MAAWG IPv6 Session

Messaging Anti-Abuse Working Group
18th Meeting, San Francisco, California
1:30-2:15PM, February 16th, 2009

Joe St Sauver, Ph.D. (joe@uoregon.edu)
Senior Technical Advisor

http://www.uoregon.edu/~joe/maawg18-ipv6/

Disclaimer: All opinions strictly my own.

Change of Agenda

- This session was originally going to be chaired by John Jason Brzowski of Comcast. Unfortunately, however,since he's unable to be with us today, so I'm going to be "pinch hitting" for him as the senior technical advisor for MAAWG's IPv6 activities.
- This session was originally scheduled as an IPv6 document review session, but since John can't be here we're going to push that review back to the Barcelona meeting this summer.
- Although we discussed simply canceling today's IPv6 session altogether, there was reluctant to do that given the urgency of the IPv6 issues we all collectively face.
- So, assuming everyone agrees, even though we won't do a document review, we will at least go over some IPv6 related material and have a chance to chat a little about IPv6.
- But first, a housekeeping note…

The MAAWG Meeting Network Is IPv6 Enabled

- If you connect to the MAAWG wireless network, you'll have both IPv4 and IPv6 connectivity (unless you explicitly pick the IPv6 **only** network!). For example:

```
% traceroute6 ipv6.google.com
traceroute6 to ipv6.l.google.com (2001:4860:b006::63) from
2607:f0d8:201:998:203:93ff:fee9:db56, 30 hops max, 12 byte
packets
 1  2607:f0d8:201:998::1  2.332 ms  1.268 ms  1.842 ms
 2  2607:f0d8:201:69::1  25.996 ms  27.122 ms  27.367 ms
 3  2607:f0d8:200:1::1  28.736 ms  28.079 ms  28.206 ms
 4  2607:f0d8:0:74::1  27.411 ms  27.363 ms  27.959 ms
 5  2607:f0d8:0:61::2  38.065 ms  37.439 ms  37.787 ms
 6  2607:f0d8:0:60::1  58.757 ms  44.365 ms  44.14 ms
 7  2607:f0d8:0:6::2  44.805 ms  38.362 ms  44.146 ms
 8  v6-six.sea01.google.com  50.556 ms  78.998 ms  45.138 ms
```

Trying IPv6 While You're Here

- At a user level, IPv6 should "just work." However, during this transitional period, for some O/S, you may need some tweaks to browsers and other applications for IPv6 to "just work." To see if your system is "just working" go to www.whatismyipv6.net -- do you see an IPv6 address such as 2607:f0d8:201:998:203:93ff:fee9:db56
- If you're not getting an IPv6 address while you're on the MAAWG network, you may need to tweak your system or browser. Some handouts that may be helpful for this process are:

  -- www.uoregon.edu/~joe/ipv6/mac-os-x-ipv6-one-pager.pdf
  -- www.uoregon.edu/~joe/ipv6/mac-firefox-camino-opera-saf
  ari-ipv6-one-pager.pdf (URL split due to length)
  -- www.uoregon.edu/~joe/ipv6/windows-xp-ipv6-with-teredo.pdf
  -- www.uoregon.edu/~joe/ipv6/windows-firefox-opera-ie-ip
  v6-one-pager.pdf (URL split due to length)

Don't Forget to Also Think About IPv6 Security

- Because you do have IPv6 connectivity while you're at MAAWG (while you may not have IPv6 connectivity on your home or work network), you may be concerned about security.
- We talked a little about IPv6 security considerations at MAAWG Amsterdam. Those slides are still available to you if you'd like a copy of them -- see "MAAWG and IPv6 Security," www.uoregon.edu/~joe/ipv6_training/maawg-ipv6-security.pdf
- The key message from that talk: people think that if they do IPv6, doing so will somehow make their security better, or that if they do IPv6, it will somehow make their security worse. In reality, while there are some new things you need to pay attention to, IPv6 security should neither be a prime driver for doing IPv6 nor a roadblock to deploying IPv6. Oh yes: and even if you don't deploy native IPv6, your users will still be able to use a variety of transition mechanisms (such as Teredo) to access IPv6 sites.

The Sun Is Still Coming Up Outside…

- While MAAWG's meeting network is IPv6 enabled, if you weren't an IPv6 geek, you probably didn't notice.

- **The network, even with IPv6 ubiquitously enabled, just works.**

  This should be tremendously reassuring to you.

  Enabling IPv6 on your networks does NOT need to be something that disrupts or interferes with ongoing routine day-to-day regular use of the Internet.

- But why are we talking about IPv6 here today?

A Michael Goldman-ish "Why Should I Care?" or "Why Is This Topic Important?" Slide

- Michael Goldman is MAAWG's facilitator, and he always urges us to explain **"Why Is Today's Topic Important?"**
- While there are many reasons why IPv6 is important, the most compelling reason is simply that **we are quickly running out of IPv4 addresses.**
- The best IPv4 address exhaustion estimate is probably the one which has been done by Geoff Huston. Huston predicts that IANA will exhaust its pool of unallocated IPv4 addresses on 16-Sep-2011, and regional Internet registries (such as ARIN) will exhaust their stock of unallocated IPv4 addresses roughly a year later, on 04-Oct-2012. (see www.potaroo.net/tools/ipv4/)
- **04-Oct-2012 is less than a thousand days from now -- you're quickly running out of time to get ready for IPv6.**

Tying IPv6 to Messaging Abuse

- Because this isn't NANOG or some other regional network engineering meetings, it isn't sufficient to just point to IPv4 network address exhaustion as a reason why you should be paying attention to IPv6 -- we also need to tie IPv6 to problems of messaging abuse if we're to make IPv6 relevant to MAAWG.
- Let me try to do so via just a few questions:
  -- Have you thought about whether you'll accept mail over IPv6?
  -- If you use DNSBLs, do those DNSBLs support IPv6 listings?
  -- If you use (or you sell!) commercial anti-spam appliances, are those commercial anti-spam appliances "IPv6 aware?"
  -- If you're a spam researcher, are you instrumented to collect IPv6 netflow data just as you do IPv4 netflow data?
  -- If you're a sender, should you begin trying to send via IPv6?
  -- Is your abuse/security staff trained and ready for IPv6?
- **IPv6 will directly impact your anti-spam activities.**

The "100,000 Foot" Question: *Will Your Company Be Ready for IPv6?*

- If nothing else, you should have a project or committee that is charged with looking at how you will address the challenge of deploying or managing IPv6.

- That group's conclusion, after looking at this issue, might be:

  -- We're not going to do IPv6
  -- We're going to wait before deploying IPv6
  -- It's time to start doing IPv6

- **Whatever you decide, the point is that you really should be having that conversation/thinking about IPv6 if you haven't already done so.**

ISPs: You Need A Cross-Departmental IPv6 Team

- ISPS: when you're planning for IPv6, because it touches so many different areas, you'll want a cross-departmental planning team.
- If you're an ISP, at a minimum you need participation from:
  -- senior management
  -- your network engineering team
  -- your system administration group
  -- your domain name service operational people
  -- your web team, your email team, <insert additional applications here>
  -- your customer provisioning department
  -- your customer support group
  -- your abuse department
  -- marketing folks
  -- finance folks, etc.
- IPv6 will touch virtually every department's work.

Vendors: You Need A Broad IPv6 Effort, Too

- If you're a vendor, and not an ISP, you will need a broadly-based IPv6 planning and analysis effort too. You'll likely need participants from:

  -- senior management
  -- product engineering, development and testing
  -- marketing
  -- your customer support engineering team
  -- your company's internal network and IT support group

  Again, planning how your company will deal with IPv6 is an issue which will involve virtually every part of your company's work.

Senders: IPv6 Is Something You Need To Be Planning To Handle, Too

- While IPv4 may continue to be your dominant channel for communicating with your customers, a growing number of ISPs will be deploying IPv6 MTAs along side their IPv4 servers.

- If you have a choice of sending to either, which should you choose and why? Do you have the connectivity, servers and software you'd need to do IPv6, if that turns out to be your choice?

Example Mainstream IPv6-Enabled Mail Server

-
  ```
  % dig ucla.edu mx
  [snip]
  ucla.edu.            21600   IN     MX      5 smtp.ucla.edu.
  ```

-
  ```
  % dig smtp.ucla.edu aaaa
  [snip]
  smtp.ucla.edu.       21500   IN     AAAA    2607:f010:3fe:302:1013:72ff:fe5b:6032
  smtp.ucla.edu.       21500   IN     AAAA    2607:f010:3fe:302:1013:72ff:fe5b:60c3
  [snip]
  ```

-
  ```
  % telnet 2607:f010:3fe:302:1013:72ff:fe5b:6032 25
  Trying 2607:f010:3fe:302:1013:72ff:fe5b:6032...
  Connected to smtp-6.smtp.ucla.edu.
  Escape character is '^]'.
  220 smtp-6.smtp.ucla.edu ESMTP Sendmail 8.14.3/8.14.3; Tue, 16 Feb 2010 12:11:01
  -0800
  quit
  ```

- **Key takeaway: very mainstream sites -- such as UCLA -- ARE deploying IPv6 connected mail servers.**

Key Takeaway From the Preceding Slide

- Very mainstream sites -- such as UCLA -- ARE deploying IPv6 connected mail servers.

Even If You Decide You Aren't Going to Do IPv6, You Still Have Some IPv4 Things To Think About

- Some sites, already stretched thin just trying to cope with everything that's going on in the regular IPv4 Internet, may decide that they're going to punt on doing IPv6 at least for now.

- If that's your decision, and it is a perfectly understandable one, **you may still have IPv4-related things you should be attending to...**

"IPv4 Things" You Might Want To Be Thinking About/Working On During The Next 1000 Days

- **If you have a pending project that has a legitimate need for additional IPv4 address space, I would NOT wait to request that space** (although some believe that it may already be too late for you to successfully get additional "large" netblocks at this time). [If you don't do IPv6, the sufficiency of your IPv4 address supply will be doubly important to you in the future!]
- **If you have any legacy netblocks that your company obtained during the pre-ARIN "Postel era" (e.g., prior to 22 Dec 1997), review the ARIN Legacy Registration Services Agreement** (see www.arin.net/resources/legacy/). If your company decides that it wants to sign the Legacy RSA, do so before 30 Jun 2010. *Please note that I'm not expressing an opinion about whether you should or shouldn't sign the Legacy RSA -- that's up to you.*

Legacy IPv4 /8's As Potential Acquisition Targets?

- Speaking of legacy allocations,you should be aware that various commercial entities have legacy /8 allocations, including GE (3/8), Level3 (4/8), IBM (9/8), ATT Bell Labs (12/8), Xerox (13/8), HP (15/8), Digital (16/8), Apple (17/8), Ford (19/8), CSC (20/8), Halliburton (34/8), PSI (38/8), Eli Lily (40/8), Prudential (48/8), duPont (52/8), Cap Debis CCS (53/8), and Merck (54/8). See http://www.iana.org/assignments/ipv4-address-space/
- As IPv4 address exhaustion occurs, some of these companies may become attractive targets for potential merger and acquisition activity -- **not** because of their products or facilities or personnel or patents per se, but simply because of the large blocks of address space they control! Even "just" /16's may be a "big deal" in the future. **Should you be considering corporate "poison pill" measures to protect any large allocations of address space you control?**

Hopefully, Though, Most of You Are/Will Be Moving Ahead with IPv6

- I think (and hope!) that most of you are here today because you want to move ahead deploying IPv6.

- The rest of this talk is based on that assumption.

Address Space and Connectivity

- If you're an ISP, have you requested provider independent IPv6 address space yet? The process for doing this from ARIN can be found at www.arin.net/resources/request/ipv6_initial_alloc.html

  Have you reviewed your peering and/or Internet transit providers (if any) to determine which if any of those are ready and willing to provide IPv6 connectivity for you and your customers.

- If you're a sender or product vendor, have you talked with your Internet transit provider (e.g., your upstream ISP) about getting IPv6 address space and IPv6 connectivity? If your upstream ISP isn't doing IPv6 (yet), what are their plans for doing so? If they aren't ready to support your needs, do you want to change ISPs or add an additional ISP which is IPv6-ready, or do you want to arrange for an IPv6 tunnel from an IPv6 tunnel broker?

Tunnel Brokers

- While native IPv6 connectivity is definitely preferred, tunneled IPv6 connectivity may temporarily suffice for testing and development work while your normal provider comes up to speed.

- Wikipedia has a list of IPv6 tunnel brokers broken out by region, see http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers

- Tunnel brokers may vary in reliability and connectivity quality. I would urge you to be careful about using tunneled connectivity for production purposes.

All That Said, What's Newsworthy From the Larger IPv6 World?

- I wanted to also take a little time to talk about some of the IPv6 things that have recently been happening.

DNS Block Lists Are Starting to Add Support for IPv6

- There is now at least one DNS block list with the ability to support IPv6 addresses, see http://virbl.bit.nl/index.php#ipv6

- We can also chat a little about some of the implications associated with blocklisting IPv6 addresses, including:

  -- does it make sense to block individual /128's?

  -- implications of Windows IPv6 using Privacy Addresses by default

  -- will we even need IPv6 blocklists? or will we be using IPv6 whitelisting instead?

If You Weren't Seeing Enough IPv6 Traffic…

- Youtube is now available via IPv6 for sites participating in the Google IPv6 access program:

  http://news.cnet.com/8301-30685_3-20000052-264.html

ISPs are Moving Ahead With Consumer IPv6

- For example, Comcast has announced IPv6 pilot plans:

  http://www.comcast6.net/volunteer.php

- How about your ISP?

The Research and Education Communmity Is Also Deploying IPv6

- Some campus deployment stories:

  University of Pennsylvania
  www.internet2.edu/presentations/jt2010feb/20100201-huque.pdf

  University of Hawaii
  www.internet2.edu/presentations/jt2010feb/2010
  0201-whinery.pdf (URL split due to length)

- DREN, the Department of Defense Research Network, also has some interesting IPv6 deployment insights:
  www.internet2.edu/presentations/jt2010feb/2010
  0202-broersma.pdf (URL split due to length)

Some Things Are Still Stalled

- Although stateless autoconfiguration can work fine for assigning IP addresses to consumer hosts, many ISPs believe that they need DHCPv6 for scalable and accountable customer IP address assignment and configuration.

- Although DHCPv6 works fine for some operating systems (such as Windows Vista), I'm still not seeing any discernable progress when it comes to convincing Apple to support DHCPv6 for MacOSX. External DHCPv6 implementations (such as Dibbler) are available for the Mac, but that isn't a scalable model for average consumers.

Hidden Subtleties Are Still Being Discovered

- As part of the process of developing a draft IPv6 anonymization policy for netflow data that Internet2 will be collecting and sharing with researchers, I've developed a much greater appreciation for some of the subtleties associated with IPv6 addresses. Anonymizing IPv6 in a releasable way is far more complicated than anonymzing IPv4 data.

- If you're interested, feel free to see: http://www.uoregon.edu/~joe/ipv6-mask.pdf

Making Pure IPv6 (More) Possible

- Many sites would like to be able to offer IPv6 (only) networks. However, the sticking point preventing that has historically been "how do we offer IPv6 only customers access to IPv4 only websites (and other IPv4 only content)?
- One solution that some have experimented with is IVI, however that product has not proven to be fully satisfactory for a variety of reasons.
- Fortunately, there's a new option: Viagenie has announced the availability of two NAT64-DNS64 open source implementations (see http://ecdysis.viagenie.ca/) which might be of interest to those who aren't excited by IVI as a technology for making IPv4 content available to IPv6 *only* networks

Discussion/Questions