



Measuring and reporting on unauthorized use of IPv4 address space

APNIC 31, Hong Kong
February 2011

Agenda



- There's a problem
- Investigate
- Investigate more
- Share the results
- And now...

We were told about ‘hijackings’

Over five years ago we were told about the Hamachi/Logmein service using 5.0.0.0/8 without authorization.

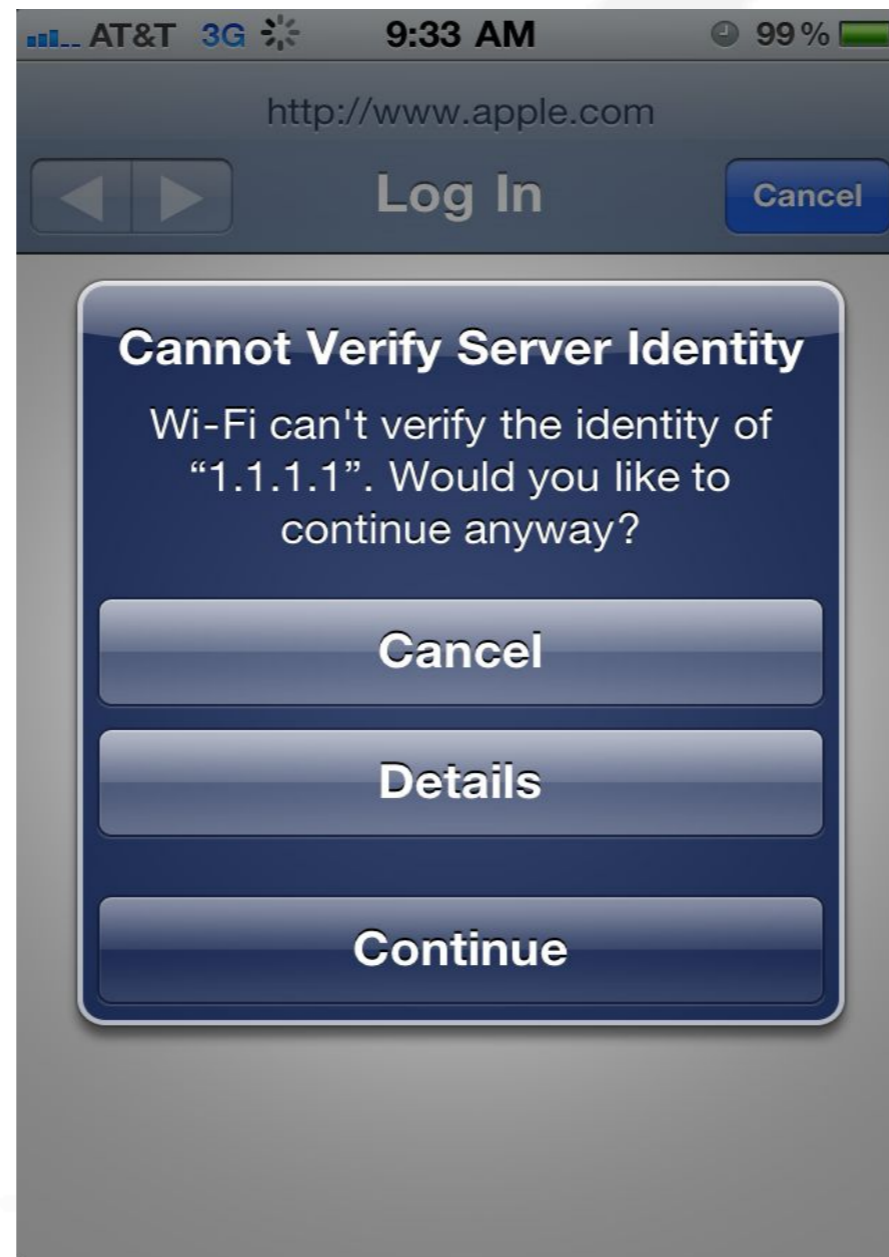
5.0.0.0/8 was allocated to RIPE NCC in November 2010.



The screenshot shows a web browser window with the URL <https://secure.logmein.com/products/hamachi2/>. The page features the LogMeIn logo and navigation links for Sales (1-866-478-1805) and Support (1-800-993-1790). The main content area includes a navigation menu with 'Solutions', 'Products', 'About Us', 'Support', 'Contact', and 'Labs & Betas'. The 'PRODUCT HOME' section lists links for 'DOWNLOAD', 'BUY NOW', 'FEATURES', 'RESOURCES', 'LICENSING', and 'TELL A FRIEND'. A central graphic illustrates the 'Now in Beta' status and the 'HUB & SPOKE' and 'GATEWAY' network architecture. A 'Login' form is visible on the right, with fields for 'Email' and 'Password', and a 'Log Me In' button. Below the graphic, the text reads: 'Finally, a VPN That Just Works' and 'LogMeIn Hamachi² is a hosted VPN service that securely connects devices and networks, extending LAN-like network connectivity to mobile users, distributed teams and business applications. You can easily create secure virtual networks on demand, across public and private networks.'

Poorly designed config defaults

Many commercial WiFi hotspots use 1.1.1.1. Users can only access the Internet after visiting a portal and registering or paying.



We researched others

We researched other prefixes that had been used without authorization and published our findings in IPJ.

We were asked for more specifics. Data not anecdotes.

The screenshot shows a web browser window displaying the Cisco Systems website. The page title is "Awkward /8 Assignments" and it is part of "The Internet Protocol Journal - Volume 10, No. 3". The main content area features an article titled "Used but Unallocated: Potentially Awkward /8 Assignments" by Leo Vegoda, ICANN. The article discusses the depletion of the IANA free pool of IPv4 address space and the potential for conflicts between unregistered and registered addresses. A sidebar on the left contains a navigation menu with links to various sections of the journal, including "Awkward /8 Assignments" which is highlighted. The bottom of the page has a navigation bar with links for "My Cisco", "Log In", "Account", "Register", and "Worldwide".

Awkward /8 Assignments - Cisco Systems

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/

Log In Account Register My Cisco

Products & Services Support How to Buy Training & Events Partners

The Internet Protocol Journal - Volume 10, No. 3

Awkward /8 Assignments

[HOME](#)
[ABOUT CISCO](#)
[PUBLICATIONS AND MERCHANDISE](#)
[THE INTERNET PROTOCOL JOURNAL](#)
[BACK ISSUES](#)
[VOLUME 10, NUMBER 3, SEPTEMBER 2007](#)

[Secure Multivendor Networks](#)
[IPv4 Address Depletion](#)
[IPv4 Address Consumption](#)
[Awkward /8 Assignments](#)
[Book Review](#)
[Call for Papers](#)
[Download PDF](#)

Used but Unallocated: Potentially Awkward /8 Assignments

by Leo Vegoda, ICANN

IPv4 has proven to be exceedingly popular, so it should be no surprise that the time is rapidly approaching when the last /8 block will be allocated and the *Internet Assigned Numbers Authority's* (IANA's) free pool of address space will be empty. At the time of writing, Geoff Huston of the *Asia Pacific Network Information Centre* (APNIC) is projecting [1] the IANA free pool will run out in mid-2010. Unfortunately, it is possible that some of these remaining /8s may cause problems for enterprise and *Internet Service Provider* (ISP) network operators when they are put back into use. These blocks are not the /8s that have been returned to IANA by the original registrants; they are previously unassigned address blocks.

Concerns

There are many concerns about the IANA free pool depletion, but one of them seems particularly straightforward to identify and fix. Many organizations have chosen to use unregistered IPv4 addresses in their internal networks and, in some cases, network equipment or software providers have chosen to use unregistered IPv4 addresses in their products or services. In many cases the choice to use these addresses was made because the network operators did not want the administrative burden of requesting a registered block of addresses from a *Regional Internet Registry* (RIR) [2, 11]. In other cases they may not have realized that RFC 1918 [3] set aside three blocks of address space for private networks, so they just picked what they believed to be an unused block, or their needs exceeded the RFC 1918 set-aside blocks. Other organizations used the default address range suggested by their equipment vendor, or supplied in example documentation, when configuring *Network Address Translation* (NAT) devices. Regardless of the reason, these uses of unregistered addresses will conflict with routed addresses when the /8s in question are eventually assigned to ISPs or enterprise users.

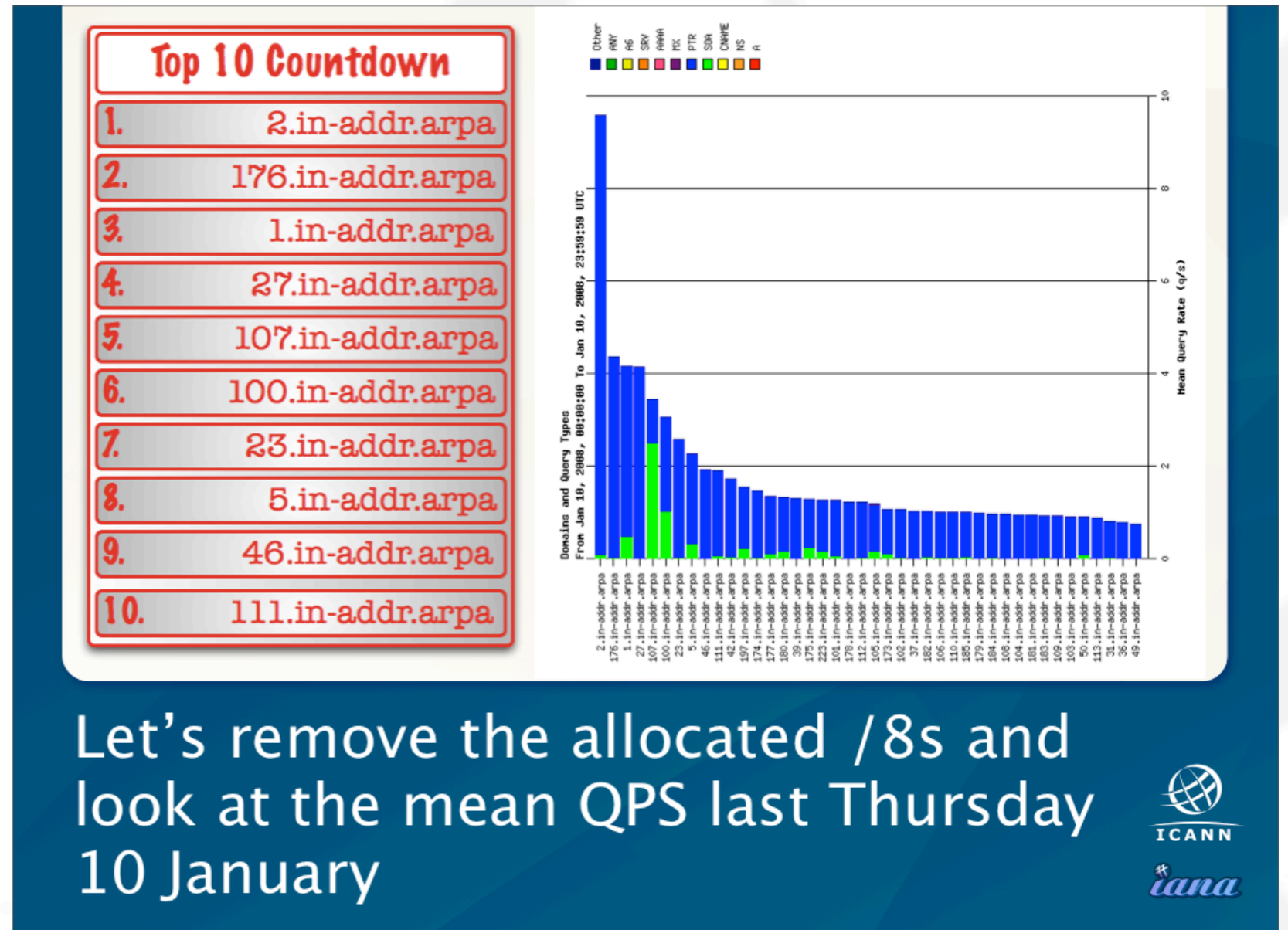
My Cisco Log In Account Register Worldwide

http://cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/

We had an idea...

We decided to look for DNS queries for unallocated IPv4 addresses.

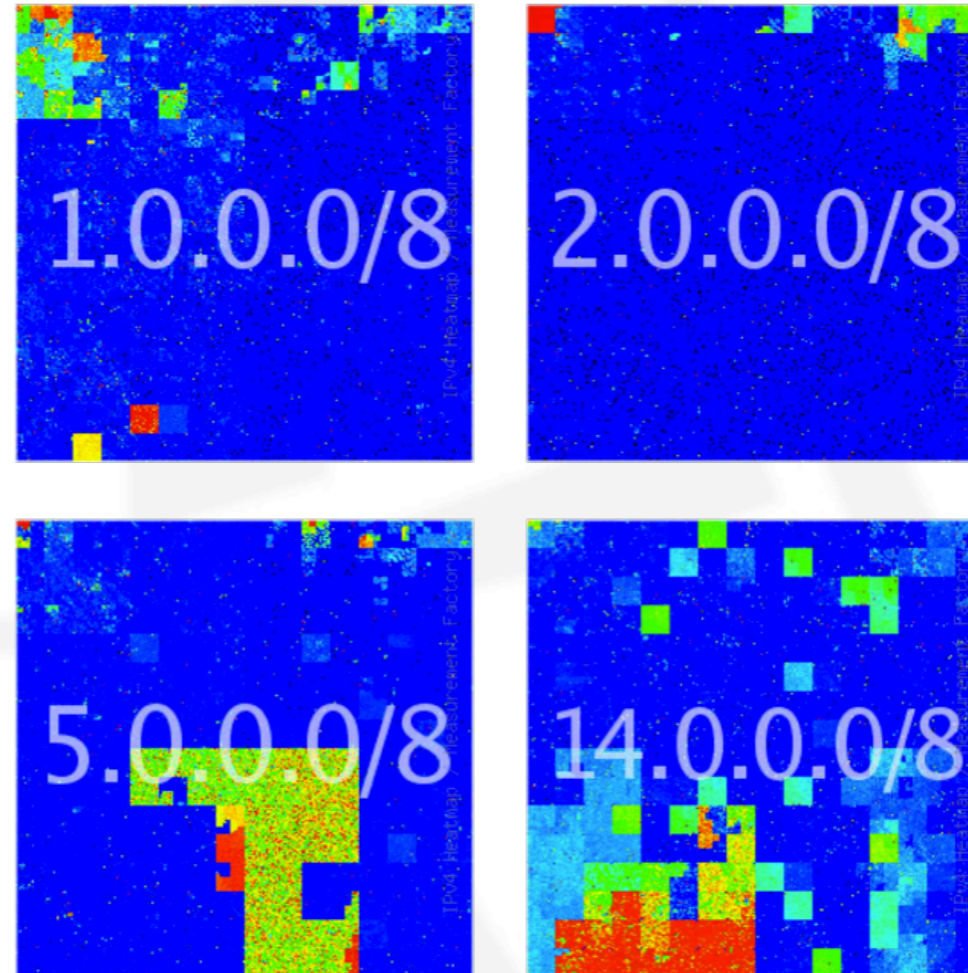
We knew that this research would only find evidence of usage on poorly managed networks. Well managed networks would not leak these queries.



Then we sponsored research

Duane Wessels (CAIDA/TMF) used DITL data to do a more thorough study which looked at the queries in more detail.

He identified which parts of /8s saw most activity as well as which /8s the activity was in.



But nothing's unallocated now

The central pool of IPv4 address space is now fully allocated. It is time for any 'bogon' filters for previously unallocated /8s to be removed.

All we are left with is the 'martian' filters for address space reserved by various RFCs.

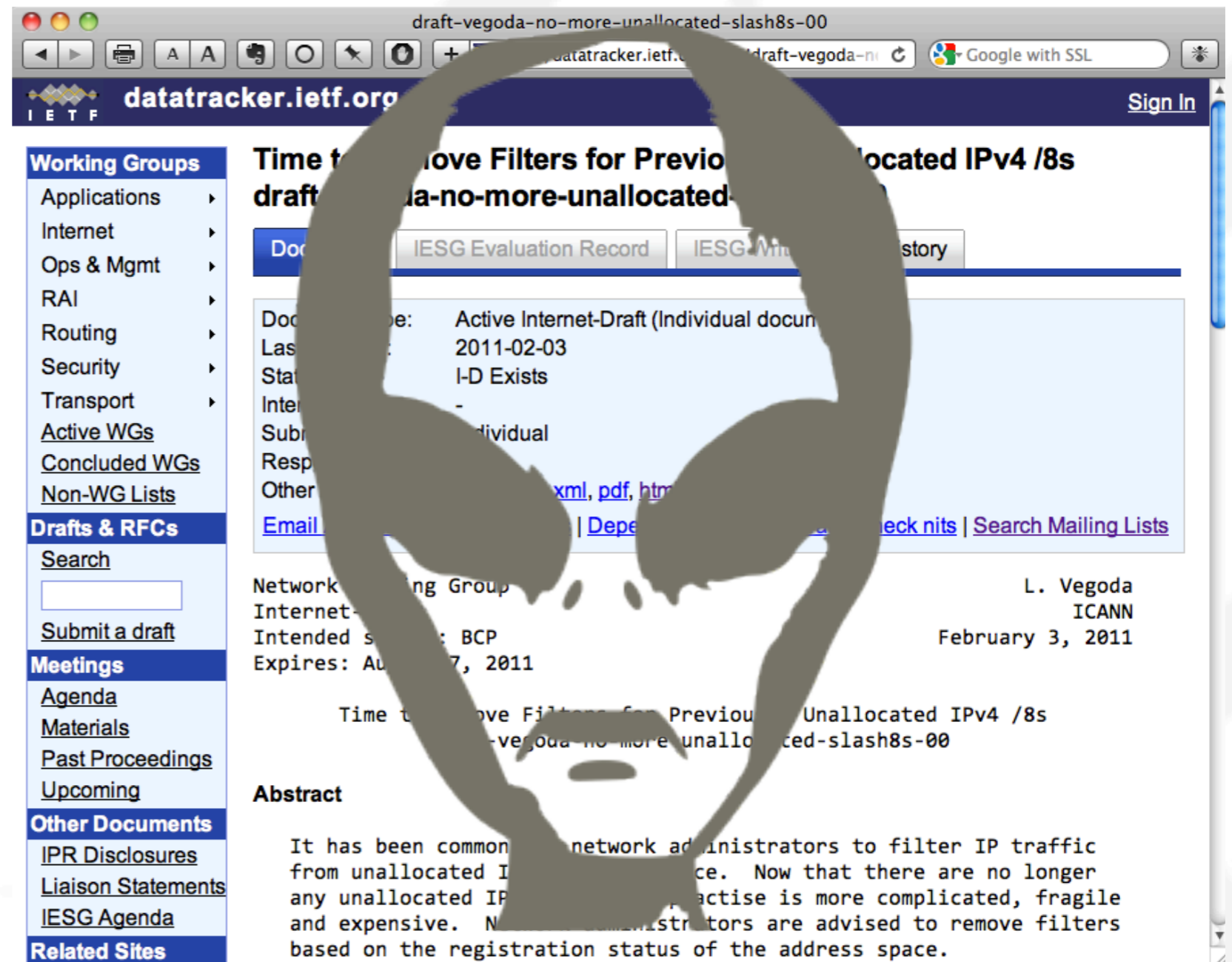
The screenshot shows a web browser window with the URL <http://datatracker.ietf.org/doc/draft-vegoda-no-more-unallocated-slash8s-00>. The page title is "Time to Remove Filters for Previously Unallocated IPv4 /8s draft-vegoda-no-more-unallocated-slash8s-00". The document is an Active Internet-Draft (Individual document) last updated on 2011-02-03. The state is "I-D Exists" and the intended status is "BCP". The submission is "Individual" and the responsible AD is "-". Other versions are available in plain text, xml, pdf, and html. The document is part of the Network Working Group, Internet-Draft, and expires on August 7, 2011. The author is L. Vegoda from ICANN, dated February 3, 2011. The abstract states: "It has been common for network administrators to filter IP traffic from unallocated IPv4 address space. Now that there are no longer any unallocated IPv4 /8s, this practise is more complicated, fragile and expensive. Network administrators are advised to remove filters based on the registration status of the address space."

<http://tools.ietf.org/id/draft-vegoda-no-more-unallocated-slash8s-00.txt>

But nothing's unallocated now

The central pool of IPv4 address space is now fully allocated. It is time for any 'bogon' filters for previously unallocated /8s to be removed.

All we are left with is the 'martian' filters for address space reserved by various RFCs.



draft-vegoda-no-more-unallocated-slash8s-00

datatracker.ietf.org

Working Groups

- Applications
- Internet
- Ops & Mgmt
- RAI
- Routing
- Security
- Transport
- Active WGs
- Concluded WGs
- Non-WG Lists

Drafts & RFCs

Search

Submit a draft

Meetings

- Agenda
- Materials
- Past Proceedings
- Upcoming

Other Documents

- IPR Disclosures
- Liaison Statements
- IESG Agenda

Related Sites

Time to Remove Filters for Previously Unallocated IPv4 /8s

draft-vegoda-no-more-unallocated-slash8s-00

Document Type: Active Internet-Draft (Individual document)

Last Modified: 2011-02-03

Status: I-D Exists

Intended Status: -

Submitted: Individual

Response: -

Other: [xml](#), [pdf](#), [html](#)

[Email](#) | [Dependencies](#) | [Check nits](#) | [Search Mailing Lists](#)

Network Working Group
Internet-Draft
Intended status: BCP
Expires: August 7, 2011

L. Vegoda
ICANN
February 3, 2011

Time to Remove Filters for Previously Unallocated IPv4 /8s

draft-vegoda-no-more-unallocated-slash8s-00

Abstract

It has been common for network administrators to filter IP traffic from unallocated IP address space. Now that there are no longer any unallocated IP address space, this practice is more complicated, fragile and expensive. Network administrators are advised to remove filters based on the registration status of the address space.

<http://tools.ietf.org/id/draft-vegoda-no-more-unallocated-slash8s-00.txt>



Thank you