Network Working Group
Request for Comments: 5514
Category: Experimental

E. Vyncke
Cisco Systems

1 April 2009

IPv6 over Social Networks

Status of This Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Abstract

There is a lack of IPv6 utilization in early 2009; this is partly linked to the fact that the number of IPv6 nodes is rather low. This document proposes to vastly increase the number of IPv6 hosts by transforming all Social Networking platforms into IPv6 networks. This will immediately add millions of IPv6 hosts to the existing IPv6 Internet. This document includes sections on addressing and transport of IPv6 over a Social Network. A working prototype has been developed.

1. Introduction

While the IPv6 protocols are well-known for years, not every host uses IPv6 (at least in March 2009), and most network users are not aware of what IPv6 is or are even afraid by IPv6 because it is unknown.

On the other hand, Social Networks (like Facebook, LinkedIn, etc.) are well-known by users and the usage of those networks is huge.

This document describes how to leverage Social Networks in order to make more people aware of IPv6 and to add several thousands of IPv6 routers to the Internet.

2. Architecture

With IPv6 over Social Network (IPoSN):

- Every user is a router with at least one loopback interface;
- Every friend or connection between users will be used as a point-to-point link.

On social networks, users want to have multiple friends, partners, or relations with other users. Therefore, it can be expected that there is a heavily meshed network among these users. This will provide for good IPv6 connectivity because each user (IPoSN router) will be IPv6 connected to all his/her friends (IPoSN neighbor routers).

Several Social Network Applications (SNAs) allow for plug-ins or for other applications to be mashed with the social network. Those applications can then generate IPv6 packets on the behalf of the users. Those packets can then be transferred hop by hop, or rather user by user, over the mashed SNA/IPv6, until they reach their destination.

The usual policy of an SNA is to only allow the account owner to modify an account. Therefore, the IPv6 processing of a packet received by an SNA account must be explicitly executed by the account owner using a web action; this action will give the router CPU a nudge to process all received IPv6 packets. This behavior has two impacts on the IPv6 network:

1. the account owner must explicitly 'run the CPU' in order to forward or to receive IPv6 packets; this is an opportunity for IPoSN to detail all its operation (one goal is education)

2. the latency between two nodes over such a network can be very high, and timers (especially the routing timers; see Section 3) will have to be modified.

A latency of several hours has an impact on the transport protocols. UDP SHOULD be used, and TCP SHOULD NOT be used.

2.1. Addressing

In SNA, all users have a unique numerical identification. Assuming that there are less than 2**64 users on the SNA, the IPv6 global address of the router loopback will be a /64 prefix (such as 2001:db8:face:b00c::/64) followed by the SNA identification. As this address is a loopback address, the prefix length will always be /128. As the same /64 prefix is used for all SNA users, they will all appear as being part of the same /64 network.

On each interface, the link-local address will be generated by appending the SNA identification to the fe80::/64 prefix.

For example, here are two IPoSN addresses generated for the user 620147832 (this is 0x24f6b478 in hexadecimal):

- Global: 2001:db8:face:b00c::24f6:b478/128
- Link-local: fe80::24f6:b478/64

2.2. Address Translation

With the choice of the example prefix for all global addresses, an IPv6-to-IPv6 Non-Carrier Grade NAT (NCGN) must be implemented and linked to at least one 'edge' SNA user whose account will be used to pass (and translate) IPv6 packets between IPoSN and the real IPv6 Internet. The gateway and NAT functions are out of scope of the present document.

3. Choice of IGP

As seen in the architecture section (Section 2, the propagation of IPv6 packets only happens when a user activates the IPoSN application linked to his/her SNA account. Therefore, propagation delays are measured in hours or days compared to microseconds over the Internet fishbone. Moreover, the jitter is also very high as different users have different habits regarding the use of SNA.

IPoSN SHOULD implement RIPng [RFC2080], which is relatively immune to jitter and does not rely on flooding messages to all neighboring routers. OSPFv3 [RFC5340] SHOULD NOT be used over IPoSN.

Routing protocols for Delay Tolerant Networks MAY be use for IPoSN.

4. Working Prototype

A working prototype has been developed by the author and is freely available: IPv6 over Facebook Social Network [IPv6overFacebook]. It uses the LAMP architecture.

Some statistics as of March 26, 2009 (pre-standard implementation of course):

- Packet rate: 160 packets per minute
- Number of nodes: 3800
- Largest FIB: 1352
- NAT66 packet counters:
  - to the Internet: 8,500
  - from the Internet: 53,000

The extreme value of the latency makes network operation and trouble-shooting quite interesting.

A high latency ICMP echo request/reply:

```
2009-02-24 10:23:01: Ping to 2001:db8:face:b00c::2a42:4346
2009-02-26 21:52:24: Got a PING reply from 2001:db8:face:b00c::2a42:4346
```

A high latency UDP-based traceroute:

```
 2009-02-25 13:38:05: Traceroute to 2001:db8:face:b00c::21ca:5ab1
 2009-02-25 13:40:41: 2001:db8:face:b00c::28ef:7c60, intermediate node
 2009-02-25 18:04:21: 2001:db8:face:b00c::312a:c8cb, intermediate node
 2009-02-26 00:55:32: 2001:db8:face:b00c::2707:a4a0, intermediate node
 2009-02-26 00:55:33: 2001:db8:face:b00c::1e21:338b, intermediate node
 2009-02-26 00:56:25: 2001:db8:face:b00c::4c13:9577, intermediate node
 2009-02-26 07:44:17: 2001:db8:face:b00c::5422:2f57, intermediate node
 2009-02-27 10:16:45: 2001:db8:face:b00c::5422:2f57, intermediate node
 2009-02-27 10:16:45: 2001:db8:face:b00c::2726:8ed8, intermediate node
 2009-03-01 15:41:50: 2001:db8:face:b00c::21ca:5ab1, destination reached
 2009-03-01 16:22:54: 2001:db8:face:b00c::3e22:92b9, intermediate node
```

5. Security Considerations

As the users cannot really control what they are sending (they send IPv6 packets through a well-controlled web interface), there is no threat to send spoofed packets. The only exception is at the NAT66 gateway where packets from the real Internet can be received; therefore, NAT66 gateway MUST implement anti-spoofing.

Denial of service (packet flooding) can happen if a malicious user uses a web tool to request a ping diagnostic every second. Therefore, implementation SHOULD implement a rate limit on each web page that can generate an IPv6 packet.

Denial of service (packet flooding) can also happen at the NAT66 gateway from the real Internet. A rate limiter SHOULD also be implemented at the NAT66 gateway.

6. Acknowledgments

Many thanks to all first users of the IPv6 over Facebook [IPv6overFacebook] application: Isabelle Dehousse, Yves Hertoghs, Thomas Kernen, Simon Leinen, and so many others.

7. References

7.1. Normative References

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

7.2. Informative References

[IPv6overFacebook] Vyncke, E., "IPv6 over the Facebook Social Network", <http://apps.facebook.com/ipoverfb/>.

Author's Address

Eric Vyncke
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2 778 4677
EMail: evyncke@cisco.com