

Network Working Group
Internet-Draft
Expires: November 20, 2003

P. Thubert
M. Molteni
P. Wetterwald
Cisco Systems
May 22, 2003

IPv4 traversal for MIPv6 based Mobile Routers
draft-thubert-nemo-ipv4-traversal-01

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/lid-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 November 20, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

Since IPv6 connectivity is not yet broadly available, there is a need in NEMO for a simple technology that allows a MIPv6 based Mobile Router to roam over IPv4 networks.

The Doors Protocol proposed in this memo allows an arbitrary Mobile Node to roam even within private IPv4 address spaces, across both Network Address Translations (NAT), reverse NAT, and even Port Address Translation (PAT), in order to cope with the reality of today's Internet.

Internet-Draft

Doors

May 2003

Table of Contents

1.	Introduction	3
2.	Terminology and concepts	3
2.1	Doors Handle	3
2.2	Other definitions	5
3.	MIPv6 Doors support	5
3.1	Known Restrictions	7
3.2	Operation for a MIPv6 Mobile Node roaming over IPv4	7
3.2.1	MR Sending packets over the Doors tunnel	8
3.2.2	MR Receiving packets over the Doors tunnel	9
3.3	Operation for the Door	9
3.3.1	Door Receiving packets over the Doors tunnel	10
3.3.2	Door Sending packets over the Doors tunnel	11
3.4	Advantages of the Doors protocol	12
4.	IANA considerations	12
5.	Acknowledgements	12
	References	12
	Authors' Addresses	14
	Full Copyright Statement	15

Internet-Draft

Doors

May 2003

[1](#). Introduction

This document assumes that the reader is familiar with Mobile IPv6 defined in [\[12\]](#), with the concept of Mobile Router (MR) and with the Nemo terminology defined in [\[13\]](#), as well as IPv4 Network Address Translation (NAT) and Port Address Translation (PAT).

During the transition phase from IPv4 to IPv6, hot spots that actually provide IPv6 connectivity will be scarce and Mobile Routers should support an alternate roaming technology over IPv4.

There is an existing panel of solutions from the V6 ops (ISATAP, 6to4, TEREDO), but these solutions fail to traverse in a simple fashion all types of NAT and PAT that are heavily deployed today.

There is a real value in combining MIPv6 and IPv4 traversal technologies. MIP brings a MN-HA tunnel and a binding cache into the picture, as well as a keep alive procedure. The MIP cache can be used to store the PAT/NAT states, while the Binding flow can be tuned to keep the PAT/NAT active. As a result, it is possible for a IPv6 Mobile Router to traverse PAT/NAT with no protocol overhead or additional states in the network.

The Doors Protocol developed in this draft extends Mobile IPv6 and is more particularly aimed at the Nemo problem space. Some restrictions apply that could be circumvented by additional work.

[2](#). Terminology and concepts

[2.1](#) Doors Handle

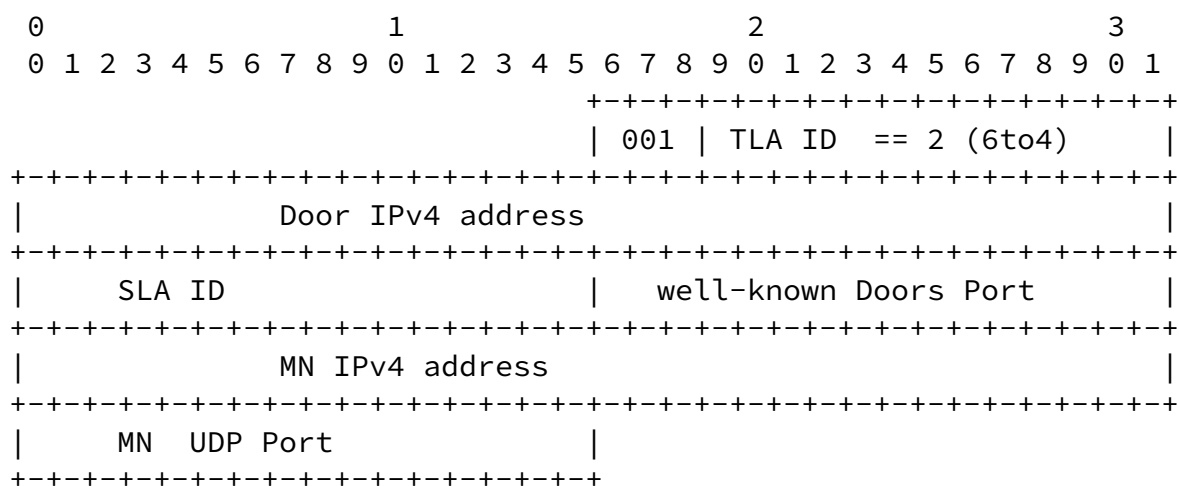
Doors inherits from 6to4 [\[10\]](#), that uses synthetized IPv6 addresses to build automatic tunnels across IPv4. In the Doors case, that IPv6 global unicast address is named a Doors Handle. The Doors Handle follows the 6to4 formatting rules, but it points on a IPv4 (UDP)

tunnel, as opposed to an interface on a machine.

Due to a NAT/PAT or reverse NAT traversal, the handle may be subject to IPv6 level Address Translation. Since we do not want to reintroduce the complexity of Application Level Gateways, the handle MUST NOT to be used as source or destination address as seen by upper layer protocols.

Rather, the only use of a Handle is as a CareOf address for Mobile IPv6 as defined in [12]. Note that some ICMP messages such as DHAAD may be need the Handle as source or destination. In that case, the ICMP layer chacksum must be updated when the Handle is modified.

The Doors Handle has the following format:



Doors Handle

001

Format Prefix (3 bit) for Aggregatable Global Unicast Addresses

TLA ID

Top-Level Aggregation Identifier (13 bits). Set to 2 as prescribed by RCF 3046 [10].

Door IPv4 Address

32-bits public IPv4 address of the door, that the MN learns dynamically while roaming, using DHCP or IPCP extension (TBD), or that is statically configured on the MN.

SLA ID

Site-Level Aggregation Identifier

Doors Port

16-bits UDP Destination port. A well known value DOORSPORT to be assigned by IANA (434 in the meantime).

Mobile Node IPv4 address and UDP port

The parameters of the socket on the MN side, generally obtained dynamically by the mobile Node.

Thubert, et al.

Expires November 20, 2003

[Page 4]

Internet-Draft

Doors

May 2003

[2.2](#) Other definitions

DoG

The Doors Gateway (DoG) is the function that terminates the Doors Tunnel on both Home and Mobile ends. The DoG performs IPv4/UDP automatic tunneling and a IPv6 level Network Address Translation.

DooR

A Doors Router (DooR) is a router that implements the Doors Gateway. The Door is connected to the Home Network via the IPv6 infrastructure. A Home Door may be implemented at the ingress of the Home Network. But Exit Doors may also be implemented at by private networks in order to avoid IPv4 NAT and PAT operations. In that case, the IPv4 address of the Exit Door should be available dynamically, for instance by means of DHCP or IPCP extensions.

Doors Tunnel

The Doors Tunnel is an IPv4/UDP automatic tunnel that encapsulates a Mobile IPv6 tunnel. The Tunnel has two Directions, InDoors and OutDoors.

InDoors and OutDoors

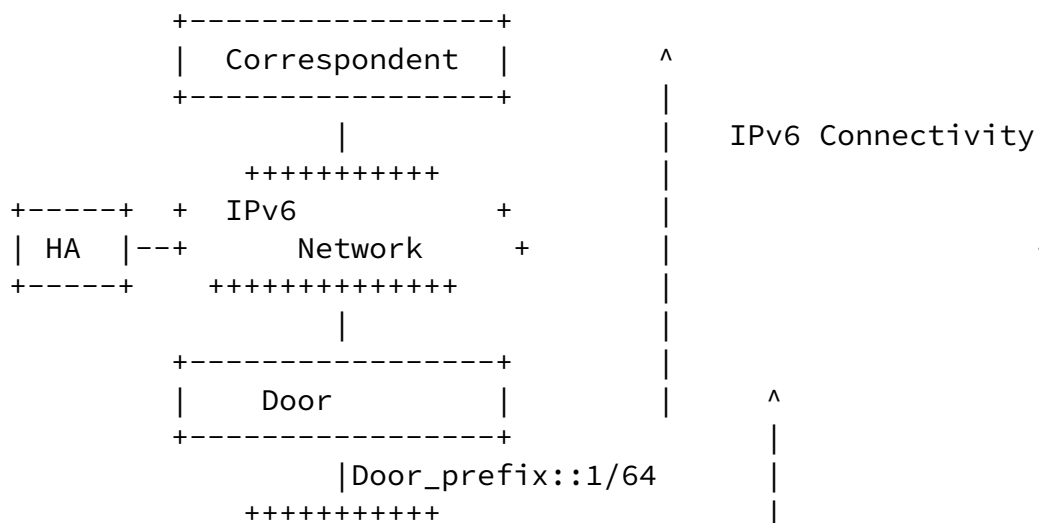
A packet going InDoors flows between the Mobile Node and the Door. A packet going OutDoors flows between the Door and the Mobile Node. In both cases, the packet is formed by an IPv6 packet that is encapsulated over IPv4 and UDP. A packet flowing InDoors as a source IPv6 address that is a Doors Handle. Reciprocally, a packet flowing OutDoors as a destination IPv6 address that is a Doors Handle. InDoors and OutDoors are mutually exclusive.

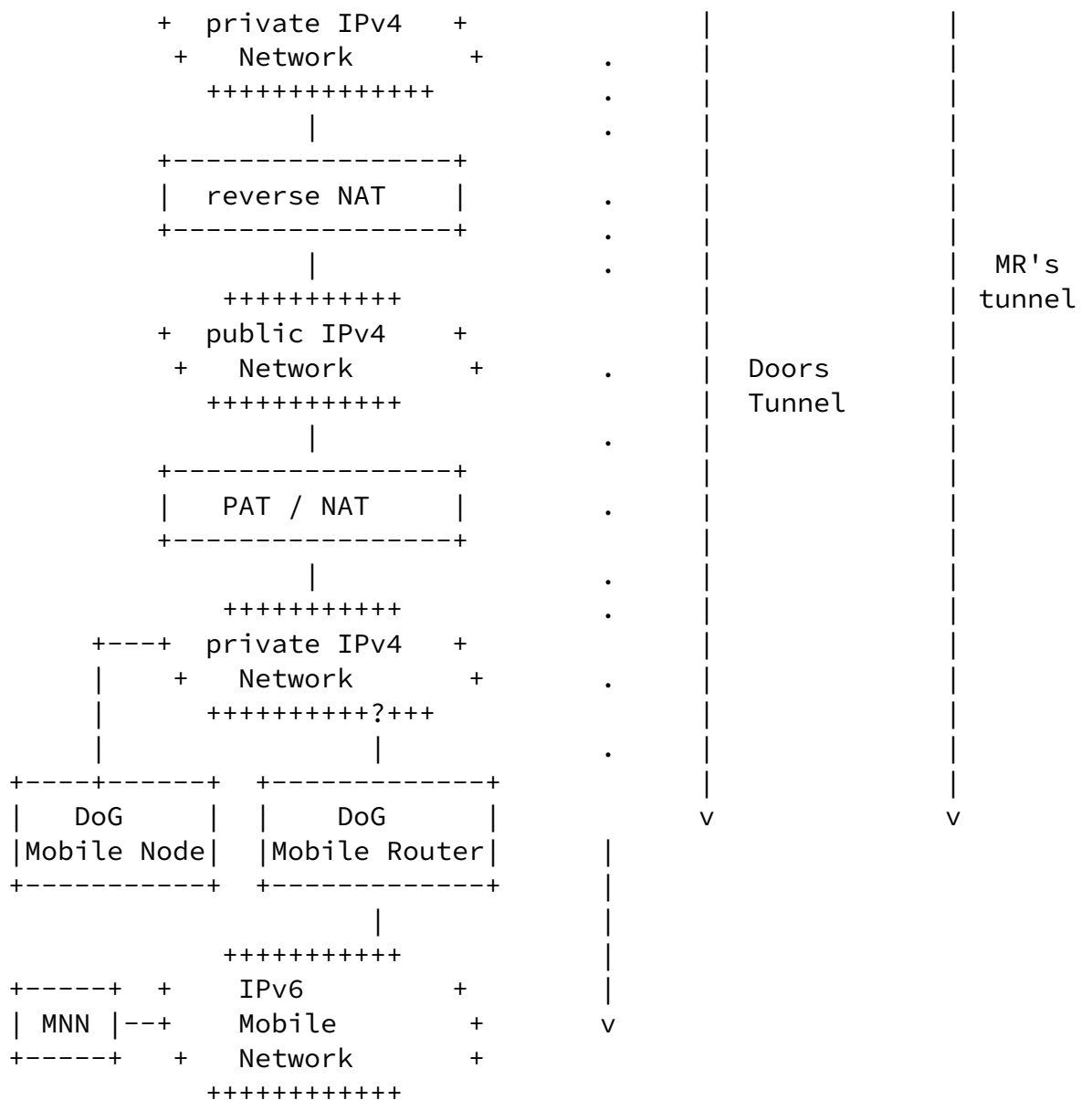
Doors Prefix

The prefix of a Doors Handle. It is a /64 prefix built with the Door IPv4 address and an arbitrary SLA ID. This prefix is assigned to the interface that owns the associated IPv4 address. If the IPv4 address is private, the prefix distribution MUST be limited accordingly, which prevents Route Optimization.

3. MIPv6 Doors support

With Doors, a roaming MIPv6 Mobile Node generates a Doors Handle and uses it as CareOf to Bind over a Doors Tunnel to its Home Agent.





Doors Model (worst case!!)

[3.1](#) Known Restrictions

Since the CareOf can be translated on the way, it may cause problems to Authentication Header and upper layer checksum computations. So the CareOf can not be included in the signed information. As a result, the reference packet for AH is always a packet where the IPv6 source and destination addresses are the Home Address of the MN and

the address of the HA, and the slots and segment left of a Routing Header are set to 0. This is true for RH type 2 and the Reverse Routing Header defined in [14].

In any case, the Doors prefix must be reachable at IPv6 level from the Home Agent, and from the Correspondent Nodes in case of Route Optimization (RO). This is why RO may not be possible if the Handle is based on a private address, which may occur if the Door is behind a reverse NAT.

3.2 Operation for a MIPv6 Mobile Node roaming over IPv4

A MN roaming generates its Doors Handle as follows:

16	32	16	16	32	16	bits
2002	Door IPv4 addr	SLA	Door UDP Port	MN private addr	MN UDP Port	

MR Doors Handle

Door IPv4 address: the public address of the door.

Doors Port: DOORSPORT

MN IPv4 address: the private IPv4 CoA obtained by the mobile router on his roaming interface by any mechanism (configuration, DHCP, IPCP, ...). Maybe private.

MN UDP port: A value chosen dynamically by the Mobile Node. It may be a signature used for verification purposes.

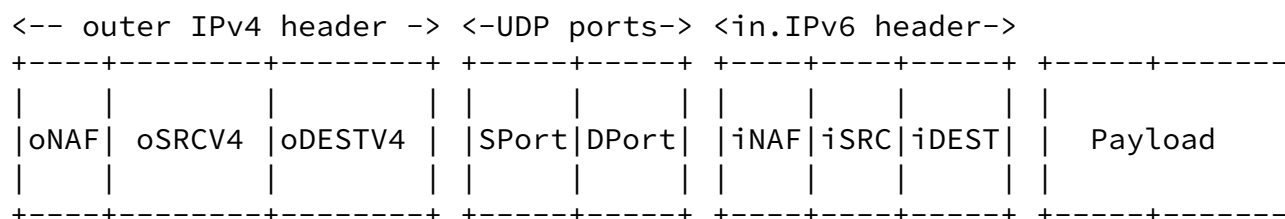
The Mobile Node may recompute a new port periodically, build a new CareOf and rebind.

The Mobile Node MUST be tuned to send Binding Updates often enough to make sure that the NAT/PAT states are kept alive. As a result, there is no additional control traffic for that purpose.

3.2.1 MR Sending packets over the Doors tunnel

The Doors Tunnel can be seen as an internal hop between the Mobile Node and its CareOf. With that acceptance, the MIPv6 model, between the CareOf and either the Home Agent or an arbitrary Correspondent Node, still applies.

When sending or forwarding a IPv6 packet with a Source address that is a Doors Handle, a Mobile Node MUST encapsulate the packet into a IPv4/UDP tunnel using the following settings:



InDoors Packet

NAF represents the Non-Address Fields of a IP header

Sport is the UDP Source port, set to the MN UDP port from the Handle

DPort is the UDP Destination Port, set to the Doors Port from the Handle

SRCV4 is the Source IPv4 address, set to the MN IPv4 address from the Handle

DESTV4 is the Destination IPv4 address, set to the Door IPv4 address from the Handle.

SRC is the IPv6 Source Address, set to CoA == Doors Handle

DEST is the Home Agent Address

The Payload may be Home Address Dest Option and a Mobility Header or a IPv6 packet from a Node in the Mobile Network

This causes packets in the MN-HA tunnel to be automatically reencapsulated into an IPv4/UDP tunnel to the HA IPv4 address, as long as the CareOf Address is a Doors Handle.

Fragmentation may occur at IPv6 and/or at IPv4 encapsulation level. the rules defined in [7] and [10] apply respectively.

Internet-Draft

Doors

May 2003

[3.2.2](#) MR Receiving packets over the Doors tunnel

The process of terminating the Doors tunnel on the MN side is:

- Decapsulating the IPv6 packet from the IPv4/UDP encapsulation

- Recomposing the original IPv6 address as known on the MN side.

- Recomputing the checksum of ICMP messages.

When receiving a packet over UDP with Source Port equal to DOORSPORT, a Mobile Node checks whether there's an inner IPv6 packet with a Destination IPv6 address that is actually a Doors Handle.

If so, the MN restores it by:

- Overwriting the MN IPv4 address and UDP port fields in the handle with the IPv4 Destination information from the received packet

- Overwriting the Door address and UDP port fields in the handle with the UDP Source information from the received packet

If the generated Doors Handle does not match its CareOf, the node drops the packet.

Otherwise, the node decapsulates the UDP tunnel and receives the resulting IPv6 packet. The next step is either yet an other level of decapsulation, or, if a RH type 2 is present, a forwarding to the next hop in the RH, that should be the node's home address.

This causes the MN-HA tunnel to be automatically decapsulated from an IPv4/UDP tunnel as long as the Doors Handle is the CareOf.

[3.3](#) Operation for the Door

The Door does not need to keep any PAT/NAT related state since that information is stored as CareOf in the Binding Cache by the Home Agent and the Correspondent Nodes.

The Binding Cache Entries are created regardlessly whether the CareOf is a Handle or a plain IPv6 address. As a result, the gating factor to Doors scalability is MIP itself.

When the support of Door is configured on a dual stack interface of a router, an IPv6 address is configured manually or automatically on that interface, based on the Door Prefix associated to the IPv4 address of that interface, with a suffix of ::1. The router MAY start redistributing the Doors prefix at that time.

[3.3.1](#) Door Receiving packets over the Doors tunnel

The process of terminating the Doors Tunnel on the Door side is:

Decapsulating the IPv6 packet from the IPv4/UDP encapsulation

Translating the original source IPv6 address into an OutDoors Handle.

Recomputing the checksum of ICMP messages.

When receiving a packet over UDP with Source Port equal to DOORSPORT, the DoG function in a HA checks whether there's an inner IPv6 packet with a Source IPv6 address that is actually a Doors Handle.

If so, the Door translates the Handle by:

Overwriting the MN IPv4 address and UDP port fields in the handle with the IPv4 Source information from the received packet.

Overwriting the Door IPv4 address and UDP port fields in the handle with the IPv4 Destination information from the received packet.

As a result, the layout of the OutDoors Handle is as follows:

16	32	16	16	32	16	bits
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+	
2002	Door	SLA	Door	MN	MN	
	IPv4		UDP	public	PATd	
	addr		Port	(NATd) addr	Port	
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+	

Door Handle

Doors Port: DOORSPORT

Door IPv4 address: The IPv4 address of the Door. Maybe private.

MN IPv4 address: the public IPv4 address of the MN.

MN UDP port: May have been PATed

After computing the OutDoors Handle, the DoG decapsulates the UDP tunnel and forwards the resulting IPv6 packet. If the HA or CN is collocated with the DoG, the packet is received, and in any case the OutDoors Handle is used as CareOf and stored in the binding cache of the destination.

[3.3.2](#) Door Sending packets over the Doors tunnel

Since the Door advertises the Door prefix, and since the OutDoors Handle belongs to that prefix, normal IPv6 routing take place between the HA or CN and the Door on the way to the MN.

When forwarding a packet to a destination that is a OutDoors Handle, a router running as a Door checks whether it has an IPv6 connected route to that prefix. If so, instead of looking up the Link Layer address of the Handle, it MUST encapsulate the packet over IPv4/UDP using the following settings:

```
<-- outer IPv4 header -> <-UDP ports-> <in.IPv6 header->
+---+-----+-----+ +---+-----+ +---+-----+ +---+-----+
|oNAF| oSRCV4 | oDESTV4 | |SPort|DPort| |iNAF|iSRC|iDEST| | Payload
|    |      |      | |    |    | |    |    |    | |
+---+-----+-----+ +---+-----+ +---+-----+ +---+-----+
```

OutDoors Packet

NAF represents the Non-Address Fields of a IP header

Sport is the UDP Source port, set to the Doors Port from the Handle

DPort is the UDP Destination Port, set to the MN UDP port from the Handle

SRCV4 is the Source IPv4 address, set to the Door IPv4 address from the Handle.

DESTV4 is the Destination IPv4 address, set to the MN IPv4 address from the Handle

SRC is the Home Agent Address

DEST is the IPv6 Source Address, set to the mapped CoA == OutDoors Handle

The Payload may start with a Routing Header of type 2, or be a IPv6 packet from a Node in the Mobile Network

When applied to Nemo, between a Mobile Router and its Home Agent, the Doors protocol maintains a single state in the PAT/NAT for all the communications of all the Mobile Network Nodes.

[3.4](#) Advantages of the Doors protocol

This solution presents a number of advantages:

This solution does not keep states in the gateways. The NATed addresses are stored and maintained in the MIP binding cache, only as long as they are needed, by the Mobile IPv6 protocol. Note that in case of a symmetrical PAT, the CNs and the HAs may not see the same CareOf for a same MN.

The MN may swap its Doors Gateway whenever it needs, since this will be seen as yet another roaming. In particular, the address of a local Doors Gateway may be available in a DHCP or a IPCP extension.

The transition between Doors or between IPv4 and IPv6 roaming is smooth, handled by the DoG function, transparently to the HA and CN support.

There is only one entry in the NAT/PAT gateway for a full Nested Nemo configuration with no route optimization. This limits the size of the tables that the NAT gateway has to maintain.

[4.](#) IANA considerations

A port number value is required for DOORSPORT. Note that this requirement could be alleviated by a common configuration on both sides, but this makes the deployment a bit more complex.

Today we use TLA of 02 which is reserved to 6to4. We see Doors as a subset of the general 6to4 prefix, but a Door can not function as a general purpose 6to4 gateway. Is that worth using a different TLA?

[5.](#) Acknowledgements

The authors wish to thank:

Ole Troan, Vincent Ribiere, Massimo Lucchina, Daniel Shell, Ravi Samprathi, William Ivancic and the coffee machine for their various contributions.

References

- [1] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.
- [2] Callon, R. and D. Haskin, "Routing Aspects Of IPv6 Transition",

Thubert, et al. Expires November 20, 2003 [Page 12]

Internet-Draft Doors May 2003

[RFC 2185](#), September 1997.

- [3] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 2373](#), July 1998.
- [4] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [5] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.
- [6] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [7] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6

Specification", [RFC 2473](#), December 1998.

- [8] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", [RFC 2529](#), March 1999.
- [9] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", [RFC 2893](#), August 2000.
- [10] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC 3056](#), February 2001.
- [11] Vaarala, S. and O. Levkowitz, "Mobile IP NAT/NAPT Traversal using UDP Tunnelling", [draft-ietf-mobileip-nat-traversal-07](#) (work in progress), November 2002.
- [12] Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", [draft-ietf-mobileip-ipv6-21](#) (work in progress), March 2003.
- [13] Ernst, T. and H. Lach, "Network Mobility Support Terminology", [draft-ernst-monet-terminology-01](#) (work in progress), July 2002.
- [14] Thubert, P. and M. Molteni, "IPv6 Reverse Routing Header and its application to Mobile Networks", [draft-thubert-nemo-reverse-routing-header-01](#) (work in progress), October 2002.
- [15] Castelluccia, C., Malki, K., Soliman, H. and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", [draft-ietf-mobileip-hmipv6-07](#) (work in progress), October 2002.
- [16] Petrescu, A., "Issues in Designing Mobile IPv6 Network Mobility with the MR-HA Bidirectional Tunnel (MRHA)", [draft-petrescu-nemo-mrha-02](#) (work in progress), March 2003.

Authors' Addresses

Pascal Thubert
Cisco Systems Technology Center
Village d'Entreprises Green Side
400, Avenue Roumanille
Biot - Sophia Antipolis 06410
FRANCE

EMail: pthubert@cisco.com

Marco Molteni
Cisco Systems Technology Center
Village d'Entreprises Green Side
400, Avenue Roumanille
Biot - Sophia Antipolis 06410
FRANCE

EMail: mmolteni@cisco.com

Patrick Wetterwald
Cisco Systems Technology Center
Village d'Entreprises Green Side
400, Avenue Roumanille
Biot - Sophia Antipolis 06410
FRANCE

EMail: pwetterw@cisco.com

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.