Home Networking with IPv6

Brian Haberman, Nortel Networks
George Tsirtsis, BT

Abstract

In this paper we show that the Internet Protocol Version 6 (IPv6) is a crucial enabler of the home networking market. It has a number of well-known, advanced features, such as stateless autoconfiguration, enhanced mobility support, and mandatory security that will allow for its widespread use in the home. As IPv6 matures and vendors include IPv6 in their standard equipment and software releases, different sectors of the global Internet will start taking advantage of this new and exciting technology. Existing Internet service providers can benefit greatly from IPv6, using the much larger address space and advanced features of IPv6 to expand their offerings. More importantly, however, IPv6 is becoming the enabler for a number of new services that, although recognizably valuable for some time now, were being hampered by technical limitations of the legacy IPv4 systems. The IPv6 protocol will allow Internet technology to expand further than ever before, especially into consumer electronic devices. This paper makes the case for IPv6 as an enabler of the home networking technology that can provide the platform for accelerated growth of the high value consumer electronic devices and Internet access markets.

1. **Introduction**

The need for home networks is growing at a rapid rate. There are several factors driving this increase. In general, there are three main drivers of home networks today. These are the continual growth in the use of home PCs, the rapid introduction of smart devices, and the phenomenal growth of home-based businesses and telecommuting.

In 1999, 43.1 million homes in the United States owned a PC. Of these, 9.4 million owned two PCs and 3 million owned 3 or more PCs. As the PC becomes more and more of a commodity, the number of homes with PCs will increase as will the number of homes containing multiple PCs. The owners of these machines will want to be able to share data, both with other machines in the home and with machines via the Internet.

The introduction of smart devices is giving consumers the flexibility of automating tasks. Devices such as Personal Digital Assistants (PDAs), smart phones, and set-top boxes are offering new capabilities and features. Smart devices will be able to control such systems as smart appliances (Internet refrigerator, microwave), electronics (home theater, stereo), and home security systems. In order to perform these tasks, the smart devices and the smart appliances will have to be network-capable and globally reachable.

The home-based workforce is increasing at an incredible rate. In 1998, there were 13 million home-based businesses with a double-digit growth rate. From 1995 to 1997 the number of telecommuters in the United States grew by 30%. In 1998 alone, that number grew by another 40%. As the number of home-based workers increases, so will the need for home networks. Home-based businesses will want the capability of operating on the World Wide Web, accessing home resources while traveling, and sharing data with customers and co-workers.

As these markets grow, the need for flexible home-networking tools increases. The home network will have to be robust, but simple. Much like the PC, users will want to be able to plug new devices into the network and have them work. If a customer has to maintain a complex system in the home, it will not be widely used. For these reasons, the Internet Protocol Version 6 (IPv6)[1] will play a critical roll in the home networking market.

2. **Goals**

If widespread use of home networks is to be realized, the technology needed to build these networks must meet some important goals. These goals are meant to ensure that the non-technical user will be willing to use the technology. If the tools are too complicated, the market for home networks will be limited to those people who are willing to invest time in learning new technology.

The first goal is to have a network that requires a low amount of configuration and maintenance. If the user spends a large period of time setting up or maintaining the network, it will decrease the willingness to use the technology. If things are kept simple, widespread acceptance will be more likely. This should apply to both devices installed during the original network setup as well as the introduction of new devices into an existing home network.

The next goal is to allow a wide range of devices to participate in the home network. These networks should not be limited to the devices that are network capable today. The technology used to for these networks should be flexible enough to allow for their use on a wide range of devices and appliances.

Flexibility in the type of communication media is the next goal. The home networking market should not and will not be restricted to traditional copper wire networks. Home networking tools must support a wide spectrum of media. Possible media types are

Ethernet, RF (Bluetooth), firewire (IEEE 1394), wireless (IEEE 802.11) and power-line. Regardless of the media, home-networking appliances should work the same.

Finally, home-networking users will expect to be able to access their networks from remote locations. The home networking tools used must allow for secure access to the home networking user while still keeping unwanted intruders out.

Home networks are likely to follow the general trend of the Internet towards peer-to-peer based applications (e.g. VoIP) as opposed to the current client-server based (web surfing). In addition home networks are also likely to offer services to external users via the Internet (e.g. Web server, or remote control of home electrics/electronics). This is enabled with the increasing bandwidth available to home networks (cable modem, xDSL) and requires incoming connectivity i.e.: publicly addressable home networks.

3. **Functionality**

In order to meet the stated goals, a set of key functions is needed. These functions include: auto-configuration, security, mobility support, simple routing, and device and/or service discovery.

3.1. Plug & Play

Plug & Play, or Auto-configuration as is called in IPv6, allows devices to be added to a network with little or no configuration effort. If these network-capable devices are not simple to setup, users will be afraid to use them. Configuring your Internet-connected refrigerator must not require deciphering "Owner's Manual instructions written by and for nuclear physicists"[2]. IPv6 accomplishes this with its stateless auto-configuration features. Devices capable of running IPv6 can configure their own IPv6 addresses based on configuration information that they receive from the router controlling the home network. This allows the user to introduce new devices to the network with little effort; no IP address, network mask, DNS server, or gateway address to configure.

Stateless auto-configuration [3] is the key to keeping the home network simple, yet flexible. By allowing devices to auto-configure network information (e.g. address, gateway, DNS server, etc), the user is relieved of the need to know how to configure network information in every device in use on the network. This simplicity will allow users who normally would not use networking to utilize it without feeling overwhelmed.

The auto-configuration capabilities of IPv6 do not require an administrative server. However, if a user does wish to have such a server, IPv6 supports the use of stateful configuration services that might actually be required for some advanced or legacy applications. A home PC or a service provider could administer this type of application. This flexibility allows for either a peer-to-peer (i.e. VoIP) or a client-server (i.e. security system control) paradigm to exist within the home network.

3.2. Security

The need for security is clear. Home networking users do not want unauthorized people accessing their networks. In addition, these users may also want to make sure that communications that they originate to outside users can be authenticated and/or encrypted. The IPv6 protocol supports all of the features of IPSec [4] that allow for the use of encryption and authentication. The security capabilities of IPv6, networks can be protected from attacks with the use of firewalls rather than the perceived security of network address translators.

A common misconception is that the security of a network requires the use of Network Address Translators (or NATs)[5]. NATs are used to provide IPv4 networks based on private address space connectivity with the publicly addressed Internet. NATs "hide" the addresses of the network behind it, providing a "poor" man's security since no one from the Internet can directly attack one of the nodes in the private network. This kind of security, however, comes at a high price since a number of important services are not possible through NATs, the most important of which are the ability to support incoming sessions and end to end IP Security (IPSEC).

Incoming sessions (e.g.: Incoming VoIP call) are not possible for the same reason the network is secure, i.e.: no one from the Internet can directly connect with one of the nodes in the private network due to address translation. A number of mechanisms are continuously being devised to allow certain types of Incoming calls through NATs, which of course work against the security premise of NATs. The bottom line is that NAT-based security comes with restrictions of use; attempting to alleviate the restrictions, potentially weakens its security.

IP Security is used to provide a secure communication channel for all communications between 2 nodes in the network. For example IPSEC can be used to connect one of the nodes in the home network to a corporate network for home-working purposes. IPSEC works by making sure (by encryption and signing) that nothing can be changed in a packet from the IP layer and above providing authentication, integrity and encryption services to the two points of communication. NATs change the IP addresses of packets in flight and to IPSEC looks like, what is known in security terms as a "man in the middle" attack.

Finally, a number other applications i.e.: some types of file transfer (FTP), gaming (Quake), Internet presence (ICQ) etc. also have difficulty in running over address translation. Thus, typically, NATs are also equipped with a number of Application Layer Gateways (ALGs) that service the above types of applications. While ALGs are seamless to the end user when they work properly, you need one ALG per application. This means that if a new application is created and does not run over NATs, a new ALG may be able to help but it will need to be installed in the network's gateway.

With the abundance of IPv6 addresses, address translation is being rendered unnecessary and with it all its limitations eliminated. With IPv6, the level of security provided is defined by the needs of the particular network/customer and is not imposed by limitations of the technology. Thus, a variety of security levels are available to fit the needs of any customer. From no security at all (not recommended but clearly possible) to very high standards of security that require elaborate techniques and configuration. For most people a simple firewall incorporated in the gateway would allow maximum flexibility of use in a relatively secure environment. More advanced IPSEC will also be used for access to corporate networks and/or mobility.

In addition to more globally reachable addresses, there is an increase in the number of IP addressable appliances. There will be a need to allow for secure incoming connections to the home network. For example, if a user's air conditioning unit is mal-functioning, a service representative could be granted access to the A/C unit via the home network gateway. The service representative would be able to collect diagnostic information prior to any repairman visiting the home. There are a large number of similar applications/functions that will be available to home networking users and these will require similar, secure access.

3.3. Mobility

In order to allow home networking users to access their networks while they are out of the home, the support of mobile [6] networking is critical. This function will allow those users to either access resources within the home network from outside the network or allow them to be a part of the network from a remote location (office, etc.). This capability is supported with the mobile IPv6 specifications [7]. This type of functionality requires mobile nodes to have special capabilities. These special capabilities are a part of the base specification of IPv6.

Mobile IPv6 does not require Foreign Agents (as Mobile IPv4 does), meaning that the mobile user can access its home network from anywhere in the world without local mobility configuration requirements. The only thing required is a Home Agent deployed in the Home Network for the forwarding of packets to the mobile's current location. Mobile IPv6 Home Agents would typically be combined with the Home Network's Gateway functions.

3.4. Routing

Since home networks will typically not be complex, routing function should be simple. In most instances, there will not be a need for routing within the home network at all. A simple router/gateway that connects the home to a service provider can be the default gateway for all devices in the network. This allows the network to be kept as simple as possible. In the cases where the home network is slightly more complex and requires some routing functionality, an IPv6-based home network can be controlled with static

routes or with the use of RIPng [8]. Ideally, an IPv6-based home network gateway would consist of simple routing functions combined with a firewall.

3.5. Device and Service Discovery

The function of device discovery is accomplished with the Neighbor Discovery protocol [9] in IPv6. This protocol allows devices on a shared network to efficiently discover the information needed in order for them to communicate. Of more importance to a network user may be the capability to do service discovery. The Service Discovery protocol, much like Jini, allows users to determine if a particular function is available on the network. An example of its use would be a Personal Digital Assistant trying to determine if a VCR was active on the network so that it could be configured to tape a show. The Service Discovery protocol [10] supports the use of IPv6 at the network layer and can exist and cooperate with Jini and Jini scenarios.

4. Deployment

With the development of Internet-capable appliances, it should be noted that embedded devices have capability limitations. These types of devices do not have the capacity to include a fully functional IP stack, such as DHCP client code or a configuration interface. These types of devices should be developed with IPv6 today. This will allow them to utilize the benefits of IPv6 and avoid having to upgrade or replace these appliances in the future.

However, IPv4 is a widely deployed protocol and this leads to a number of interesting challenges in utilizing IPv6. One of the most important challenges is whether IPv6 should be deployed as a Single Stack or side-by-side IPv4 as Dual Stack architecture. In brief, Dual Stack is what the developers of IPv6 had in mind when they created the protocol, for the simple reason that migration to IPv6 across the Internet is likely to take a long time, during which, native communication with both IPv6 and legacy IPv4 is desirable!

The problem is that Dual Stack has a couple of drawbacks. First, it is obviously bigger, in terms of lines of code, than IPv6 Single Stack since it also has some code related to IPv4. The importance of this is often exaggerated and is the authors' belief that all but the smallest of micro-devices (e.g.: light switches and pin head computers) will be able to easily cope with the Dual Stack option.

A far more significant problem with Dual Stack is the fact that the IPv4 stack will need to be configured and addressed in order to be usable, with the danger of loosing some of the most important advantages that IPv6 offers i.e.: autoconfiguration and unlimited address space. The developers of IPv6 technology, however, have again foreseen this problem and have provided a number of mechanisms that use the superior features of IPv6 to configure efficiently the IPv4 stack in a Dual Stack implementation. Such a mechanism is DSTM [11] that uses DHCPv6 [12] to configure the IPv4 stack of a node.

Now, the alternative of IPv6 Single Stack has its own problems. IPv6 is not backwards compatible to IPv4 and thus, a Single Stack IPv6 implementation will need to use some form of Protocol Translation (e.g.: SIIT [13] or NAT-PT [14]) to communicate with the IPv4 based Internet. The problem is that Protocol Translation has the same side effects with Address Translation (NAT), which is one of the main reasons for moving to IPv6!

So is the authors' advice that, if you believe that IPv6 migration is going to take long time, as expected, and if communication with the legacy IPv4 systems during this period is vital to your business and other needs, you should seriously look at Dual Stack and the mechanisms that will allow you to take advantage of IPv6 technology while maintaining full connectivity with the current systems.

5. **Alternatives**

There are possible alternatives to an IPv6-based home network. These could be non-IP based solutions or an IPv4 based solution.

A non-IP based solution has a very limited usefulness. Most features and services that are network based are IP-based. This severely limits the feasibility of a non-IP network. In order to make such a configuration interoperate with the Internet, some type of translation gateway would be needed.

An IPv4 home network has better potential than a non-IP based network, but it has several limitations to overcome. First and foremost, IPv4 does not support stateless autoconfiguration. Without stateless autoconfiguration, many devices would be difficult to configure and/or use. What autoconfiguration is supported is done with an address range that cannot be routed onto the Internet. This limitation would require either a globally routable IPv4 address for each device or the use of private addresses with a Network Address Translator (NAT). With the shortage of IPv4 addresses increasing, there is little chance for users to obtain global IPv4 addresses. If the user is forced into using a NAT, then there is a possibility that certain applications will not work and that it will be difficult for the user to access the home network from remote locations.

6. **Conclusion**

The opportunity home networking presents is clear and well recognized, as are the limitations of IPv4 technology in providing an adequate platform for its development. IPv6 provides the important features that can enable deployment of Home Networks in an efficient and user-friendly way, while enabling application and service providers to develop innovative ideas and create new markets without restrictions from the underlying technology. IPv6 can be the springboard for a new customer experience in the developing Home Networks market.

7. **Example**

The following figures show how the stateless auto-configuration feature of IPv6 allows devices to configure globally routable IPv6 addresses.

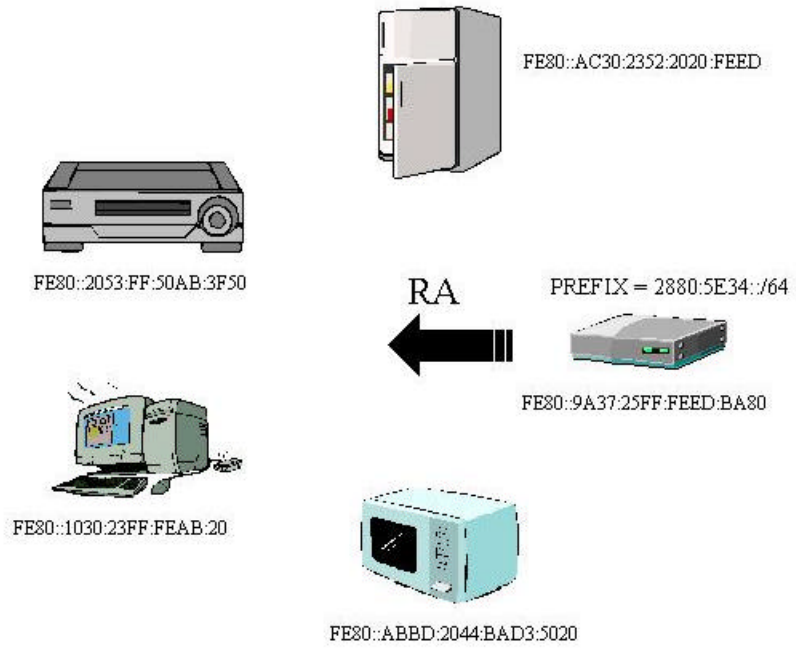

Figure 1

In Figure 1, all of the IPv6 capable devices have configured local-use IPv6 addresses. These addresses allow the devices to communicate with one another on the local communications media. For many home network applications, these local-use addresses will be sufficient. In the case where global reachability is needed, the home gateway device can transmit an advertisement message that indicates the global IPv6 prefix assigned to the network.

In Figure 2, all of the devices have received the advertisement. The devices extract the IPv6 prefix information and use it to automatically generate their own global IPv6 addresses. These addresses can be used by the devices to communicate with any other network-capable device that is reachable via the service provider(s).

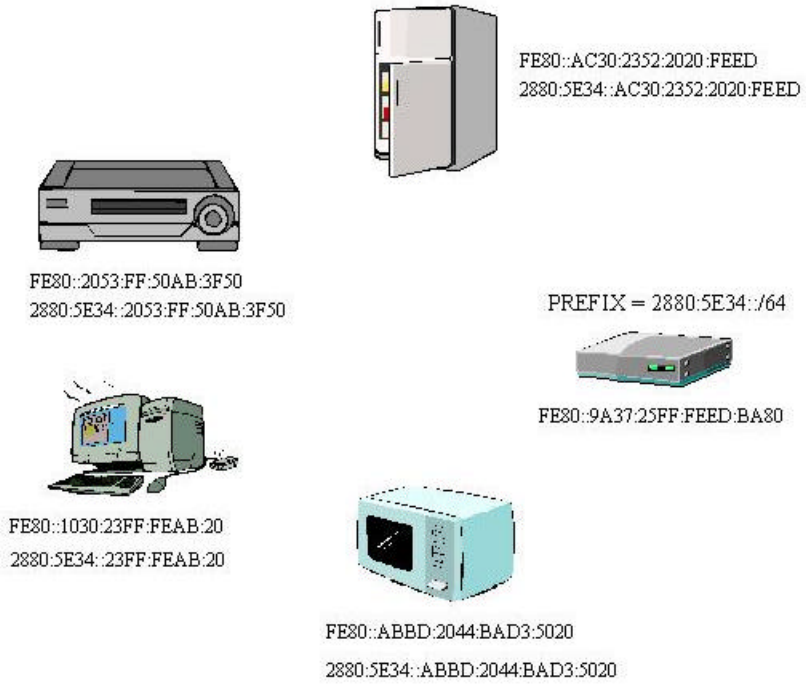

Figure 2

The major benefit of this functionality is that end-users will not have to know how to configure network information into each individual device. This feature will also help alleviate problems caused by configuration errors.

8. **Acknowledgements**

The authors would like to thank Jim Bound, Richard Hovey, and Petri Mahonen for their review and comments on this document.

9. **References**

1 Deering, S. and Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

2 Barry, D., "In a battle of wits with kitchen appliances, I'm toast", Miami Herald, http://www.herald.com/content/archive/living/barry/1999/docs/feb27.htm, February 24, 2000.

3 Thomson, S. and Narten, T.,"IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

4 Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
5 Egevang, K. and Francis, P., "The IP Network Address Translator", RFC 1631, May 1994.
6 Solomon, J., "Applicability Statement for IP Mobility Support", RFC 2005, October 1996.
7 Johnson, D. and Perkins, C., "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-12.txt, April 2000, Work in Progress.
8 Malkin, G. and Minnear, R., "RIPng for IPv6", RFC 2080, January 1997.
9 Narten, T., Nordmark, E., and Simpson, W., "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
10 Guttman, E., "Service Location Protocol Modifications for IPv6", draft-ietf-svrloc-ipv6-09.txt, July 2000, Work in Progress.
11 Bound, J., et. al., "Dual Stack Transition Mechanism (DSTM)", draft-ietf-ngtrans-dstm-02.txt, July 2000, Work in Progress.
12 Bound, J., Carney, M., Perkins, C., "Dynamic Host Configuration Protocol for IPv6", draft-ietf-dhc-dhcpv6-15.txt, May 2000, Work in Progress.
13 Nordmark, E., "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.
14 Tsirtsis, G. and Srisuresh, P., "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

10. **Authors' addresses**

Brian Haberman
Nortel Networks
e-mail: haberman@nortelnetworks.com

George Tsirtsis
BT
e-mail: george.tsirtsis@bt.com
e-mail: gtsirt@hotmail.com