Messaging Anti-Abuse Working Group

# MAAWG IPv6 Training for Senders and Others

## Segment 1 of 3

## Basic IPv6 For Senders

October 4th-6th, 2010

MAAWG 20th General Meeting, Washington DC


Messaging Anti-Abuse Working Group

**Joe St Sauver, Ph.D.,**

MAAWG Sr. Technical Advisor

joe@oregon.uoregon.edu

www.uoregon.edu/~joe/maawg-senders-ipv6-training/

***Disclaimer:*** All opinions expressed in this talk are strictly my own, and do not necessarily represent the opinions of any other entity. This talk is provided in a detailed written form to insure accessibility and for ease of web indexing.

# MAAWG IPv6 Training – Video Segments

| Segment 1 - 21 minutes<br>Basic IPv6 For Senders | Segment 2 – 25 minutes<br>Understanding IPv6 Drivers & Myths | Segment 3 – 21 minutes.<br>IPv6 Technology Primer |
|---|---|---|
| 1-Do Mail Senders *Really* Need IPv6 Today? | Drivers:<br>6a-IPv4 Address Exhaustion | 8a-IPv6 Addresses |
| 2-IPv6 and SMTP | 6b-Regaining Internet Transparency | 8b-IPv6 Prefixes |
| 3-Obtaining Native IPv6 Connectivity and Address Space | 6c-Controlling Route-Table Bloat | 8c-Types of IPv6 Addresses |
| 4-Enabling IPv6 on Your Servers | 6d-Regulatory Compliance | 8d-Addresses and Systems |
| 5-Enabling IPv6 in Your MTA | Myths:<br>7a-Improve "Network Security" | 8e-IPv6 DNS |
| | 7b-*Everyone's* Running Out of IPv4 Address Space | 8f-Enabling IPv6 in Desktop Operating Systems |
| | 7c-IPv6 Will Simplify Renumbering . . . | 8g-IPv6 Web Browsers |
| | 7d-Access to "Cool New Stuff" | 8h-IPv6 Email Clients |
| | 7e-Techies Will Stretch Out What IPv4 Space | 8i-ssh for IPv68. (j): Web Servers |
| | 7f-Customers Just Aren't Asking For IPv6 | |

# Welcome to the DC Area and MAAWG's IPv6 Training for Senders (and Others)!

- We're excited to be with you here today to talk for about seventy five minutes about what you might want to know about IPv6 if you're a sender.

- Just to get started, let's go around the room and have each person briefly say:

  -- who they are
  -- what they do
  -- the company you're with
  -- a little about your interest in/experience with IPv6
  -- your technical level (non-technical, semi-technical, hard-core geek, or whatever)

# PART I.
# Basic IPv6 For Senders

# 1. Do Mail Senders *Really* Need IPv6 Today?

# If You're A Mail Sender, Do You *Really* Need IPv6 Today? Well, No.

- You obviously already have IPv4 address space.
- The sites you're sending to, with perhaps just a few exceptions, will **not** have IPv6-enabled mail transfer agents (MTAs), so even if you wanted to talk to them via IPv6, they may not be ready for you to do so.
- If the sites you're sending to **do** have IPv6-enabled MTAs, in virtually every case those MTAs will be actually be "dual stack," e.g., they'll support **both** IPv6 **and** IPv4 transport, they **won't** be IPv6-only MTAs. So, if you can already reach a site via IPv4, why bother trying IPv6 instead, particularly if some of that IPv6 connectivity may be tunnelled and indirect, slow, lossy, or otherwise lower quality than also-available IPv4 links?

# But, Even If *You* Don't Need To Move to IPv6 As A Sender, Others Do

- For example, within a year or two, there will not be any more IPv4 address space to allocate to **growing ISPs** working hard to hook up new customers, or ISPs trying to accommodate a growing number of devices/customer.
- **Alternatives to IPv6, such as using Network Address Translation (NAT) with private address space, pose some really ugly operational challenges** for ISPs (particularly for things like tracking down malware-infested customers living behind a NAT box)
- **Software and hardware vendors** that need to service a market that's moving to IPv6 **also** need to "make the IPv6 leap" and enable IPv6 in their products as a result of their customers' emerging requirements.

# Bottom Line

- Since you're already here, you might as well at least learn a little about IPv6, and maybe even give it a try when you get back home

- The process doesn't have to be painful, and if you don't like it, as a sender you can always "back it back out" and go back to just using IPv4.

- The first part of this talk will be for those of you who are bsuy and goal oriented: we'll start by looking at what you'd need to do if you did want to begin sending email traffic from an IPv6-enabled server on an IPv6-enabled network.

# 2. IPv6 and SMTP

# Email Is The "Forgotten" Application of IPv6

- While many people are very excited about the thought of using IPv6 for the **web**, for some reason there seems to be a lot less excitement about using IPv6 for **email**.

- Thus, while many mainstream mail software products support IPv6, relatively few mail administrators apparently bother to enable IPv6 support.

- But some sites ARE deploying IPv6-accessible mail servers right now. For example...

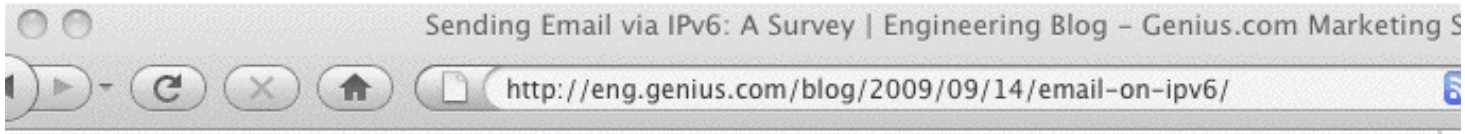
# Sample Institutional IPv6 Enabled MX

```
% dig ucla.edu mx +short
5 smtp.ucla.edu.

% dig smtp.ucla.edu a +short
169.232.46.240
169.232.46.241
169.232.46.242
169.232.46.244
etc.

% dig smtp.ucla.edu aaaa +short
2607:f010:3fe:302:1013:72ff:fe5b:60c3
2607:f010:3fe:102:101c:23ff:febe:116e
2607:f010:3fe:102:101c:23ff:febf:cfa7
2607:f010:3fe:102:101c:23ff:fed0:918c
etc.
```

# Examples of Other IPv6 Enabled Domains/MXs

brocade.com (mx10.brocade.com)
maine.edu (mail-relay.maine.edu)
vt.edu (inbound.smtp.vt.edu)
iij.ad.jp (omgi.iij.ad.jp)
ams-ix.net (betonmix.noc.ams-ix.net)
apnic.net (hoisin.apnic.net)
arin.net (smtp2.arin.net)
dren.net (drenmail.dren.net)
es.net (mail.es.net)
he.net (he.net)
jpnic.net (mx15.nic.ad.jp)
lacnic.net (mail.lacnic.net)
ripe.net (postgirl.ripe.net)
icann.org (pechora2.icann.org)
ietf.org (mail.ietf.org)
isc.org (mx.ams1.isc.org)
kth.se (mx.kth.se)

# Code To Check for IPv6 MX Records




### Email and IPv6

But what about email? How many servers can receive email via IPv6? We took a sample of 500,000 domains. Unfortunately we cannot use the list from Alexa as they are web sites and not domains with mail servers. Instead, we sampled 500,000 email domains known to Genius.com and went to look for their MX records. For each MX record we checked if the host has an AAAA record (reachable via IPv6).

We used the simple program below against a csv file of domains:

```
<?php
$file=$argv[1];
$f=fopen($file,"r");
$buffer = fgets($f, 4096);
$i=1;
while (!feof($f)) {
    $buffer = fgets($f, 4096);
    $domain=substr($buffer,1,-2);
    echo $i."|".$domain."|";

    //look for MX record
    $mxhosts=array();
    $foundMX=getmxrr($domain,&amp;$mxhosts);
    if ($foundMX) {
        //loop through MX records
        $ipv6=false;
        foreach($mxhosts as $host) {
            if (checkdnsrr($host,"AAAA")) {
                $ipv6=true;
                break;
```

<-- must be php5 (for getmxrr)

<-- ($buffer,0,-1)

<-- ($domain,&$mxhosts)

[continues; see the original site for the full code]

# Important Note:

- While we may be curious to find out who's currently running with SMTP enabled over IPv6, we do **NOT** need to manually keep track of those sites, **NOR** do we need to change any of the addresses we mail to once both the sender and receiver are IPv6 enabled and IPv6 accessible.
- In most cases, mail servers will simply **automatically select IPv6 transport** if both the sender and the receiver support IPv6.
- As a sender, then, you simply need to:
  -- get IPv6 connectivity (and IPv6 address space)
  -- enable IPv6 for your server's operating system
  -- enable IPv6 for your MTA
- Go over ALL the things you'll need to do before you start ordering connectivity and start modifying gear, etc.!

# 3. Obtaining Native IPv6 Connectivity And Address Space

# Add IPv6 Internet Transit Connectivity

- This task is largely a business office/financial one.
- Contact your account manager at your current colo or network service provider and tell him/her that you'd like to add IPv6 transit to your existing IPv4 connectivity.
- While you're at it, ask them for IPv6 address space, too. You'll probably get a /48 worth of IPv6 address space by default (we'll talk about that later); a /48 should be fine.
- If your account manager doesn't know what IPv6 transit connectivity is, press them to ask their sales engineering support person (or otherwise escalate your question).
- If they check and they really don't offer native IPv6 (or they do, but not at your location/not for you, etc.), see the list of providers who do have IPv6 transit available at http://www.sixxs.net/faq/connectivity/?faq=ipv6transit

# How *Much* IPv6 Connectivity Do I Need?

- Your initial IPv6 connectivity requirements will probably be relatively modest. Ideally, your IPv6 connectivity and your IPv4 connectivity will share your existing bandwidth and links, and if you're able to do that, then you won't end up needing to purchase separate IPv6 connectivity.
- If you do need to purchase separate IPv6 connectivity, perhaps because your current provider isn't able to deliver IPv6 connectivity to you, I'd suggest starting modestly, maybe with IPv6 transit capacity at no more than 10-15% of your current IPv4 transit bandwidth level.
- You'll probably have more capacity than you'll initially need, but you'll find that usage will grow over time. Be sure that whatever plan you select gives you flexibility to adjust your IPv6 transit capacity if you need to do so.

# "What About Just Using a Free Tunnel?"

- An alternative to getting IPv6 transit connectivity from a network service provider is getting a free IPv6 tunnel from a tunnel broker, such as Hurricane Electric (see http://tunnelbroker.net/ ).

- Their free tunnel service, and similar tunnel services, are great as far as they go, but IPv6 tunnel services tend to be oriented toward developers and experimenters, and since you're a sender, you're going to want production grade native IPv6 service instead.

- If you can't get native IPv6 connectivity, I'd probably wait until you can do so before "taking the IPv6 leap."

# Networking Equipment: Routers and Switches

- Depending on your setup, you may have your own customer premises equipment (CPE), such as a Cisco or Juniper border router, or you may just get a 100Mbps or gigabit ethernet handed to you from your provider, perhaps fanned out across some layer 2 ethernet switches.
- Virtually all layer 2 ethernet switches will transparently pass IPv6 traffic without requiring any tweaking or adjustment.
- If you have your own layer 3 device, such as a Cisco or Juniper router, you will need to have your network engineer enable IPv6 on it.
- Note that some older-generation Ciscos may not be able to process IPv6 at full wirespeed; you should be planning to upgrade or replace geriatric equipment of that sort.

# Networking Equipment: Firewalls

- Some sites may have an IPv4 hardware or software firewall configured in front of their servers. Two things to be aware of...
- First, some firewalls may not be "IPv6 aware" and may just drop any IPv6 packets they see. Those firewalls may need to be upgraded, replaced or bypassed.
- Second, assuming your existing firewall *is* able to handle IPv6, and you want similar protection for connections over IPv6 as for IPv4, don't forget to create rules allowing desired IPv6 traffic and blocking remaining IPv6 traffic! Your IPv4 rules will NOT automatically be extended to encompass IPv6 traffic, and so, by default, you may either unexpectedly block legitimate IPv6 traffic, or unexpectedly permit unwanted IPv6 traffic.

# Networking Equipment: DNS Servers

- Most senders will routinely use two sorts of DNS servers: recursive resolvers and authoritative name servers.
  -- Authoritative name servers answer DNS queries for your domains
  -- Recursive resolvers resolve all other domain names
- Both sort of name servers will need to support IPv6 resource records (such as AAAA records), however neither needs to support **access** to the name servers over IPv6 (for now, you can just continue to access your recursive resolvers and authoritative name servers over IPv4).
- If your local recursive resolvers don't support IPv6 and you don't want to upgrade them to do so, one alternative would be to use Google's intentionally open recursive resolvers at 8.8.8.8 and 8.8.4.4 -- they do support IPv6.

# Networking Equipment: Other Stuff

- Unlike ISPs with end users, senders don't need to worry about things like dynamically assigning IPv6 addresses to end users/customers; we assume that you'll be manually/statically assigning all IPv6 server addresses instead. Therefore, you don't need to worry about DHCPv6 or stateless autoconfiguration or any of the associated IP address assignment gyrations.

- Similarly, if you do central syslogging, or centralized device monitoring and management, or centralized NTP (time service) currently, we assume that you will continue to do those things over IPv4 -- for now, the only things that will be talking over IPv6 transport are your MTAs.

# Your New IPv6 Address Space

- If you're a sender who currently maybe has an IPv4 /24 with 255 addresses, and you suddenly get a /48 worth of IPv6 space (e.g., 2^(128-48), or 1,208,925,819,614,629,174,706,176 IPv6 addresses), you may be overwhelmed by all your new address space.
- It may help if you think of that as "just" 65,536 subnets, with each subnet being 64 bits long (or having 2^64 or 18,446,744,073,709,551,616 addresses). You will likely only need one of those, but it's good to have room to grow. :-)
- For now, let's just assume that your network engineer (or your network service provider/colo provider) will recommend appropriate IPv6 host IP addresses from your IPv6 range, and we'll also assume that he or she will tell you your default upstream IPv6 gateway address.

# 4. Enabling IPv6 on Your Servers

# Most Modern Operating Systems Ship "IPv6 Ready"

- In general, most modern operating systems are IPv6 ready; if you're configuring a mail server, you just need to enable IPv6 and supply basic configuration information (such as the server's static IPv6 address).

- **Q.** "Help! My operating system doesn't have built in support for IPv6! Should I patch it or something?"
  **A.** If your operating system requires a patch to support IPv6, it is ancient and riddled with unpatched (and unpatchable) security issues. Before spending time experimenting with IPv6, first things first: upgrade your operating system to the current production release of your O/S (it *will* have native support for IPv6).

# Enabling IPv6 with A Static IPv6 Address

- Recipes to enable IPv6 and assign a static IPv6 addr for common OS:

  -- Redhat/CentOS:
  www.cyberciti.biz/faq/rhel-redhat-fedora-centos-ipv6-network-configuration/
  -- SuSE Linux:
  www.cyberciti.biz/faq/configuring-ipv6-in-sles10-opensuse-linux/
  -- Ubuntu Linux:
  www.cyberciti.biz/faq/ubuntu-ipv6-networking-configuration/
  -- FreeBSD and friends:
  www.cyberciti.biz/faq/freebsd-configure-ipv6-networking-static-ip-address/
  -- Windows Server 2008/R2
  technet.microsoft.com/en-us/library/cc732106.aspx

  Mac user? Just set a static IP in System Preferences
  -> Network -> Configure -> Configure IPv6 -> Manually

# Example: Enabling IPv6 in Redhat with A Static IP

- In /etc/sysconfig/network

  NETWORKING_IPV6=yes

- In /etc/sysconfig/network-scripts/ifcfg-eth0

  IPV6INIT=yes
  IPV6ADDR=your_servers_IPv6_address_here
  IPV6_DEFAULTGW=your_servers_default_gw_here

- # service network restart

# 5. Enabling IPv6 in Your MTA

# IPv6 Support In Mainstream Email Software Products

- Virtually all modern mail transfer agents support IPv6; a lack of IPv6 MTA software support is typically NOT an issue...

  -- Exchange 2007 SP1 (only under Windows Server 2008, and only with both IPv4 and IPv6 enabled); see http://technet.microsoft.com/en-us/library/bb629624.aspx
  -- Exim ( http://www.exim.org/exim-html-current/doc/html/spec_html/ch04.html at section 9)
  -- Postfix ( http://www.postfix.org/IPV6_README.html )
  -- Qmail (via Qsmtp, see http://opensource.sf-tec.de/Qsmtp/ )
  -- Sendmail (see the Sendmail Installation and Operation Guide, http://www.sendmail.org/doc/sendmail-current/doc/op/op.pdf)

- What about Procmail as a local mail delivery agent? Umm, well, unfortunately see http://www.procmail.org/todo.html

# What It Takes to Enable IPv6 in postfix

- For now, we'll assume that you have a ready-to-go IPv6-enabled network, and the only thing holding you up is a non-IPv6 aware MTA
- Let's assume you want to use Postfix. Get postfix 2.7 (or whatever's the latest production code) from www.postfix.org/download.html
- Review http://www.postfix.org/IPV6_README.html
- When configuring for IPv6, in /etc/postfix/main.cf,
  set inet_protocols = ipv6, ipv4  (if you're dual stacking)
- Also include in /etc/postfix/main.cf the address you want to use for outgoing IPv6 SMTP connections:
  smtp_bind_address6 = 2001:468:d01:d6::80df:d617  <-- sample only!
- Check your config and start postfix; typically:
  /usr/sbin/postfix check
  /usr/sbin/postfix start
- Confirm that you can connect OK to your IPv6 smtpd:
  % telnet 2001:468:d01:d6::80df:d617 25  <-- sample only!
  quit

# IPv6 and DNS Blocklists

- DNS blocklists, such as those offered by Spamhaus, are a key anti-abuse tool in today's IPv4-dominated Internet, directly blocking spam while also "encouraging" ISPs to employ sound anti-abuse practices.
- Virtually all sites that use DNS-based blocklists rely on rbldnsd (see www.corpit.ru/mjt/rbldnsd/rbldnsd.8.html ). rbldnsd does NOT support IPv6 records at this time. :-(
- Spamhaus does not maintain any substantive IPv6 **blocklists**; Spamhaus has, however, just recently announced a new IPv4 **and** IPv6 **whitelist** (see http://www.spamhauswhitelist.com/en/rationale.html )
- From a sender's point of view, you will obviously want to get your IPv6 MTAs whitelisted at Spamhaus (and anywhere else doing whitelisting) as soon as possible.

# Other Key Mail Technologies Are Already IPv6 Ready

- SPF supports IPv6 (see the "ip6 mechanism" at http://www.openspf.org/SPF_Record_Syntax )

- DKIM (and ADSP, for that matter) are IPv6 "agnostic" -- what they do doesn't depend on IPv4 or IPv6 addresses

# So Now You're At Least "Dangerous..."

- You know what you need to do to get IPv6 connectivity, how to enable IPv6 on your servers, and how to enable IPv6 in your MTAs.
- If you complete those tasks for your servers, your MTAs will begin to send mail via IPv6 when the opportunity to do so presents itself.
- **Bail Out Opportunity #1:** If that's all you're looking for, you can now leave and find a suitable beverage -- you now know enough to at least be "dangerous." If, however, you're a glutton for punishment, you can stick around.
- Next we'll explain why others are finding IPv6 a matter of some urgency, and not an optional experiment (as it is for senders), and we'll also talk about some IPv6 "myths."

**This video is presented by the**
**Messaging Anti-Abuse Working Group**

# MAAWG IPv6 Training for Senders and Others

can be viewed in three segments from the training pages at www.MAAWG.org.
This has been part 1 of 3.

Our thanks to MAAWG Senior Advisor Joe St Sauver, Ph.D.,
for developing the materials in this training session
and allowing MAAWG to videotape it
for the benefit of professionals worldwide.