Coping with IP Address Literals in HTTP URIs with IPv6/IPv4 Translators

draft-wing-behave-http-ip-address-literals-00

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 April 11, 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

A small percentage of HTTP URIs contain an IPv4 address literal as the hostname which is not accessible to IPv6-only HTTP clients using an IPv6/IPv4 translator and DNS64. This document proposes a
workaround for this problem using an HTTP proxy to handle that traffic.

Table of Contents

1. Introduction .................................................. 3
2. Proposed Workaround ........................................ 3
3. Disadvantages of Workaround ................................. 4
4. Security Considerations ..................................... 5
5. IANA Considerations .......................................... 5
6. Acknowledgements ............................................. 5
7. Informative References ...................................... 5
Appendix A. Example PAC files ................................. 6
Appendix B. HTTP IPv4 Address Literals on the Internet ... 6
Author’s Address ................................................... 7
1. Introduction

Two of the translation scenarios involve IPv6-only hosts accessing IPv4-only hosts (Scenario 1, "an IPv6 network to the IPv4 Internet" and Scenario 5, "an IPv6 network to an IPv4 network" [I-D.ietf-behave-v6v4-framework]). For this to work, the IPv6-only host sends a DNS AAAA query and receives a synthesized AAAA response. While it is common practice to use domain names in many application protocols, most applications do not require using domain names. IPv4 address literals occur in HTTP URI hostname fields (e.g., http://192.0.2.1) on the Internet (see Appendix B) and on some corporate networks. Such occurrences do not cause problems today, because both IPv4 hosts and dual-stack hosts can connect to those addresses just fine. However, those IPv4 address literals are inaccessible to IPv6-only clients using an IPv6/IPv4 translator and DNS64.

This document proposes a workaround to this problem when an HTTP browser, running on an IPv6-only host, encounters an HTTP URI containing an IPv4 address literal (instead of containing a domain name).

2. Proposed Workaround

Nearly all modern web browsers can be configured with a Proxy auto-config (PAC) [PAC] file. A PAC allows a browser to have an HTTP proxy handle traffic to a host with an IPv4 address literal, while allowing direct access (through the IPv6/IPv4 translator) for the majority of traffic, as shown in Appendix A. With this workaround, an IPv6-only HTTP client can access HTTP URIs that contain IPv4 address literals. The HTTP proxy needs to be able to send packets to the IPv4 Internet, and can be located parallel to the translator (as shown in Figure 1) or on either side of the IPv6/IPv4 translator, including in the host itself. To be located on the IPv6-only side of the translator, the proxy needs to understand how to formulate an IPv6 address from an IPv4 address [I-D.wing-behave-learn-prefix].
The Web Proxy Autodiscovery Protocol (WPAD) [I-D.ietf-wrec-wpad] is useful to autoconfigure web browsers for non-technical users or for a large community of users (e.g., inside of an enterprise).

3. Disadvantages of Workaround

While the workaround is helpful, the PAC and WPAD workarounds have several disadvantages:

- operating an HTTP proxy, even for the relatively small amount of the HTTP traffic that contains IPv4 address literals, is generally considered more resource-intensive than operating an IPv6/IPv4 translator because the HTTP proxy has to terminate a TCP connection and originate a separate TCP connection and shuffle data between them. For this reason alone, the PAC workaround described in this document is inferior to the web browser handling IPv4 native addresses itself [I-D.wing-behave-learn-prefix].

- The workaround only provides assistance to IPv4 address literals in hostnames. It does not help IPv4 address literals that appear, for various reasons, in the URL path or query string (e.g., http://www.example.com?host=1.2.3.4>, Java, or Javascript.

- Interworking an existing PAC file with the new functionality described in this document may be difficult.

- WPAD increases the attack surface.

- Both PAC and WPAD are de facto standards.
4. Security Considerations

WPAD increases the attack surface, because of how WPAD uses unauthenticated DHCP or DNS to find the PAC file, searches domain names for PAC files, and because the PAC file is retrieved via unauthenticated HTTP.

5. IANA Considerations

This document requires no IANA actions.

6. Acknowledgements

Thanks to Stig Venaas and Andrew Yourtchenko for their review comments. Thanks to Shin Miyakawa for suggesting this same technique is useful for IPv4-only hosts to connect to IPv6 address literals.

7. Informative References


Appendix A. Example PAC files

A simple example of a PAC file that causes HTTP or HTTPS URIs containing IPv4 address literals to be proxied to v6v4-proxy.example.net on port 8080. This would be useful for an IPv6-only client that needs to access content with IPv4 address literals in the HTTP URI:

```javascript
function FindProxyForURL(url, host) {
  var regexpr = /^https?:\/%/%d{1,3}\.%d{1,3}\.%d{1,3}\.%d{1,3}/
  if (regexpr.test(url))
    return "PROXY v6v4-proxy.example.net:8080";
  else
    return "DIRECT";
}
```

Figure 2

Figure 3: Example PAC for IPv4-only client

Appendix B. HTTP IPv4 Address Literals on the Internet

There has been some doubt that HTTP URIs on the Internet contain hostnames with IPv4 address literals. This section provides some scripts which demonstrate the relatively low -- but prevalent -- existence of IPv4 address literals.
An examination of Alexa’s top 1 million domains [Alexa] at the end of August, 2009, showed 2.38% of the HTML in their home pages contained IPv4 address literals. This can be verified with:

```bash
wget http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
unzip top-1m.csv.zip
cat top-1m.csv |
cut -d "," -f 2 |
xargs -I % -n 1 -t wget -nv % -O - --user-agent="Mozilla/5.0" |
grep -E "https?://[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}"
```

Of the top 1 million websites at the end of August, 2009, 3455 (0.35%) of them are IPv4 address literals (e.g., http://192.0.2.1). This can be verified with:

```bash
wget http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
unzip top-1m.csv.zip
grep -E "[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" top-1m.csv | wc
```

Author’s Address

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA  95134
USA

Email:  dwing@cisco.com