Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: September 29, 2012

R. Despres, Ed.
RD-IPtech
R. Penno
Juniper Networks
Y. Lee
Comcast
G. Chen
China Mobile
J. Qin
March 28, 2012

# IPv4 Residual Deployment via IPv6 - Unified Solution (4rd)
# draft-despres-softwire-4rd-u-06

Abstract

The 4rd automatic tunneling mechanism makes IPv4 Residual Deployment possible via IPv6 networks without maintaining for this per-customer states in 4rd-capable nodes (reverse of the IPv6 Rapid Deployment of 6rd). To cope with the IPv4 address shortage, customers can be assigned IPv4 addresses with restricted port sets. In some scenarios, 4rd-capable customer nodes can exchange packets of their IPv4-only applications via stateful NAT64s that are upgraded to support 4rd tunnels (in addition to their IP/ICMP translation of RFC6145).

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 September 29, 2012.

Table of Contents

## 1. Introduction

For deployments of residual IPv4 service via IPv6 networks, the need for a stateless solution is expressed in [I-D.ietf-softwire-stateless-4v6-motivation] (no per customer state in IPv4-IPv6 gateway nodes of the provider). This document specifies such a solution, named "4rd" for IPv4 Residual Deployment. With it, IPv4 packets are transparently tunneled across IPv6 networks (reverse of 6rd [RFC5969] in which IPv6 packets are statelessly tunneled across IPv4 networks). While IPv6 headers are too long to be mapped into IPv4 headers, so that 6rd requires encapsulation of full IPv6 packets in IPv4 packets, IPv4 headers can be reversibly mapped into IPv6 headers so that 4rd tunnel packets can be designed to be valid IPv6 packets, thus ensuring compatibility with IPv6-only middle boxes that perform deep-packet-inspection.

In order to deal with the IPv4-address shortage, customers can be assigned shared IPv4 addresses, with statically assigned restricted port sets (a particular application of the A+P approach of [RFC6346]).

The design of 4rd builds on a number of previous proposals made for IPv4-via-IPv6 transition technologies listed in Section 9.

In some use cases, IPv4-only applications of 4rd-capable customer nodes can also work with stateful NAT64s of [RFC6146], provided these are upgraded to support 4rd tunnels in addition IP/ICMP translation of [RFC6145], with the advantage of a more complete IPv4 transparency.

Terminology is defined in Section 2. How the 4rd model fits in the Internet architecture is summarized in Section 3. The protocol specification is detailed in Section 4. Section 5 illustrates a few typical 4rd use cases. Section 6 and Section 7 respectively deal with security and IANA considerations. Previous proposals that influenced this specification are listed in Section 9.

The key words "MUST", "SHOULD", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 2. Terminology

ISP: Internet-Service Provider. In this document, the service it offers can be DSL, fiber-optics, cable, or mobile. The ISP can also be a private-network operator.

4rd (IPv4 Residual Deployment): An extension of the IPv4 service where public-IPv4 addresses can be statically shared with restricted port sets assigned to customers.

4rd domain (or Domain): An ISP-operated IPv6 network across which 4rd is supported according to the present specification.

Tunnel packet: An IPv6 packet that transparently conveys an IPv4 packet across a 4rd domain. Its header has enough information to reconstitute the IPv4 header at Domain exit. Its payload is the original IPv4 payload.

CE (Customer Edge): A customer-side tunnel endpoint function. It can be in a node that is a host, a router, or both.

BR (Border Relay): An ISP-side tunnel-endpoint function. Because its operation is stateless (neither per CE nor per session state) it can be replicated in as many nodes as needed for scalability.

4rd IPv6 address: IPv6 address used as destination of a Tunnel packet sent to a CE or a BR.

NAT64+: An ISP NAT64 of [RFC6146] that is upgraded to support 4rd tunneling when IPv6 addresses it deals with have the 4rd-IPv6-address format.

4rd IPv4 address: A public IPv4 address or, in case of a shared IPv4 address, a public transport address (public IPv4 address plus port number).

PSID (Port-Set Identifier): A flexible-length field that algorithmically identifies a port set.

4rd IPv4 prefix: A flexible-length prefix that may be a a public IPv4 prefix, a public IPv4 address, or a public IPv4 address followed by a PSID.

Mapping rule: A set of parameters that BRs and CEs can use either to derive a 4rd IPv6 address from a 4rd IPv4 address, or that CEs can use to build an IPv6 address that will reach a NAT64+. Mapping rules are also used by CEs to derive their own 4rd IPv4 prefixes from their delegated IPv6 prefixes.

EA bits (Embedded Address bits): Bits that are the same in a 4rd IPv4 address and in the 4rd IPv6 address derived from it.

BR mapping rule: The mapping rule applicable to off-domain IPv4 addresses reachable via BRs.

CE mapping rule: A mapping rule applicable to public IPv4 addresses, shared or not, assigned to some CEs.

NAT64+ mapping rule: The mapping rule applicable to IPv4 addresses reachable via a NAT64+.

CNP (Checksum Neutrality preserver): A field of 4rd IPv6 addresses that ensures that TCP-like checksums do not change when IPv4 addresses are replaced by 4rd IPv6 addresses.

V octet: An octet whose value permits to distinguish 4rd IPv6 addresses from native IPv6 addresses.

## 3. The 4rd Model

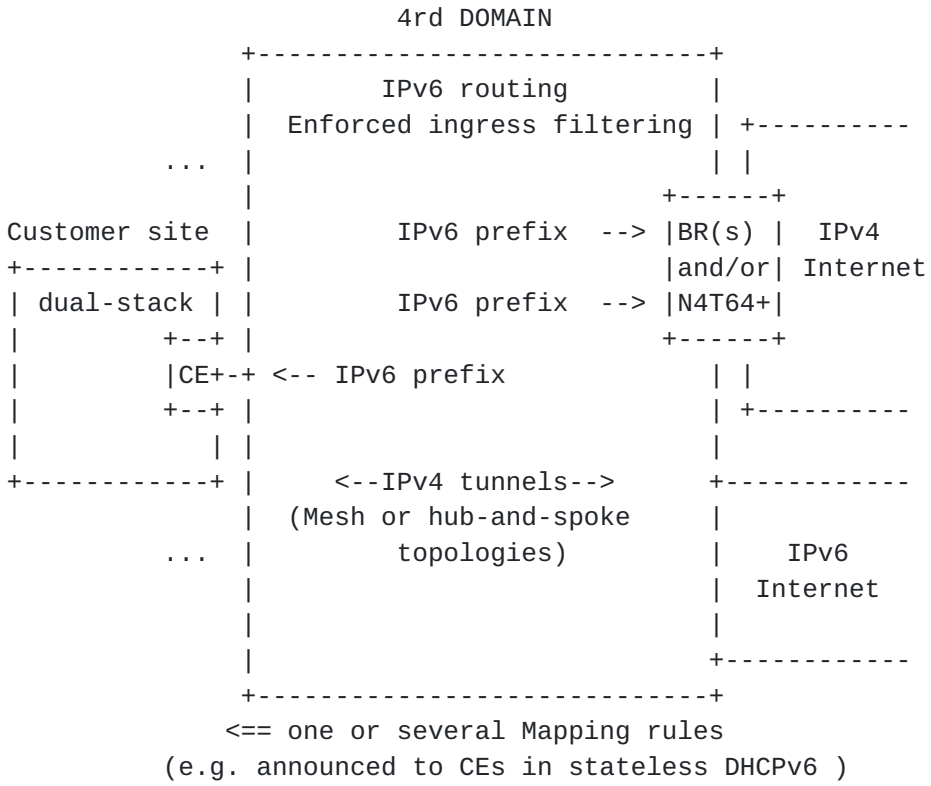


Figure 1

How the 4rd model fits in the Internet architecture is represented in Figure 1.

One or several Mapping rules are announced to CEs so that they can find, based on their delegated IPv6 prefixes, their assigned IPv4 address space. This space can be specified by a public IPv4 prefix, a public IPv4 address, or a shared public IPv4 address with a restricted port set. It can also be no IPv4 address if the ISP operates a NAT64+.

R-1: A node whose CE is assigned a shared IPv4 address MUST include a NAT44 [RFC1631]. This NAT44 MUST only use external ports that are in the CE assigned port set.

NOTE 1: An ISP NAT64 that has per-session stateful operation can be also upgraded to support 4rd Mapping rules. Thus, for each customer whose delegated IPv6 prefix matches a CE or BR mapping rule, it can have per-customer and per-session stateless operation even if this customer's node is IPv6 only. Details of such an upgrade are beyond the scope of this specification.

NOTE 2: This specification only concerns IPv4 communication between IPv4-capable endpoints. For communication between IPv4-only endpoints and IPv6 only remote endpoints, the BIH specification of [RFC6535] can be used. It can coexist in a node with the CE function, including if the IPv4-only function is a NAT44 [RFC1631].

## 4. Protocol Specification

### 4.1. Mapping rules and other Domain parameters

R-2: CEs and BRs MUST be configured with the following Domain parameters:

A. One or several Mapping rules, each one comprising:

1. Rule IPv4 prefix

2. EA-bits length

3. Rule IPv6 prefix

4. WKPs authorized (OPTIONAL)

5. Rule IPv6 suffix (OPTIONAL)

B. Domain PMTU

C. Hub&spoke topology (Yes or No)

D. Tunnel traffic class (OPTIONAL)

"Rule IPv4 prefix" is used to find which Mapping rule applies to a 4rd IPv4 address (Section 4.4). Rules where it is longer than /0 are CE mapping rules. It is a /0 in BR and NAT64+ mapping rules.

"EA-bits length" specifies the number of bits of 4rd IPv4 addresses that, with this Mapping rule, are copied into the derived 4rd IPv6 address. It MUST be 32 in BR and NAT64+ mapping rules.

"Rule IPv6 prefix" is the prefix that is substituted to the Rule IPv4 prefix found in a 4rd IPv4 address to derive a 4rd IPv6 address (Section 4.4). In a BR mapping rule, it MUST be a /80 whose 9th octet is the V octet. In a NAT64+ mapping rule it MUST be a /80 whose 9th octet is the "u" octet of [RFC6052].

"WKPs authorized" can be set if the mapping rule assigns shared IPv4 addresses to CEs (length of Rule IPv4 prefix plus EA-bits length > 0). It then specifies that well-known ports can be assigned to some CEs depending on their PSID values. If not set, fairness is privileged, with no well-known port assigned to any CE, whatever its PSID value (privilege to fairness).

"Rule IPv6 suffix", if provided, is a field to be added after EA bits of a 4rd IPv6 address after its EA bits.

> It is only used in Domains where a CEs can be placed in customer sites behind third-party CPEs, and where these CPEs use some address bits to route packets among their physical ports (one CE per site, always attached to the same CPE physical port). A use case where it applies is presented in Section 5.3.2.

"Hub&spoke topology", if set to Yes, requires CEs to tunnel all IPv4 packets via BRs. If set to No, CE-to-CE packets take the same routes as native IPv6 packets between the same CEs.

"Domain PMTU", is the IPv6 path MTU that the ISP can guarantee for all its IPv6 paths between CEs and between BRs and CEs. It MUST be

at least 1280 [RFC2460].

"Tunnel traffic class", if provided, is the IPv6 traffic class that BRs and CEs MUST set in Tunnel packets.

If this parameter is not specified, Explicit Congestion Notification of [RFC3168], which may be set by intermediate nodes during tunnel traversal, are propagated to IPv4 destinations.

## 4.2. Tunnel-packet Format

R-3: Domain-entry nodes that receive IPv4 packets with IPv4 options MUST discard them, and return the ICMPv4 error message of [RFC0792] that signals such an IPv4-option incompatibility: Type = 12, Code = 0, Pointer = 20).

NOTE: This limitation is made to privilege simplicity, knowing that no IPv4 option is necessary for IPv4 operation.

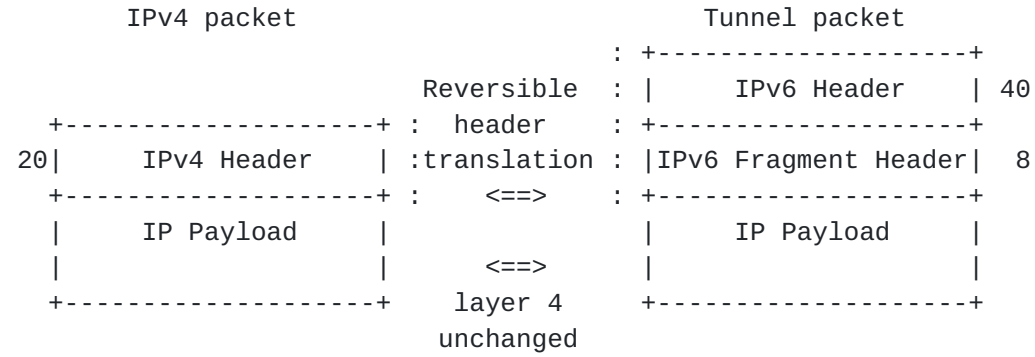


Figure 2

R-4: Domain-entry nodes that receive IPv4 packets without IPv4 options MUST convert them into Tunnel packets, and Domain-exit nodes MUST convert them back into IPv4 packets (Figure 2). Fields values to be set at Domain entry and at Domain exit are detailed in Table 1, and those to be set at Domain-exit are detailed in Table 2. IPv4 DF, IPv4 TOS, and IPv4 ID, are placed in IPv6 Identifications as detailed in Figure 3.

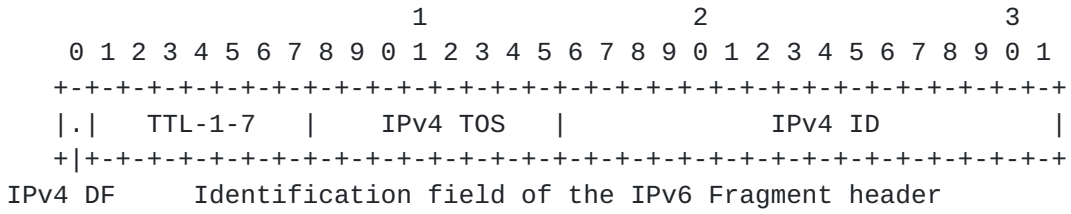


Figure 3

| IPv6 FIELDS | VALUES SET AT DOMAIN ENTRY |
|---|---|
| Version | 6 |
| Traffic class | TOS or parameter (Section 4.6) |
| Flow label | 0 |
| Payload length | Total length - 12 |
| Next header | 44 (Fragment header) |
| Hop limit (bit 0) | Time to live (bit 0) |
| Hop limit (bits 1-7) | 127 |
| Source address | See Section 4.4 |
| Dest. address | See Section 4.4 |
| 2nd next header | Protocol |
| Frag. offset | Frag. offset |
| M | More fragments (MF) |
| IPv4 DF | Don't fragment (DF) |
| TTL-1-7 | TTL (bits 0-7) |
| IPv4 TOS | Type of service (TOS) |
| IPv4 ID | Identification |

Table 1

| IPv4 FIELDS | VALUES SET AT DOMAIN EXIT |
|---|---|
| Version | 4 |
| Header length | 5 |
| TOS | Traffic class or IPv4 TOS (Section 4.6) |
| Total Length | Payload length + 12 |
| Identification | IPv4 ID |
| DF | IPv4 DF |
| MF | M |
| Fragment offset | Fragment offset |
| Time to live (bit 0) | Hop limit (bit 0) |
| Time to live (bits 1-7) | TTL-1-7 |
| Protocol | 2nd Next header |
| Header checksum | Computed as per [RFC0791] |
| Source address | Bits 80-11 of source address |
| Destination address | Bits 80-11 of destination address |

Table 2

## 4.3. From IPv6 Prefixes to 4rd IPv4 prefixes and port sets

R-5: A CE whose delegated IPv6 prefix starts with the Rule IPv6 prefix of one or several Mapping rules MUST select the rule for which the match is the longest. It then derives its 4rd IPv4 prefix and follows (Figure 4). First, the CE replaces the Rule IPv6 prefix by the Rule IPv4 prefix and, if the found Mapping rule has a Domain IPv6 suffix, deletes its last s bits, where s is the Rule-IPv6-suffix length. The result is the CE 4rd IPv4 prefix. If this CE 4rd IPv4 prefix has less than 32 bits, the CE takes it as its assigned IPv4 prefix. If it has exactly 32 bits, the CE takes it as its IPv4 address. If it has more than 32 bits, the CE MUST takes the first 32 bits as its shared IPv4 address, and bits beyond the first 32 as its Port-set identifier (PSID). Ports of its restricted port set are by default those that have any non-zero value in their first 4 bits, followed by the PSID, and followed by any values in

remaining bits. If the WKP authorized option is set, all ports can be assigned: there is no 4-bit offset before the PSID (Figure 4).

NOTE: The choice of the default PSID position in Port fields has been guided by the following objectives: (1) for fairness, avoid having any of the well-known ports 0-1023 in the port set specified by any PSID value (these ports have more value than others); (2) for compatibility RTP/RTCP [RFC4961], include in each port set pairs of consecutive ports; (3) in order to facilitate operation and training, have the PSID at a fixed position in port fields; (4) in order to facilitate documentation in hexadecimal notation, and to facilitate maintenance, have this position nibble aligned. With the choice made, port range 0-4095 is unassigned instead of only 0-1023, the minimum required, but this is a trade-off in view of other objectives, in particular nibble alignment and overall simplicity.

R-6: A CE whose delegated prefix matches the Rule IPv6 prefix of no CE Mapping rule, but matches that of the BR mapping rule, MUST take as it IPv4 address the 32 bit that follow this /80 prefix in its delegated IPv6 prefix. If this delegated prefix is not a /112, 4rd cannot be enabled, and an implementation-dependent administrative action MAY be taken.

A CE whose delegated prefix matches the Rule IPv6 prefix of neither any CE Mapping rule or BR mapping rule, but is in a Domain that has a NAT64+ mapping rule, MUST take as its IPv4 address the unspecified IPv4 address 0.0.0.0.

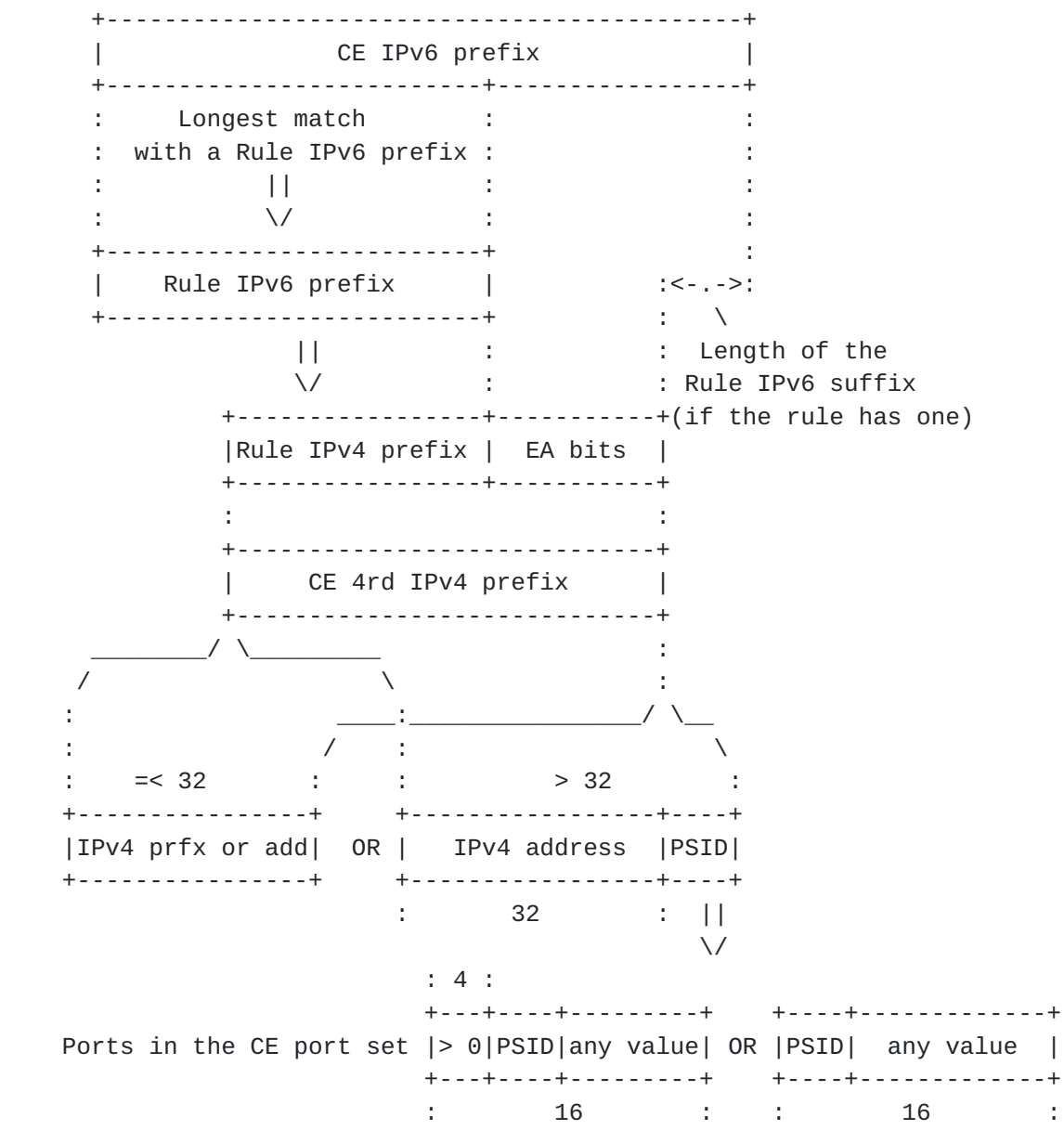


Figure 4

## 4.4. From 4rd IPv4 addresses to 4rd IPv6 Addresses

R-7: BRs, and CEs that are assigned public IPv4 addresses, shared or not, MUST derive 4rd IPv6 addresses from 4rd IPv4 addresses by the steps below (or their functional equivalent (Figure 5 details the shared address case):

(1) If Hub&spoke topology is No in the Domain, find the Mapping rule whose Rule IPv4 prefix has the longest match with the IPv4 address.

(2) If none is found with an IPv4 prefix longer than /0, or if Hub&spoke topology is Yes in the Domain, take the BR mapping rule, if it exists, the NAT64+ mapping rule otherwise.


Figure 5

(3) If the Rule IPv4 prefix plus EA-bits length does not exceed 32, i.e. 4rd IPv4 prefix = 32 - k with >= 0, delete the last k bits of the IPv4 address.

Otherwise, i.e. if the Rule IPv4 prefix plus EA-bits length is 32 + k with k >= 0, take k as the PSID length, and append to the IPv4 address the PSID copied from bits 4 to 4 + k - 1 of a field whose place depends on whether the address is source or destination, on whether the packet is ICMP or not, and, if it is ICMP, whether it is an error message or an echo message:

a. If the packet Protocol is not ICMP, bits 0-15 for an IPv4 source address, and bits 16-31 for a destination address.

b. If the packet is an ICMPv4 error message, bits 240-255 for a source address; bits 224-239 for a destination address.

c. If the packet is an ICMPv4 echo or echo-reply message, the Port field is the ICMPv4 Identification field (bits 32-47).

NOTE: Using Identification fields of ICMP messages as port fields permits to exchange Echo requests and Echo replies between shared-address CEs and and IPv4 hosts having exclusive IPv4 addresses. Echo exchanges between two shared-address CEs remain impossible, but this is a limitation inherent to address sharing (one reason among many to use IPv6).

Editor's note following questions on the WG mailing list: As specified, the PSID, when applicable, is taken in the TCP-like port field of the available IPv4 payload without checking that the protocol is one that really has a port field. This is what keeps BR operation independent from layer-4 protocols. A consequence to be noted is that a packet may go from a BR to a shared-address CE with a protocol that is not supported by this CE. In this case, the normal CE-node-NAT44 reaction is to returns an ICMPv4 "protocol unreachable" error message. The IPv4 source is thus informed of its mistake.

(4) Replace in the result the Rule IPv4 prefix by the Rule IPv6 prefix.

(5) If the Mapping rule has a Domain IPv6 suffix, append this suffix to the result.

(6) If the result is shorter than a /64, append to it a null padding up to 64 bits, followed by a V octet (0x03), followed by a null octet, and followed by the IPv4 address.

NOTE: The V octet is a 4rd-specific mark. Its function is to ensure that 4rd does not interfere with the choice of subnet prefixes in CE sites. For this, the V octet has its "u" and "g" bits of [RFC4291] both set to 1. This differs from "u" = 0, reserved for local-scope Interface IDs, and also differs from "u" = 1 and "g"= 0, reserved for unicast Interface IDs using the EUI-64 format. Bits other than "u" and "g", are proposed to be 0, giving V = 0x03.

With the V octet, IPv6 packets can be routed to the 4rd function within a CE node based on a /80 prefix that no native-IPv6 address can contain.

The V octet can also facilitate maintenance by the parameterless distinction it introduces between Tunnel packets and native-IPv6 packets. A tunnel packet has at least one of its IPv6 addresses having the V octet.

(7) Add to the result a Checksum-neutrality preserver (CNP) equal, in one's complement arithmetic, to minus the sum of the five 16-bit words of address-bits 0-79.

NOTE: CNP guarantees that, for all protocols that have ports at the same place as in TCP and use the same checksum algorithm as TCP, Tunnel packets are valid IPv6 packets, and this independently from where the checksum field is placed for each protocol. Today, such protocols are UDP [RFC0768], TCP [RFC0793], UDP-Lite [RFC3828], and DCCP [RFC5595]. Should new ones be specified, BRs will support them without needing an update.

(8) CEs that are assigned unspecified IPv4 addresses (Section 4.3), MUST use source and IPv6 addresses as detailed in Figure 6, (a) and (b) respectively. A NAT64+ uses as IPv6 source address (b), and as IPv6 destination address that it has in its binding information base.

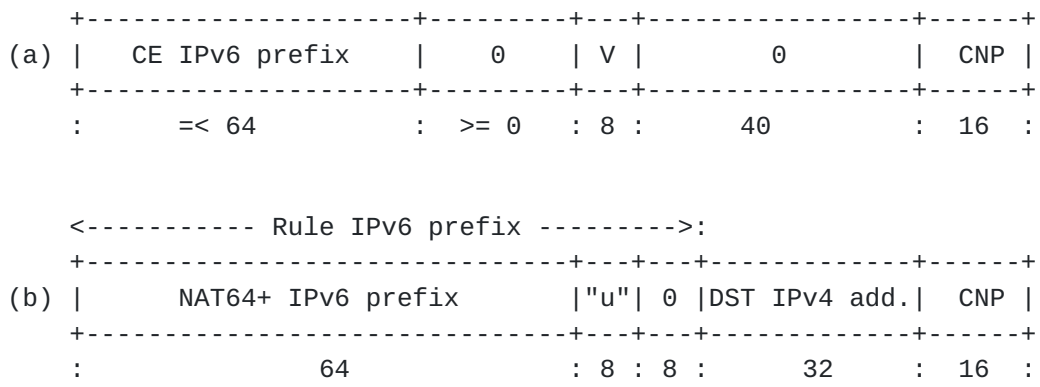


Figure 6

## 4.5. Fragmentation Considerations

### 4.5.1. Fragmentation at Domain Entry

R-8: If an IPv4 packet enters a CE or BR with a size such that the size of a directly derived Tunnel packet would exceed the Domain PMTU, the packet has to be either fragmented or discarded. The Domain-entry node MUST discard it if it has DF = 1 (with an ICMP error message returned to the source). It MUST fragment it otherwise. The payload length of each fragment MUST be at most Domain PMTU - 48.

### 4.5.2. Ports of Fragments addressed to Shared-Address CEs

Because ports are available only in first fragments of IPv4 fragmented packets, a BR needs a mechanism to send to the right shared-address CEs all fragments of fragmented packets.

For this, a BR MAY systematically reassemble fragmented IPv4 packets before tunneling them. However, but this consumes large memory space, opens denial-of-service-attack opportunities, and can significantly increase forwarding delays.

R-9: BRs SHOULD support an algorithm whereby received IPv4 packets can be forwarded on the fly. The following is an example of such algorithm:

(1) At BR initialization, if at least one CE mapping rule concerns shared IPV4 addresses (length of Rule IPv4 prefix + EA-bits length > 32), the BR initializes an empty "IPv4-packet table" whose entries have the following items:

- IPv4 source
- IPv4 destination
- IPv4 identification.
- Destination port.

(2) When the BR receives an IPv4 packet whose matching Mapping rule is one of shared addresses (length of Rule IPv4 prefix + EA-bits length > 32), the the BR searches the table for an entry whose IPv4 source, IPv4 destination, and IPv4 Identification, are those of the received packet. The BR then performs actions detailed in Table 3 depending on which conditions hold.

(3) The BR performs garbage collection for table entries that remain unchanged for longer than some limit. This limit, normally longer that the maximum time normally needed to reassemble a packet is not critical. It should however not be longer than 15 seconds [RFC0791].

| - CONDITIONS - | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| First Fragment (offset=0) | Y | Y | Y | Y | N | N | N | N |
| Last fragment (MF=0) | Y | Y | N | N | Y | Y | N | N |
| An entry has been found | Y | N | Y | N | Y | N | Y | N |
| - RESULTING ACTIONS - | | | | | | | | |
| Create a new entry | - | - | - | X | - | - | - | - |
| Use the port of the entry | - | - | - | - | X | - | - | - |
| Update port of the entry | - | - | X | - | - | - | X | - |
| Delete the entry | X | - | - | - | X | - | - | - |
| Forward the packet | X | X | X | X | X | - | X | - |

Table 3

R-10: For the above algorithm to be effective, CEs that are assigned shared IPv4 addresses MUST NOT interleave fragments of several fragmented packets.

R-11: CEs that are assigned IPv4 prefixes, and are in nodes that route public IPv4 addresses rather than only using NAT44s, MUST have the same behavior as described just above for BRs.

### 4.5.3. Packet Identifications from Shared-Address CEs

When packets go from CEs that share the same IPv4 address to a common destination, a precaution is needed to guarantee that packet Identifications set by sources are different. Packet reassembly at destination, which is based only on source IPv4 address and Identification, could otherwise be confused. Probability of such confusions may in theory be very low but, in order to avoid creating new attack opportunities, a safe solution is needed.

R-12: A CE that is assigned a shared IPv4 address MUST only crete packet Identifications that have the CE PSID in their bits 4 to 4 + PSID length - 1.

R-13: A BR or a CE that receives a packet from a shared-address CE MUST check that bits 4 to 4 + PSID length - 1 of the packet Identification are equal to the PSID found in source 4rd IPv4 address.

## 4.6. TOS and Traffic-Class Considerations

In networks that support Explicit congestion notification (ECN), the TOS of IPv4 headers and the Traffic class of IPv6 headers have the same meanings [RFC3168]. Their first 6 bits are a Differentiated Services CodePoint (DSCP), and their two last bits are an Explicit Congestion Notification (ECN). [RFC6040] details how the ECN field MAY evolve if a packet traverses a router that signals congestion condition before packets are dropped.

R-14: In a 4rd domain that has a Tunnel-traffic-class parameter, BRs and CE's MUST, at Domain entry, copy this parameter to set Traffic-class fields of Tunnel packets they transmit, and copy the IPv4 TOS into the IPv4-TOS field of Figure 3. At Domain exit, they MUST copy back the IPv4-TOS-field value into the TOS field of the IPv4 packet.

R-15: A 4rd domain that has no Tunnel-traffic-class parameter MUST support the ECN normal mode of [RFC6040]. Its BRs and CEs MUST copy the IPv4 TOS into the IPv6 Traffic class at Domain entry, and copy back the IPv6 Traffic class (which may have a changed ECN value), into the IPv4 TOS at Domain exit.

## 4.7. Tunnel-Generated ICMPv6 Error Messages

If an Tunnel packet is discarded on its way across a 4rd domain because of an unreachable destination, an ICMPv6 error message is returned to the IPv6 source (an address starting with the BR IPv6 prefix, or with a CE IPv6 and having the V octet). For the source of the discarded IPv4 packet to be informed of packet loss, the ICMPv6 message has to be converted into an ICMPv4 message.

R-16: If a CE or BR receives an ICMPv6 error message [RFC4443], it MUST synthesize an ICMPv4 error packet [RFC0792]. This packet MUST contain the first 8 octets of the discarded-packet IP payload. If the CE or BR has a global IPv4 address, this address MUST be used as source of this packet. Otherwise, 192.70.192.254 SHOULD be used as this source (address taken in the /24 range proposed for such a purpose in draft-xli-behave-icmp-address-04, and subject to IANA confirmation). ICMPv6 Type = 1 and Code = 0 (Destination unreachable, No route to destination") MUST be translated into ICMPv4 Type = 3 and Code = 0 (Destination unreachable, Net unreachable). ICMPv6 Type = 1 and Code = 0 (Time exceeded, Hop limit exceeded in transit) MUST be translated into ICMPv4 Type = 11 and Code = 0 (Time exceeded, Time to live exceeded in transit).

## 4.8. Provisioning 4rd Parameters to CEs

Domain parameters listed in Section 4.1 are subject to the following constraints:

R-17: Each Domain MUST have a BR mapping rule and/or a NAT64+ mapping rule.

The BR mapping rule is used by CEs that are assigned public IPv4 addresses, shared or not, and the NAT64+ mapping rule is used by CEs that are assigned unspecified IPv4 addresses (Section 4.3).

R-18: Each CE and each BR MUST support up to 32 Mapping rules.

This number of is to ensure that independently acquired CEs an BR nodes can always interwork. (Its value, which is not critical, can easily be changed if another value is found by the WG more desirable.)

ISPs that need Mapping rules for more IPv4 prefixes than this number SHOULD split their networks into multiple Domains. Communication between these domains can be done in IPv4, or by

some implementation-dependent but equivalent other means.

R-19: For mesh topologies (CE-CE paths without BR traversal), all mapping rules of the Domain MUST be sent to all CEs. For hub-and-spoke topologies (all CE-CE paths via BRs), each CE MAY only be sent the BR mapping rule of the Domain plus, if different, the CE mapping rule that applies to its IPv6 prefix.

R-20: CEs MUST be able to acquire Parameter listed in Section 4.1 in DHCPv6 (ref. [RFC2131]), with formats detailed in Figure 7 and Figure 8.

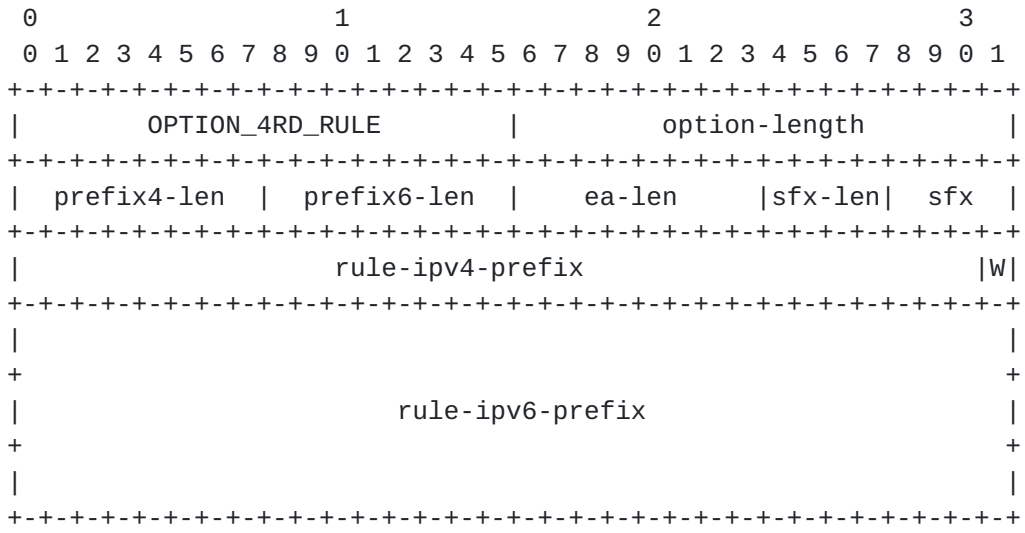


Figure 7

- option-code: OPTION_4RD_RULE (TBD1)
- option-length: 20
- prefix4-len: number of bits of the Rule IPv4 prefix
- prefix6-len: number of bits of the Rule IPv6 prefix
- sfx-len: number of bits of the Rule IPv6 suffix (= 0 if the rule has no suffix)
- ea-len: EA-bits length

- rule-ipv4-prefix: Rule IPv4 prefix, left aligned
- W: WKP authorized, = 1 if set
- rule-ipv6-prefix: Rule IPv6 prefix, left aligned

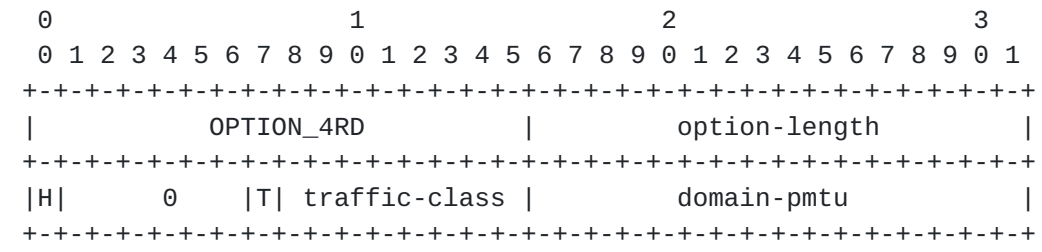


Figure 8

- option-code: OPTION_4RD (TBD2)
- option-length: 4
- H: Hub&spoke topology (= 1 if Yes)
- T: Traffic-class flag (= 1 if a Tunnel traffic class is provided)
- traffic-class: Tunnel-traffic class
- domain-pmtu: Domain PMTU (at least 1280)

Other means than DHCPv6 that may prove useful to provide 4rd parameters to CEs are off-scope for this document. The same or similar parameter formats would however be recommended to facilitate training and operation.

## 5. Use-Case Examples

### 5.1. Textual representation of Mapping rules

In the next sections, each Mapping rule will be represented as follows, using 0bXXX to represent binary number XXX, and square brackets [ ] for what is optional:

{Rule IPv4 prefix, EA-bits length, Rule IPv6 prefix[, Rule IPv6 suffix]}

EXAMPLES:

```
{0.0.0.0/0, 32, 2001:db8:0:1:3000::/80}
                    (a BR mapping rule)
{0.0.0.0/0, 32, 2001:db8:0:1::/80}
                    (a NAT64+ mapping rule)
{198.16.0.0/14, 22, 2001:db8:4000::/34}
                    (a CE mapping rule)
{198.16.0.0/14, 22, 2001:db8:4000::/34, 0b0010}
                    (a CE mapping rule with a suffix)
```

## 5.2. A pragmatic method to configure Mapping Rules

As far as mapping rules are concerned, the simplest deployment model is that in which the Domain has only one rule (the BR mapping rule). To assign an IPv4 address to a CE in this model, an IPv6 /112 is assigned to it comprising the BR /64 prefix, the V octet, a null octet, and the IPv4 address. This model has however the following limitations: (1) shared IPv4 addresses are not supported; (2) IPv6 prefixes used for 4rd are too long to be used also for native IPv6 addresses; (3) if the IPv4 address space of the ISP is split with many disjoint IPv4 prefixes, the IPv6 routing plan must be as complex as an IPv4 routing plan based on these prefixes.

With more mapping rules, CE prefixes used for 4rd can be those used for native IPv6. How to choose CE mapping rules for a particular deployment needs not being standardized.

The following is only a particular pragmatic approach that can be used for various deployment scenarios, and which is used in use-cases that follow:

(1) Select a "Common IPv6 prefix" that will appear at the beginning of all 4rd CE IPv6 prefixes.

(2) Choose all IPv4 prefixes to be used for 4rd, and which of them will be used for rule i.

(3) Choose the sharing ratio 2^Ki applicable to rule i, thus determining PSID_length(i) = Ki. For a rule that assigns IPv4 prefixes of length L shorter than /32 to CEs take as negative PSID length L - 32.

(4) Choose the length of CE IPv6 prefixes applicable to rule i.

(5) Derive from these data, and for each rule, the length of the "Rule code" that will be appended to the Common prefix to get the Rule IPv6 prefix (Figure 9):

```
   L[Rule code(i)] = L[CE IPv6 prefix(i)]
                   - L[Common_IPv6_prefix]
                   - 32 - L[Rule IPv4 prefix(i)] + PSID_length(i)
```

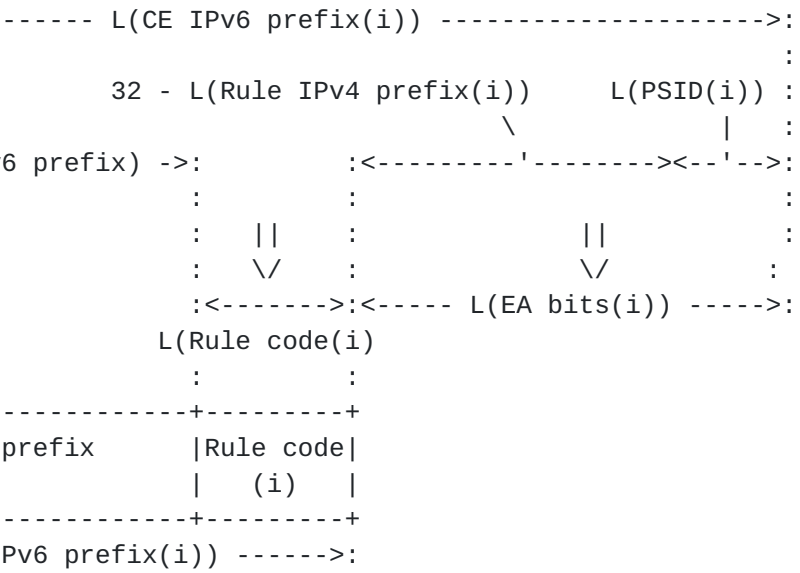


Figure 9

(6) For each rule taken successively, take as Rule code the prefix which has the obtained length, which does not overlap with previously chosen Rule codes, and which, to make a systematic choice, has the lowest value. (Lowest if interpreted as fractional part of a binary number: with successive lengths 4, 3 , 5, and 2, this gives for example, in binary notation, 0000, 001, 00010, and 01)

## 5.3. Adding Shared IPv4 Addresses to an IPv6 Network

### 5.3.1. With CEs within CPEs

We consider an ISP that offers IPv6-only service to up to 2^20 customers. Each customer is delegated a /56, starting with common prefix 2001:db8:0::/36. It wants to add public IPv4 service to customers that are 4rd-capable. It prefers to do it with stateless operation in its nodes, but has largely less IPv4 addresses than IPv6 addresses so that a sharing ratio is necessary.

The only IPv4 prefixes it can use are 192.8.0.0/15, 192.4.0.0/16, 192.2.0.0/16, and 192.1.0.0/16 (neither overlapping nor aggregetable). This gives 2^(32-15) + 3*2^(32-16) IPv4 addresses, i.e. 2^18 + 2^16). For the 2^20 customers to have the same sharing ratio, the number of IPv4 addresses to be shared has to be a power of 2. The ISP can therefore renounce to use one /16, say the last one. (Whether it could be motivated to return it to its Internet Registry is off-scope for this document.) The sharing ratio to apply is then 2^20 / 2^18 = 2^2 = 4, giving a PSID length of 2.

Applying principles of Section 5.2 with L[Common IPv6 prefix] = 36, L[PSID] = 2 for all rules, and L[CE IPv6 prefix(i)] = 56 for all rules, Rule codes and Rule IPv6 prefixes are:

| CE Rule IPv4 prefix | EA bits length | Rule-Code length | Code (binary) | CE Rule IPv6 prefix |
|---|---|---|---|---|
| 192.8.0.0/15 | 19 | 1 | 0 | 2001:db8:0::/37 |
| 192.4.0.0/16 | 18 | 2 | 10 | 2001:db8:800::/38 |
| 192.2.0.0/16 | 18 | 2 | 11 | 2001:db8:c00::/38 |

Mapping rules are then the following:

```
{192.8.0.0/15, 19, 2001:0db8:0000::/37}
{192.4.0.0/16, 18, 2001:0db8:0800::/38}
{192.2.0.0/16, 18, 2001:0db8:0c00::/38}
{0.0.0.0/0,    32, 2001:0db8:0000:0001:3000::/80}
```

The CE whose IPv6 prefix is, for example, 2001:db8:0bbb:bb00::/56, derives its IPv4 address and its port set, according to Section 4.3, as sfollows:

```
IPv6 prefix         : 2001:0db8:0bbb:bb00::/56

Rule IPv6 prefix(i) : 2001:0db8:0800::/38 (longest match)
Rule IPv4 prefix(i) : 192.4.0.0/16
EA-bits length(i)   : 18

PSID length(i)      : 16 + 18 - 32 = 2
EA bits             :   11 1011 1011 1011 1011
Rule IPv4 prefix(i) : 1100 0000 0000 0100

IPv4 address        : 1100 0000 0000 0100 1110 1110 1110 1110

PSID                : 11

IPv4 address        : 192.4.238.238  (1110 1110 = 238)
Ports               : yyyy 11xx xxxx xxxx
                        with y..y > 0, and x...x any value
```

An IPv4 packet sent to address 192.4.238.238 and port 7777 is tunneled to the IPv6 address obtained as follows (Section 4.4):

```
   IPv4 address         : 192.4.238.238
   Port field           : 7777  (0x1E61)

   Rule IPv4 prefix (i) : 192.4.0.0/16  (longest match)
   EA-bits length (i)   : 18
   Rule IPv6 prefix (i) : 2001:0db8:0800::/38

   IPv4 address         : 1100 0000 0000 0100 1110 1110 1110 1110
   EA bits
   Rule IPv4 prefix (i) : 1100 0000 0000 0100
   IPv4 suffix          :                     1110 1110 1110 1110

   PSID length (i)      : 19 - 17 = 2
   Port field           : 0001 1110 0110 0001  (7777)
   PSID                 :      11

   EA bits              :                     1110 1110 1110 1110 11
                        :                      11 1011 1011 1011 1011
   CE IPv6 prefix       : 2001:0db8:0bbb:bb00::/56
   IPv6 address         : 2001:0db8:0bbb:bb00:3000:192.4.238.238:YYYY
                          with YYYY = the computed CNP
```

### 5.3.2. With some CEs behind Third-party Router CPEs

We now consider an ISP that has the same need as in the previous section except that, instead of using only its own IPv6 infrastructure, it uses that of a third-party provider, and that some of its customers use CPEs of this provider to use specific services that it offers. In these CPEs, a non-zero index is used to route IPv6 packets to the physical port to which CEs are attached, say 0x2. Each such CPE delegates to the CE nodes the customer-site IPv6 prefix followed by this index.

The ISP is supposed to have the same IPv4 prefixes as in the previous use case, 192.8.0.0/15, 192.4.0.0/16, and 192.2.0.0/16, and to use the same Common IPv6 prefix, 2001:db8:0::/36.

We also assume that only a minority of customers use the third-party CPE, so that it is sufficient to use only one of the two /16s for them.

Mapping rules are then:

```
{192.8.0.0/15, 19, 2001:0db8:0000::/37}
{192.4.0.0/16, 18, 2001:0db8:0800::/38, 0b0001}
{192.2.0.0/16, 18, 2001:0db8:0c00::/38}
{0.0.0.0/0,    32, 2001:0db8:0000:0001:3000::/80}
```

CEs that are behind third-party CPEs derive their own IPv4 addresses and port sets as in Section 5.3.1, except that, because the Mapping rule that applies to their IPv6 prefixes have a Rule IPv6 suffix, they delete this suffix from the end of their delegated IPv6 prefixes before deriving their 4rd IPv4 prefixes (Section 4.3).

In a BR, and also in a CE if the topology is mesh, the IPv6 address that is derived from IPv4 address 192.4.238.238 and port 7777 is obtained as in the previous section, except for the two last steps which become:

```
CE IPv6 prefix       : 2001:0db8:0bbb:bb20::/60 (suffix 0x2 appended)
IPv6 address         : 2001:0db8:0bbb:bb20:3000:192.4.238.238:YYYY
                       with YYYY = the computed CNP
```

## 5.4. Replacing Dual-stack Routing by IPv6-only Routing

In this use case, we consider an ISP that offers IPv4 service with public addresses individually assigned to its customers. It also offers IPv6 service, having deployed for this dual-stack routing. Because it provides its own CPEs to customers, it can upgrade all its CPEs to support 4rd. It wishes to take advantage of this capability to replace dual-stack routing by IPv6-only routing without changing any IPv4 address or IPv6 prefix.

For this, the ISP can use the single-rule model described at the beginning of Section 5.2. If the prefix routed to BRs is chosen to start with 2001:db8:0:1::/64, this rule is:

```
{0.0.0.0/0, 32, 2001:db8:0:1:3000::/80}
```

All what is needed in the network before disabling IPv4 routing is the following:

- In all routers, where there is an IPv4 route toward x.x.x.x/n, add a parallel route toward 2001:db8:0:1:3000:x.x.x.x::/(80+n)

- Where IPv4 address x.x.x.x was assigned to a CPE, now delegate IPv6 prefix 2001:db8:0:1:3000:x.x.x.x::/112.

NOTE: In parallel with this deployment, or after it, shared IPv4 addresses can be assigned to IPv6 customers. It is sufficient that IPv4 prefixes used for this be different from those used for exclusive-address assignments. Under this constraint, Mapping rules can be set up according to the same principles as those of Section 5.3.

### 5.5. Adding IPv6 and 4rd Service to a Net-10 network

In this use case, we consider an ISP that has only deployed IPv4, possibly because some of its network devices are not yet IPv6 capable. Because it did not have enough IPv4 addresses, it has assigned private IPv4 addresses of [RFC1918] to customers, say 10.x.x.x to support up to 2^24 customers ("Net-10" network, NAT444 model of [I-D.shirasaki-nat444]). It wishes to offer IPv6 service without further delay, using for this 6rd [RFC5969]. It also wishes to offer incoming IPv4 connectivity to its customers with a simpler solution than that of PCP [I-D.ietf-pcp-base].

The IPv6 prefix to be used for 6rd is supposed to be 2001:db8::/32, and the public IPv4 prefix to be used for shared addresses is supposed to be 192.16.0.0/16 (0xc610). The resulting sharing ratio is 2^24 / 2^(32-16) = 256, giving a PSID length of 8.

The ISP installs one or several BRs, at its border to the public IPv4 Internet. They support 6rd, and 4rd above it. The BR prefix /64 is supposed to be that which is derived from IPv4 address 10.0.0.1 (i.e. 2001:db8:0:100:/64).

In accordance with [RFC5969], 6rd BRs are configured with the following parameters IPv4MaskLen = 8, 6rdPrefix = 2001:db8::/32; 6rdBRIPv4Address = 192.168.0.1 (0xC0A80001).

4rd Mapping rules are then the following:

```
{192.16.0.0/16, 24, 2001:db8:0:0:3000::/80}
{0.0.0.0/,      32, 2001:db8:0:100:3000:/80,}
```

Any customer device that supports 4rd can then use its assigned shared IPv4 address with 240 assigned ports. It can thus avoid cascading its NAT44 with the NAT44 carrier-grade NAT44 of the ISP.

A CE whose NAT44 supports port forwarding, to provide incoming IPv4 connectivity either statically or dynamically with UPnP an/or NAT-PMP, can use this port forwarding with ports of the assigned port set (a possibility that does not exist in Net-10 networks without 4rd/6rd).

## 6. Security Considerations

Spoofing attacks

R-21: Domain-exit nodes MUST check, in each Tunnel packet they receive, that source the IPv6 address is that which is derived from the source 4rd IPv4 address of the packet. If the check fails the packet MUST be silently discarded.

This is needed because IPv6 ingress filtering [RFC3704] does not guarantee that the Tunnel packets are built in compliance with rules of the present specification.

With this precaution, and provided IPv6 ingress filtering is effective in the Domain, no opportunity for spoofing attacks in IPv4 is introduced by 4rd.

Routing-loop attacks

Routing-loop attacks that may exist in some automatic-tunneling scenarios are documented in [RFC6324]. No opportunity for routing-loop attacks 4rd has been identified with 4rd.

Fragmentation-related attacks

As discussed in Section 4.5, each BR of a Domain that assigns shared IPv4 should maintain a dynamic table for fragmented packets that go to these shared-address CEs.

This opens a vulnerability to a denial of service attack from hosts that would send very large numbers of first fragments, with different Identifications, without sending last fragments having the same Identifications. This vulnerability. Compared to that of BRs that reassemble fragmented packets, This vulnerability, which is is inherent to IPv4 address sharing (static or dynamic), is mitigated by the algorithm of Section 4.5.2 (it uses much less memory space than algorithms that store some fragments for some time.

## 7. IANA Considerations

IANA is requested to allocate the following:

- Two DHCPv6 option codes TBD1 and TBD2 for OPTION_4RD_RULE and OPTION_4RD of Section 4.8 respectively (to be added to section 24.3 of [RFC3315]

- A reserved IPv4 address to be used as source of ICMPv4 messages due to ICMPv6 error messages. Its proposed value is 192.70.192.254 (Section 4.7).

- An IPv6 Interface-ID type reserved for 4rd (the V octet of Section 4.4). For this a registry is recommended for Interface-ID types of unicast addresses that have neither local scope nor the universal scope of Modified EUI-64 format [RFC4291]), i.e. that have neither "u"=0 nor "u"=1 and "g"=0. is recommended. It would be available to for new Interface IDs that may be useful in the future.

## 8. Relationship with Previous Works

The present specification has been influenced by many previous IETF drafts, in particular those accessible at http://tools.ietf.org/html/draft-xxxx where xxxx are the following (in order of their first versions):

- bagnulo-behave-nat64 (2008-06-10)
- xli-behave-ivi (2008-07-06)
- despres-sam-scenarios (2008-09-28)
- boucadair-port-range (2008-10-23)
- ymbk-aplusp (2008-10-27)
- xli-behave-divi (2009-10-19)
- thaler-port-restricted-ip-issues (2010-02-28)
- cui-softwire-host-4over6 (2010-05-05)
- xli-behave-divi-pd (2011-07-02)
- dec-stateless-4v6 (2011-03-05)
- matsushima-v6ops-transition-experience (2011-03-07)
- despres-intarea-4rd (2011-03-07)
- deng-aplusp-experiment-results (2011-03-08)
- murakami-softwire-4rd (2011-07-04)

- operators-softwire-stateless-4v6-motivation (2011-05-05)
- murakami-softwire-4v6-translation (2011-07-04)
- despres-softwire-4rd-addmapping (2011-08-19)
- boucadair-softwire-stateless-requirements (2011-09-08)
- chen-softwire-4v6-add-format (2011-10-2)
- mawatari-softwire-464xlat (2011-10-16)
- mdt-softwire-map-dhcp-option (2011-10-24)
- mdt-softwire-mapping-address-and-port (2011-11-25)
- mdt-softwire-map-translation (2012-01-10)
- mdt-softwire-map-encapsulation (2012-01-27)

## 9. Acknowledgements

This specification has benefited over several years from independent proposals, questions, comments, constructive suggestions, and useful criticisms, coming from numerous IETF contributors. The author would like to thank all of them, but more particularly, in first name alphabetical order, Brian Carpenter, Behcet Sarikaya, Cameron Byrne, Congxiao Bao, Dan Wing, Francis Dupont, Gabor, Bajko, Gang Chen, Hui Deng, Jan Zorz, James Huang, Jaro Arkko, Laurent Toutain, Leaf Yeh, Mark Townsley, Maoke Chen, Marcello Bagnulo, Mohamed Boucadair, Nejc Skoberne, Olaf Maennel, Ole Troan, Olivier Vautrin, Peng Wu, Qiong Sun, Rajiv Asati, Ralph Droms, Randy Bush, Satoru Matsushima, Simon Perreault, Stuart Cheshire, Teemu Savolainen, Tetsuya Murakami, Tomasz Mrugalski, Tina Tsou, Tomasz Mrugalski, Washam Fan, Wojciech Dec, Xiaohong Deng, Xing Li,

## 10. References

### 10.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 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.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC6040] Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, November 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

## 10.2. Informative References

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", draft-ietf-pcp-base-19 (work in progress), December 2011.

[I-D.ietf-softwire-stateless-4v6-motivation]
Boucadair, M., Matsushima, S., Lee, Y., Bonness, O., Borges, I., and G. Chen, "Motivations for Stateless IPv4 over IPv6 Migration Solutions",

draft-ietf-softwire-stateless-4v6-motivation-00 (work in progress), September 2011.

[I-D.shirasaki-nat444] Yamagata, I., Shirasaki, Y., Nakagawa, A., Yamaguchi, J., and H. Ashida, "NAT444", draft-shirasaki-nat444-04 (work in progress), July 2011.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC1631] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, July 2004.

[RFC4961] Wing, D., "Symmetric RTP / RTP Control Protocol (RTCP)", BCP 131, RFC 4961, July 2007.

[RFC5595] Fairhurst, G., "The Datagram Congestion Control Protocol (DCCP) Service Codes", RFC 5595, September 2009.

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147,

April 2011.

[RFC6219] Li, X., Bao, C., Chen, M., Zhang, H., and J. Wu, "The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition", RFC 6219, May 2011.

[RFC6324] Nakibly, G. and F. Templin, "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", RFC 6324, August 2011.

[RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the IPv4 Address Shortage", RFC 6346, August 2011.

[RFC6535] Huang, B., Deng, H., and T. Savolainen, "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)", RFC 6535, February 2012.

## Authors' Addresses

Remi Despres (editor)
RD-IPtech
3 rue du President Wilson
Levallois,
France

Email: despres.remi@laposte.net

Reinaldo Penno
Juniper Networks
1194 N Mathilda Avenue
Sunnyvale, California 94089
USA

Email: rpenno@juniper.net

Yiu Lee
Comcast
One Comcast Center
Philadelphia, PA 1903
USA

Email: Yiu_Lee@Cable.Comcast.com

Gang Chen
China Mobile
53A, Xibianmennei Ave.
Xuanwu District, Beijing 100053
China

Email: phdgang@gmail.com

Jacni Qin
Shanghai,
China

Email: jacni@jacni.com