

v6ops Working Group
Internet-Draft
Intended status: Informational
Expires: February 17, 2011

G. Van de Velde
C. Popoviciu
T. Hain
S. Venaas
Cisco Systems
k. Chittimaneni
Google Inc
August 16, 2010

Network signaling for IPv4/IPv6 protocol selection for end-systems
<[draft-vandevelde-v6ops-pref-ps-00.txt](#)>

Abstract

Within an administrative realm, especially during an IPv6 implementation period, the network operator has interest to have control on the IP protocol version (IPv4 or IPv6) used by the end systems and network devices. This document provides a problem statement about both protocol preference and protocol selection many network operators face when implementing IPv6 in a controlled process.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 17, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft Network signaling for protocol selection

August 2010

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Draft Network signaling for protocol selection August 2010

Table of Contents

1.	Introduction	4
2.	Components	4
2.1.	IPv6 deployment model	4
2.2.	Policy table	5
3.	Considerations for IPv4 and IPv6 selection on end-systems . . .	5
3.1.	Dynamics of end-system configuration	5
3.2.	Hosts with multiple interfaces	5
3.3.	Backward compatibility	5
3.4.	Network based learning	5
3.5.	Impact on RFC3484	6
3.6.	Influence of IPv4/IPv6 protocol preference on applications	6
3.7.	Dynamic tunneling	6
4.	Considerations for IPv4 and IPv6 selection on network infrastructure elements	6
4.1.	Signaling IPv4/IPv6 preference	6
4.2.	Influence of IPv4/IPv6 preference on network infrastructure elements	7
4.3.	IPv4/IPv6 policy table location	7
4.4.	Backward compatibility	7
5.	IANA Considerations	7
6.	Security Considerations	7
7.	Acknowledgements	7
8.	References	7
8.1.	Normative References	7
8.2.	Informative References	7
	Authors' Addresses	7

Internet-Draft Network signaling for protocol selection August 2010

[1.](#) Introduction

With IPv6 TCP/IP stacks preferring IPv6 over IPv4 for forwarding, network administrators don't have control over which protocol end hosts use. Such lack of control has the potential to negatively impact the end host, especially in cases where the network is dual stacked well before the backend systems and/or applications are. It is thus preferable to have control over the device preference or selection of IP4 or IPv6. This control will allow network administrators to seamlessly implement IPv6 on the network with the ability to carefully integrate IPv6 into production as and when all other critical non-network components are found to be working as expected.

This document describes a problem statement to control and potentially communicate the IPv4/IPv6 protocol preference for devices. The document outlays the various considerations for protocol preference selection. This capability improves the ability of hosts to pick an appropriate protocol (IPv4 or IPv6) for off-link and on-link destinations.

Note that this procedure is applicable to end-systems and their applications only; the forwarding algorithm used by routers is not affected.

[2.](#) Components

[2.1.](#) IPv6 deployment model

When a network operator is in process of deploying a new technology on the network, the network operator will likely include a set of fallback mechanisms and will try to place as much control as possible in each of the deployment steps. An element of control during the integration of IPv6 is the management of IPv6 use by the end-systems and the applications running on those systems. The protocol preference management is done thorough a signaling mechanism. This signaling allows the network operator to introduce IPv6 on the routers and other network infrastructure elements without impacting existing IPv4 behavior of the end-systems. Once the network operator decides to activate IPv6 for end-systems, in order to allow each end-system to include IPv6 as valid communication protocol following [RFC3484](#) address selection.

This operational sequence will help the enablement of IPv6 in a controlled manner once the network infrastructure is found correctly working according the expectations of the network operator.

[2.2.](#) Policy table

The policy table references to an information database defining the expected behavior regarding IPv4/IPv6 protocol preference and selection behavior for various parts of the administrative domain.

[3.](#) Considerations for IPv4 and IPv6 selection on end-systems

This section will detail considerations for an end-system with respect to IPv4/IPv6 protocol preference.

[3.1.](#) Dynamics of end-system configuration

An end-system is usually configured in three possible ways:

(a) Preset configuration: these end-systems have a configuration which has been defined during the manufacturing of the device; (b) Manual configuration: In this case the end-systems are configured by a set of parameters and settings which are individually configured on the device through human interaction; (c) Dynamic configuration: Some end-systems download through the network infrastructure a set of

parameters i.e. IP and DNS addresses through DHCP

[3.2.](#) Hosts with multiple interfaces

Lots of end-systems are connected to the network infrastructure with only a single interface. For these systems, the IPv4 and IPv6 preference can be quite simply defined, either using or not-using IPv6. However, there are many end-systems connected through two or more interfaces to the network infrastructure. These systems require a protocol preference to be defined for each interface independently. These additional considerations also include aspects of conflicting information received through the different interfaces regarding the IPv6 protocol preference.

[3.3.](#) Backward compatibility

A solution for the IPv4/IPv6 preference shouldn't have an impact on end-systems not capable to understand this functionality.

[3.4.](#) Network based learning

The IPv4/IPv6 protocol preference on an end-system should be signaled by the 'network' (network devices or other infrastructure components such as DHCP) to automate the end-systems behavior, however the IP4/IPv6 protocol preference solution should not exclude manual configuration on end-systems.

[3.5.](#) Impact on [RFC3484](#)

A solution for IPv4/IPv6 protocol preference may influence the availability or better the non-availability of IPv6 parameters within the [RFC3484](#) end-system address selection algorithm. This influence must be understood very clearly for end-systems with single and with multiple interfaces attached to the network infrastructure.

[3.6.](#) Influence of IPv4/IPv6 protocol preference on applications

The IPv4/IPv6 protocol preference should be propagated by the end-system towards the applications running on the end-system. It should not be excluded that a protocol preference solution may have more specific information per application of importance to the end-systems. As consequence the end system could use this information

for IPv4/IPv6 protocol preference per application or session for example.

[3.7.](#) Dynamic tunneling

Some end systems make usage of dynamic tunnels for IPv6 even when the network infrastructure does not support IPv6 as a native protocol. The IPv4/IPv6 preference signal could influence the creation of these tunnels based upon the signaled IPv4/IPv6 protocol preference.

[4.](#) Considerations for IPv4 and IPv6 selection on network infrastructure elements

This section will detail considerations for network infrastructure devices with respect to IPv4/IPv6 protocol preference.

[4.1.](#) Signaling IPv4/IPv6 preference

The IPv4/IPv6 preference signal can be sent by four methods.

(a) The end-system is configured during manufacturing of the system; (b) A network operator configures the end-system by the console of the end-system; (c) The network infrastructure could signal the end-systems the IPv4/IPv6 preference through existing or new link-local packets; (d) The network infrastructure signals the end-system that there are elements that influence protocol selection, and that the end-system may want to request the network infrastructure what these elements exactly are.

[4.2.](#) Influence of IPv4/IPv6 preference on network infrastructure elements

The IPv4/IPv6 preference selection should only have impact on the end-systems and the network infrastructure devices should be ignoring the preference signal.

[4.3.](#) IPv4/IPv6 policy table location

The IPv4/IPv6 protocol preference needs to be stored somewhere within the network. This could be done either centrally or distributed. Crucial is that the network infrastructure device is directly connected to the end-system it wants to signal IPv4/IPv6 preference, so that link-local communication between the end-system and the network infrastructure device can be used. Between the network infrastructure device and the policy table location non-link local addresses may be utilized.

[4.4.](#) Backward compatibility

There should be no impact on either the network infrastructure when end-systems do not understand the IPv4/IPv6 protocol preference solution.

[5.](#) IANA Considerations

There are no extra IANA consideration for this document.

[6.](#) Security Considerations

[7.](#) Acknowledgements

[8.](#) References

[8.1.](#) Normative References

[8.2.](#) Informative References

Gunter Van de Velde
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 476 476 022
Email: gvandeve@cisco.com

Ciprian Popoviciu
Cisco Systems
7025-6 Kit Creek Road
Research Triangle Park, North Carolina NC 27709-4987
United States

Phone: +1 919 392-3723
Email: cpopovic@cisco.com

Tony Hain
Cisco Systems
500 108th Ave. NE
Bellevue, Wa.
USA

Email: alh-ietf@tndh.net

Stig Venaas
Cisco Systems
Tasman Drive
San Jose, CA 95134
USA

Phone:
Email: stig@cisco.com

Kiran Kumar Chittimaneni
Google Inc
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Phone: +1 650 253 6185
Email: kk@google.com

