

Issues With Port-Restricted IP Addresses  
draft-thaler-port-restricted-ip-issues-00.txt

## Abstract

This document discusses issues with assigning an IP address to a host interface such that the IP address may only be used with a restricted set of ports. This concept is referred to herein as a port-restricted IP address. A number of issues with this concept are documented, and the issues are contrasted with other approaches to dealing with IPv4 address exhaustion.

## 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/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 September 1, 2010.

## Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

---

Internet-Draft Issues With Port-Restricted IP Addresses February 2010

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

## Table of Contents

|                       |                                       |                   |
|-----------------------|---------------------------------------|-------------------|
| <a href="#">1.</a>    | Introduction . . . . .                | <a href="#">3</a> |
| <a href="#">2.</a>    | IP Model Issues . . . . .             | <a href="#">3</a> |
| <a href="#">3.</a>    | Host Implementation Issues . . . . .  | <a href="#">5</a> |
| <a href="#">4.</a>    | Application/Protocol Issues . . . . . | <a href="#">6</a> |
| <a href="#">5.</a>    | Management Issues . . . . .           | <a href="#">6</a> |
| <a href="#">6.</a>    | Personnel Issues . . . . .            | <a href="#">7</a> |
| <a href="#">7.</a>    | Security Considerations . . . . .     | <a href="#">7</a> |
| <a href="#">8.</a>    | IANA Considerations . . . . .         | <a href="#">7</a> |
| <a href="#">9.</a>    | Conclusion . . . . .                  | <a href="#">7</a> |
| <a href="#">10.</a>   | References . . . . .                  | <a href="#">8</a> |
| <a href="#">10.1.</a> | Normative References . . . . .        | <a href="#">8</a> |
| <a href="#">10.2.</a> | Informative References . . . . .      | <a href="#">8</a> |
|                       | Author's Address . . . . .            | <a href="#">9</a> |

---

Internet-Draft   Issues With Port-Restricted IP Addresses   February 2010

## 1. Introduction

In this document we use the term "port-restricted IP address" to mean an address assigned to an interface of some device, where that address can only be used with a restricted set of port numbers in TCP, UDP, and/or other transport protocols.

Port-restricted IP addresses have been proposed as one mechanism to allow address re-use (using disjoint sets of port numbers) among many nodes, which is motivated by IPv4 address scarcity.

A port-restricted IP address differs from other types of shared addresses, such as resulting from a classic Network Address Translator (NAT) in that a port-restricted IP address is actually assigned to an interface of some device. In contrast, in a typical network address translation deployment, a public IPv4 address is shared among many hosts by being assigned to an external interface of the NAT device (where it is usable with all protocols and ports, and hence is not port-restricted). Each host on the private side of the NAT uses a separate, private IPv4 address assigned to its own interface, and the private IPv4 address is usable on the private subnet with all protocols and ports.

There are three types of issues with the concept of port-restricted IP addresses:

- a. Issues inherent in any type of address sharing, including Network Address Translation (NAT). These issues are discussed in [\[I-D.ford-shared-addressing-issues\]](#) and hence are outside the scope of this document.
- b. Issues that exist in other types of address sharing such as NATs, but which are made worse in some way with port-restricted IP addresses.
- c. Issues unique to port-restricted IP addresses.

This document covers the latter two types of issue.

## 2. IP Model Issues

A "unicast address" is defined (e.g., in [\[RFC4291\]](#)) as an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address. Many protocols, including ARP [\[RFC0826\]](#) [\[RFC5227\]](#) rely on this fact.

Creating a port-restricted unicast IP address would require a change to the above definition so that it could be assigned to multiple interfaces (on different hosts) within the address's scope.

This change to the IP model would be as big as, but quite different from, the introduction of NAT. This issue is unique to port-restricted IP addresses, since in classic NAT, each IP address is only assigned to a single interface.

The closest concept that exists today is that of an "anycast" address [\[RFC1546\]](#) [\[RFC4291\]](#). An anycast address is defined as an identifier for a set of interfaces, where a packet sent to an anycast address is delivered to the "nearest" interface according to the routing protocols' measure of distance. For additional discussion of anycast considerations, see [\[I-D.iab-anycast-arch-implications\]](#). An anycast address differs from a port-restricted IP address in that an anycast address may still be used with any protocol or port, and all interfaces with the same anycast address are considered equivalent.

It is also worth noting the distinction between a port-restricted IP address, and an address/port obtained from a NAT by an application using a protocol such as UPnP or NAT-PMP. In the UPnP/NAT-PMP model, the address is still assigned to the NAT's public interface, not an interface of the host on which the application is running. As such, UPnP/NAT-PMP-unaware applications that see addresses of the local machine via local APIs (e.g., `getsockaddr`) will never see such an address, and hence no API contract is affected. Thus, applications opt in to use addresses obtained via UPnP or NAT-PMP by writing to specific APIs for those protocols.

A discussion of considerations around changes to the IP model can be found in [\[I-D.iab-ip-model-evolution\]](#). It concludes that any changes to the IP model need to be done with extreme care. Extensions that

merely add additional optional functionality without impact any existing applications (as in the approach UPnP and NAT-PMP took) are much safer.

We must also consider the long-term impact of any change to the IP model. We have learned by experience that there is a consistent demand for any IPv4 hacks to also show up in IPv6. Typically the rationale is that once administrators and support personnel are used to something, they want to continue to use it, and specifically they want it to work the same way in IPv6. For example, whereas it was originally expected that NAT would only ever be deployed for IPv4 since IPv6 had plenty of address space. However, recently there has been some vocal demand for NAT in IPv6 so that it can work the same way. Hence the key learning is that simply declaring "this hack is only for IPv4" does not work.

### [3.](#) Host Implementation Issues

To actually apply a port restriction, host stack implementations would need to change. Without such a change, a host may naturally attempt to use the IP address with arbitrary protocols and ports, which would be akin to address spoofing in a port-restricted IP address model.

Even with a modified host stack implementation, applications expecting to bind to a specific port number (such as an application with an IANA-assigned port number) would fail. One difference from a classic NAT is that in a typical NAT deployment, if an application sees that an interface has a global IP address on it, the application has no reason to believe there is any restriction on its use.

One mitigation that has been proposed is to implement a NAT in the host kernel. However, this means that an application cannot communicate even with other nodes on the same physical subnet without going through the host NAT. As a result, intra-link communication that depends on broadcast, multicast, TTL=1, or transparency (e.g., because of payloads embedding IP addresses) would fail. In contrast, in a classic NAT deployment, communication between two nodes on the

private side can occur normally. Hence this issue is specific to port-restricted IP addresses.

Another potential issue with introducing a NAT in the host kernel is that if the NAT is done in a way that introduces another hop, the topology is thus modified in a way that a user would not expect. So applications and utilities that expose the topology to the user in some way will result in user confusion.

Another host issue with port-restricted IP addresses arises whenever multiple interfaces exist that have port-restricted IP addresses with disjoint ports. For example, if an application binds to IN\_ADDR\_ANY for on-link communication, the host stack must pick a port that is independent of interface or address. However, in this case, there is no such port, and hence the bind would fail.

Finally, consider a host roaming between two networks, one of which is a typical network today, and the other uses a port-restricted IP address. In this case, an application may have already issued a bind (e.g., for UDP) before roaming, and been assigned a port. After roaming, the port would be invalid and there may be no way to inform an existing application. Hence introducing port-restricted IP addresses would require changes to many applications, not just host stacks.

#### [4.](#) Application/Protocol Issues

One limitation of a port-restricted IP address is that non-port-based protocols cannot work. This is more severe than a classic NAT, since with a port-restricted IP address, they cannot be used even within the same link, whereas with a classic NAT, private IP addresses can still be used with non-port-based protocols between hosts on the private side of the NAT.

In some scenarios, a port-restricted IP address might be designed to be assigned to the public side of a classic NAT device. However, this would still result in two issues. First, the NAT device itself would lose the ability to use non-port-based protocols (e.g., the ability to respond to IPv4 pings, the ability to support 6to4 [[RFC3056](#)], etc.). Second, if an end host is connected to the network

instead of the expected NAT device, unexpected failures would occur.

## 5. Management Issues

ICMP messages that don't embed a packet have no port numbers. As such, they could not be used with port-restricted IP addresses. With some effort, ICMP messages initiated from a port-restricted IP address could be made to work, but not ICMP messages (that have no embedded packet) destined to such an address.

Hence there would be no way for a service provider technician to ping such an address. If a port-restricted IPv4 address were used alongside a normal IPv6 address, the IPv6 address could be pinged, but such a ping would provide no liveness indication of the IPv4 stack on the destination. In contrast, ping, traceroute, and similar mechanisms today work fine within the area behind a classic NAT. Hence this issue is specific to port-restricted IP addresses.

In addition, the existing IP MIB [[RFC4293](#)] surfaces the existing IP Model to management applications, and cannot express port-restricted IP addresses. Introducing this concept would require new MIB and management tool work.

Another aspect of management is provisioning. In order to configure an interface with a port-restricted IP address, the network's provisioning system would need to evolve. For example, this may involve changes to DHCP, databases, management tools, auditing/accounting systems, etc. These systems are often complex and hence their evolution is costly and takes time.

This issue could be compounded by stateful dynamic port range allocation. In addition, there would be fairness issues resulting

from the fact that not all port ranges are of equal value. For example, system ports are often considered more valuable than user ports, and ports IANA has assigned to popular protocols/applications are more valuable than other ports.

## 6. Personnel Issues

Introducing such a far-reaching change would require retraining personnel, such as developers, technical support personnel, consultants, and enterprise IT pros. This training is in addition to anything already inherent in address sharing.

We already understand what fails with NATs and double NATs (since many homes are already double NAT-ed today). Port-restricted IP addresses introduce significant complexity with new and hence unknown (to existing personnel) failure modes. This would likely increase costs significantly compared to multiple levels of NAT.

## [7.](#) Security Considerations

One mitigation for security attacks against TCP is port randomization [[I-D.ietf-tsvwg-port-randomization](#)]. Reducing the port space available to host thus reduces its ability to randomize ports, and hence has negative security implications. This issue would be made worse if there were any port sub-delegation (where sub-ranges are allocated out of larger ranges), since each hierarchy level would introduce some wasted ports.

## [8.](#) IANA Considerations

This document has no actions for IANA.

## [9.](#) Conclusion

The notion of port-restricted IP addresses would be a drastic change to the IP model with far-reaching impact. The impact would include lots of complexity, with many problems known (as enumerated herein) and probably more. In any new and complex change, some people/ implementations would likely get it wrong or incomplete the first time.

In conclusion, all things considered, the impact of port-restricted IP addresses is believed to be worse overall than the impact of multiple layers of NAT. The primary cause of the issues unique to



a device's interface. This concept does not occur in classic NAT, even when used with protocols such as UPnP or NAT-PMP. It is possible that the same state benefits motivating the concept of port-restricted IP addresses may be possible in other approaches that do not involve assigning a port-restricted IP address to an interface, but this investigation is left to other documents.

## [10.](#) References

### [10.1.](#) Normative References

- [RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, [RFC 826](#), November 1982.
- [RFC1546] Partridge, C., Mendez, T., and W. Milliken, "Host Anycasting Service", [RFC 1546](#), November 1993.
- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC 3056](#), February 2001.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", [RFC 4293](#), April 2006.
- [RFC5227] Cheshire, S., "IPv4 Address Conflict Detection", [RFC 5227](#), July 2008.

### [10.2.](#) Informative References

- [I-D.ford-shared-addressing-issues]  
Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", [draft-ford-shared-addressing-issues-01](#) (work in progress), October 2009.
- [I-D.iab-anycast-arch-implications]  
McPherson, D. and D. Oran, "Architectural Considerations of IP Anycast", [draft-iab-anycast-arch-implications-00](#) (work in progress), February 2010.
- [I-D.iab-ip-model-evolution]  
Thaler, D., "Evolution of the IP Model",

[draft-iab-ip-model-evolution-01](#) (work in progress),  
November 2008.

[I-D.ietf-tsvwg-port-randomization]

Larsen, M. and F. Gont, "Transport Protocol Port  
Randomization Recommendations",

[draft-ietf-tsvwg-port-randomization-06](#) (work in progress),  
February 2010.

#### Author's Address

Dave Thaler  
Microsoft  
One Microsoft Way  
Redmond, WA 98052  
USA

Phone: +1 425 703 8835  
Email: [dthaler@microsoft.com](mailto:dthaler@microsoft.com)

Thaler

Expires September 1, 2010

[Page 9]