# Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

# M³AAWG Recommendations: Methods for Sharing Dynamic IP Address Space Information with Others

Updated May 2018 (2008)

The reference URL for this document is www.m3aawg.org/SharingDynamicIP

## Updated in this Version

This May 2018 version has been updated to include information on IPv6. Other minor changes have been made to improve the clarity and update the text.

## Introduction

While M³AAWG is on record as recommending that the best option for controlling the flow of unwanted email traffic from an ISP's customer space, especially the ISP's dynamic address space, is to block outbound port 25 traffic from that space(1), M³AAWG recognizes that such blocks may not be possible for some internet service providers in either the short term or the long term. This document will spell out alternatives for such ISPs, recommending methods they can use to share their dynamic space information with others and allow remote sites to reject inbound mail traffic from dynamic address space.

### Definition of Terms

The meaning of the phrase "dynamic IP address" has evolved over time. In the days when most ISP customers accessed the internet through a dialup connection, the pairing of an IP address to a customer was in most cases truly "dynamic." An IP address could be assigned to multiple different customers over the course of a day, depending on how many dialup connections the ISP could support; or, customers might use multiple IP addresses in a given day, depending on how many times they connected to their provider at various times during the course of the day.

Today, with the "always on" nature of DSL, cable modem, mobile phone, and other emerging technologies, a customer might conceivably have a dynamic IP address that does not change for months at a time. So long as the modem is not powered off for a long period of time, and so long as the ISP does not assign a new IP address to that modem, there is no reason to think that the IP address will ever change. The IP address is still, however, properly called "dynamic": it is not "static," as control over the assignment of the IP address to the modem lies solely with the ISP and that assignment is done using DHCP(2).

### Background

Computers infected with malicious software are the sources of most spam today. Typically these computers use DSL or a cable modem with a dynamic IP address to connect to the internet. These computers are organized into networks called "botnets" and used by criminal spammers, almost certainly unbeknownst to the physical owner of the infected computer, i.e., the ISP customer. These spammers then use the infected computer to send their unwanted traffic to mail servers around the world.

In years past, the only solution to this problem considered acceptable by internet experts was for the ISP providing connectivity to an infected computer to work with its customer to clean up the computer and stem the flow of infected mail from it. Allowing email traffic from such compromised host computers to egress the ISP's network and reach remote mail servers was seen as inflicting unnecessary cost on the remote networks, and so ISPs were called upon to prevent such traffic. While the responsibility for cleaning up infected computers and controlling traffic from them still ultimately lies with the ISP and its customers, the preponderance of heavy network traffic – such as video and music downloads, peer-to-peer file sharing, and other file exchanges – has made email traffic such a minimal part of the overall network-usage picture that sites now consider blocking the inbound traffic at their own edge to be an acceptable alternative. As long as the spam does not reach a site's mailbox holders and inflict any damage on them, the problem is considered solved as far as the target site is concerned. In order to assist target sites that have a local policy to refuse traffic from dynamic IP address space, ISPs must make such space easily and correctly identifiable so that sites can implement such policies at little risk to legitimate mail traffic.

## Sharing Dynamic IP Address Information

So long as their policies permit, ISPs should share their dynamic address space with others by doing one or more of the following:

- Share address lists, by CIDR block, with public information sources, such as, but not limited to, the Spamhaus PBL, the SORBS DUHL, and other lists of dynamic address space.
- Share address lists, by CIDR block, with other sites and providers which may not be making use of commercial or public DNSBLs (DNS Block Lists) listing dynamic address space. Make this information easily found on your postmaster or support website.
- Make dynamic address space easily identifiable by reverse DNS pattern, **preferably by a right-anchor string;** by "right-anchor string," we mean that the pattern chosen should be such that one may say that all reverse DNS records ending in *.some.text.example.com are those that identify dynamic space. See Making Dynamic IP Space Easily Identifiable by Reverse DNS Pattern below for examples.
- Make dynamic address space easily identifiable by WHOIS lookup. See Making Dynamic IP Space Easily Identifiable through WHOIS below for recommendations.

## Advantages and Disadvantages for each Approach

Each approach discussed above has both good points and (potentially) bad, and these must be understood by any ISP undertaking any of the strategies.

### Sharing IP Address Lists

Before an ISP can consider sharing its IP address lists with others, it must first ensure that it has maximum homogeneity in its space assignment. Dynamic address space must be kept separate from static space to the

fullest extent possible. A good rule of thumb to follow here is to ensure that any given /24 CIDR block (i.e., a network mask of 255.255.255.0) is either entirely dedicated to dynamic address space, or that it have no dynamic IP addresses in it. Sites wishing to block inbound traffic from dynamic space may not be able to filter on networks with a mask smaller than /24 (e.g., 255.255.255.128).

The advantages to an ISP sharing IP address lists with others include:

- IP address lists are most easily incorporated into existing filtering schemes, either through mail server rejection lists or policy rules implemented at the network level.
- ISPs that share their address lists with multiple public DNSBLs ensure the widest dissemination of the data, as each list is used by thousands upon thousands of sites.

The disadvantages to this approach include:

- Another step is added to the ISP's process for maintaining IP address assignment information. Whenever new space is put into use, or a space's assignment changes from or to dynamic address space, the ISP must notify all consumers of the information as part of its processes.
- In concert with the ISP notifying others about the new space assignments, the ISP then must rely on the consumers of the data to make updates to their lists in a timely fashion. A DNSBL or site that lags behind the ISP in reclassifying the ISP's space can adversely impact traffic from the ISP's static address space.

## Making Dynamic IP Space Easily Identifiable by Reverse DNS Pattern

Another way that an ISP can announce its dynamic space to others is to ensure that it all has a consistent reverse DNS pattern assigned to it, and that the reverse DNS pattern clearly indicates that the space is dynamic. Moreover, having this pattern be part of a right-anchor string for the rDNS, rather than a regular expression with a variable part in the middle, is the ideal approach to minimize the number of patterns and allow for effective usage of them. While both Matthew Sullivan[3] and D. Senie and Sullivan[4] have written extensively on this topic, some examples of both good and bad existing approaches should be mentioned here:

Examples of right-anchor strings in use at the time of this writing include:

- res.rr.com
- dynamic.covad.net
- dhcp.bluecom.no
- ipt.aol.com

The advantages to sharing dynamic address space by reverse DNS pattern include:

- It adds no extra steps to the publishing process.
- The ISP controls the DNS data for its own space, and therefore it has full control over the timing of the publishing of such data.
- DNS change management, including lowering of TTLs (Time to Live), can be done in concert with network space allocation.

The disadvantages to this approach include:

- Filtering traffic based on reverse DNS has not been as widely adopted as has filtering by IP address or network and such a scheme does not lend itself easily to policy rules on network devices.

- ISPs that do not have a right-anchor string pattern currently will face challenges to put one in place. The work is not technically difficult, but depending upon the amount of network space involved, it could entail significant amounts of effort. It is not impossible to get this done, even in a large ISP; one M[3]AAWG member with millions of customers successfully migrated its customer space to a common right-anchor string pattern over a period of several months in 2005.

## Making Dynamic IP Space Easily Identifiable through WHOIS

The last approach this document will discuss is for ISPs to make their dynamic space easily identifiable through WHOIS information. For given WHOIS output, such as this:

```
OrgName:         Road Runner HoldCo LLC
OrgID:           RRMA
Address:         13241 Woodland Park Road
City:            Herndon
StateProv:       VA
PostalCode:      20171
Country:         US

ReferralServer: rwhois://ipmt.rr.com:4321

NetRange:        24.24.0.0 - 24.29.255.255
CIDR:            24.24.0.0/14, 24.28.0.0/15
NetName:         ROAD-RUNNER-1
NetHandle:       NET-24-24-0-0-1
Parent:          NET-24-0-0-0-0
NetType:         Direct Allocation
NameServer:      DNS1.RR.COM
NameServer:      DNS2.RR.COM
NameServer:      DNS3.RR.COM
NameServer:      DNS4.RR.COM
Comment:
RegDate:         2000-06-09
Updated:         2002-08-22

RTechHandle:     ZS30-ARIN
RTechName:       ServiceCo LLC
RTechPhone:      +1-703-345-3416
RTechEmail:      abuse@rr.com

OrgAbuseHandle: ABUSE10-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-703-345-3416
OrgAbuseEmail:  abuse@rr.com

OrgTechHandle:  IPTEC-ARIN
OrgTechName:    IP Tech
OrgTechPhone:   +1-703-345-3416
OrgTechEmail:   abuse@rr.com
```

ISPs can assign to the NetType or Comment field — preferably the NetType field — a value that clearly indicates that the range in question is dynamic space. WHOIS data has a well-known format and tools exist or can be built to parse it. Therefore, so long as a standard term can be agreed upon to communicate that the space is dynamic, this can serve as another method for announcing that network space is dynamic.

The advantages to the ISP choosing this method for sharing its dynamic space include:

- As with the reverse DNS method of sharing dynamic space information, the ISP controls the entire process, in that it can update the NetType field in its RWHOIS answer as part of its space allocation management process.

The disadvantages to this method include:

- There is no useful way for a site to make direct use of this information during the SMTP transaction; WHOIS queries cannot be made and parsed while the SMTP connection is active at any meaningful volume. Any site wishing to block mail from an ISP's dynamic space will have to write tools that make periodic WHOIS queries based on IPs seen in its own inbound logs, and then build its filter lists based on data received from those queries.
- It is also incumbent on the site consuming the WHOIS data to make regular validation queries to ensure that the data it has previously collected about a given ISP's space is current and correct. As there is no push notification available for WHOIS data, an ISP changing its NetType for a given range has no way to notify those who may have consumed the previous data before changes were made. Therefore, sites will have to query this data at least once per day to ensure currency.

## IPv6 Address Space

Since the IPv6 address space is so large, ISPs typically assign each customer a block of address space that never changes. Although this customer address space is static, the same policies apply as to dynamic IPv4 address space, such as not sending mail directly. Also since the address space is so large, only static servers have DNS names, and only the IP addresses of those servers have reverse DNS. (The smallest customer address allocation, a /64, is four billion times larger than the entire IPv4 address space, so assigning names to every address is both impractical and not useful since only a handful of the addresses in any /64 will ever be assigned to computers.) Hence any address without rDNS can be assumed to be the practical equivalent of a dynamic address. WHOIS data for IPv6 address ranges should be provided just as for IPv4 ranges. The size of the range assigned to each customer varies by ISP from a /64 to as much as /48. At this point there is no mechanical way to determine the size an ISP assigns.

## Conclusion

This document enumerates ways that ISPs can share their dynamic address space with others, and includes advantages and disadvantages to each approach. While an ISP preventing direct-to-MX (i.e., outbound port 25) traffic from leaving its dynamic customer address space is still the preferred solution to the problem of spam coming from these networks, M$^3$AAWG recognizes that some ISPs cannot implement this step at this time. For those ISPs, it is important they make their dynamic address space known in as many different formats and forums as possible by one or more of the methods discussed in this document. Doing this will support the many sites wishing to refuse traffic from such space, in keeping with their policies.

## References


[1] MAAWG Recommendation – Managing Port 25 for Residential or Dynamic IP Space – Benefits of Adoption and Risks of Inaction

[2] Dynamic Host Configuration Protocol (DHCP), http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[3] Suggested Generic DNS Naming Schemes for Large Networks and Unassigned hosts, Matthew Sullivan, IETF, 2006, http://www.tools.ietf.org/html/draft-msullivan-dnsop-generic-naming-schemes-00.txt

[4] Considerations for the use of DNS Reverse Mapping, D. Senie and A. Sullivan, IEFT, 2007, http://tools.ietf.org/html/draft-ietf-dnsop-reverse-mapping-considerations-05.txt


As with all documents that we publish, please check the M³AAWG website (www.m3aawg.org) for updates.


M3AAWG021-updated