IPv4 Rapid Deployment on IPv6 Infrastructures (4rd)
draft-vautrin-softwire-4rd-00

Abstract

This document specifies an automatic tunneling mechanism tailored to
advance deployment of IPv4 to end users via an IPv6 network
infrastructure. This document aims at giving an alternative to
family translation to operate an IPv6-only network.

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 January 30, 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
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.

Table of Contents

1. Introduction ................................................. 3
2. Requirements Language ....................................... 4
3. Terminology .................................................. 4
4. 4rd Model and operation ..................................... 5
   4.2. Traffic from CE to IPv4 Internet [BR Behavior] .......... 6
   4.3. Traffic from IPv4 Internet to CE [CE Behavior] .......... 6
   4.4. Traffic from IPv4 Internet to CE [BR Behavior] .......... 6
5. IPv6-only Deployment considerations .......................... 6
6. Acknowledgements ............................................. 7
7. IANA Considerations .......................................... 7
8. Security Considerations ...................................... 7
9. Normative References ........................................ 7
Author’s Address ................................................. 8
1. Introduction

4rd specifies a protocol mechanism to deploy IPv4 to sites or Host via an IPv6 network. It builds on [I-D.ietf-softwire-ipv6-6rd] and [I-D.ietf-softwire-dual-stack-lite]. 4rd could be seen either as the opposite of [I-D.ietf-softwire-ipv6-6rd] or as [I-D.ietf-softwire-dual-stack-lite] without NAT (or leaving NAT as optional).

IPv6-only network are not common. But IPv6-only networks is the end goal in the IPv4 to IPv6 transition. Thus it is worthwhile to define viable mechanism to ease the use of IPv6-only network. The alternatives to 4rd are defined in [I-D.ietf-behave-v6v4-framework] and such mechanisms have well known limitation most of them described in [RFC4966].

The 4rd mechanism relies upon a tunneling of IPv4 inside IPv6 to a well known IPv6 address to allow automatic IPv4 operation in an IPv6-only Network. The mechanism can be stateless or stateful depending on the selection of the IPv6 address. If the IPv6 address is using the IPv4-Embedded IPv6 Address Format described in [draft-ietf-behave-address-format] then the 4rd operation will be stateless. If the algorithmic mapping is not used, 4rd will fall back to a Standard DS-Lite operation. 4rd views the IPv6 network as a link layer for IPv4 and supports an automatic tunneling abstraction similar to the Non-Broadcast Multiple Access (NBMA) [RFC2491] model.

A 4rd domain consists of 4rd Customer Edges (CE) and one or more 4rd Border Relays (BRs). IPv4 packets encapsulated by 4rd follow the IPv6 routing topology within the network among CEs and BRs. 4rd BRs are traversed only for IPv4 packets that are destined to or are arriving from outside the 4rd domain. The CE can be either a host (which would need to have a 4rd client capability) or a router (On the LAN side of the router, IPv4 is implemented as it would be for any native IP service delivered by the network).

4rd relies on IPv6 and is designed to deliver production-quality IPv4 alongside IPv6 with as little change to IPv6 networking and operations as possible. 4rd can be deployed and thus remove the need for a Dual stack Network completely helping the transition to a full IPv6 internet in the future.

4rd used with a short IPv4 DHCP lease time or in conjunction with NAT44 (DS-Lite) can also be seen as an IPv4-depletion mitigation solution.
2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Terminology

4rd_IPv4_prefix - An IPv4 prefix selected for use by a 4rd domain. There is exactly one 4rd IPv4-prefix for a given 4rd domain. A network may deploy 4rd with a single 4rd domain or multiple 4rd domains.

4rd Customer Edge - A 4rd CE is a device functioning as a Customer Edge in a 4rd deployment. A 4rd CE may also be referred simply as a "CE" within the context of 4rd.

4rd domain - A set of 4rd CEs and BRs connected to the same virtual 4rd link.

4rd Border Relay (BR) - A 4rd-enabled router managed at the edge of a 4rd domain. A border relay router has at least one of each of the following: an IPv6-enabled interface, a 4rd virtual interface acting as an endpoint for the 4rd IPv4 in IPv6 tunnel, and an IPv4 interface connected to the native IPv4 network. A 4rd BR may also be referred to simply as a "BR" within the context of 4rd.

BR_IPv6_address - The IPv6 address of the 4rd Border Relay for a given 4rd domain. This IPv6 address is used by the CE to send packets to a BR in order to reach IPv4 destinations outside of the 4rd domain.

CE_IPv6_address - The IPv6 address given to the CE through normal means (i.e., configured via DHCP, or otherwise). With proper DHCP and Network design planning, this address can match the CE_IPv4_address that the CE will receive and thus use an IPv4-Embedded IPv6 Address Format described in [draft-ietf-behave-address-format]).

CE_IPv4_address - The IPv4 address given to the CE through the IPv6 tunnel (i.e., configured via DHCP, or otherwise). This means the CE can only get its CE_IPv4_address when it already has an CE_IPv6_address. This address may be global or private [RFC1918]. This address is used to send and receive IPv4 packets.
4. 4rd Model and operation

![Diagram of the 4rd model]

**Figure 1**

4.1. Traffic from CE to IPv4 Internet [CE Behavior]

the CE encapsulate the IPv4 packet into an IPv6 tunnel (aka Softwire). The IPv4 source packet can be either private or public. It can be learned through the IPv6 tunnel or by other means. The IPv6 source address can be either an IPv4-Embedded IPv6 Address or not. The choice to use IPv4-Embedded IPv6 Address or not will have an impact on the BR as this will switch between the stateless mode or the stateful mode.
4.2. Traffic from CE to IPv4 Internet [BR Behavior]

If the IPv6 packet source address is using an IPv4-Embedded IPv6 Address, then in this direction the BR just decapsulate the IPv4 packets from the IPv6 tunnel and forward it to the IPv4 Internet. This is what we call the Stateless 4rd mode. If the CE_IPv6_address is *not* using an IPv4-Embedded IPv6 Address, then the BR need to keep track of the relationship of this IP session and the IPv6 tunnel. The IPv6 address becomes the ID of the session. This is what we call the Stateful 4rd mode.

The BR is either doing NAT44 with the IPv6 address as the host identifier if the CE_IPv4_address is a private address or the BR is creating a mapping table between the softwire ID and the CE_IPv4_address if this last one is public and should not be modified. Note that 1:N NAPT can be used in parallel either on the same device or on another one. This mechanism is then similar to DS-Lite.

4.3. Traffic from IPv4 Internet to CE [CE Behavior]

The CE decapsulate the IPv4 packets from the IPv6 packets.

4.4. Traffic from IPv4 Internet to CE [BR Behavior]

If a session or a mapping information already exist in the system that matches the IPv4 packets, the IPv6 packets will be created with the information based on this session information. The session can exist because of traffic that originated from the IPv6 side or because some Port or address forwarding have been configured on the BR. If no sessions exist, the stateless mechanism will be used and the IPv6 packets will be created using the IPv4 address as defined by the IPv4 Mapped address mapping.

5. IPv6-only Deployment considerations

- Scenario 1: Service Provider with IPv6-only access would like to give an IPv4 address to end subscribers.

4rd used with a short IPv4 DHCP lease time or in conjunction with NAT44 (DS-Lite) can also be seen as an IPv4-depletion mitigation solution. With more and more internet content accessible through IPv6, An IPv4 address could be needed in the future just to access some legacy content. This means an IPv4 address could be needed only temporarily. This means temporary allocation of IPv4 addresses with short lease time can be a useful IPv4-depletion mitigation solution.
- Scenario 2: An IPv6-only Enterprise would like to give IPv4 connectivity.

In this case, operating systems would have to support 4rd the same way current operating systems support 6to4, Teredo or ISATAP. An alternative would be to deploy island of IPv4 with 4rd Clients running on routers.

- Scenario 3: An IPv6-only Enterprise would like to restore their servers connectivity from IPv4 Internet. In this case, the 4rd client will be started either on the server itself or on the 1st hop router.

6. Acknowledgements

None

7. IANA Considerations

None

8. Security Considerations

To be defined.

9. Normative References

[I-D.ietf-behave-v6v4-framework]
draft-ietf-behave-v6v4-framework-09 (work in progress), May 2010.

[I-D.ietf-softwire-dual-stack-lite]
draft-ietf-softwire-dual-stack-lite-05 (work in progress), July 2010.

[I-D.ietf-softwire-ipv6-6rd]


Author’s Address

Olivier Vautrin
Juniper Networks
1194 N Mathilda Avenue
Sunnyvale, CA 94089
USA

Email: Olivier@juniper.net