IPv6: Necessary for Mobile and Wireless Internet

ISOC MEMBER BRIEFING #14

June 20, 2003

Authors: Alper Yegin, Carl Williams

1. Background

Internet architecture is going through an exciting evolution with the emergence of wireless access technologies. This new Internet not only requires a larger IP address space, but also a number of fundamental features to enable wireless networking and mobility. The current state of IPv4-NAT architecture simply does not adequately serve this new Internet especially in terms of security, mobility, extensibility, and dynamic reconfigurability. IPv6 is rapidly emerging as the preferred platform to meet the many needs of the new Internet.

2. Technical Issues and Implications

2.1. Devices Providing Application Services

One of the most critical deficiencies of the IPv4-NAT architecture is its inability to allow hosts to run as the connection-receiving end of a communication session (similar to servers). Internet access devices are becoming more capable and powerful, thanks to their faster CPU, increased bandwidth and storage capacity, as well as new peripherals - such as cameras, sensors, GPS, etc. This leads to a new trend that enables such devices to provide application services, in addition to being ordinary clients.

A wireless IPv4-NAT access network simply does not allow client devices to run as servers, because of NAT's inability to map incoming connections to its clients' private IP addresses. One workaround to this problem is to deploy an ALG (Application Level Gateway) on the NAT for each service of interest. This solution incurs significant protocol design and service deployment complexity. Furthermore, this is not a scalable solution since it requires protocol-specific changes for each service that needs to go through NAT. Therefore, while ALGs could provide a costly solution for enabling few services through NATs, they fail to restore the much-needed end-to-end transparency that is lost upon NAT deployment. Meanwhile, none of these aforementioned limitations is an issue for an IPv6 access network as it does not have to deploy NATs.

Expanded Coverage from ISOC
In-depth articles, papers, links and other resources on a variety of topics are available from the ISOC site at:
www.isoc.org/internet/issues

Examples in the News
Nordic Wireless Watch
Wireless Week

Relevant IETF RFCs
A detailed list of relevant RFCs and Internet-drafts can be found from the working group web pages listed under "For More Information".

From OnTheInternet
http://www.isoc.org/oti/articles/
1201/g8.html
http://www.isoc.org/oti/articles/
1201/wilkinson.html
http://www.isoc.org/oti/
articles/0601/rao3.html
http://www.isoc.org/oti/
articles/0601/wang.html

For More Information
IP Version 6 Working Group:
www.ietf.org/html.charters/ipv6-charter.html
IP Routing for Wireless/Mobile Hosts (Mobile IP) Working Group:
www.ietf.org/html.charters/mobileip-charter.html
IPsec Protocol Working Group:
www.ietf.org/html.charters/ipsec-charter.html
Network Mobility (NEMO) Working Group:

not have to deploy NATs.

2.2. Plug-and-Play

While consumer devices are becoming more capable, another trend is the miniaturization of devices that are used for other purposes, such as sensor networks. Lack of a user interface for configuration and the sheer number of devices at any given time, combined with mobility, simply make enhanced dynamic reconfigurability an absolute necessity. IPv6's plug-and-play capabilities, such as address auto-configuration and anycast address support, are indispensable features for large-scale sensor networks.

2.3. Security

Security of wireless Internet is another reason why IPv6 is a necessity. Before the Internet started going wireless, it had been enjoying security provided by the wired networks. A dial-up client's access to the Internet could be assumed reasonably secure by relying on the physical security of phone lines and trust in the operator's network. A similar trust is established on the other end of the communication where the server is connected to the Internet via a similar setup. Furthermore, the Internet backbone between two access networks has always been regarded as reasonably secure.

This trust model is changing with the introduction of wireless access networks on the Internet. Not only are the access networks of the client susceptible to various threats - depending on the level of security mechanisms applied, but also the access networks of their peers are affected. The current state of wireless network security is far from adequate, and the future prospects do not look as if they will ever get to be as good as wired network security. While your clients can ensure that they are protected from threats on their access network by using appropriate security mechanisms, they can never be sure about the same for their peers' side. This leaves the end-to-end security the only sure bet for securing the communication without regard to where the traffic passes through.

End-to-end security should be accomplished by deploying IPsec. Unfortunately IPsec cannot be used adequately through NATs today. There are on-going efforts to solve this problem, but in most cases the solutions appear to be kludges that come with limitations and various risks. The best solution to prevent vulnerabilities stemming from wireless Internet is to use end-to-end IPsec over IPv6. It

www.ietf.org/html.charters/nemo-charter.html
Securing Neighbor Discovery (SEND) Working Group: www.ietf.org/html.charters/send-charter.html
3rd Generation Partnership Project (3GPP): www.3gpp.org
3rd Generation Partnership Project 2 (3GPP2): www.3gpp2.org
IPv6 Wireless Internet Initiative: www.6winit.org

Related Organizations

http://www.ipv6forum.com IPv6 Forum
http://www.ietf.org Internet Engineering Task Force (IETF)

About the Authors

Alper Yegin is a senior research engineer at DoCoMo USA Labs. His interest and expertise are in the areas of mobility management and security of wireless networks. He has been actively involved with protocol design, implementation, and product and service development aspects of IPv6. Alper is a co-chair of IETF PANA Working Group, member of IETF Wireless Directorate and active contributor of various wireless related IETF working groups. He contributes to the IPv6 transition of Internet as an active member of the IPv6 Forum Technical Directorate.

should be noted that while IPv6 is necessary, it is not sufficient for global deployment of end-to-end IPsec on the Internet, which depends on factors that are outside the scope of base IP protocol.

2.4. Mobile IP

Mobile IPv4 is the IETF (Internet Engineering Task Force) standard protocol for handling mobility of an IPv4 node across the Internet. This protocol allows the use of a single fixed IP address regardless of the IP subnet changes, and hence enables continuous reachability for mobile nodes. The fixed IP address is called a home address, and the IP address acquired at each visited network is called a care-of address. The mapping between the home address and the care-of address of a mobile node is maintained at a special redirection server called a home agent. Home agent intercepts packets on behalf of the mobile node and sends them to its care-of address when the mobile node is away from its home network.

Due to the sheer number of mobile nodes, a typical Mobile IPv4 node would have a non-routable private IPv4 home address. Also, since they cannot be given a unique globally routable IPv4 care-of address at the visited networks, either a special mobility agent, called a foreign agent, should be deployed in those networks, or mobile node and its home agent should deploy an additional NAT-traversal mechanism. Mobile IPv4 NAT-traversal protocol extension is specified in a separate RFC that is IPR-encumbered. Furthermore, this extension generates various security vulnerabilities. Regardless of which solution is used, presence of private IPv4 addresses leads to compulsory tunneling of both incoming and outgoing packets between the mobile node and its home agent. Effectively what that means is that even when two mobile IPv4 nodes are attached to the same visited network, the end-to-end communication between the two has to traverse through the home agent of each node. In an extreme case this can very well incur an extra full round-trip around the world. This sub-optimal routing is the result of Mobile IPv4 design that has been impacted by the lack of IPv4 addresses.

On the other hand, Mobile IPv6 design and deployment enjoys both the availability of addresses and the extensibility provided by IPv6 protocol. Route optimization signaling enables a mobile IPv6 node to inform its correspondent node about its new care-of address. This allows both mobile node and the correspondent node to send and receive packets using the shortest path between the two. One useful

Carl Williams is a founder of MCSR Labs. Carl has interest in IP mobility, micro-mobility and ad-hoc routing areas. While at Sun Microsystems, Carl participated in the IPv6 protocol design, Solaris IPv6 implementation, and product development. He was the Solaris Mobile IP Project Lead and initiated Mobile IP/IPv6 testing at Connectathon Interoperability events. Prior to founding MCSR Labs Carl worked as a researcher and project lead at DoCoMo USA Labs. Carl is a co-chair of IETF TRIGTRAN BOF, member of North American IPv6 Task Force and IPv6 Forum Technical Directorate. He has authored numerous papers on IPv6 and mobility as part of the North America IPv6 Task Force and he currently contributes to the US Moonv6 testbed.

Acknowledgments
The authors would like to thank Jim Bound and the ISOC Member Briefing Review Board for their valuable feedback. This paper is produced with the editorial support of the IPv6 Forum. The ISOC Member Briefing series is made possible through the generous assistance of ISOC's Platinum Program Sponsors: APNIC, ARIN, Microsoft, Qualys and Ripe NCC. *More information on the Platinum Sponsorship Program*: http://www.isoc.org/isoc/membership/platinum.shtml

by-product of this feature is location-based services. Mobile IPv6 location update signaling can be used by a correspondent node to infer the geographic location of a mobile node, and hence provide customized service or content. This optional protocol signaling can be turned off if the mobile node's location privacy is an issue.

Deployment of Mobile IPv4 foreign agents imposes additional infrastructure cost for service providers when NAT-traversal mechanism is unavailable or its security deficiencies are unacceptable. This creates either an additional burden on the service provider when they want to enable Mobile IPv4, or a limitation of IP-layer mobility of mobile nodes on the access networks - where the provider avoided this additional cost. On the other hand, a mobile IPv6 node can use mobility protocol wherever it can get simple IPv6 service. Mobile IPv6 protocol does not require or even define foreign agents. This leads to scalable Internet-wide mobility management.

In addition to making mobile IPv6 more attractive to users, IPv6 also opens up business opportunities for new service providers. Internet-wide IPv6 mobility management can be provided by running a home agent anywhere on the Internet. IPv6 Internet access and mobility management can be provided by separate entities. Hence, building and maintaining costly access networks is not a requirement for providing IPv6 mobility service.

2.5. Extensibility and Standardization

In general, it is extremely hard to predict what kind of new requirements the future will impose on Internet architecture. An extensible protocol like IPv6 has more prospects to meet the unforeseen needs than its rigid IPv4 counterpart. IPv6's flexibility is made possible by extension headers and options in its design. While IPv6 enjoys its architecturally clean extensibility, IPv4 is limited to a slow, costly and limited patching process that further upsets its original design principals.

IETF has been creating new working groups to tackle ever-increasing needs of the mobile and wireless Internet. Mobile IP, Seamoby, NSIS, NEMO, SEND are among such groups. In many of these working groups it is a proven fact that designing protocols that can work through NAT is a painful task. Protocols get more complicated and it takes longer to design them. Any service provider who relies on standards-based products from vendors should take both this delay and possible additional costs into consideration.

About the Background Paper Series

Published by:
The Internet Society
1775 Wiehle Avenue, Suite 102
Reston, Virginia 20190 USA
Tel: +1 703 326 9880
Fax: +1 703 326 9881

4, rue des Falaises
CH-1205 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

Email: info@isoc.org
Web: http://www.isoc.org/

Series Editor: Martin Kupres

Furthermore, some of these working groups are only tackling IPv6 problems, leaving IPv4 counterpart problems unsolved. For example, SEND Working Group is working on extending security of IPv6 neighbor and router discovery, while IPv4 ARP and router discovery are not in its scope. NEMO Working Group is developing a network mobility protocol for IPv6 only. When standards-based solutions are important and proprietary ones are costly and non-interoperable, choosing the right base protocol for the future becomes a critical decision for service providers.

2.6. Architectures

Currently, 3GPP architecture mandates IPv6 for its IMS (IP-based Multimedia Subsystem). All IMS elements are IPv6-only, and both the protocol signaling and media-flow are carried only over IPv6. 3GPP2 architecture is based on IPv4, but there are on-going efforts to support IPv6 on this system. Wireless LANs appear to be the most effective platform to deploy IPv6 and get it on the air today.

3. Summary

Current and future challenges of mobile and wireless Internet can only be met by IPv6. IPv4 can merely provide costly, limited, inefficient, insecure, and patchy solutions to today's and tomorrow's problems. IPv6 further improves upon its predecessor by allowing new services to be added over time. IPv6 is the only solution for the truly mobile and wireless Internet, both from the users' and the service providers' perspective.