IPv6 in Amateur Radio

Bryan Fields, W9CR
St Petersburg, FL • bryan@flscg.org • M:727-409-1194

Abstract

A historical overview of legacy Internet protocols and their limitations will be presented here. IPv6 is the internationally-recognized standard replacing these protocols. A short introduction to IPv6 and a case for its support in the amateur radio community is lacking. Finally an overview of the coming IPv6 deployment in HamWAN Tampa Bay is presented as a study of deployment for use by radio amateurs. Some background in IPv4 and Internet protocols is assumed.

Table of Contents

Introduction to Internet Protocol Use

The Internet currently speaks a common protocol suite known as Internet Protocol Version 4, commonly known as IPv4. This has not always been the case, as many networking protocols exist and have been run on the Internet. Prior to Flag Day (Jan 1, 1983) Network Control Protocol was the protocol in use. NCP had many limitations and the up-and-coming IPv4 protocol was chosen to replace it. On Flag Day all NCP connections were shut down and IPv4 connections brought up to replace it. In less than 24 hours the entire Internet switched protocols!

Such a massive change today would be impossible.

Currently the Internet is facing major limitations to IPv4:

- Address space, only 4.3 Billion address possible, 7.4 billion people in the world[1]
- Performance issues (Difserv)
- Security and authentication
- Deployment configuration
- Routing table bloat
- Unequal distribution of address space across the globe

History of IPv6/IPv4 end times

IPv4 was originally designed in the early 1980's with it being formally codified in RFC 791[2] in 1981. At the time a common computer on the Internet was a 36bit PDP or Honeywell system with 10MB of disk and a megabyte of memory. The decision was made early on[3] to use 32 bits for address space, which was thought to provide a virtually unlimited amount of space for the dozens of sites on the Internet.

Of interest to Amateur radio operators is RFC790[4], the assignment of numbers. This is the first official record of 44/8 being given to AMPRNET on behalf of Hank Magnuski, KA6M. This small request at the time endowed amateur radio with an amazing resource now worth hundred of millions of dollars. ARDC is the current owner of this block and after many years they are allowing some limited use of this for amateur radio operators directly on the Internet.

Fast forward a bit to the early 90s and the Internet has taken off; it's no longer for research only. Commercial users have taken over and individual users can buy access over 9600 baud Unix shell dialup for 24.99 per month. Packet radio is booming and amateur radio is defining state of the art. There are some initial rumblings about eventual exhaustion of IPv4 number space on the Internet and the ever-important growth of routing tables on the limited IP routers of the day.

---

[1] http://www.worldometers.info/world-population/
[2] https://tools.ietf.org/html/rfc791
[3] http://dltj.org/article/vint-cerf-ip-addressing/
[4] https://tools.ietf.org/html/rfc790

IPv4 allocation is managed by Jon Postel[5][6] on a classful basis; A, B or C blocks. There is writing on the wall that class B IP space will be exhausted in a few years. Work is started at the IETF to develop a solution to this; many ideas are proposed with Classless Inter-Domain Routing [7] being the winner. The CIDR (pronounced cider as in the fermented apple drink) solution does away with the concept of classful addressing and breaks space down based on bit boundaries. An organization could now request a /19 from IANA rather than a class B block (/16) to use for connections on the Internet.

The problem now turned to routing as the protocol of the day, the Exterior Gateway Protocol (EGP) does not support CIDR blocks. It lacks a number of features and a redesign is being worked predating CIDR. The replacement routing protocol would be known as Border Gateway Protocol (BGP). This is standardized in 1994 as BGP version 4[8] with Cisco supporting it in IOS version 10.0. The Internet switches to using this protocol in a mater of months. This protocol is still used to for routing on the Internet, over 20 years later.

The Internet is still growing at an exponential rate, and for the first time global routing table growth is becoming a major issue. The GRT is the table of all active IP allocations on the Internet maintained by a router on the Internet. Every directly attached router must keep a full table (in some cases multiple copies) of these routes in a special area of memory. By 1996 the 64k route boundary was crossed and it was still climbing. Most router vendors are barely able to keep up by releasing new routing engines supporting this growth.

Contributing to this is the piecemeal way in which IPv4 is allocated. Rather than get a /16 and announce a single route, most sites started off small with a /19 and get another and another until they have eight /19's (equivalent in number of addresses to a /16). Something has to be done, and the IPng, "IP the Next Generation" working group is started at the IETF to study replacing IPv4 with a new protocol. Unfortunately routing table growth continues to grow exponentially.

In December 1995 IPng was released to the world as Internet Protocol, Version 6[9]. This is commented on and extended over the next few years, reaching production quality in 1998. Linux adds support for IPv6 in Kernel 2.1.8 in the end of 1996. The general consensus is the Internet will move to IPv6 by the early 2000's.

IPv6 is not an extension to IPv4; it is an entirely new protocol. This means IPv4 and IPv6 nodes can't talk directly to each other. The migration strategy proposed is called "dual stack", meaning each router and end node will run IPv4 and IPv6 address space at the same time. This ensures connectivity for both protocols, as IPv4 would continue to be used for the next couple years, and plenty of IPv4 was available to dual stack. As the mass migration to IPv6 didn't materialize, most users were stuck in an IPv4-only world. Making matters worse, most routers and networks of the day offered abysmal

[5] https://en.wikipedia.org/wiki/Jon_Postel
[6] https://tools.ietf.org/html/rfc2468
[7] https://tools.ietf.org/html/rfc1519
[8] https://tools.ietf.org/html/rfc1771
[9] https://tools.ietf.org/html/rfc1883

IPv6 performance when compared to IPv4 performance. This performance gap existed until 2014 and still presents itself in some edge cases to this day.

Making matters worse, 1996 saw the development of a technology called Network Address Translation, or NAT. This allowed a router to use one public IP or block of IP's and translate it so hundreds of nodes behind it could access out to the Internet. For the first time the Internet is now utilized with uni-directional connectivity. A node behind a NAT can access other nodes on Internet but cannot be accessed from the Internet. This breaks multiple protocols and forces all new peer-to-peer applications to engage in NAT transversal. In many cases a helper server on the Internet must be used to connect users behind a NAT. For the first time, the core goal of end-to-end network connectivity is broken on the Internet, though NAT does slow IP address consumption slightly.

The dot com crash of 2000-2001 causes IPv6 to take a back seat once again as the pressure on IPv4 has been reduced in the US. IPv4 is running and being deployed at a break-neck pace in Asia during this time. IPv4 address limits are well known in Asia and Europe as these areas of the world received about ¼ the IPv4 space allocated to the US. Asia is one of the early adopters of combining IPv4 NAT and IPv6 (NAT-PT) to their customers. <u>For the first time a real IPv4 address on an Internet connection is now an additional cost</u>.

The writing is on the wall, but many US-based users still have no interest in IPv6 deployment, and most users cannot get IPv6 even if they want it. Most ISP's have cut back and started to charge for static IP service. Some smaller US ISP's start to deploy NAT by default. Cellular networks go default NAT in, the exceptions being the larger carriers. An example for this in the cellular space is Alltel. Alltel has 40M subscribers, with 22M active data users; even using the entire 10/8 IPv4 space they do not have enough IP's for their customer base. The only solution for a provider of this size is public IPv4. Most can still get IPv4 from the RIR's, but it's become much harder to justify and more scrutiny applied to the applications with ARIN.

"I don't need IPv6; I'll be dead by time I need it." is a common phrase heard. In 2008 IANA and RIR's develop a policy for IPv4 exhaustion. The plan is when IANA gets down to five /8's in the unallocated pool it will give one to each of the five RIR's and be out of unallocated IP space. ARIN begins to draft policies related to IPv4 run out for its members and starts a named transfer process, where a holder of addresses can designate a given recipient of a transfer. This officially starts the IPv4 marketplace.

On Monday January 31, 2011 IANA allocates two /8 blocks to APNIC. This leaves five /8 blocks left in the free pool, triggering the run out plan at IANA. On Thursday February 3, 2011 IANA makes the announcement "**The IANA IPv4 Address Free Pool is Now Depleted".**[10] The RIR's still have IP space, but its limited and finite. ARIN has 2.5 of /8's available of IPv4 for allocation and triggers its policy preventing anyone from requesting an initial allocation larger than a /22. Existing members may continue to receive IP blocks based on what can be justified in the next 90 days. Legacy IP space (those allocated by Jon Postel) commands a premium in the IPv4 market as it's owned rather than assigned. The 44/8 AMPRNET block is one of these legacy address blocks.

[10] https://www.arin.net/vault/announcements/2011/20110203.html

By April 2014 ARIN has reached its last /8 of IPv4. This triggers the end phase policies and a /24 is now the smallest block which can be requested and the largest which can be requested initially. In June 2015 ARIN has its first unable-to-allocate issue, meaning a justified request for a /17 block from a larger ISP is unable to be filled. In June I'm approached at NANOG 61[11] in 2014 by an IPv4 brokerage service asking about the AMPRNET 44/8 allocation. This was completely unsolicited; they had researched me as I am on the ARDC technical advisory committee. Things are getting weird!

On Thursday September 24, 2015 the ARIN free IPv4 address pool reaches zero. At this point no further IPv4 is available, even if justified, and requests are wait listed in the event it becomes available. IPv4 brokerage services and auction sites take over trading IP space as a commodity.

With the exhaustion of IPv4 there is no way we can extend it again and buy time. We must migrate and support IPv6; the can cannot be kicked farther down the road.

IPv6 to the rescue

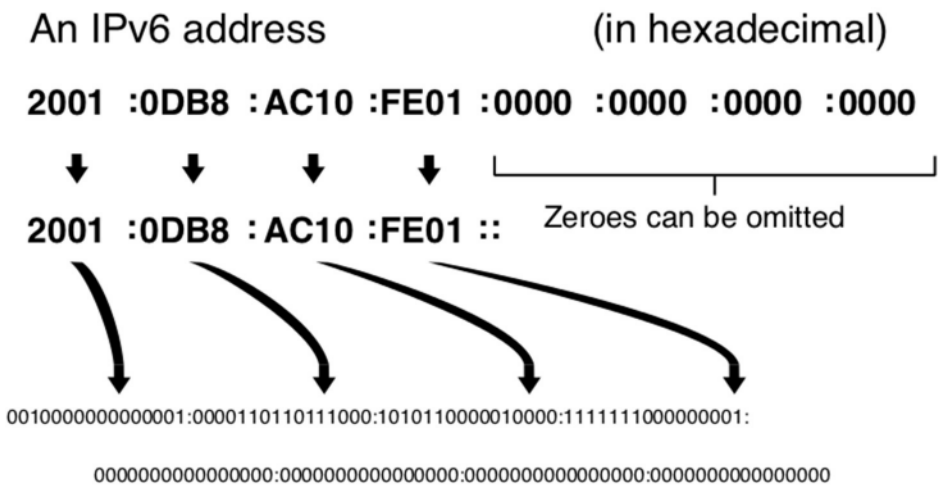
Clearly there must be a path forward here and it's IPv6. There are many who debate it still but it's the globally agreed and deployed standard.

IPv6 improves on IPv4 by quadrupling the address space to 128 bits. This gives 2^128 = 340,282,366,920,938,000,000,000,000,000,000,000,000 IPv6 addresses, an unfathomable number. Put another way, there are 100 IPv6 address for every atom on earth.

In actuality, based on how IPv6 is deployed we typically only use 64 bits as a network, with 64 bits for the host address, a subnet, known as a /64. Each person on earth still gets 10^8 subnets using this method of subnetting. It's a big, really, huge amount of space. IPv6 supports VLSM and it is possible to use a /127 as a point-to-point interface if needed.

The typical IPv6 address is expressed in hexadecimal format with colons separating 2 bytes. Example: 2603:2880:FFFE:0000:0000:0000:0000:0035. The extra padded 0's can be omitted as follows 2603:2880:FFFE::35. You're allowed to do this once in writing an address and all systems will expand this to the full address.

[11] https://www.nanog.org/meetings/nanog61/home

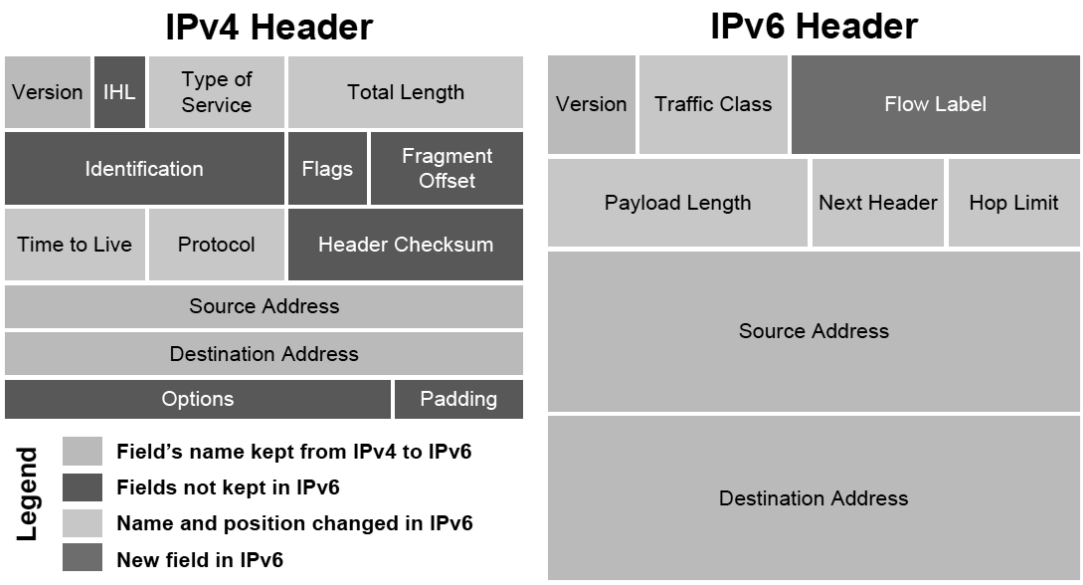


IANA will allocate the RIR's a /12 worth of IPv6 out of the global IPv6 space (2000::/3)
A RIR will allocate a /32 to an ISP, and each ISP will then allocate a /48 to their directly attached customers. This provides the possibility that over a billion service providers are able to be supported out of a RIR's pool, each with 65536 customers getting a /48. Some larger service providers qualified for much larger than a /32, receiving as much as a /19.

Difference From IPv4

IPv6 has a number of differences from v4, and most are designed to speed up communications on the faster connections of today. IPv4 was designed in a time when backbone links were 64k circuits and IP packet forwarding in hardware was thought to be impossible. Today, backbone links are 100g, with 400g and terabit Ethernet coming soon.

Of course the first difference expected is the expanded address space. Per-hop segmentation is removed between transport routers letting end nodes manage the path MTU, rather than each router along the way needing to perform this. The IP layer checksum is removed as Ethernet provides this, and the header format is simplified. As the header is aligned at 40 bytes with additional headers being "popped" into the stack, allows routers to process IPv6 in custom silicon. IPv4 by contrast has headers and optional information inserted into the existing headers. A router has to buffer the entire packet before it makes a routing lookup for that packet. In IPv6 the rest of the packet can still be coming into the router while it starts performing a lookup on where to send it.

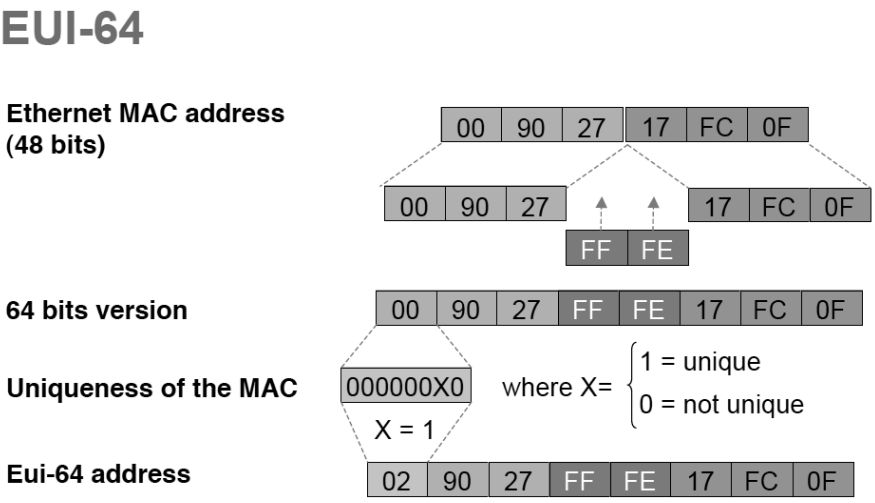


IPv6 is aligned at 64 bits for the subnet and the host portion of the address. This is known as a /64 and is the smallest typical subnet most will see in IPv6. Even point-to-point connections should utilize a /64 even though a /127 is legal. There are some advanced reasons to avoid these small subnets but the most compelling is that auto-configuration only works on a /64 subnet.

IPv6 supports a much larger Maximum Transmission Unit (MTU) than the 64 byes of IPv4. 1280 is the smallest link MTU supported by IPv6 and it expects the end nodes to handle path MTU if the MTU is greater than 1280 bytes. This is of interest to developers as PMTU can be ignored if all packets are kept under 1280 bytes. On the opposite end, packets up to 2^32 bytes are supported; however the need for these "Jumbograms" is not apparent as of yet.

Auto-configuration of addresses is part of the protocol[12]. A router on a subnet announces a prefix and the client uses its MAC address to create a EUI-64 address. This only works on /64 subnets and is the main reason IPv6 should be deployed using only /64 subnets. A router or groups of routers announce a prefix on the networks, and node is able to request an address on that network based on its MAC address. This is independent of any higher-level protocol (i.e. DHCP) and works at the network layer. A mesh wireless network would be able to auto-configure in this manner and never worry about the IP address conflicts which happen in IPv4.

[12] https://tools.ietf.org/html/rfc2462



Broadcasts are dead in IPv6, replaced by multicast. This means the ARP protocol from IPv4 would not work; its been replaced with Neighbor Discovery[13] to build a table of IPv6 to MAC address mapping on the local interface. The elimination of broadcast traffic secures against broadcast storms that can cripple attached networks in IPv4.

Security and authentication is built into the IPv6 protocol. This is known as IPSEC and could be a whole book (and is) itself. While encryption is generally not legal over amateur radio frequencies, there is nothing preventing cryptographically-secure authentication. What this mean is we can tell if the data has been modified or is from a trusted source. The data is not encrypted, but rather authenticated as being from a given sender. This is ideal for management of amateur equipment over radio networks.

Types of Address space in IPv6

Unique-Local is defined as FC00::/7 and it's designed to be analogous to RFC1918 space in IPv4. This space is intended to be used in an organization and is not routable on the global Internet. There is debate as to the usefulness of this space as most users can easily get IPv6 space from their providers and upstream.

Link-Local is perhaps the most interesting of the IPv6 address we can use in amateur radio. A link local is an address valid only on the link, its not globally significant. These addresses are under FE80::/10 and can be used for direct layer 3 connections to a neighbor on the same network segment. This uses the EUI-64 based addressing as described above.

Linux (and most operating systems) for example will have a link local IPv6 address present on all interfaces by default. This is very handy for network management in the event connectivity is lost or autoconfiguration fails. I have used this to secure shell hop-by-hop through a network of Linux

[13] https://www.ietf.org/rfc/rfc2461.txt

servers to restore IPv4 configurations on the interfaces. At the time I was over 1500 miles away and our console server was offline. IPv6 saved the day due to Link-Local addressing.

Global-Unicast address space is what most users will receive from their ISP and in keeping with its name is globally routable. IANA has allocated 2000::/3 as this space (2000:: - 3FFF::) to be handed out to regional internet registries and then onto ISP's and onto customers. When an amateur radio user makes use of IPv6 these are the address they will be using.

Multicast address space works almost the same as in IPv4 and is allocated from FF00::/8. The addition of a scope bits to the address specifies if the scope of the multicast group. A multicast address can be scoped valid over a Link, a Site, an organization, or globally. The scope bits are in the second byte of the multicast address. FF02::9 would mean it's a multicast address valid over a scope, in this case the RIPng routing protocol address. FF08::4 would be an organizationally valid address which could be use network wide in amateur radio, perhaps an audio stream.

DNS

DNS is expected to be a must-have in IPv6. Most skilled network engineers will be unable to remember IPv6 address, even for testing. This means we must have DNS as a core deployment of IPv6 and have the address in use registered in the DNS server.

DNS adds a new record type AAAA for IPv6. This is the same as an A record for IPv4, and most resolvers will return both if available.

The PTR record is the same, however the format is a bit different. Each hex digit in the address has its own field in DNS. An example is 2006:bd8:c18:1::2 would be looked up as 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.8.b.d.0.6.0.0.2.ip6.arpa. in DNS for the PTR record. Note the ip6.arpa. zone for IPv6.

It's common to provide reverse DNS for all IPv4 addresses live or allocated in subnets on the network. Currently there are hooks to do this as real assignments are given out via DHCP, but you must define each address in the reverse zone file. While this is easy to script for IPv4, a zone file for a single /64 would be around 400 EiB. Most deployments only provide reverse lookups for real hosts do to this. There are some drafts[14] addressing this but it's still open as to how it will be deployed.

Why not NAT?

"NAT is evil" or so the saying goes in the industry. Here is a small listing of what NAT breaks and why its not a solution to IPv4 run out.

- NAT breaks the fundamental precept the Internet was designed on: end-to-end connectivity between all nodes
- NAT is not adding real security (a statefull firewall would)

[14] https://tools.ietf.org/html/draft-ietf-dnsop-isp-ip6rdns-02

- NAT must maintain a state, and there are timeouts to this. An inactive SSH session will be closed depending on the settings of the NAT device
- NAT obscures the source of connections (could be a good or bad thing)
- Carrier Grade NAT breaks inbound connections with no control over port forwarding. Have you seen SIP phone where you can dial out, but can't receive calls?
- Scaling of NAT is hard to do. An ISP deploying NAT will be looking at millions of dollars in equipment just to cope with not having enough IPv4 addresses

What does this mean for amateur radio

Amateur radio has 44/8 and plenty of IPv4 space for the foreseeable future in building out packet networks or other high-speed networks such as HamWAN. This allocation is very special and after many years, the organization in control of it is allowing hams to make use of it directly. HamWAN Tampa has a /21 of IPv4 from this space, and various other users have anywhere from a /24 to /16 worth of 44net space.

However in the increasingly interconnected station and remote control nature of radio, we must support IPv6 going forward lest we get left behind. The global nature of amateur radio dictates this, as many areas of the world are going to see their access to the IPv4 Internet fade due to deployment of Carrier Grade Nat (CGN) breaking end-to-end connectivity. This will make it impossible to communicate directly with applications needed by most amateur radio operators.

For example AllStarLink requires a public IP or control over inbound port mapping in a NAT environment. As CGN is done by the service provider, the end user cannot request port forwarding and thus cannot link into the Allstar network. Had this application supported IPv6, it would have made use of the IPv6 address assigned and would work.

All amateur vendors and even developers must start supporting IPv6 if we are to lead technically in digital communications. We must demand this of our vendors and ask them for this support. The solution of running over a VPN overlay is not ideal and should not be accepted as a work around for new products. The support of IPSEC and secure authentication could be leveraged using LOTW certificates as keying for the authentication of data on the air.

Current state of IPv6 support in Amateur radio

Sadly most application amateurs use are not supporting of IPv6 even if the underlying OS is. A brief survey finds most ham radio Internet applications are unable to utilize IPv6. Most vendor websites do not publish an AAAA record and a small sampling are below:

Websites:

- ARRL website, not reachable on IPv6
- FCC.gov is reachable on V6
- Hamwan.org is reachable on v6
- TAPR.org not on v6
- remotehamradio.com not on v6

Remote control software:

- Flexradio – No support for v6
- Allstar – No support for v6
- Remoterig RCC control products – No support for v6
- Remotehamradio, perhaps supports v6 now?

The last one, remote ham radio, is interesting as they offer an iPhone app for operating. Apple has made IPv6 support a requirement of any app sold in the app store. You cannot get an app certified which does not make use of IPv6 properly.

Most embedded systems and OS stacks support IPv6 in some capacity or have a library to support it. Developers need to take advantage of such libraries and support IPv6 on their products. In 10 years we may be running a VPN simply to maintain connectivity with old outdated systems such as these. If you're a developer working on a new device, please check into IPv6 support. The hardest part of it in most existing platforms is learning about it, writing code to take advantage of it is as simple as writing for IPv4.

Support in Amateur Radio Networks

BBHN – Not currently, though some planning is taking place[15] they don't intend to implement this anytime soon.

ARDEN – Have no plans published for IPv6 at this time and they force everything via NAT. Reference the NAT is evil section above and you'll have to agree this is not the way forward. It's a shame, as they would benefit from the automatic addressing provided by IPv6. Imagine ARDEN with end-to-end connectivity using IPv6 and NAT for IPv4 connectivity, this would be an ideal compromise with their stated goals.

IPv6 over AX.25 – There is some use of IP over slow packet radio still, but IPv6 has not been deployed in any documented manner. There is not a reason why it couldn't work, but at 9600 bit/s it's to slow by contemporary standards.

HamWAN – There is no reason HamWAN based networks cannot deploy IPv6 today. Seattle HamWAN has dual stack partially deployed and clients receive an IPv6 address if they support it. A deployment strategy for HamWAN Tampa Bay is discussed in the next section.

AMPR – also known as ARDC (Amateur Radio Digital Communications)[16], is the holder of the 44/8 IP block. It would be logical for ARDC to obtain a /32 or greater for amateur radio use and could then delegate this space in hand when handing out 44net allocations to hams. The issue here is planning for IPv6 was done long ago and ARDC would not permit 44net space to be used on the Internet until ~2009. As ARDC operates a bit like a RIR for amateur radio it would be logical to have an allocation

[15] http://www.broadband-hamnet.org/section-blog/36.html
[16] http://www.ampr.org/

from IANA, which would be unprecedented. Perhaps this could be obtained from ARIN, as ARDC is based in California, but there is a yearly cost associated with this. ARDC would need to revisit its management and bylaws, as they are not structured well in this author's opinion, to uphold the needs of amateurs. Of the five members on the board, only one is a licensed amateur radio operator[17], and there are no provisions for the amateur members to vote for board members.

I write this as a call to reform as amateurs generally have no way to obtain IPv6 space for themselves other than through their upstream service providers.

An IPv6 Strategy for HamWAN

Discussed below is a high-level numbering design for HamWAN type networks focusing on IPv6. It's assumed IPv4 is running already, and this will be a true dual stack design.

Background

HamWAN Tampa is currently a single site network covering most of Tampa with plans to grow in the near future into Pinellas County. We can deliver a 20-30 Mbit/s connection almost anywhere in our coverage area with clear line-of-sight to our prime site in downtown Tampa.

All client radios will receive a 44.98.248/24 IP and bridge into the common Vlan on the network. HamWAN Tampa Bay's network is a bit different than the Seattle network in how we manage our connections to the AP's. In our network the AP's trunk to a switch and share a common client Vlan

[17] http://www.ampr.org/about/who-we-are/

40, and have management in Vlan 20. HamWAN Seattle uses routing on the AP's assigning /28 blocks to each AP, and then converges the network to their core using OSPF. Our design makes better use of IP space as the 3 AP's are able to share a single /27 for user and management space.

IPv6 Numbering Plan

Our switch handles DHCP for IPv4 and would be doing SLACC for IPv6 if enabled. As AMPRNET does not have IPv6 space we received 2607:f3f0:2::/48 from our upstream provider routed to our switch on 2607:f3f0:0:2::14/124. Note the provider chose the interface IP for us; they are not using /64's as suggested by the standards.

For the HamWAN clients we'd like to do a bit more than simple SLACC and hand them space in a shared /64. Larger providers are moving to a solution known as Prefix-Delegation[18] which hands out configuration to the client via DHCPv6. This will not only assign name servers and routes, but also assign an IPv6 prefix and route it to the end user router. In this way the user gets a subnet they can use on their network(s) on the other side of their router/firewall. As there is no concept of IPv6 NAT (and NAT is evil) this ensures end-to-end connectivity for a customer with out them having to renumber their networks.

Our plan is to subdivide our /48 into /52's on a per-site basis, giving us 16 possible sites. If we exceed this we can request another /48 from our upstream. This makes it very convenient to divide on a nibble boundary (4 bits) from a readability perspective. Note how the high nibble signifies the subnets in the abbreviated table below.

```
2607:f3f0:0002:0000::/52  Site 1    2607:f3f0:0002:c000::/52  Site 13
2607:f3f0:0002:2000::/52  Site 2    2607:f3f0:0002:d000::/52  Site 14
2607:f3f0:0002:3000::/52  Site 3    2607:f3f0:0002:e000::/52  Site 15
2607:f3f0:0002:4000::/52  Site 4    2607:f3f0:0002:f000::/52  Site 16
```

Industry practice seems to be leaning to giving a client a /56 or/60 for their needs. We are planing to use a /60 as this is 16 /64 subnets for the client use. Note how this aligns on a nibble boundary as well. If we take 2607:f3f0:0002:4000::/52, this would give us 256 networks to delegate to clients, but we'll be reserving one for site use, making the total clients we can serve 255, and we'll run out of IPv4 before we ever see 255 HamWAN clients on a single site.

Site example 2607:f3f0:0002:b000::/52 > /60 for clients:

```
Network                 - 2607:f3f0:0002:b000:0000:0000:0000:0000 - INT
Network                 - 2607:f3f0:0002:b010:0000:0000:0000:0000 -
Network                 - 2607:f3f0:0002:b020:0000:0000:0000:0000 -
Network                 - 2607:f3f0:0002:b030:0000:0000:0000:0000 -
SNIP
Network                 - 2607:f3f0:0002:bfc0:0000:0000:0000:0000 -
Network                 - 2607:f3f0:0002:bfd0:0000:0000:0000:0000 -
Network                 - 2607:f3f0:0002:bfe0:0000:0000:0000:0000 -
Network                 - 2607:f3f0:0002:bff0:0000:0000:0000:0000 –
                                                  ^^
```

[18] https://tools.ietf.org/html/rfc3633

Note how the two bytes change in this, clearly showing the range of the /60 for each client. The INT network is used for networking at the site.

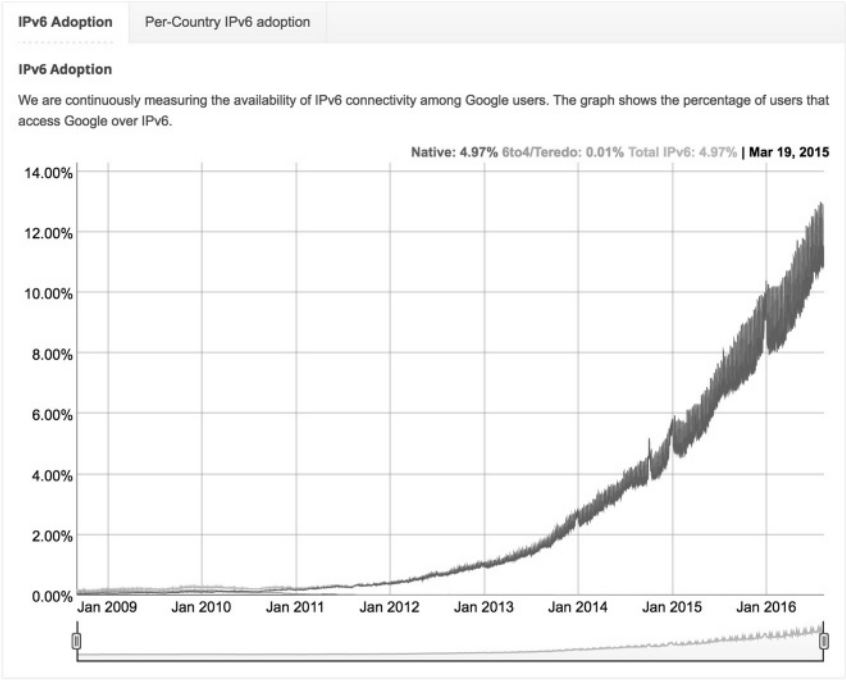
On-site networking will be in the 2607:f3f0:0002:b000::/60 with 2607:f3f0:0002:b000::/64 assigned to the local Vlan40 for client use/SLACC, and 2607:f3f0:0002:b001::/64 assigned for Vlan20 for management. Point-to-Points and uplinks to other sites will go over 2607:f3f0:0002:b002::/64 to 2607:f3f0:0002:b00f::/64. Notice how using a nibble boundary gives an easy-to-identify network.

The next part to deploy this numbering plan would be to configure the DHCPv6 server, which is beyond the scope of this document. Typically ISC DHCPd is used and there are a number of documents showing how to configure prefix delegation on the Internet. It's also possible to enable the DHCP server on Junos[19] and IOS. In any event, the router/switch the clients are bridged into must have DHCPv6 relay enabled pointing back at your DHCP server. This will relay the DHCP requests to the server if it's not local on the network segment.

Parting thoughts

This was not meant to be a step-by-step implementation plan but a rough guide providing background on how to choose IPv6 numbering plans for both client and administration ease. There is much that goes into operating a network and number planning is a small but important part of it.

IPv6 is exploding after many years of only consisting of ping and traceroute traffic on the Internet. The images below are Google's view of IPv6 Traffic to their servers over the past couple years.



[19] http://www.juniper.net/documentation/en_US/junos12.3x48/topics/example/security-dhcpv6-server-option-configuring.html

Almost every smart phone has IPv6 enabled on it today, and some of the largest IPv6 networks are in cellular providers. Apple will not allow apps in its store that do not support IPv6.

It's of critical importance that we as amateurs learn about IPv6 and demand support of it from our vendors or include support in our own projects. The future of communications depends on it.