

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: January 29, 2010

W. Townsley  
O. Troan  
Cisco  
July 28, 2009

**IPv6 via IPv4 Service Provider Networks**  
**draft-townsley-ipv6-6rd-01**

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 29, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document specifies a protocol mechanism tailored to advance deployment of IPv6 to end users via a Service Provider's IPv4 network infrastructure. Key aspects include automatic IPv6 prefix delegation

to sites, stateless operation, simple provisioning, and service which is equivalent to native IPv6 outside of the SP's IPv4 network infrastructure.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Requirements Language . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">4.</a>	6rd Prefix Delegation . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Address selection . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Provisioning the 6rd CE router . . . . .	<a href="#">7</a>
<a href="#">6.1.</a>	6rd DHCP option . . . . .	<a href="#">8</a>
<a href="#">6.2.</a>	6rd PPP IPCP option . . . . .	<a href="#">9</a>
<a href="#">6.3.</a>	6rd Broadband Forum TR-69 Object . . . . .	<a href="#">9</a>
<a href="#">7.</a>	Provisioning the Service Provider 6rd Border Relay . . . . .	<a href="#">9</a>
<a href="#">8.</a>	Encapsulation considerations . . . . .	<a href="#">10</a>
<a href="#">8.1.</a>	Receiving Rules . . . . .	<a href="#">11</a>
<a href="#">9.</a>	Transition Considerations . . . . .	<a href="#">11</a>
<a href="#">10.</a>	Address space usage . . . . .	<a href="#">11</a>
<a href="#">11.</a>	Security Considerations . . . . .	<a href="#">12</a>
<a href="#">12.</a>	IANA Considerations . . . . .	<a href="#">12</a>
<a href="#">13.</a>	Acknowledgements . . . . .	<a href="#">12</a>
<a href="#">14.</a>	References . . . . .	<a href="#">13</a>
<a href="#">14.1.</a>	Normative References . . . . .	<a href="#">13</a>
<a href="#">14.2.</a>	Informative References . . . . .	<a href="#">14</a>
	Authors' Addresses . . . . .	<a href="#">14</a>



## 1. Introduction

The original idea and the name of the mechanism (6rd) specified in this document is described in [draft-despres-6rd](#) [[I-D.despres-6rd](#)], which details a successful commercial "rapid deployment" of the 6rd mechanism by a residential Service Provider and is recommended background reading.

This document describes the 6rd mechanism, extended for use in more general environments, and intended for advancement on the IETF Standards Track. Throughout this document, the term 6rd is used to refer to the new mechanisms described here and 6to4 as that which is described in [RFC 3056](#).

6rd specifies a protocol mechanism to deploy IPv6 to sites via a Service Provider's (SP's) IPv4 network. It builds on 6to4 [[RFC3056](#)], with the key differentiator that it utilizes an SP's own IPv6 address prefix rather than 2002::/16. By using the SP's IPv6 prefix, the operational domain of 6rd is limited to the SP network and under its direct control. From the perspective of customer sites and the IPv6 Internet at large connected to the 6rd-enabled SP network, the IPv6 service provided is equivalent to native IPv6.

6rd does not translate IPv4 into IPv6, it encapsulates IPv6 in IPv4 with a destination IPv4 address which is either encoded within the IPv6 destination address itself, or is the destination address of a preconfigured 6rd Border Relay router that can decapsulate the IPv4 header and route the IPv6 packet outside the SP's IPv4 network. This way, IPv6 packets follow the IPv4 routing topology within the SP network, and Border Relays are traversed only for IPv6 packets which are destined or are arriving outside the SP's IPv4 network. The 6rd mechanism is fully stateless, so the Border Relay routers may be addressed via anycast within the SP network for added resiliency.

The 6rd Customer Edge router (6rd CE) plays a critical role in a 6rd deployment. 6rd decouples deployment of IPv6 on the "LAN" side of the 6rd CE router from that on the "WAN" side, allowing IPv6 on either side to be deployed and evolve independently. On the LAN (e.g., "Home") side of the 6rd CE router, 6rd expects that IPv6 is implemented as it would be for any native dual-stack IP service delivered by the SP. On the WAN side of the 6rd CE router, the 6rd CE WAN interface itself, the access network between it and partnering 6rd equipment, and the OSS system including DHCP, AAA, etc. may remain IPv4-only (e.g., there is no need to deploy DHCPv6 [[RFC3315](#)], IPv6 Neighbor Discovery, IPv6 routing, create IPv6 address plans, etc. within the SP network to deliver IPv6 to the customer site).

6rd relies on IPv4 and is designed to deliver "production-quality"



dual-stack IPv6 and IPv4 Internet access to customer sites. IPv6 deployment within the SP network itself may continue for the SP's own purposes outside of delivering IPv6 service to customers. Once IPv6 is fully available, 6rd may be discontinued and IPv4 eventually turned off or tunneled over IPv6 as described in [draft-ietf-softwire-dual-stack-lite](#) [I-D.durand-softwire-dual-stack-lite].

## 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

6rd Delegated Prefix	The IPv6 prefix determined by the 6rd CE device for use by hosts within the customer site. This prefix can be considered logically equivalent to a DHCPv6 IPv6 Delegated Prefix [RFC3633], though it is calculated by combining the 6rd SP Prefix and the end user's IPv4 address obtained via IPv4 configuration methods.
6rd SP Prefix	An IPv6 prefix selected by the Service Provider for use by a given 6rd deployment. This may be the entire IPv6 prefix obtained from an RIR and announced to the IPv6 Internet, or a more-specific assigned just to given 6rd deployment.
6rd CE	The 6rd "Customer Edge" router that sits between an IPv6-enabled site and an IPv4-enabled SP network. In a residential broadband deployment this is sometimes referred to as the "Residential Gateway (RG)," "Customer Premises Equipment," (CPE) or "Internet Gateway Device" (IGD). This router has a one internal 6rd Virtual Interface acting as an endpoint for the IPv6 in IPv4 encapsulation and forwarding, at least one "6rd CE LAN Side" interface and "6rd CE WAN Side" interface, respectively.



6rd CE LAN Side	The functionality of a 6rd CE router that serves the "Local Area Network (LAN)" or "Home" side of a broadband service provider connection. The 6rd CE LAN Side interface is fully IPv6 enabled.
6rd CE WAN Side	The functionality of a 6rd CE Router that serves the "Wide Area Network" or "Service Provider" side of the 6rd CE Router. The 6rd CE WAN side is IPv4-only, except that it delivers IPv6 packets encapsulated in IPv4 by the 6rd Virtual Interface.
6rd BR	A 6rd-enabled "Border Relay" router located at the SP premises. The 6rd BR router has at least one IPv4 interface, an internal 6rd Virtual Interface for multi-point tunneling, and at least one IPv6 interface that is reachable via the IPv6 Internet or IPv6-enabled portion of the SP network.
6rd Virtual Interface	Internal multi-point tunnel interface where 6rd encapsulation and decapsulation of IPv6 packets inside IPv4 occurs. A typical 6rd CE or 6rd BR implementation requires one 6rd Virtual Interface.

#### 4. 6rd Prefix Delegation

In 6rd, a customer site's IPv6 Delegated Prefix is derived from 2 elements:

1. An IPv6 Prefix selected by the SP to be the common 6rd SP Prefix for the given 6rd deployment (an SP can have multiple 6rd deployments called domains).
2. An assigned IPv4 address for the subscriber. This IPv4 address may be a global IPv4 address, or a Private [RFC 1918](#) [[RFC1918](#)] IPv4 address.

From these three items, the 6rd Delegated Prefix is automatically created for the customer site when IPv4 service is obtained. From the perspective of the 6rd CE LAN-Side functionality, this IPv6 delegated prefix is used in the same manner as a prefix obtained via DHCPv6 Prefix Delegation [[RFC3633](#)].

In 6to4, the location of the stored 32-bit IPv4 prefix is at a fixed





location within the IPv6 address. In 6rd it varies, so the size of the SP IPv6 prefix is important. Also, in 6rd the SP chooses how many suffix bits of the IPv4 prefix are used in the algorithm to create the IPv6 prefix for its subscribers. This allows the SP to adjust the balance between IPv6 addresses used by the 6rd mechanism, and how many are left to be delegated to end user sites. To allow for stateless address auto-configuration and sub delegation a 6rd delegated prefix MUST be shorter than a /64.

The 6rd Delegated Prefix is created by concatenating the 2 items above in order. The sum of the number of bits used by each determines the size of the prefix that is delegated to the 6rd CE router for use by the customer site.

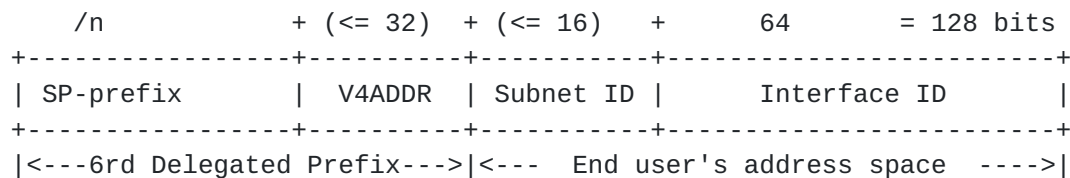


Figure 1

For example, if a 6rd SP Prefix (SP-prefix) is /28 bits, and we use 24 suffix bits of an IPv4 address (V4ADDR), and we want to support 16 6rd domains (4 bits), the delegated 6rd prefix for the site is  $28 + 24 + 4 = 56$  bits. This allows a /56 prefix to be delegated to each end user site.

Embedding less than the full 32 bits of an IPv4 address is possible only with an aggregated block of IPv4 addresses for a given 6rd SP Prefix. This may not be practical for global IPv4 addresses at a given SP, but is quite likely in a deployment where private addresses are being assigned to end users (for example 10.0.0.0/8). If private addresses overlap within a given 6rd deployment, the deployment may be subdivided into separate 6rd Domains, likely along the same topology lines the NAT-based IPv4 deployment itself would also require. In this case, each domain is addressed with a different 6rd SP Prefix. An implementation MAY expose this to the operator for configuration as a single 6rd SP Prefix coupled with a Domain ID which is appended to the 6rd SP Prefix during operation.

Multiple encodings are possible within a single 6rd deployment. For example, if global and private IPv4 addresses are used within the same 6rd site, and the number of IPv4 bits encoded in the IPv6 Delegated Prefix varies between the two (e.g., 32 bits for global, and 24 bits for private), then a different 6rd SP Prefix must be used



to disambiguate the two different encoding settings.

Since 6rd IPv6 prefixes are selected algorithmically from an IPv4 address, changing the IPv4 address will cause a change in the IPv6 delegated prefix which would normally ripple through the site's network and be disruptive. As such, if possible the service provider should utilize a long-lived IPv4 address assignment for a given end user.

6rd IPv6 address assignment and hence the IPv6 service itself is tied to the IPv4 address lease (whether set via DHCP, PPP, or otherwise), thus the 6rd service is also tied to this in terms of authorization, accounting, etc. For example, the 6rd Delegated Prefix has the same DHCP lease time as its associated IPv4 address. The prefix lifetimes advertised in Router Advertisements or used by DHCP on the 6rd CE LAN side MUST be equal or shorter than the IPv4 address lease time.

For trouble-shooting and traceability, a 6rd IPv6 address and the associated IPv4 address for the same site can always be determined algorithmically. This may be useful for referencing logs and other data at an SP that may be limited to IPv4 address assignment activity.

## **5. Address selection**

A 6rd delegated prefix is a native IPv6 prefix in the LAN-side of 6rd CE. For the purpose of source and destination address selection the prefix should be treated as native IPv6 and no changes to the source address selection or destination address selection policy table [[RFC3484](#)] is needed.

## **6. Provisioning the 6rd CE router**

The 6rd CE router must be configured with the 6rd SP prefix, the common IPv4 prefix length and a 6rd BR router IPv4 address. A given 6rd CE router is expected to exist in only one 6rd Domain (as indicated by the 6rd SP prefix).

This information can be configured into the device in a variety of ways including manual configuration. DHCP and IPCP are defined here, other automatic provisioning protocols may be used as well.



6.1. 6rd DHCP option

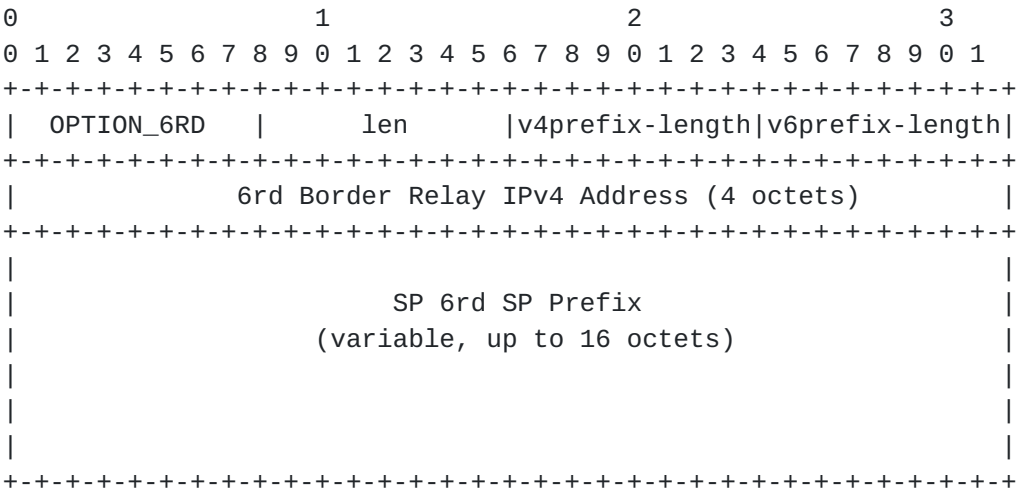


Figure 2

option code	OPTION_6RD(TBD)
len	Total length of option in octets.
v4prefix-length	Prefix length of the common part of the encoded IPv4 address in number of bits. This number of bits MUST be removed from the IPv4 address when generating the 6rd Delegated Prefix. For example, if this value is 8, 24 bits of the subscriber IPv4 prefix will be used when creating the IPv6 Delegated Prefix, determining the destination IPv4 encapsulation address, etc. If the value is 0, then the whole 32 bits of the IPv4 address is used in the encoding.
v6prefix-length	IPv6 Prefix length of the SP IPv6 prefix in number of bits.
6rd BR IPv4 address	The IPv4 address of the 6rd Relay (may be anycast).
SP 6rd IPv6 prefix	Variable length field containing the Service Provider's 6rd IPv6 prefix for this deployment and this 6rd CE router, zero padded to at least a full octet. Length of



the field is determined by the reported length of the entire DHCP option (len). An implementation must handle receipt of this option with zero padding up to a full 16 octets, for deployments preferring to send a fixed size option.

The client must validate the values received in the option as follows:

The 6rd IPv6 prefix includes the domain ID embedded within it, sizing the v6prefix-length accordingly to cover both the 6rd SP prefix size and domain ID for this 6rd route entry.

The 6rd router MUST install a default route to the relay. It should also install a sink route for the delegated prefix. Using the addresses in the example above with a 6rd IPv4 relay address of 10.0.0.1, the RIB will look like:

```
::/0 -> 2001:ABC1:0000:0100:: (default route)
2001:ABC1:6464:0100::/56 -> Null0 (6rd prefix sink route)
```

## **6.2. 6rd PPP IPCP option**

PPP [[RFC1661](#)], and PPPoE [[RFC2516](#)], remains a common way for a residential broadband end user to obtain configuration. In such deployments, the DHCPINFORM message may be used along with the DHCP option described above after IPCP [[RFC1332](#)] completes. However, PPP-based deployments often have no DHCP infrastructure in place, obtaining IP configuration solely from RADIUS servers and network equipment via IPCP.

The PPP IPCP option is identical to the DHCP option, aside of the OPTION\_6RD field, which is assigned by IANA. It's fields and their function are identical, and not repeated here.

## **6.3. 6rd Broadband Forum TR-69 Object**

A large number of 6rd CE routers are managed directly by service providers via the Broadband Forum's "TR-69" management interface. This section will make informational reference to the associated Broadband Forum document that describes this object.

## **7. Provisioning the Service Provider 6rd Border Relay**

As the 6rd IPv4 relay address is configurable, there is no need for a





well known anycast address as specified in [RFC3068](#) [[RFC3068](#)]. For increased reliability and load-balancing, the relay address can be an anycast address shared by all of the SP BRs for a given 6rd Domain. As 6rd is stateless, any BR may be used at any time. The 6rd relay MUST use its anycast IPv4 address as the source address in packets relayed via the SP network to the 6rd CE router.

Since 6rd uses provider address space, no specific routes need to be advertised externally for 6rd to work, neither in IPv6 nor IPv4 BGP. However, the 6rd IPv4 relay anycast addresses must be advertised in the providers IGP.

This example show how the 6rd prefix is created based on a /32 IPv6 prefix with a private IPv4 address were the first octet is "compressed" out:

```
SP prefix: 2001:0DB8::/32
6rd IPv4 prefix: 10.0.0.0/8
6rd router IPv4 address: 10.100.100.1
6rd site IPv6 prefix: 2001:0DB8:6464:0100::/56
```

## **8. Encapsulation considerations**

IPv6 in IPv4 encapsulation is done as specified in 6to4 [[RFC3056](#)] and in Basic Transition Mechanisms for IPv6 Hosts and Routers [[RFC4213](#)].

IPv6 packets from a 6rd CE router are encapsulated in IPv4 packets when they leave the site via its 6rd CE WAN side interface. The V4ADDR MUST be configured to send and receive packets on this interface.

MTU and fragmentation issues for IPv6 in IPv4 tunnelling is discussed in detail in [section 3.2 of RFC4213](#) [[RFC4213](#)]. 6rd's scope is limited to a service provider network. If the MTU is well-managed such that the IPv4 MTU on the 6rd CE WAN interface is set so that no fragmentation occurs within the boundary of the SP, then the IPv6 MTU should be set to the IPv4 MTU minus the size of the encapsulating IPv4 header (20 bytes). IPv4 Path MTU discovery MAY be used to adjust the MTU of the tunnel as described in [section 3.2.2 of RFC4213](#) [[RFC4213](#)] or the IPv6 tunnel MTU may be explicitly configured.

The IPv6 tunnel MTU, whether determined automatically or configured directly, MUST be advertised on the LAN-side by setting the MTU option in Router Advertisements [[RFC4861](#)] messages to the IPv6 tunnel MTU.



### **8.1. Receiving Rules**

In order to prevent spoofing of IPv6 addresses, the BR and CE MUST validate the source address of the encapsulated IPv6 packet with the address of the IPv4 it is encapsulated by. If the addresses do not match, the packet is dropped.

The 6rd CE router should drop packets received on the 6rd virtual interface for destinations not covered by the 6rd Delegated prefix.

## **9. Transition Considerations**

6rd is intended to deliver a production-level service to customer sites. Once 6rd IPv6 access is available, the SP network can migrate to IPv6 at its own pace with little or no affect on the customer. When native IPv6 is fully available, the 6rd CE router is provisioned with IPv6 on its WAN side. 6rd and native IPv6 can coexist for a time while the customer site is adopts the new IPv6 native prefix, and then 6rd deprovisioned. Alternatively, the same numbering plan for 6rd may be used for the native service, though this might require a "flag day" when the 6rd service is turned off and native service is initialized.

While 6rd bears resemblance to 6to4 and utilizes the same encapsulation and base mechanisms, it is not intended as a replacement for 6to4. Unlike 6to4, 6rd is for use only in an environment where a service provider cooperates closely to deliver the IPv6 service. 6to4 routes with the 2002::/16 prefix may exist alongside 6rd in the 6rd CE router, and doing so may offer some efficiencies when communicating directly with 6to4 routers.

## **10. Address space usage**

The 6rd prefix is an RIR delegated IPv6 prefix. It must encapsulate an IPv4 address and must be short enough so that a /56 or /60 can be given to subscribers. Using the full IPv4 address assigning a /56 for subscribers would mean that each service provider using 6rd would require a /24 for 6rd in addition to other IPv6 address needs they have. Assuming that 6rd would be stunningly successful and taken up by almost all AS number holders (32K) then the total address usage of 6rd would be equivalent to a /9. If instead delegated /60s to subscribers the service provider would require a /28 and the total global address consumption by 6rd would be equivalent to a /13. Again, this assumes that 6rd is used by all AS number holders in the IPv4 Internet today at the same time, and that none have moved to native IPv6 and reclaimed the 6rd space which was being used.



As 6rd uses service provider address space, 6rd uses the normal address delegation a service provider gets from its RIR and no global allocation of a single 6rd address block like for example the 6to4 2002::/16 is needed.

The 6rd address block can be reclaimed when all users of it has transitioned out of it into native IPv6 service. This requires renumbering and usage of additional address space during the transition period.

To alleviate concerns about address usage 6rd allows for leaving out redundant IPv4 prefix bits in the encoding of the IPv4 address inside the 6rd IPv6 address. This is most useful where the IPv4 address space is very well aggregated. For example to provide each customer with a /60, if a service provider has all its IPv4 customers under a /12 then only 20 bits needs to be used to encode the IPv4 address and the service provider would only need a /40 IPv6 allocation for 6rd. If private address space is used then a 10/8 would require a /36. If multiple 10/8 domains are used then up to 16 could be supported within a /32.

## **11. Security Considerations**

A 6to4 router as specified in [RFC 3056](#) [[RFC3056](#)] can be used as an open relay. It can be used to relay IPv6 traffic and as a traffic anonymizer. By restricting the 6rd Domain to within a provider network a 6rd router only needs to accept packets from a single or small set of known 6rd relay routers. As such many of the threats against 6to4 as described in [RFC3964](#) [[RFC3964](#)] do not apply.

When applying the receiving rules [Section 8.1](#) IPv6 packets are as well protected against spoofing as IPv4 packets are within an SP network.

## **12. IANA Considerations**

IANA is requested to assign a new DHCP Option code point for OPTION\_6RD.

IANA is requested to assign a new IPCP Type for 6RD\_IPCP\_TYPE.

## **13. Acknowledgements**

This draft is based on Remi Despres' original idea described in [[I-D.despres-6rd](#)] and the work done by Rani Assaf, Alexandre Cassen,



and Maxime Bizon at Free Telecom. Brian Carpenter and Keith Moore documented 6to4, which all of this work is based upon. Review and encouragement have been provided by many others and in particular Alain Durand, Wojciech Dec, Thomas Clausen, Martin Gysi and Remi Despres.

## **14. References**

### **14.1. Normative References**

- [RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", [RFC 1332](#), May 1992.
- [RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, [RFC 1661](#), July 1994.
- [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), February 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", [RFC 2516](#), February 1999.
- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC 3056](#), February 2001.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.
- [RFC3964] Savola, P. and C. Patel, "Security Considerations for 6to4", [RFC 3964](#), December 2004.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", [RFC 4213](#), October 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.





## **14.2. Informative References**

- [I-D.despres-6rd]  
Despres, R., "IPv6 Rapid Deployment on IPv4 infrastructures (6rd)", [draft-despres-6rd-03](#) (work in progress), April 2009.
- [I-D.durand-softwire-dual-stack-lite]  
Durand, A., Droms, R., Haberman, B., and J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion", [draft-durand-softwire-dual-stack-lite-01](#) (work in progress), November 2008.
- [RFC3068] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", [RFC 3068](#), June 2001.
- [RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", [RFC 3484](#), February 2003.

### Authors' Addresses

Mark Townsley  
Cisco  
Paris,  
France

Phone: +33 15 804 3483  
Email: [townsley@cisco.com](mailto:townsley@cisco.com)

Ole Troan  
Cisco  
Bergen,  
Norway

Phone: +47 917 38519  
Email: [ot@cisco.com](mailto:ot@cisco.com)

