April 2021
Geoff Huston

IPv4 in the Headlines

The world of IPv4 addresses is a relatively obscure backwater of the Internet. All that drama of IPv4 address exhaustion happened with little in the way of mainstream media attention. So it came as a bit of a surprise to see a headline in the Washington Post about IPv4 addresses.


The Washington Post
Democracy Dies in Darkness

Tech Consumer Tech Future of Transportation Innovations Internet Culture Space Tech Policy Video Gaming

Technology

Minutes before Trump left office, millions of the Pentagon's dormant IP addresses sprang to life

After decades of not using a huge chunk of the Internet, the Pentagon has given control of millions of computer addresses to a previously unknown company in an effort to identify possible cyber vulnerabilities and threats

https://www.washingtonpost.com/technology/2021/04/24/pentagon-internet-address-mystery/

The US Department of Defence holds some 221,828,864 addresses in the ARIN registry, with some 1,207 individual address prefixes, including 11 /8 prefixes. Many of these address prefixes were assigned by the IANA in the very early days of the Internet when the Internet itself was part of a research project sponsored by the Defence Advanced Research Projects Agency, and 10 allocations have been registered since 2000. These 10 more recent allocations span 1,904,896 addresses and occurred in 2000 and 2004 according to the registry.

How significant is this advertising of the DOD IPv4 address space?

At the start of each year, I've reported on the various movements in IP address space over the previous 12 months. There are many stories embedded in this data about addresses and their use. There are the various national stories about the deployment of Internet technologies and the relative rates of progress in digitisation in both business and consumer markets. There is the story about the increasing levels of consolidation of suppliers in many Internet markets and the decline in the levels of competition as a consequence. There is also of course our progress on the extended transition to IPv6. When the supply of IPv4 addresses from the residual free pools waned we shifted to transfer markets for addresses, and we were able to observe the cross-border flow of addresses as an outcome of this address trading activity.

The address distribution function is performed in a two-level hierarchy, with the IANA performing a role of the wholesale distribution point. The IANA registries describe the status of the entire address space for both IPv4 (https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml) and IPv6 (https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-

assignments.xhtml). IANA assigns address blocks to Regional Address Registries (RIRs) when the RIR's operating pool falls below a defined threshold. The RIRs further assign these addresses to service providers in accordance with locally adopted assignment policies. These policies may vary in terms of details but follow a consistent theme of responding to a demonstrated need. The registries maintained by these RIRs describe the current state of these address assignments, and a time series of the state of these registries can be used to observe trends in this space.

It is up to the address holders to determine what they do with these IP addresses. Typically, the addresses would be used in support of a public service provided on the Internet, and to achieve this we would expect to see these addresses advertised in BGP (the Internet's inter-domain routing protocol) at some time after the RIR assignment. There are other uses for IP addresses that do not involve advertising them on the public Internet, or the addresses may be held in a dormant state. The registries do not contain this level of information, so we use BGP snapshots to define these addresses as "advertised" or "unadvertised".

Figure 1 shows the total span of all assigned addresses since 2000, and also their status as either advertised in BGP or unadvertised.

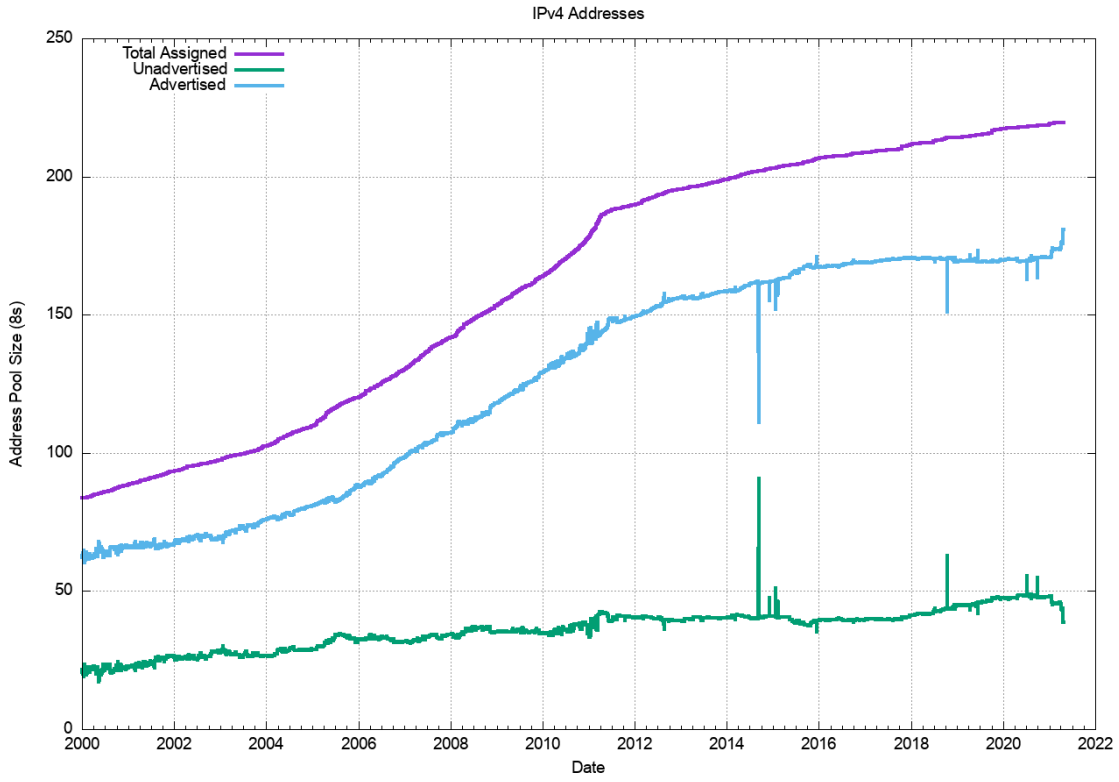

Figure 1 – Daily snapshot of IPv4 Address pools since 2000

The initial IPv4 exhaustion threshold in April 2011 is clearly evident in this data. The continuing growth of the total address pool since that data is the result of some level of movement of addresses from being unadvertised to becoming visible in BGP, the residual allocations being performed by RIRs from their various "last /8" address pools, so amount of addresses being returned to the RIRs and continuing efforts by the RIRs to drain their pools of addresses that were marked as "reserved" (some 12,493,024 IPv4 addresses are still marked as "reserved" today).

The advertisement of the DOD address space is visible in the changes in the advertised and unadvertised pool sizes in 2021. We can look at this in a little more detail in Figure 2.

It's evident that the DOD address space has been announced in three events: the 20th and 21st January, 6th and 7th of April and the 19th and 20th April.

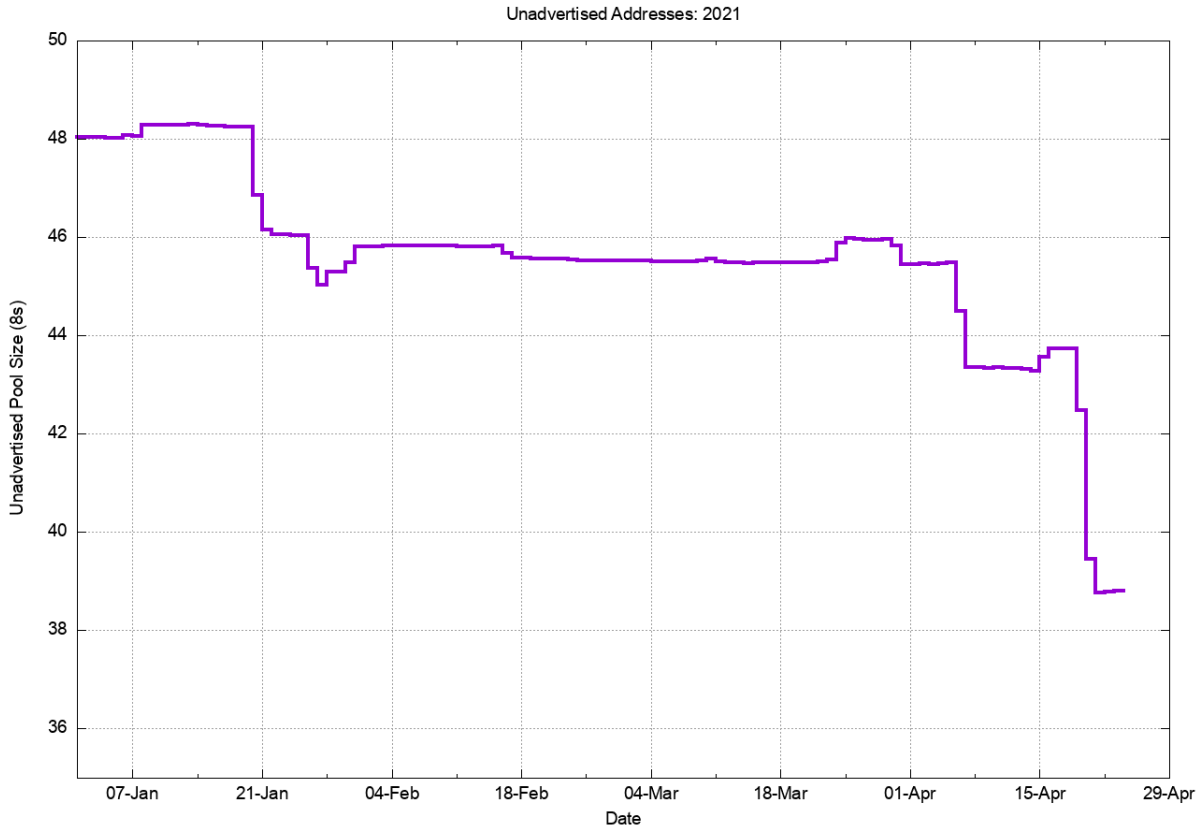

Figure 2 – Daily snapshot of IPv4 Unadvertised Address Pool in 2021

All these announcements use AS 8003 as the originating AS number, and the total span of addresses announced by that AS now total 178,348,288 addresses, (from a total of 221,828,864 addresses held by the US DOD).

Why are they advertising these addresses now?

This remains an area of speculation. An update to the Washington Post story reports that the Pentagon "has now provided a very terse explanation for what it's doing". The report continues: "The military hopes to "assess, evaluate and prevent unauthorized use of DoD IP address space," said a statement issued Friday by Brett Goldstein, chief of the Pentagon's Defense Digital Service, which is running the project. It also hopes to "identify potential vulnerabilities" as part of efforts to defend against cyber-intrusions by global adversaries, who are consistently infiltrating U.S. networks, sometimes operating from unused internet address blocks." (https://www.washingtonpost.com/politics/the-big-pentagon-internet-mystery-now-partially-solved/2021/04/24/eb26bff8-a539-11eb-b314-2e993bd83e31_story.html).

The issue relating to "unauthorised use" of supposedly dormant IPv4 space is very much an ongoing concern, and a number of networks, both large and small, have used parts of the DOD IPv4 address as a way of augmenting their internal private IP address pools over the years. If we look at the prefixes being advertised by AS8003 of this DOD IP space, we see a mix of covering aggregate prefixes and more specifics (https://as8003.potaroo.net). As of the 26th of April, AS8003 advertises 754 address prefixes, of which 724 are more specific prefixes of covering aggregates. For example, we see an advertisement of 11.0.0.0/8 and also 11.0.0.0/13, 11.0.0.0/22, and 7.0.0.0/24. At the same time, we see 30.0.0.0/8 and no more specific advertisements.

One speculative theory is that these more specifics are doing what many ISPs do already: use more specific advertisements to mitigate the impact of potential route hijack efforts that use more specifics as the hijack approach. This is quite a common occurrence and while the proportion of more specifics is not as high as the 96% seen with AS8003, the Internet-wide average is some 54% (https://bit.ly/3sTspJu)

It also may assist in supporting another line of defence against hostile attack scenarios where the attack uses route hijacking to seize control over prefixes in this address space in the context of the public Internet.

Getting back to the concept of defensive more specifics, why wouldn't they use ROAs and leverage Route Origination Validation to "defend" these advertisements? That way those networks that use ROV filtering would drop any unauthorised efforts to hijack this address space without splattering the routing system with more specifics. So if they are so concerned about routing hijacks then it seems slightly anomalous that they are not using ROAs to enlist the assistance from the rest of the routing system to combat this form of address abuse.

This action could also be an expression of the adage "use it or lose it!" If the unauthorised use of DOD IP space becomes commonplace over time, then the conventions of current practice could usurp the original ownership of this address space. It could also be a consideration that in some (highly improbable) future scenario where the DoD needed to use this IP space in the public Internet it the address advertisements may not be accepted by the Internet. This could be seen as a prudent form of "pre-provisioning". Admittedly, this is an unlikely scenario.

The most likely explanation is that advertising IP address space, even if this address space is not used in the content of the public Internet, is one more way to enlist the routing system itself to make it more challenging for others to use these addresses to mount hostile attacks on their systems located within their networks. I see nothing sinister here. It's just one more prudent step to help defend critical IT assets in a hostile world. Indeed, the only question in my mind is: "What took them so long to do this?"

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston AM, M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net