

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 3, 2010

M. Boucadair, Ed.
P. Levis
J-L. Grimault
A. Villefranke
France Telecom
July 2, 2009

Port Range Configuration Options for PPP IPCP
draft-boucadair-pppext-portrange-option-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 3, 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 memo defines two IPCP (IP Configuration Protocol, [[RFC1332](#)])

Options to be used in the context of Port Range solutions. IPCP is the configuration protocol used when PPP (Point-to-Point Protocol, [RFC1661]) is deployed.

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].

Table of Contents

1.	Introduction	3
2.	Port Range Options	3
2.1.	Terminology	3
2.2.	Description	4
2.3.	Illustration Examples	6
2.3.1.	Overview	6
2.3.2.	Successful Flow: Port Range Options supported by both the Client and the Server	7
2.3.3.	Port Range Options not supported by the Server	8
2.3.4.	Port Range Options not supported by the Client	10
3.	IANA Considerations	12
4.	Security Considerations	12
5.	Acknowledgements	12
6.	References	12
6.1.	Normative References	12
6.2.	Informative References	13
	Authors' Addresses	13

1. Introduction

Recently, within the context of IPv4 address depletion, several solutions have been submitted to the IETF to propose viable alternative solutions to Carrier Grade NAT (CGN).

[I-D.boucadair-port-range] is an example of these solutions which propose to share the same (public) IP address among several devices and to constrain the values used as port sources to a limited set of values. These solutions do not require an additional NAT level in the service provider's domain. Several means may be used to convey Port Range information.

This memo defines new IPCP options to be used to carry Port Range information. IPCP has been widely used to convey configuration information such as IP Compression Protocol [[RFC3241](#)][RFC3544] or IP-Address [[RFC1332](#)].

Concretely, this memo defines the notion of Port Mask which is generic and flexible. Several allocation schemes may be implemented when using a Port Mask. This draft proposes a basic mechanism that allows the allocation of a unique Port Mask.

IPv4 address exhaustion is only provided as an example of the usage of the PPP IPCP Options defined in this memo. Other usages may be considered in the future.

2. Port Range Options

This section defines the Port Range IPCP Options.

2.1. Terminology

To differentiate between a Port Range containing a contiguous span of port numbers and a Port Range with non contiguous port numbers, the following denominations are used:

- Contiguous Port Range: a set of port values which form a contiguous sequence.
- Non Contiguous Port Range: a set of port values which does not form a contiguous sequence.

Moreover, unless explicitly mentioned, Port Mask refers to the couple (Port Range Value, Port Range Mask).

This memo uses the same terminology as per [[RFC1661](#)].

2.2. Description

The Port Range Options are used to specify one range of ports (contiguous or not contiguous) pertaining to a given IP address. Concretely, these options are used to notify a remote peer about the Port Mask to be applied when selecting a port value as a source port. The Port Range Option is used to infer a set of allowed port values. A Port Mask defines a set of ports that all have in common a subset of pre-positioned bits. This set of ports is also called Port Range. Two port numbers are said to belong to the same Port Range if and only if, they have the same Port Mask.

A Port Mask is composed of a Port Range Value and a Port Range Mask:

- o The Port Range Value indicates the value of the significant bits of the Port Mask. The Port Range Value is coded as follows:
 - * The significant bits may take a value of 0 or 1.
 - * All the other bits (a.k.a., non significant ones) are set to 0.
- o The Port Range Mask indicates, by the bit(s) set to 1, the position of the significant bits of the Port Range Value.

These IPCP Configuration Options provide a way to negotiate the Port Range to be used on the local end of the link. It allows the sender of the Configure-Request message to state which Port Range associated with a given IP address is desired, or to request the peer to provide the configuration. The peer can provide this information by NAKing the options, and returning a valid Port Range (i.e., (Port Range Value, Port Range Mask)).

IPCP Port Range Value and Port Range Mask **MUST** be supported simultaneously.

When the server assigns only shared IP addresses, the peer must include Port Range Options in its request. If not, 0.0.0.0 is assigned by the server to that peer.

When a peer issues a request enclosing IPCP Port Range Options, and if the server does not support these options, Port Range Options are rejected by the server.

The formats of these IPCP Options are provided in Figure 1 and Figure 2.

The format of Port Range Value IPCP Option is illustrated in Figure 1

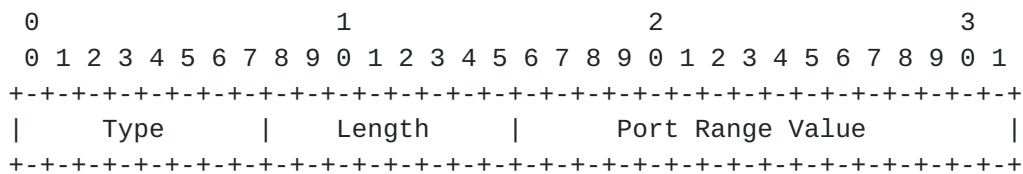


Figure 1: Format of the PRV IPCP Option

- o Type: To be assigned.
- o Length: This field includes the length of the overall option including the Type, Length and the PRV. It must be set to 4 bytes
- o Port Range Value (PRV): PRV indicates the value of the significant bits of the Port Mask. By default, no PRV is assigned.

The format of Port Range Mask IPCP Option is illustrated in Figure 2:

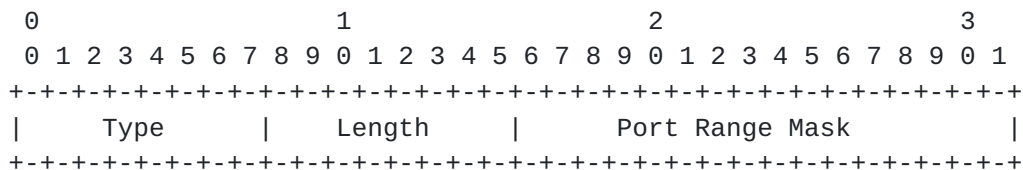


Figure 2: Format of the PRM IPCP Option

- o Type: To be assigned.
- o Length: This field includes the length of the overall option including Type, Length and PRV fields. It must be set to 4 bytes.
- o Port Range Mask (PRM): Port Range Mask indicates the position of the bits which are used to build the Port Range Value. By default, no PRM value is assigned. The 1 values in the Port Range Mask indicate by their position the significant bits of the Port Range Value.

Figure 3 provides an example of the resulting Port Range:

- Port Range Mask is set to 0001010000000000 (5120) and
- Port Range Value is set to 0000010000000000 (1024).

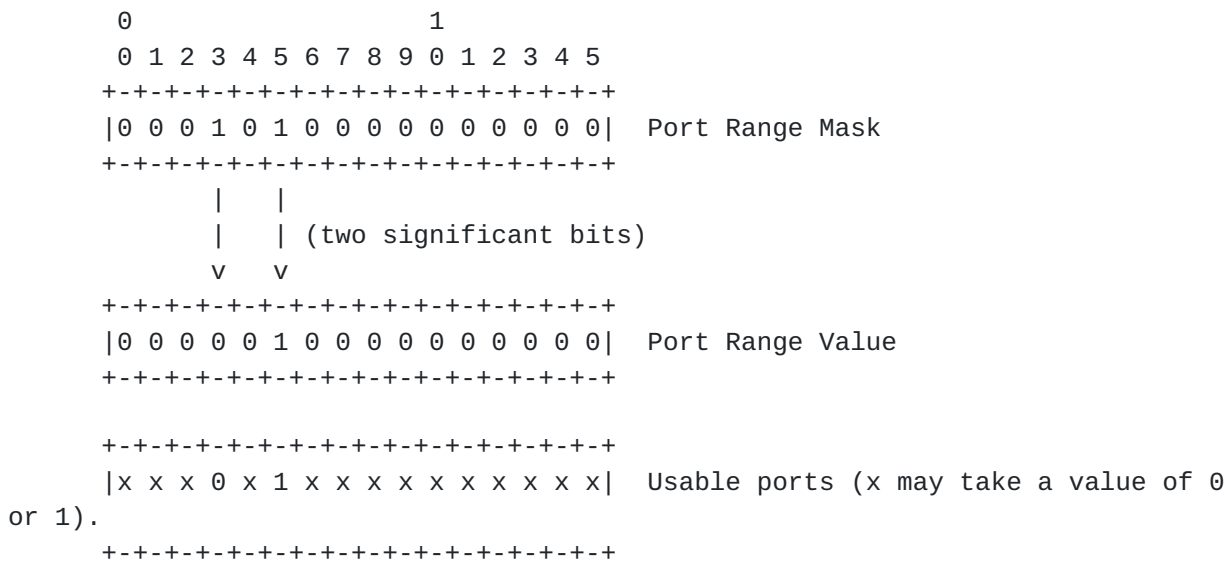


Figure 3: Example of Port Range Mask and Port Range Value

Port values belonging to this Port Range must have the 4th bit (resp. the sixth one), from the left, set to 0 (resp. 1). Only these port values will be used by the peer when enforcing the configuration conveyed by PPP IPCP.

2.3. Illustration Examples

2.3.1. Overview

These flows provide examples of the usage of IPCP to convey Port Range Options. As illustrated in Figure 4, IPCP messages are exchanged between a Host and a BRAS (Broadband Access Server).

1. The first example illustrates a successful IPCP exchange;
2. The second example shows the IPCP exchange that occurs when Port Range Options are not supported by the server;
3. The third example shows the IPCP exchange that occurs when Port Range Options are not supported by the client;
4. The fourth example shows the IPCP exchange that occurs when Port Range Options are not supported by the client and a non null IP (i.e., an address different from 0.0.0.0) address is enclosed in the first configuration request issued by the peer.

2.3.2. **Successful** Flow: Port Range Options supported by both the Client and the Server

The following message exchange (i.e., Figure 4) provides an example of successful IPCP configuration operation when Port Range IPCP Options are used.

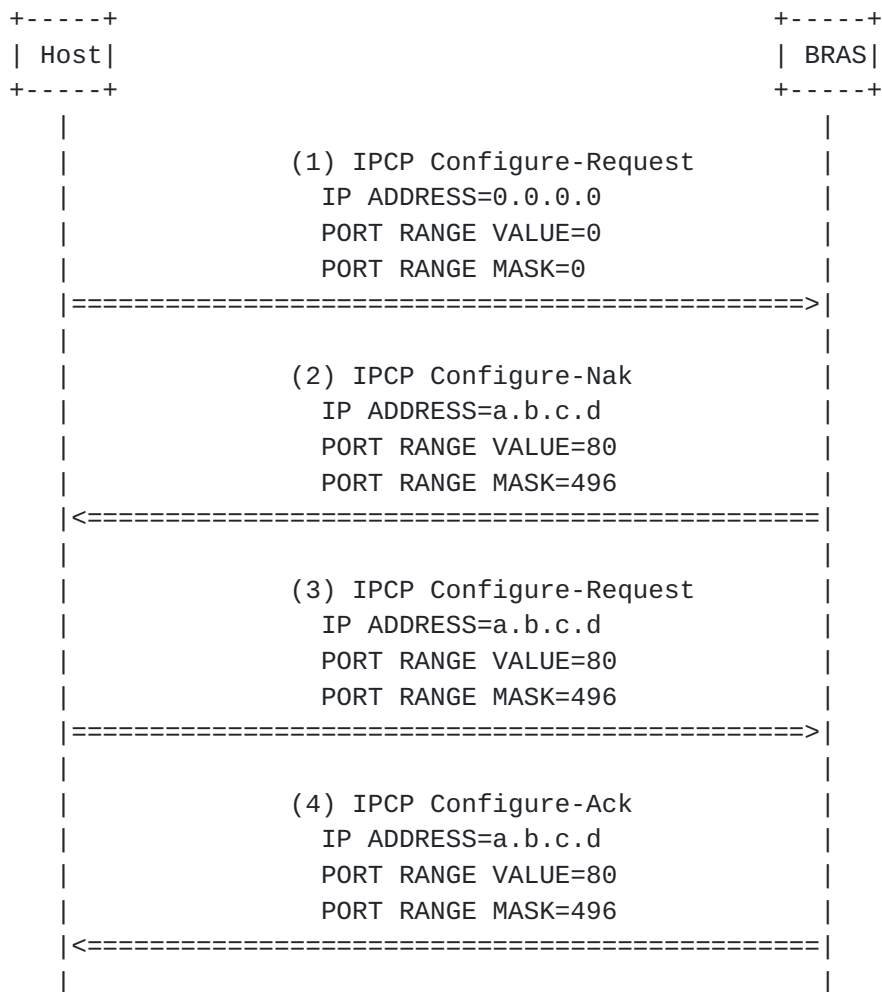


Figure 4: Successful flow

The main steps of this flow are listed below:

- (1) The Host sends a first Configure-Request which includes the set of options it desires to negotiate. All these Configuration Options are negotiated simultaneously. In this example, Configure-Request carries information about IP-address, Port Range Value and Port Range Mask Options. In this example, IP-address Option is set to 0.0.0.0, Port Range Value is set to 0 and Port

Range Mask is set to 0.

(2) BRAS sends back a Configure-Nak and sets the enclosed options to its preferred values. In this example: IP-Address Option is set to a.b.c.d, Port Range Value is set to 80 and Port Range Mask is set to 496.

(3) The Host re-sends a Configure-Request requesting IP-address Option to be set to a.b.c.d, Port Range Value to be set to 80 and Port Range Mask to be set to 496.

(4) BRAS sends a Configure-Ack message

As a result of this exchange, Host is configured to use as local IP address a.b.c.d and the following 128 contiguous Port Ranges resulting of the Port Mask (Port Range Value == 0, Port Range Mask == 496):

- from 80 to 95
- from 592 to 607
- ...
- from 65104 to 65119

2.3.3. Port Range Options not supported by the Server

This example (Figure 5) depicts an exchange of messages when the BRAS does not support IPCP Port Range Options.

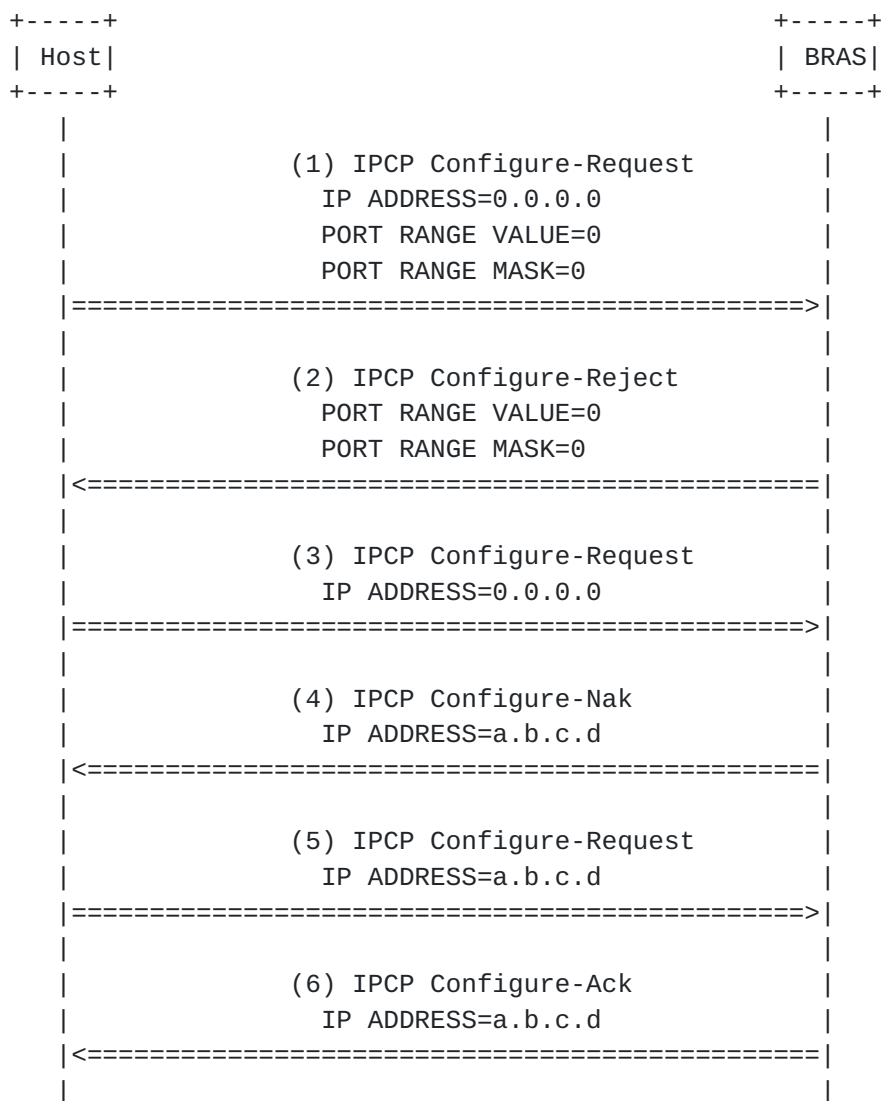


Figure 5: Failed flow: Port Range Options not supported by the server

The main steps of this flow are listed hereafter:

(1) The Host sends a first Configure-Request which includes the set of options it desires to negotiate. All these Configuration Options are negotiated simultaneously. In this example, Configure-Request carries the codes of IP-address, Port Range Value and Port Range Mask options. In this example, IP-address Option is set to 0.0.0.0, Port Range Value is set to 0 and Port Range Mask is set to 0.

(2) BRAS sends back a Configure-Reject to decline Port Range Value and Port Range Mask options.

(3) The Host sends a Configure-Request which includes only the codes of IP-Address option. In this example, IP-Address Option is set to 0.0.0.0.

(4) BRAS sends back a Configure-Nak and sets the enclosed option to its preferred value. In this example: IP-Address Option is set to a.b.c.d.

(5) The Host re-sends a Configure-Request requesting IP-Address Option to be set to a.b.c.d.

(6) BRAS sends a Configure-Ack message.

As a result of this exchange, Host is configured to use as local IP address a.b.c.d. This IP address is not a shared IP address.

2.3.4. Port Range Options not supported by the Client

This example (Figure 6) depicts exchanges when only shared IP addresses are assigned to end-user's devices. The support of IPCP Port Range Options is MANDATORY.

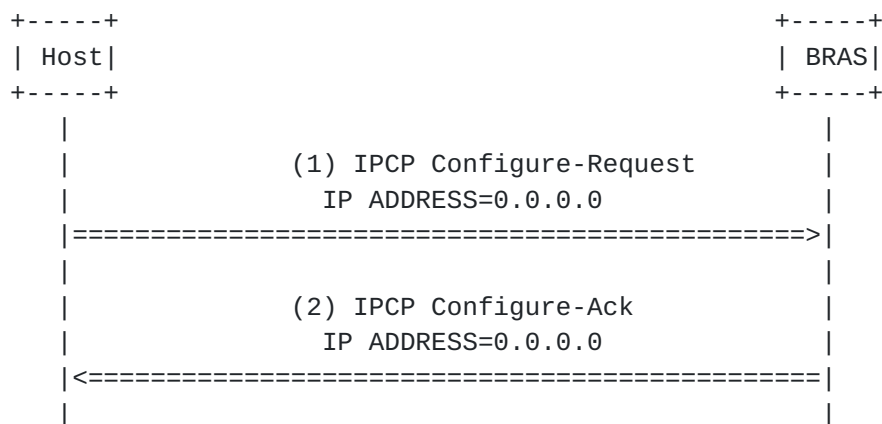


Figure 6: Port Range Options not supported by the Client

The main steps of this flow are:

(1) The Host sends a Configure-Request requesting IP-Address Option to be set to 0.0.0.0 and without enclosing Port Range Options.

(2) BRAS sends a Configure-Ack message and sets the IP address to 0.0.0.0 since only shared IP addresses are assigned.

As a result of this exchange, Host is configured to use as local IP address 0.0.0.0. Host is not able to access the service.

If in the first Configure-Request, a valid IP address is enclosed, the following exchange (Figure 7) should be experienced:

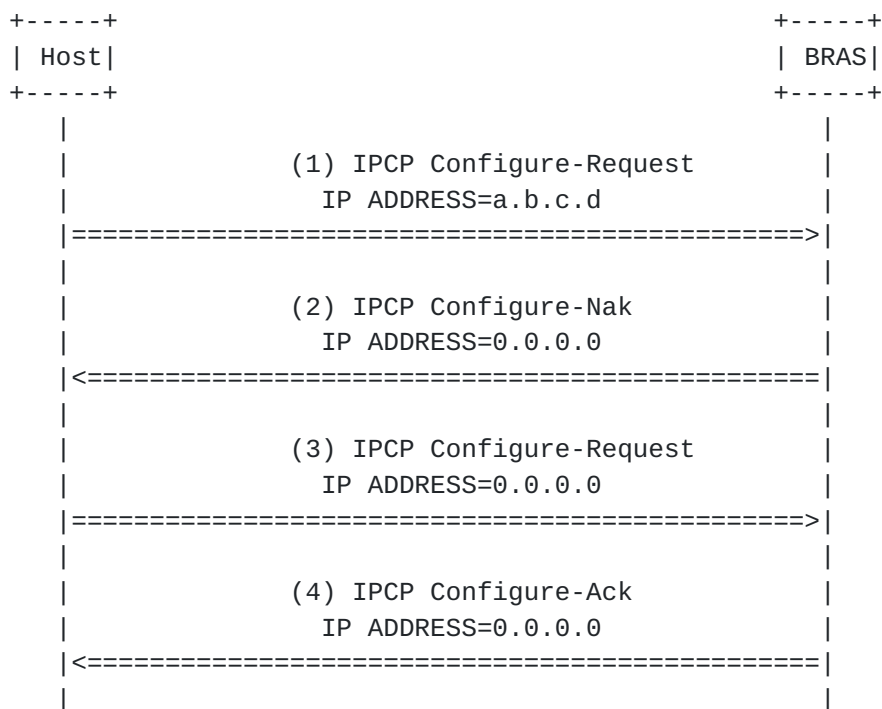


Figure 7: Port Range Options not supported by the Client (2)

The main steps of this flow are described below:

- (1) The Host sends a Configure-Request requesting IP-Address Option to be set to a.b.c.d and without enclosing Port Range Options.
- (2) BRAS sends a Configure-Nak and sets the enclosed option to its preferred value. In this example: IP-Address Option is set to 0.0.0.0 since only shared IP addresses are assigned.
- (3) The Host re-sends a Configure-Request requesting IP-Address Option to be set to 0.0.0.0.
- (4) BRAS sends a Configure-Ack message and confirms to set the IP address to 0.0.0.0.

As a result of this exchange, Host is configured to use as local IP

address 0.0.0.0. Host is not able to access the service.

3. IANA Considerations

This document requests IANA to assign numbers for the following IPCP Options:

- Port Range Value Option;
- Port Range Mask Option.

4. Security Considerations

This document does not introduce any security issue in addition to those related to PPP. Service providers should use authentication mechanisms such as CHAP [[RFC1994](#)] or PPP link encryption [[RFC1968](#)].

5. Acknowledgements

The authors would like to thank Christian JACQUENET for his review and inputs.

6. References

6.1. 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.
- [RFC1968] Meyer, G. and K. Fox, "The PPP Encryption Control Protocol (ECP)", [RFC 1968](#), June 1996.
- [RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", [RFC 1994](#), August 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2290] Solomon, J. and S. Glass, "Mobile-IPv4 Configuration Option for PPP IPCP", [RFC 2290](#), February 1998.

[RFC3241] Bormann, C., "Robust Header Compression (ROHC) over PPP", [RFC 3241](#), April 2002.

[RFC3544] Koren, T., Casner, S., and C. Bormann, "IP Header Compression over PPP", [RFC 3544](#), July 2003.

6.2. Informative References

[I-D.boucadair-port-range]
Boucadair, M., Levis, P., Bajko, G., and T. Savolainen,
"IPv4 Connectivity Access in the Context of IPv4 Address
Exhaustion", [draft-boucadair-port-range-01](#) (work in
progress), January 2009.

Authors' Addresses

Mohamed Boucadair (editor)
France Telecom
3, Av Francois Chateau
Rennes 35000
France

Email: mohamed.boucadair@orange-ftgroup.com

Pierre Levis
France Telecom

Email: pierre.levis@orange-ftgroup.com

Jean-Luc Grimault
France Telecom

Email: jeanluc.grimault@orange-ftgroup.com

Alain Villefranque
France Telecom

Fax:
Email: alain.villefranque@orange-ftgroup.com

