IPV6 FOR AMATEUR RADIO

DANIEL ESTÉVEZ, EA4GPZ / M0HXM

Abstract. Amateur radio operators have allocated the IPv4 AMPRNet block 44.0.0.0/8. This is routinely used to support several operational networks and experiments, such as the Hamnet. With the increasing exhaustion of IPv4 address space and the goal of using and advancing state-of-the-art technology, it seems appropriate to start using IPv6 for this kind of Amateur activities. This paper gives a proposal of how to distribute IPv6 globally routable address space for Amateur radio use. We also explain some of the advantages of using IPv6, in comparison to the current IPv4 scheme.

1. Introduction

Currently, Amateur radio operators have the IPv4 AMPRNet [1] block 44.0.0.0/8 allocated for use in all kinds of Amateur radio related activities, such as organizing computer networks which run partially or completely over radio frequency links, and partially over the internet, or doing research and experimentation related to TCP/IP networking. An example of a large network running over the AMPRNet allocation is Hamnet [2].

This large /8 block of IPv4 address space represents more than enough to cover the necessities of all the projects that have emerged, both now and for the forseable future. However, managing and using this IPv4 address space is not exempt of inconveniences, which in the author's opinion could be solved by using IPv6 addressing instead.

First of all, Amateur radio operators are required by the ITU Radio Regulations to identify their own transmissions with their callsign. An IPv4 network for Amateur radio should have a way to map IPv4 addresses to Amateur radio callsigns, since packets can eventually be routed through radio frequency links. However, IPv4 does not provide a good solution to this problem.

Currently, this is solved in an ad-hoc manner in most cases. The endpoints of a radio frequency link comply with the regulations by broadcasting their own callsign periodically, often piggybacking this information onto an existing discovery protocol such as CDP [3]. While this may seem enough to comply with the regulations, it is often impossible to identify which callsign originated a packet that is being routed through a radio frequency link. The only data at hand is the IPv4 source address, and it is only possible to map it into a callsign using an online database such as HamnetDB [4] in limited circumstances.

On the other hand, IPv6 provides an elegant way of mapping addresses onto Amateur callsigns. The 128 bit address length of IPv6 is so large than in many applications the network part of the address uses only 64 bits, while the remaining 64 least significant bits are left to identify the device. This freedom to construct an IPv6 address is used in many applications. An example of this is the SLAAC protocol [5], which allows devices to construct an IPv6 address using their 48 bit MAC address, simplifying IPv6 address configuration. The same freedom can be used both to construct an IPv6 address from an Amateur radio callsign and to map an IPv6 address following this construction to an Amateur radio callsign.

The second disadvantage is centralized management. Even though the 44.0.0.0/8 block is very large, as any shared resource, allocations of this block need to be managed centrally to prevent addressing conflicts. Currently, AMPRNet hands off large sub-blocks to countries, which in turn split their sub-blocks into projects or individuals. All this management is a time consuming process and is prone to disputes.

Here, the advantage of IPv6 is that the address space is so large that it is relatively easy for an individual to obtain a large block of address space for his own private and/or Amateur radio use. Many ISPs are giving off /48 or /56 blocks to individual customers (from which 2^{16} or 2^8 different /64 networks can be extracted, respectively), and it is also possible to obtain similarly large networks from tunnel providers such as Hurricane Electric [6] for individuals not having a native IPv6 ISP. This

Date: May 17, 2019.

makes it possible to construct a decentralized network where individuals or projects use their own IPv6 address space, rather than having to obtain it from a common pool allocated for Amateur radio. Thus, management costs and possible conflicts are reduced significantly.

Finally, another disadvantage of IPv4 is address exhaustion. While it seems that the Amateur radio community will manage to maintain the allocation of the 44.0.0.0/8 block for the near future, IPv4 addresses are by now a very scarce resource, and this large block represents a huge commercial interest. Several large organizations have relinquished unused address space that was allocated to them in the early times of the internet. Therefore, it is not impossible that the Amateur radio community might be forced to free out some of their IPv4 space.

Motivated by how IPv6 manages to solve these problems, and in the interest of advancing Amateur radio technology to the state-of-the-art by introducing IPv6 into our networks and experiments, this short paper gives a concrete proposal about how to manage the addressing of an IPv6 Amateur radio network.

The remaining part of this paper is organized as follows. In Section 2 we show how to encode Amateur radio callsigns into IPv6 addresses. Section 3 gives a description of the proposed IPv6 Amateur radio network, as well as it advantages in comparison to the current AMPRNet. An example of the configuration of a network site using the ideas given here appears in Section 4. Section 5 gives some instructions for people interested in joining the network. Some open research ideas are given in Section 6.

The paper is based on a text hosted in the author's blog [7], which in turn was based on some posts of the author in the 44net mailing list around 2016 outlining the proposal given here.

2. Encoding Amateur callsigns into IPv6 addresses

As mentioned in the Introduction, one of the key ideas of the proposal described in this article is that all the IPv6 addresses used for Amateur radio should encode a valid Amateur radio callsign. In this section we show how to do this.

Amateur radio callsigns are usually composed of up to 6 alphanumeric characters, so it is apparent that there is plenty of space to encode an Amateur callsign into the 64 least significant bits of an IPv6 address. There are several proposals giving concrete methods of how to do this [8, 9, 10]. In this paper, we consider [8], by Robert S. Quattlebaum, which seems the more complete proposal. However, the author believes that an Amateur radio IPv6 network should be agnostic to the method used to encode callsigns into IPv6 addresses. Each participating subnet should be free to choose its own encoding method, provided that this is consistently used and registered in some online database.

For the reader's convenience, let us briefly mention the most important features of the encoding method given in [8]. Amateur callsigns are first encoded in a BASE40 character set, which comprises alphanumeric characters, as well as '-' and '/'. This allows the formation of more complicated callsigns, such as EA4GPZ/P, EA/M0HXM, and also callsigns akin to the SSIDs used in AX.25 [11] to identify different equipment belonging to the same operator (for instance, EA4GPZ-7).

A so called *chunk encoding* is given to encode three BASE40 characters into 16 bits. This makes it possible to encode up to 12 characters in 64 bits, thus allowing most kinds of non-standard callsigns. There are certain advantages to using callsigns shorter than this maximum. For instance, all callsigns up to 8 characters long (and a few 9 character callsigns) can be encoded into a valid EUI-48 address. EUI-48 addresses are used as MAC addresses in several link layer networks, such as Ethernet. The possibility to encode Amateur callsigns into not only IPv6 addresses but also Ethernet addresses allows us to have identification directly at the link layer level and also to derive IPv6 addresses automatically by using SLAAC.

3. The IPv6 Amateur radio network and its advantages

3.1. **A network of whitelisted subnets.** Another important idea of this proposal is to try to eliminate centralization and management by requiring individuals and projects to obtain address space by their own means rather than taking it from a common pool allocated to the Amateur radio community. With the very large address space of IPv6, and given its current and foreseeable use, this is much more feasible than in IPv4. Note that this view is contrary to some ongoing developments in the Amateur radio community. For instance, the IARU R1 VHF Handbook [12] recommends that a global IPv6 allocation be obtained for Amateur radio usage. In the opinion of the author, requiring that each participant uses their own address space not only simplifies administrative costs, but also has some associated technical advantages, such as solving the problems with the source address filtering done by most ISPs.

Since the IPv6 Amateur radio network is not envisioned as any particular subnet of the globally routable IPv6 address space, there must be something that gives consistence to the network. The idea is that the network is formed by an aggregation of unrelated IPv6 globally routable subnets such that:

- The packets that originate from these subnets are valid for routing via an Amateur radio frequency link. In particular, the traffic originates from a duly licenced Amateur radio operator.
- Each of these subnets is using a certain mechanism to encode Amateur callsigns into IPv6 addresses as a means to identify the Amateur radio operator which originated the traffic.

Therefore, the element that gives consistence to the IPv6 Amateur radio network is a database of the participating subnets. This database is intended to be used as a kind of whitelist when determining if a certain IPv6 packet is fit for being routed through a radio frequency link, because both the source and destination addresses belong to one of the subnets in the whitelist. The database is quite simple. It only contains an entry for each subnet, with some metadata, such as contact details for the person in charge of the subnet, and also the encoding method that each particular subnet is using to encode Amateur callsigns into IPv6 addresses. In this way, anyone can find the callsign responsible for a particular IPv6 address in the network, by first looking up the subnet in the database and taking note of the encoding method, and then using it to compute the callsign.

By now, it is not so clear how to publish and maintain this database of whitelisted subnets. It seems that an online platform such as a wiki or custom web application could be appropriate. The author has also made some experiments by publishing the whitelisted networks using BGP.

3.2. **Reduced administration costs.** The maintenance of a simple database of subnets participating in the Amateur radio IPv6 network is a much simpler task than the allocation of the shared 44.0.0.0/8 block to interested individuals. Therefore, it seems likely that this method of constructing and administrating the network will reduce both the management effort and the conflicts significantly.

In the same spirit of "every individual contributes his own resources to the network", it is also envisioned that each participating subnet or individual manages DNS by his own means. Currently, the domain `ampr.org` is used for most AMPRNet related projects and applications. This also represents an added administration effort. Reverse DNS for AMPRNet addresses is handled by the same means as the `ampr.org` domain. It seems more appropriate that each individual or project manages DNS as deemed convenient, and obtains delegations for the reverse DNS from their ISP in the appropriate manner.

3.3. **Identification of Amateur traffic.** According to the ITU Radio Regulations as well as the Amateur radio regulations in many countries, all Amateur transmissions must be identified with the callsign of the transmitting station. Moreover, there are other limitations regarding transmission of information by Amateur radio means. For instance, most countries explicitly forbid *third party traffic*, which is understood as the retransmission of messages not originated by or not intended for a licenced Amateur radio operator. Since the Amateur service cannot be used with any pecuniary interest, the contents of the allowable messages are also somewhat limited in this respect. Finally, encryption of messages is forbidden both by the ITU Radio Regulations and by many countries (except in special cases of emergency). Encryption is so often used in networking protocols that some care needs to be taken to decide which network traffic is fit for routing over an Amateur radio frequency link.

Often, this problem is not solved properly. Little is done in many cases, by using ad-hoc solutions that have evident flaws. While it does not seem easy to develop an approach that is completely fool proof, IPv6 seems to offer some technical mechanisms that can help. First of all, the requirement that all the IPv6 addresses participating in the Amateur radio IPv6 network embed the callsign of the operator responsible for that device and transmission serves both to satisfy the requirement of identification of Amateur transmissions and to prevent third party traffic. By making sure that a certain IPv6 packet has a source and destination address belonging to Amateur operators, we can be sure that its payload is not to be considered as third party traffic.

Clearly, some degree of trust is put on the people participating on the network. This scheme only works well if IPv6 addresses belonging to the Amateur radio network are used solely for Amateur radio purposes (i.e., for transmissions acceptable for the Amateur service, in particular, not having any pecuniary interest or encryption). In any case, the addressing scheme also serves as a way of separating Amateur and non-Amateur equipment in the network of an Amateur operator. Both kinds of equipment often share a home network. By dividing such network into two subnets and only publishing one in the Amateur radio whitelist, the distinction between non-Amateur and Amateur traffic is simplified.

Additionally, the whitelist can also be used to distinguish which online services can be accessed only by licenced Amateur operators. For many online applications, in particular those that may cause radio frequency transmissions, such as joining a repeater voice-over-IP conference or operating a club transceiver remotely, it is necessary to identify the user as a licenced Amateur operator. There is no readily available solution for doing this, and each service resorts to its own method, which usually involves maintaining a database of logins for allowed users.

On the other hand, there are also many uses that can be offered to the wide public over the internet, both as a way of showing Amateur radio publicly and for a matter of convenience. Some examples of these are WebSDRs or listening to a repeater voice-over-IP conference (without transmitting).

Services of these two types are often mixed and it is an added burden to separate which parts need authentication and which do not, besides implementing an appropriate authentication method. The IPv6 Amateur radio network can simplify this division. Services that require a licenced Amateur operator can be configured to be accessible only from whitelisted IPv6 subnets belonging to the network.

3.4. **Source address filtering.** Another technical problem that affects the current AMPRNet is that of source address filtering. Most ISPs will drop uplink packets that are sent from a source address other than the IP address allocated to the user by the ISP. This prevents users from using addresses from the 44.0.0.0/8 block directly on the internet, since the outgoing packets would be blocked at their ISP.

The usual solution to this problem is to use IPv4-in-IPv4 tunnels (or other tunnelling protocols) to interconnect the different AMPRNet stations over the network. However, this makes most of the AMPRNet seem like a large VPN and makes the use of globally routable IP addresses less useful. A large VPN would also work well with private IP addresses. Strictly speaking, only the few stations or subnets that are announcing their AMPRNet addresses by BGP on the internet are really using the 44.0.0.0/8 block over the internet.

The IPv6 Amateur radio network solves this problem because every user is required to use their own address space, obtained from their ISP or a tunnel provider. In this way, such an address space can be used over the internet with no limitations. Subnets participating in the Amateur network can be connected directly over the internet, without the need for any tunnelling, and IPv6 addresses participating in the network can also be used to communicate with non-Amateur equipment on the internet (often for purposes as important as downloading software updates).

3.5. **Large blocks for National Societies.** Though the proposal given in this paper envisions that each individual or small project would be required to obtain their own IPv6 address space directly from their ISP (or a tunnel provider), it also allows for the possibility that large National Societies or other Amateur societies, such as the IARU regions, may be able to request a larger block directly from their corresponding RIR, announce that block by BGP directly on the internet and use it to give access by radio frequency or other means to interested Amateur operators. In this way, such a society would effectively become an ISP. This approach could still find some problems regarding source address filtering, as detailed above, but nevertheless is compatible with all the ideas outlined in this paper.

4. A case study: the network at EA4GPZ

In this section we give a concrete example by showing how some of the Amateur radio equipment in the home network of the author has been configured following the ideas in this paper.

The block that EA4GPZ is using is 2001:470:6915:8000::/49, which has been obtained from the IPv6 tunnel broker at Hurrican Electric [6]. The method used to encode Amateur callsigns into addresses is the BASE40 method described above.

There are the following devices and callsigns in the network:

- Router: EA4GPZ-X
- Server: EA4GPZ-Z
- User access, 2.4GHz: EA4GPZ-S
- User access, 5GHz: EA4GPZ-C

Note: EA4GPZ-S and EA4GPZ-C are currently offline, but the IPv6 addresses are assigned in the DNS.

The callsigns -X and -Z have been chosen because they somehow seem suggesting for a router and a server. The callsigns -S and -C refer to S band (2.4GHz) and C band (5GHz).

The following EUI-48 addresses are assigned to the callsigns above, using the method given in this paper:

- EA4GPZ-X 42:1F:87:2E:5A:F1
- EA4GPZ-Z 92:1F:87:2E:5A:F1

- EA4GPZ-S 7A:1F:87:2E:5A:F0
- EA4GPZ-C FA:1F:87:2E:5A:ED

These EUI-48 addresses can be used directly as Ethernet MAC addresses, which is what is being currently done.

Following the Hamnet terminology, the network 2001:470:6915:8000::/64 is used as a Service-Network and the network 2001:470:6915:8001::/64 is used as a User-Network. This means that servers run in the Service-Network and users that connect by the radio frequency access points get addresses from the User-Network.

The router has the following statically assigned IPv6 addresses:

- 2001:470:6915:8000:421f:87ff:fe2e:5af1
- 2001:470:6915:8001:421f:87ff:fe2e:5af1

In this way, the following IPv6 addresses are generated automatically using SLAAC:

- EA4GPZ-Z 2001:470:6915:8000:901f:87ff:fe2e:5af1
- EA4GPZ-S 2001:470:6915:8001:781f:87ff:fe2e:5af0
- EA4GPZ-C 2001:470:6915:8001:f81f:87ff:fe2e:5aed

The devices which connect through the radio frequency access and have their MAC address properly set up with their callsign using a BASE40-derived EUI-48 address will also obtain, by using SLAAC, an IPv6 address that encodes their callsign.

The IPv6 addresses listed above are published in DNS and reverse DNS using the names:

- EA4GPZ-X router.ea4gpz.destevez.net
- EA4GPZ-Z ea4gpz.destevez.net
- EA4GPZ-S user-2ghz.ea4gpz.destevez.net
- EA4GPZ-C user-5ghz.ea4gpz.destevez.net

Ping from the internet is allowed to all these IP addresses. Access from the internet to the following services running in ea4gpz.destevez.net is also allowed:

- ssh
- mumble
- dxspider (port 7300)

5. Joining the IPv6 Amateur radio network

The author believes that a key to the success of a good idea is that it gains popularity and adoption. So far, not many people have become interested about an IPv6 Amateur radio network as detailed in this paper. There can be several reasons for this, such as the limited number of Amateur operators interested in this kind of technologies, a limited time for the hobby that gets spent on other aspects of it, or simply that not enough publicity has been given to these ideas (hopefully this paper will try to solve this last cause).

Interested Amateur radio operators are invited to contact the author at the email address given at the end of the paper. As the IPv6 Amateur radio network is a decentralized network where each user offers his own network resources, it is up to each individual to join it. Interested people with some knowledge of IPv6 are already able to join the network. This section gives an overview of the steps needed to do so, depending on the internet connection of the user.

People which already have access to the IPv6 internet and have a globally routable block which is larger than a /64 and that they can administer can use some subnet of this block for their Amateur radio equipment. Probably the best idea is to use a /64 as a Service-Network and another /64 as User-Network if user access by radio frequency is to be expected. It is recommened to allocate a subnet larger than these two /64s, as it may become necessary to give blocks to stations connected directly by radio frequency in the future. An idea is to allocate half of the block available from the ISP for personal or home use and the other half for Amateur radio use.

Then it is necessary to chose a method to encode callsigns into IPv6 addresses. The method given in [8] is recommended. It is mandatory that all the globally routable IPv6 addresses in use have a valid callsign associated using the chosen method. It is also recommended to do so for link-local addresses, but it is not necessary.

People which do not have access to the IPv6 internet but have a static IPv4 address can obtain a /48 IPv6 subnet by at least two methods:

- Using 6to4. This only requires some setup on the router. It also requires access to a 6to4 relay (the anycasted IPv4 address 192.88.99.1). Some ISPs do not give access to a relay. The performance depends on the 6to4 relay you access (there is no control about it, as this depends depends on the ISP's routing). The /48 block obtained depends only on the static IPv4 address.
- Using a tunnel broker such as Hurricane Electric [6]. This requires a registration in the broker's webpage and the set up of the tunnel, as well as some configuration in the router. The performance depends on the other end of the tunnel. The /48 block obtained in this manner is assigned by the tunnel broker from his own network.

Depending on the ISP, these methods could give better or worst performance regarding latency and bandwidth. It is possible to try out both methods and choose the one that gives better performance.

People which have a dynamic IPv4 address can use the tunnel broker from Hurricane Electric [6]. It offers a service to update the tunnel's IPv4 address, which is compatible with dyndns' update protocol.

6. Research ideas

Here we give some ideas which seem interesting topics for research or experimentation, thus advancing the state-of-the-art of Amateur radio.

- Mobile IP. The author has already performed some preliminary tests with UMIP [13].
- Using Differentiated Services to decide if the traffic should be routed by radio frequency links or through the internet (whenever both alternatives are possible). This solves the existing problem that many sites are connected both by the radio frequency links and by the internet, and it is never clear which to prefer when routing the traffic, since certain routes would be best depending on the intended application.
- Using NAT64, CLAT or SIIT to allow access to the AMPRNet from the Amateur radio IPv6 network.
- Using WHOIS to store the contact data for each subnet participating in the Amateur radio IPv6 network.

References

[1] Amateur Radio Digital Communications, Managing the AMPRNet – TCP/IP Networking for Amateur Radio, https://www.ampr.org/
[2] Highspeed Amateurradio Multimedia NETwork, https://hamnet.eu/
[3] Wikipedia, Cisco Discovery Protocol, https://en.wikipedia.org/wiki/Cisco_Discovery_Protocol
[4] HamnetDB, Hamnet IP-Database http://hamnetdb.net/
[5] RFC4862: IPv6 Stateless Address Autoconfiguration, https://tools.ietf.org/html/rfc4862
[6] Hurricane Electric Free IPv6 Tunnel Broker https://tunnelbroker.net/
[7] Daniel Estévez, IPv6 for Amateur radio https://destevez.net/ipv6-for-amateur-radio/
[8] Robert S. Quattlebaum, Amateur Radio Numeric Callsign Encoding, https://github.com/darconeous/ham-addr/blob/master/n6drc-arnce.md
[9] ham-ipv6 https://sourceforge.net/projects/hamv6/
[10] Matti Aarnio, Some idea for IPv6 addressing for radio-amateur nodes, http://ham.zmailer.org/oh2mqk/packet-ipv6.html
[11] TAPR, AX.25 Link Access Protocol for Amateur Packet Radio, https://www.tapr.org/pub_ax25.html
[12] IARU R1, VHF Handbook V8.12 https://www.iaru-r1.org/index.php/downloads/func-startdown/1009/
[13] UMIP, Mobile IPv6 and NEMO for Linux, http://www.umip.org/

E-mail address: daniel@destevez.net