this long obsolete operating system successfully using a web browser to access IPv4-only sc24.supercomputing.org via IPv6 using NAT64 and a DNS64 server which accepts IPv4 clients.



This page shows your IPv4 or IPv6 address

You are connecting with an IPv6 Address of

2607:fb90:9bda:a425:eccc:47e6:51

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ping sc24.supercomputing.org -n 1

Pinging sc24.supercomputing.org [64:ff9b::be5c:9e04] with 32 bytes of data:

Reply from 64:ff9b::be5c:9e04: time=36ms

Ping statistics for 64:ff9b::be5c:9e04:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 36ms, Average = 36ms

C:\>ping ip6.me -n 1

Pinging ip6.me [2001:4810:0:3::71] with 32 bytes of data:

Reply from 2001:4810:0:3::71: time=387ms

Ping statistics for 2001:4810:0:3::71:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 387ms, Maximum = 387ms, Average = 387ms

C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : t23
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : rfc8925.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : rfc8925.com
        Description . . . . . . . . . . . : Intel(R) PRO/100 VE Network Connecti
on
        Physical Address. . . . . . . . . : 00-D0-59-AA-C6-A3
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.12.134
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : fd00:976a::eccc:47e6:51a9:6090
        IP Address. . . . . . . . . . . . : fd00:976a::2d0:59ff:feaa:c6a3
        IP Address. . . . . . . . . . . . : 2607:fb90:9bda:a425:eccc:47e6:51a9:6
```

Fig. 7. Windows XP using NAT64/DNS64 via IPv4 DNS resolver

VI. Lessons Learned

The testbed largely accomplished the goals which both Argonne and SCinet were hoping to achieve, but there are several open items which must be considered before such an implementation is used in production. Identifying and fixing the test-ipv6.com erroneous results shown in Figure 5 is highly desired by the SC24 SCinet DevOps team. Being able to modify messages on the testing results to indicate next steps for troubleshooting will make the SC24v6 show floor experience far more user friendly. The most desired change is modifying the testing logic so that only RFC8925 clients may receive a 10/10 score. As of this writing, properly configured dual-stack clients will also receive a 10/10 score under default test-ipv6.com testing logic. Better illustrating differences between dual-stack and RFC8925 clients in SC24's test-ipv6.com mirror results would further enhance awareness into operating systems which are not yet utilizing DHCPv4 option 108.

While it is very tempting to implement an access control list further blocking IPv4 internet access (or intentionally breaking IPv4 NAT in the testbed to achieve similar results), additional restrictions to IPv4 internet may result in certain dual-stack clients experiencing Virtual Private Network (VPN) split-tunneling issues. Figure 8 illustrates what may happen when certain VPN clients featuring a split-tunneling configuration using IPv4 literals attempt to reach an IPv4-only Video Teleconference (VTC) provider. Multiple issues were reported with VPN clients on the testbed network, which is in alignment with results from other IPv6-only and RFC8925 deployments [12,32].

This behavior where a testbed client cannot access the IPv4-only VTC service due to a VPN split-tunnel configuration with IPv4 literals is currently present on Argonne's production VPN deployment. While Argonne network operations is aware of the problem and has a solution drafted, it has not yet been implemented due to higher prioritization of OMB M-22-09 memorandum related requests [28] and the possibility of said IPv4-only VTC service supporting IPv6 soon. Even if all Argonne's remote client devices began supporting RFC8925 and the IPv4-only VTC service began supporting IPv6, this still would be an issue for many users at Argonne's Advanced Photon Source (APS) Collaborative Access Teams (CATs). These users typically bring highly specialized computers from various private industry and academic research facilities onto APS beamlines [13], often using IPv4-only VPN into their home institution's networks from Argonne. Since some of these APS CATs use government furnished equipment which is now required to be IPv6-only, while others use private industry or academic institution furnished equipment without any IPv6 requirements, Argonne does not intend on further restricting IPv4 Internet access on environments such as the APS CATs for the foreseeable future.

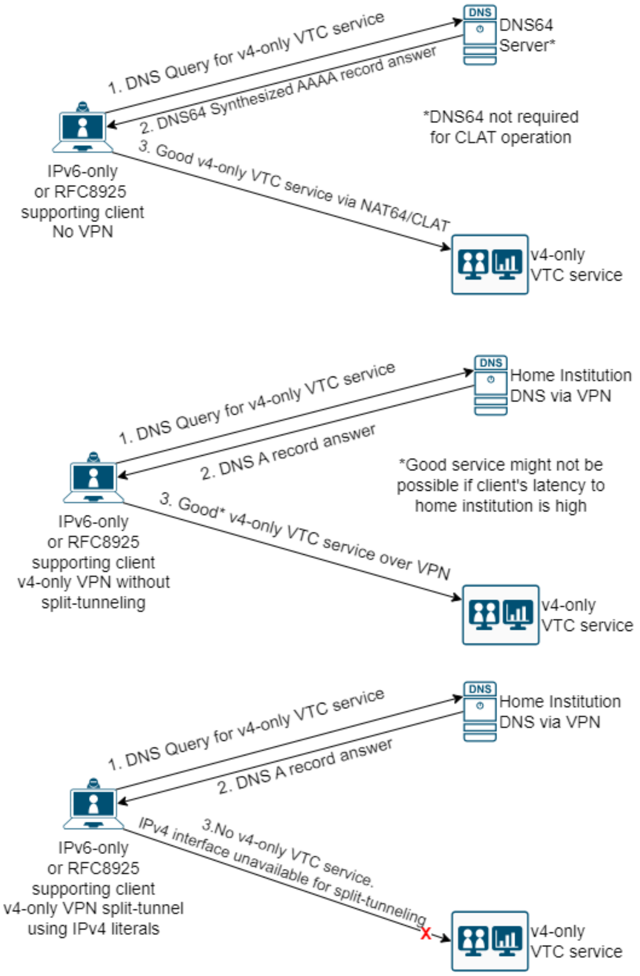
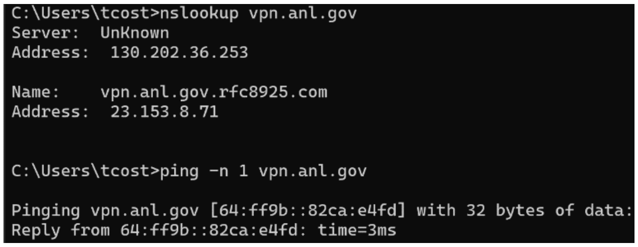


Fig. 8. VPN client behavior if IPv4 internet access is further restricted

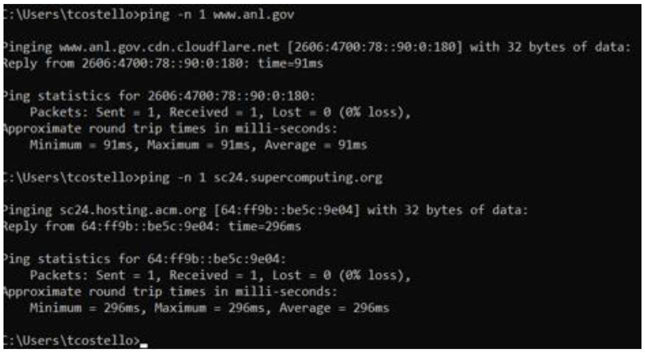
The poisoned DNS A records worked as designed to prevent IPv4-only hosts from accessing the internet and instead getting the DNS-based intervention towards an IPv6 testing website. To facilitate the DNS A record poisoning, dnsmasq was used with a two line configuration: one line of "address=/#/23.153.8.71" to return any A record query with an answer of ip6.me's IPv4 address, and another line of "server=192.168.12.251" to forward all other requests (including AAAA queries) to the testbed's healthy DNS64 server. Since dnsmasq has no logic to determine if a real-world A record exists, it will answer A record queries even for non-existent fully qualified domain names (FQDNs). Figure 9 illustrates how this may be problematic for some dual-stack hosts on operating systems which use the IPv4 DNS resolver. The client's nslookup results indicate a domain suffix search list was used to obtain a non-existant A record, but the ping results successfully obtain the desired AAAA record.



```
C:\Users\tcost>nslookup vpn.anl.gov
Server:  UnKnown
Address:  130.202.36.253

Name:    vpn.anl.gov.rfc8925.com
Address:  23.153.8.71


C:\Users\tcost>ping -n 1 vpn.anl.gov

Pinging vpn.anl.gov [64:ff9b::82ca:e4fd] with 32 bytes of data:
Reply from 64:ff9b::82ca:e4fd: time=3ms
```

Fig. 9. Non-existent A record received by nslookup, valid AAAA record received by ping

Fortunately, most Linux operating systems that are not yet supporting RFC8925 along with Windows 10 will prefer the IPv6 RDNSS resolver received via RA instead of the DHCPv4 provided DNS resolver. In these situations, all DNS queries go towards the healthy DNS64 server directly, and the poisoned IPv4 DNS server is not utilized. Unless an application is doing DNS resolution to a specific DNS server outside of the operating system's DNS client implementation, the poisoned DNS A records will not impact these systems as demonstrated in Figure 10. It was observed that some versions of Windows 11 will prefer the IPv4 DNS server received via DHCPv4 over the IPv6 DNS server received via RDNSS. Once a version of Windows 11 with RFC8925 support is released, it is presumed that only the IPv6 DNS server received via RDNSS will be used.



```
:\Users\tcostello>ping -n 1 www.anl.gov

inging www.anl.gov.cdn.cloudflare.net [2606:4700:78::90:0:180] with 32 bytes of data:
eply from 2606:4700:78::90:0:180: time=91ms

ing statistics for 2606:4700:78::90:0:180:
   Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 91ms, Maximum = 91ms, Average = 91ms

:\Users\tcostello>ping -n 1 sc24.supercomputing.org

inging sc24.hosting.acm.org [64:ff9b::be5c:9e04] with 32 bytes of data:
eply from 64:ff9b::be5c:9e04: time=296ms

ing statistics for 64:ff9b::be5c:9e04:
   Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 296ms, Maximum = 296ms, Average = 296ms

:\Users\tcostello>_
```

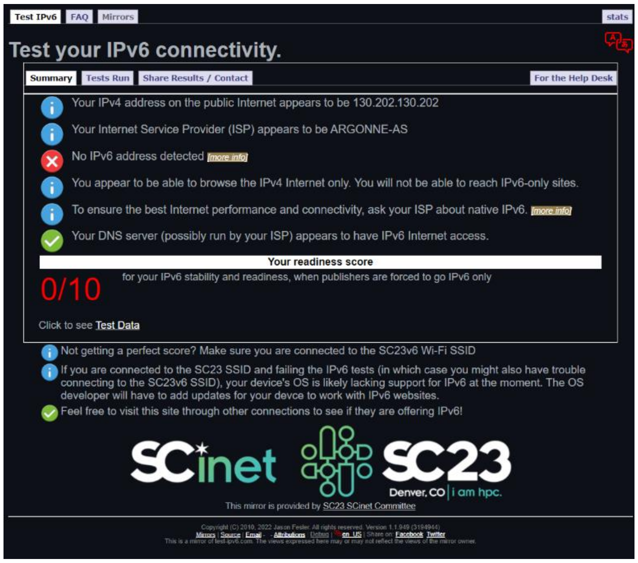
Fig. 10. Healthy native DNS AAAA and synthesized DNS64 AAAA records received on a Windows 10 client

VII. Conclusion

The testbed largely accomplished the initial goals of gracefully informing IPv4-only clients about their inability to use the current version of internet protocol, with no impact to clients supporting RFC8925 or only their IPv6 stack enabled. Dual-stack clients using the IPv6 RDNSS resolver were not impacted by the poisoned DNS A records. Certain operating systems or applications using the DNS resolver provided by DHCPv4 may experience problems related to poisoned A record answers for non-existent FQDNs. While the risks associated with these poisoned A records must be understood and accepted prior to production deployment, the upcoming Windows 11 RFC8925 client support and Windows 10 end-of-life should greatly reduce the poisoned A record concerns at Argonne and SCinet.

The SCinet SC24 IPv6 operational subject matter experts look forward to attempting this method of implementing RFC8925 with IPv4 DNS interventions on the SC24v6 wireless network. Further improvements such as replacing the dnsmasq configuration for poisoning DNS A records with a BIND9 Response Policy Zone may better mitigate the poisoned A record answers for non-existent FQDNs issue, but at the cost of additional configuration complexity. The SCinet SC24 DevOps Team intends on further enhancing their mirror of test-ipv6.com to provide more useful information for clients unable to obtain a perfect IPv6 readiness score, along with an Ansible playbook to remove the IPv4 DNS interventions should major issues be reported.

Argonne intends on implementing a pilot network configured in a near identical manner to the SC24v6 wireless network sometime after SC24 is completed, and Windows 11 RFC8925 support is available. As shown in Figure 11, Argonne VPN users scored a 0/10 when connecting via the SC23v6 wireless network due to most traffic outside of approved VTC platforms not getting split-tunneled. While a large amount of work remains to better support IPv6 on the Argonne VPN, results from the SC24v6 wireless network will most certainly assist with the transition away from legacy IP, and likely at other FFRDCs as well.



Test your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 130.202.130.202

Your Internet Service Provider (ISP) appears to be ARGONNE-AS

No IPv6 address detected

You appear to be able to browse the IPv4 Internet only. You will not be able to reach IPv6-only sites.

To ensure the best Internet performance and connectivity, ask your ISP about native IPv6.

Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

0/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see Test Data

Not getting a perfect score? Make sure you are connected to the SC23v6 Wi-Fi SSID

If you are connected to the SC23 SSID and failing the IPv6 tests (in which case you might also have trouble connecting to the SC23v6 SSID), your device's OS is likely lacking support for IPv6 at the moment. The OS developer will have to add updates for your devce to work with IPv6 websites.

Feel free to visit this site through other connections to see if they are offering IPv6!

This mirror is provided by SC23 SCinet Committee

Copyright (C) 2010, 2022 Jason Fesler. All rights reserved. Version 1.1.949 (3194944)
Mirrors | Source | Email - Attributions | Debug | en_US | Share on: Facebook Twitter
This is a mirror of test-ipv6.com. The views expressed here may or may not reflect the views of the mirror owner.

Fig. 11. SC23's test-ipv6.com mirror with 0/10 score over VPN

Completing the transition to IPv6 continues to be a challenge for Argonne and federal agencies. OMB mandates such as the IPv6 and Zerotrust memorandums along with Cybersecurity and Infrastructure Security Agency Binding Operational Directives compliance has made supporting federal information systems quite challenging. Even with all of these challenges, the October 2025 Windows 10 end-of-life deadline provides a rare opportunity to leverage the Windows 11 refresh cycle as a catalyst for sunsetting IPv4. End-users and ServiceDesk staff will require additional training to support the Windows 11 refresh regardless of whether IPv4 or IPv6 is used on these client devices. This training occasion can be used to reiterate why sunsetting IPv4 is important and that disabling IPv6 should not be a primary troubleshooting step during routine ServiceDesk calls. SC23v6's successful deployment of RFC8925 to hundreds of devices on the SC23 show floor has proved that this transition method is viable at scale. We look forward to the deployment of SC24v6's deployment with IPv4 DNS interventions as the results may further assist the public sector's transition away from IPv4.

Acknowledgment

The authors would like to thank the volunteers of SC24 SCinet, the Argonne Business Information Systems Directorate, the Energy Science Network Coordinators Committee and Sandia National Laboratory's IPv6 transition team for their input on the IPv6 deployments utilized to create this paper.

Argonne National Laboratory's work was supported by the U.S. Department of Energy, Office of Science, under contract DE-AC02-06CH11357.

ESnet is stewarded by Lawrence Berkeley National Laboratory (Berkeley Lab), which is operated by the University of California for the US Department of Energy under contract DE-AC02-05CH11231.

References

[1] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, https://www.rfc-editor.org/info/rfc791.

[2] Bradner, S. and A. Mankin, "IP: Next Generation (IPng) White Paper Solicitation", RFC 1550, DOI 10.17487/RFC1550, December 1993, https://www.rfc-editor.org/info/rfc1550.

[3] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 1883, DOI 10.17487/RFC1883, December 1995, https://www.rfc-editor.org/info/rfc1883.

[4] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, https://www.rfc-editor.org/info/rfc2460.

[5] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, DOI 10.17487/RFC1519, September 1993, https://www.rfc-editor.org/info/rfc1519.

[6] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, https://www.rfc-editor.org/info/rfc1631.

[7] "World IPv6 Launch." https://www.worldipv6launch.org/.

[8] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, https://www.rfc-editor.org/info/rfc6146.

[9] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, https://www.rfc-editor.org/info/rfc6147.

[10] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, https://www.rfc-editor.org/info/rfc6877.

[11] Colitti, L., Linkova, J., Richardson, M., and T. Mrugalski, "IPv6-Only Preferred Option for DHCPv4", RFC 8925, DOI 10.17487/RFC8925, October 2020, https://www.rfc-editor.org/info/rfc8925.

[12] K. Robinson, J. Zurawski, and T. Costello, "Designing, Constructing, and Operating an IPv6 Network at SC23: A case study in implementing the IPv6 protocol on a heterogenous network that supports the SC23 conference," OSTI OAI (U.S. Department of Energy Office of Scientific and Technical Information), July 2024, doi: https://doi.org/10.1145/3626203.3670531.

[13] J. M. Holl, R. G. Hewlett, and Ruth Roy Harris, Argonne National Laboratory, 1946-96. Urbana: University Of Illinois Press, 1997. p.123, 473.

[14] "Completing the Transition to Internet Protocol Version 6", https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf.

[15] Young, S., "M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents", August 2021, https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

[16] "11.002 Policy", May 2024, https://www.acquisition.gov/far/11.002.

[17] "ESnet IPv6 History", https://www.es.net/engineering-services/ipv6-network/ESnet-ipv6-history/.

[18] Kundra, V., "Transition to IPv6", 2010, September 28, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf.

[19] "ESnet Turns on 400G Circuits to Four DOE National Labs, Supercharging Multi-Site Scientific Research", 2023, October 25, https://www.es.net/news-and-publications/ESnet-news/2023/ESnet-turns-on-400g-circuits-to-four-doe-national-labs/.

[20] C. E. Catlett, P. H. Beckman, R. Sankaran, and K. K. Galvin, "Array of things: a scientific research instrument in the public way," Proceedings of the 2nd International Workshop on Science of Smart City Operations and Platforms Engineering - SCOPE '17, 2017, doi: https://doi.org/10.1145/3063386.3063771.

[21] Hsu, A., "Case Study: IPv4 vs. IPv6 Internet Speed Analysis Using FLOTO", 2024, May 20, https://floto.cs.uchicago.edu/2024/05/20/case-study-ipv4-vs-ipv6-internet-speed-analysis-using-floto/.

[22] "Docker Hub rate limit", https://docs.docker.com/docker-hub/download-rate-limit/.

[23] "The International Conference for High Performance Computing, Networking, Storage, and Analysis.", https://sc24.supercomputing.org/scinet/.

[24] L. Winkler, "SCinet: 25 years of extreme networking," Nov. 2015, doi: https://doi.org/10.1145/2830318.2830321.

[25] " SDSC Networking Experts Contribute to Success of SCinet at SC2003", https://www.sdsc.edu/News% 20Items/PR121503b.html.

[26] Szymanski, T., "Special Event Station N3T – Celebrating Supercomputing + Ham Radio with W9ANL & SC23 SCinet", 2024, July 25, https://blogs.anl.gov/amateur-radio/2024/07/25/special-event-station-n3t-celebrating-supercomputing-ham-radio-with-w9anl-sc23-scinet/.

[27] "IPv6 Chart: RIPE Network Coordination Centre", https://www.ripe.net/media/documents/IPv6_Chart_2015.pdf.

[28] Young, S., "M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles", 2022, January 26, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[29] Jensen, T., "Windows 11 Plans to Expand CLAT Support", 2024, March 7, https://techcommunity.microsoft.com/t5/networking-blog/windows-11-plans-to-expand-clat-support/ba-p/4078173.

[30] "End of support for Windows 10, Windows 8.1, and Windows 7", https://www.microsoft.com/en-us/windows/end-of-support?r=1.

[31] Shejy, G., Shah, D., and Gadekar, S., "IPV4-IPV6 Transition Issues Study on Handling Multiple Responses in Dual-Stack," *International Journal of Engineering Research and*, vol. 2, no. 9, Sep. 2013.

[32] Caletka, O., Deploying IPv6-mostly access networks, Apr. 24, 2023. https://www.ipv6.org.uk/wp-content/uploads/2023/02/08_UKIPv6-Deploying_IPv6_mostly.