Salo, Timothy J. "Narrowband IP over Amateur Radio Networks (NIPARnets): Next-Generation Networking for Amateur Radio". *Proceedings of the ARRL and TAPR 32nd Digital Communications Conference, Seattle, WA, September 20-21, 2013*. 55-58. <http://www.saloits.com/papers/AMSAT2013.pdf>

Narrowband IP over Amateur Radio Networks (NIPARnets)

Next-Generation Networking for Amateur Radio

Timothy J. Salo, ABØDO
Salo IT Solutions, Inc.
PO Box 141049
Minneapolis, MN 55414-6049
salo <at> saloits <dot> com
salo <at> nipar <dot> net

Abstract

The Narrowband IP over Amateur Radio Networks (NIPARnets) proposed here offer an opportunity to design, develop, and deploy a new generation of amateur radio digital networks. NIPARnets will employ state-of-the-art protocols and technologies: they will leverage and extend recent work by researchers, standards development organizations, and others. These networks will offer amateurs a digital network that will make effective use of our valuable narrowband very high frequency (VHF) and ultra-high frequency (UHF) radio frequency (RF) channels. NIPARnets will connect seamlessly with the Internet, enabling amateur devices to appear to be part of and directly accessible from the Internet. These networks will benefit amateur radio beyond simply providing a new, more capable, more efficient network for use on narrowband channels: they will help attract new members to the amateur radio community, particularly those who want to experiment directly with wireless data networks and the technologies that power the Internet. Equally importantly, NIPARnets will help protect our VHF and UHF spectrum by demonstrating how we can use this scarce resource to help advance the radio and networking arts.

Keywords: amateur radio digital networks, narrowband data networks, wireless sensor networks, IP over narrowband radios, VHF data networks

Introduction

I invite you to join in creating a new generation of amateur radio digital communication networks. These networks will employ state-of-the-art wireless networking protocols and technologies to operate effectively over narrowband radio frequency (RF) channels. I call these networks *Narrowband Internet Protocol (IP) over Amateur Radio* (NIPAR) *networks*, or NIPARnets. These networks will provide many new opportunities for radio amateurs to research, design, and implement new narrowband, wireless network protocols, and to experiment with new applications of these unique facilities.

What are NIPARnets?

NIPARnets will use state-of-the art, Internet-compatible, wireless networking protocols and technologies that make efficient use of narrowband very high frequency (VHF) and ultra-high frequency (UHF) radio channels. Each NIPARnet will provide coverage over a metropolitan area or similar geographic region. The Internet-connected NIPARnets will collectively form a unique large-scale testbed that will enable amateurs and others to develop, evaluate, and refine new networking technologies that are optimized for use in severely bandwidth-constrained, wide-area wireless networks.

Opportunities for Amateur Radio

Radio amateurs are uniquely positioned to be key players in advancing the art of narrowband wireless networking. First, we have access to the valuable VHF and UHF spectrum that is ideally suited to these networks. Second, our community includes technically sophisticated researchers, engineers, and experimenters who are capable of creating and refining the necessary technologies, and enthusiastic operators who are ready to deploy and use these networks on a large scale. Finally, these efforts will help us fulfill our mission of advancing the radio art and demonstrate the importance of preserving VHF and UHF spectrum for use by radio amateurs.

Radio amateurs are sure to find countless uses of NIPARnets. These networks, like the Internet, are *general purpose* networks that support nearly any conceivable application, within the limitations of the available bandwidth and FCC regulations concerning on-the-air activities. Some amateurs might use these new networks to collect data from meteorological and other environmental sensors that are distributed over large, remote areas and make these observations available in real time over the Internet. Other amateurs might use these networks to monitor and control remote, difficult-to-access devices and systems, such as amateur radio repeaters or vacation homes. These technologies might even provide the basis for a network that connects amateur satellites to terrestrial amateur networks and the Internet. An important lesson of the Internet is that if a general-purpose, easy-to-use network is readily and widely available, amateurs are sure to use NIPARnets in novel ways that no one has yet imagined.

An Invitation to Participate

This paper offers a vision of a new generation of amateur radio digital networks. But, realizing this vision will require the participation of many radio amateurs. I invite you to look at the NIPARnet website, www.nipar.net, download some software, ask questions, make suggestions, and perhaps join in developing and deploying the next generation of amateur radio networks.

An Architecture for NIPARnets

I propose a NIPARnet architecture that is consistent with current amateur radio operations in the VHF and UHF bands: an architecture that is built around a fixed repeater or base station, (which I call an "access point").

Infrastructure-Based Networks

NIPARnets are "infrastructure-based networks": they rely upon permanent, fixed infrastructure that is analogous to amateur repeaters. Figure 1 illustrates the major components of the NIPARnet architecture. The *access point* provides services to *remote nodes* that are within range. The access point manages the NIPARnet: it assigns network addresses to remote nodes and forwards packets between remote nodes that are unable to communicate directly. Some access points contain a *NIPARnet/Internet gateway*, which forwards packets between the NIPARnet and the Internet. Access points are generally more capable than remote nodes: they usually have a carefully positioned antenna that is designed to provide coverage over a large geographic area. Furthermore,

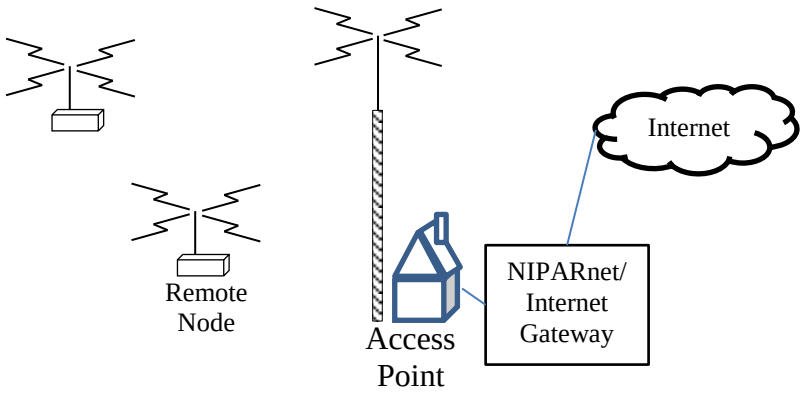

Figure 1. Preliminary NIPARnet Architecture

access points usually transmit with more power than do remote nodes and may employ more sensitive receivers. Nearly any device that can implement the NIPARnet protocols and manage a data radio may be a remote node: these devices may be as powerful as a personal computer or perhaps as constrained as an 8-bit microprocessor. Remote nodes may forward packets to and from other remote nodes that are not within range of the access point, similar to digipeaters in today's amateur radio networks. While access points will generally be fixed, the remote nodes may be either fixed or mobile.

Internet Transparency

An Internet-connected NIPARnet appears to be a transparent extension of the Internet. That is, to an Internet host, such as a personal computer, a remote NIPARnet node is indistinguishable from any other Internet node, except perhaps for greater latency and less bandwidth. Figure 2 summarizes this configuration. To applications, a NIPARnet appears to be just another IP network, albeit a slow one.

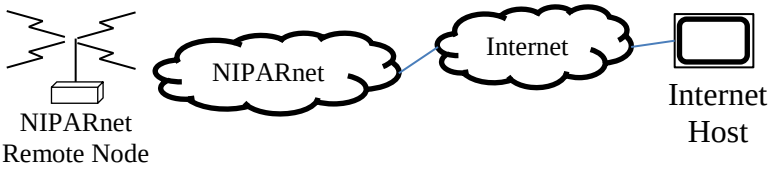

Figure 2. Internet Transparency

Figure 3. NIPARnet-NIPARnet Transparency

Internet transparency is transitive: remote nodes that are part of one Internet-attached NIPARnet can communicate transparently with remote nodes that are part of another Internet-attached NIPARnet, just as they can communicate transparently with Internet hosts[1]. This configuration is shown in Figure 3. Again, the NIPARnets in the end-to-end path are transparent (or invisible) to applications.

There are, however, limits to the transparency that NIPARnets support. Specifically, NIPARnets may only be *edge* networks. A NIPARnet may provide Internet connectivity only to the nodes in that network. NIPARnets cannot (in general) connect another *network* to the Internet: they may *not* act as *transit* networks. The configuration shown in Figure 4, where a NIPARnet connects another *network* to the Internet, is *not* permitted, (except perhaps in carefully managed circumstances).

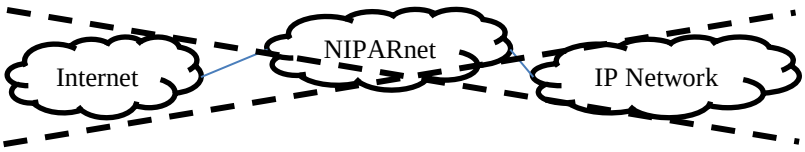

Figure 4. NIPARnets May *Not* be Transit Networks

Bandwidth-Efficient Protocols

The most distinctive characteristic of NIPARnets is that they operate over narrowband RF channels, which support speeds of as little as 9,600 bits-per-second (bps), or even less. Few people other than radio amateurs would even consider running networks over such slow links! NIPARnets also differ

[1] While achieving NIPARnet-Internet-NIPARnet transparency in the IPv6 Internet is straightforward, providing this transparency in the IPv4 Internet when a NIPARnet shares a single IP address is not.

from the most other contemporary wireless data networks, in that they may span miles or tens-of-miles, compared to a few hundred meters or less for many low-power wireless networks.

Because NIPARnets use narrowband channels, bandwidth is often the most valuable, the most scarce resource in the network. As a result, the NIPARnet protocols *must* make very efficient use of the available bandwidth. NIPARnets should avoid transmitting over the air, for example, 128-bit IPv6 addresses, when 16-bit addresses would work just as well.

The need for Internet transparency, combined with a need to use network bandwidth very efficiently, suggest that NIPARnets should use internally protocols that are impose a very low overhead, and that can easily be translated to and from the Internet protocols.

IPv6 and IPv4

NIPARnets must be able to connect to both the IPv4 Internet, the portion of the Internet that uses the current version of IP, and the IPv6 Internet, the portion that uses the emerging version of IP. Current practice in contemporary low-power wireless networks is to use internally a protocol that can easily be translated to IPv6, and then translate those IPv6 packets to IPv4 packets, when necessary. This translate-to-IPv6-first strategy is motivated by the belief that many new wireless networks will collectively connect billions of small devices to the Internet, necessitating use of the larger addresses of IPv6. An IPv6-like protocol makes sense for NIPARnet, in large part because this makes it easier to leverage recent research results and current standards.

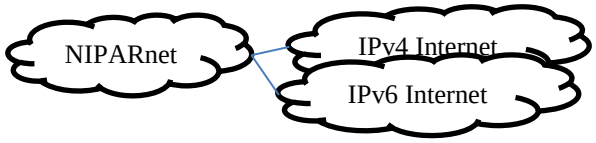

Figure n. IPv4 and IPv6 Connectivity.

Smart Access Point

The access point plays a central role in the NIPARnet architecture: it is responsible for configuring and managing the network. Because the architecture assumes that an access point is always present, functionality can be moved from the remote nodes to the access point. Functionality can be provided by the access point in order to conserve network bandwidth, or to reduce the energy, computation or storage demands that are placed on remote nodes, (which can be particularly beneficial for solar- or battery-powered remote nodes).

Configuration and Management Responsibility for managing a NIPARnet is centralized in the access point. This responsibility includes managing and assigning the 16-bit addresses used internally and supplying a remote node with configuration parameters when it joins the network.

NIPARnet/Internet Gateway When a NIPARnet is connected to the Internet, a NIPARnet/Internet gateway hosted by the access point must translate between the compact protocols used by the NIPARnet and the standard Internet protocols. Specifically, the gateway must translate between the IPv6-compatible protocols that are used within the NIPARnet and IPv6, and between IPv6 and IPv4 when the NIPARnet is attached to the IPv4 Internet.

Common Services The access point may provide common services to the remote nodes, particularly if these services conserve bandwidth. For example, the access point might translate domain names, such as `ab0do-17.nipar.net`, into a 16-bit NIPARnet address, thereby avoiding several packet exchanges over the NIPARnet. Likewise, the access point might register `ab0do-17` with the nipar.net domain name server, when one of my remote nodes connects to the NIPARnet.

Performance-Enhancing Proxies The access point could also include *performance enhancing proxies*. These proxies would employ some of the multitude of strategies that have been developed to enhance

the performance of Internet-attached wireless networks. For example, numerous techniques have been created to improve the performance of TCP in wireless/wired networks, such as avoiding unnecessarily retransmitting packets across the bandwidth-constrained wireless network.

NIPARnet Protocols

I believe that NIPARnets require new network protocols, principally because different engineering tradeoffs are appropriate when very scarce network bandwidth is the limiting resource. Furthermore, less complex protocols and algorithms can be employed when an access point is available. Additionally, Part 97 regulations impose a few additional requirements, although these necessitate only minor extensions to the protocols (e.g., on-the-air station identification using an amateur radio call sign). While I assert that NIPARnets require new protocols, a lot of prior work is available that offers good guidance in the design of the NIPARnet protocols.

Before offering a tentative roadmap for the design of the NIPARnet protocols, let me discuss some basic questions, including: How are devices identified? What is the structure of addresses? How are addresses assigned?

NIPARnet Node Identification

Network protocols usually assume that each node is assigned a permanent, machine-readable 48-bit IEEE address, often called an IEEE MAC address, but formally known as 48-bit Extended Unique Identifier (EUI-48™) [IEEE]. Most network adapters, such as Ethernet interfaces or Wi-Fi interfaces, have a 48-bit IEEE address. But, NIPARnet nodes won't necessarily contain a network interface adapter that has a 48-bit IEEE address. Plus, FCC regulations require us to use our amateur radio call sign to identify our transmissions. Therefore, I suggest that each NIPARnet node be identified by a text string that contains a call sign optionally followed by a hyphen and a string of digits, analogous to the AX.25 SSID, (e.g., `AB0DO-17`) [TAPR]. This strategy permits the node id to be used for Part 97 station identification, as well as by the NIPARnet protocols. While amateur call signs are necessary to appropriately identify an amateur radio station, they don't make very good network addresses.

Because NIPARnets don't use amateur radio call signs as addresses (they are only used to identify a node), I suggest that the call sign of a NIPARnet node may be transmitted with any packet as an IPv6 extension [RFC 6564]. If the call sign is transmitted over the air in an IPv6 hop-by-hop header, the access point will discard the call sign when forwarding the packet to the Internet, and the access point will add the call sign when a packet is forwarded from the Internet. Alternatively, NIPARnet nodes could transmit their call signs in an IPv6 destination option, if the node desires that the call sign be transmitted over the Internet. Of course, this raises the question of how an access point ought to treat a call sign in a packets received from the Internet. Ideally, text-based Part 97 on-the-air identification can occur every 10 minutes, rather than every packet.

When an Internet-connected access point assigns an address to a remote node, the access point ought to register a Domain Name System (DNS) name for that address using the Dynamic DNS Update protocol [RFC 2136], (e.g., `ab0do-17.nipar.net`)[2]. This will permit an Internet host, or a NIPARnet node, to "find" an active NIPARnet node, without needing prior knowledge about which NIPARnet the node is connected to.

[2] A hierarchical naming scheme may be necessary to make the global collection of NIPARnets more scalable (e.g., `0do-17.ab.nipar.net` or even `0do-17.b.a.nipar.net`).

NIPARnet Addresses and Address Assignment

I propose that every NIPARnet node be assigned a 16-bit address by the access point, and that this address be used by both the NIPARnet link-layer protocol and the NIPARnet network-layer protocol. Again, the access point is responsible for assigning these addresses and translating between these 16-bit addresses and IPv6 addresses. The use of a single 16-bit address contrasts with the Internet architecture, in which network nodes are assigned two types of low-level addresses: a 48-bit IEEE address used by the link-layer protocol and a 32-bit IPv4 or a 128-bit IPv6 network address. Narrowband networks running at 4,800 or 9,600 bps simply can't afford such extravagant addresses.

NIPARnet Network-Layer Protocol

The NIPARnet network layer must: 1) make very efficient use of the limited available bandwidth, and 2) be easily translated into IPv6. A lot of work has been done in this area, and I propose that the NIPARnet network protocol leverage this work.

Recent and ongoing work within the Internet Engineering Task Force (IETF) has created a set of protocols and technologies that offer a good foundation upon which to build the NIPARnet network protocol. (The IETF is the standards development organization (SDO) that is responsible for maintaining the specifications for many Internet protocols, including IP, IPv6, and TCP [IETFa].) While these protocols offer a good starting point for NIPARnet protocols, they must be substantially modified and extended to meet the demands and constraints of narrowband channels and amateur radio operations.

The IETF 6lowpan working group has developed techniques to compress IPv6 headers when IPv6 is used in IEEE 802.15.4 networks [IETFb], [RFC 4944], [RFC6282], [IEEE 2003]. (IEEE 802.15.4 networks are low-power, short-range networks, which can operate in the 2.4 GHz license-free spectrum; they are somewhat similar to Bluetooth). The 6lowpan protocols specify how to compress IPv6 packet headers, yielding headers that contain fields that are similar to the fields in the IPv6 header, but are smaller.

While the IETF 6lowpan protocols offer an excellent example of how to design a network protocol for a low-bandwidth network, they can't be used directly in NIPARnets. Most obviously, these protocols are designed to operate over the IEEE 802.15.4 protocol, rather than the NIPARnet link-layer protocol. Furthermore, I don't believe that the 6lowpan protocol design is aggressive enough in conserving network bandwidth. This may be the result of a couple of design decisions. First, the 6lowpan protocols offer more flexibility than is probably necessary for an amateur radio network, particularly when bandwidth is so scarce. Second, the 6lowpan working group adopted a design strategy of mimicking the behavior of IPv6. I believe that this constraint could beneficially be relaxed, as long as the resulting NIPARnet network protocol can be easily translated to IPv6. For example, I believe that additional on-the-air overhead reductions can be gained by minimizing the number of packets that are transmitted and storing or computing more information, rather than transmitting it.

NIPARnet Routing Protocol

NIPARnets need a routing protocol, so that remote nodes can forward packets between the access point and more distant remote nodes that can't communicate directly with the access point. While the IETF has developed several routing protocols for ad hoc mobile networks [IETFc], I believe that the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) offers the best fit for NIPARnets [RFC 6550]. The mobile ad hoc routing protocols can't take advantage of infrastructure such as the NIPARnet access point, while RPL is a good match for an access-point-based NIPARnet.

NIPARnet Link-Layer Protocol

I readily admit that I don't have a good solution for a NIPARnet link-layer protocol. Ideally, NIPARnet will use an existing link-layer protocol that consumes as little overhead as possible, and is available in low-cost, readily available, VHF data radios. It would be nice if the NIPARnet data radio used a standard link-layer protocol, in the hope that interoperable devices would be available from multiple [competing] vendors. Unfortunately, VHF and UHF data radios are often expensive and generally use non-standard or proprietary link-layer protocols. Yes, perhaps AX.25 framing could be used, for example with KISS modems. But, KISS modem / data radio combinations are generally fairly expensive and pretty much require expensive test equipment for 9,600 bps operation. To be successful, NIPARnet needs an inexpensive, easy-to-use VHF data radio.

I am open to suggestions for an inexpensive, standards-based, narrowband VHF or UHF data radio that would be appropriate for NIPARnets. If such a device were available, it would effectively define the NIPARnet link-layer protocol.

Implementing NIPARnets

I envision NIPARnet software that is designed and implemented by a group of interested, dedicated, talented radio amateurs. To stimulate interest in this project, I anticipate making available software that I am developing to support my dissertation research. Perhaps, my research and the NIPARnet development project will have a relationship similar to that of some open-source software projects, where a commercial project and an open-source project work independently, but collaboratively.

NIPARnet Phase 0 Software

I hope that the software that I am developing as part of my dissertation research can provide what might be called NIPARnet Phase 0 software. This software is being implemented under Linux. Not only does Linux offer an excellent programming environment, but it is widely used in the network research community: Linux implementations of standard and experimental protocols are generally available. I am currently using Ubuntu, although it would be nice to see the digital amateur radio community coalesce on a common distribution.

For hardware, I am using several ARM-based single-board computers, including the original BeagleBoard [BeagleBoard] and the Raspberry Pi [RaspberryPi], and I anticipate using the BeagleBone in the near future. These boards are ideally suited for this project: they are powerful enough to run Linux, they are very inexpensive, and the use little enough power to be deployed in solar- or battery-powered installations.

As I asserted earlier, the lack of an inexpensive, standards-based VHF data radio is the biggest impediment to this project, and to standards-based VHF data networks. I am currently using a pair of Maxon SD-171E VHF radios with ACC-513E 4,800 bps modems. These radios aren't cheap, but at $350 they are much less expensive than most data radios.

I anticipate that the initial version of my NIPARnet Phase 0 software will support 6lowpan header compression over IEEE 802.15.4 networks and over narrowband VHF channels using the Maxon radio. This software will include an initial version of a new NIPARnet protocol that assigns and manages 16-bit NIPARnet addresses. A subsequent version of this software will add RPL. At least initially, this software will use existing implementations of 6lowpan and RPL. Please remember that the NIPARnet Phase 0 software does not implement the NIPARnet protocols; rather, it is a platform that is intended to enable NIPARnet designers and developers to get something on the air quickly, and to support the development of the NIPARnet protocols.

Final Thoughts

I tried, in the paper, to paint a vision for a new generation of amateur radio networking. I again invite you to join in making this vision reality, perhaps by contributing code, by offering advice, or by running and extending the NIPARnet Phase 0 software. Check the NIPARnet project website, www.nipar.net, for the latest information.

But, my vision extends beyond simply creating a new amateur digital network. I hope that this project will help nurture greater interest in wireless network research among radio amateurs. Greater collaboration and interchange between radio amateurs and network researchers will undoubtedly enrich both groups.

References

1. [BeagleBoard] BeagleBoard.org Foundation, Project website, <http://beagleboard.org/>.
2. [IEEE] IEEE, "Guidelines for use of a 48-bit Extended Unique Identifier (EUI-48™)", <http://standards.ieee.org/develop/regauth/tut/eui48.pdf>.
3. [IEEE 2003] IEEE Computer Society, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std. 802.15.4-2003, October 2003.
4. [IETFa] Internet Engineering Task Force (IETF), IETF Home Page, <http://www.ietf.org/>.
5. [IETFb] Internet Engineering Task Force (IETF), IPv6 over Low power WPAN (6lowpan) working group documents web page, <http://datatracker.ietf.org/wg/6lowpan/>.
6. [IETFc] Internet Engineering Task Force (IETF), Mobile ad hoc networks working group documents web page, <http://datatracker.ietf.org/wg/manet/>.
7. [RaspberryPi] Raspberry Pi Foundation, Project website, <http://www.raspberrypi.org/>.
8. [RFC 2316] Vixie, P, ed, Editor," Dynamic Updates in the Domain Name System (DNS UPDATE)", ISSN: 207-1721, Internet Engineering Task Force RFC 2136, April 1997, <http://tools.ietf.org/html/rfc2136>
9. [RFC 4944] Montenegro, et al., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", Internet Engineering Task Force (IETF) RFC 4944, September 2007. <http://datatracker.ietf.org/doc/rfc4944/>
10. [RFC 6282] J. Hui, Ed. And P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", ISSN: 2070-1721, Internet Engineering Task Force (IETF) RFC 6282, September 2011. < http://datatracker.ietf.org/doc/rfc6282/>
11. [RFC 6550] Winter, T. Ed., P. Thubert, Ed., et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", ISSN: 2070-1721, Internet Engineering Task Force (IETF) RFC 6550, March 2012, <http://tools.ietf.org/html/rfc6550>.
12. [RFC 6564] S. Krishnan, et al., "A Uniform Format for IPv6 Extension Headers", ISSN: 2070-1721, Internet Engineering Task Force RFC 6564, April 2012.
13. [TAPR] TAPR, "AX.25 Link-Layer Protocol Specification: Version 2.0", October 1984. <http://www.tapr.org/pub_ax25.html>