ATTACHMENT 1

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

INTERNET ARCHIVE

www.archive.org
415.561.6767
415.840-0391 e-fax

Internet Archive
300 Funston Avenue
San Francisco, CA 94118

AFFIDAVIT OF CHRISTOPHER BUTLER

1. I am the Office Manager at the Internet Archive, located in San Francisco, California. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to surf more than 400 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a list of available dates. The visitor may select one of those dates, and then begin surfing on an archived version of the Web. The links on the archived files, when served by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the page upon which the link appeared and was clicked.

4. The archived data made viewable and browseable by the Wayback Machine is compiled using software programs known as crawlers, which surf the Web and automatically store copies of web files, preserving these files as they exist at the point of time of capture.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]. Thus, the Internet Archive URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). A web browser may be set such that a printout from it will display the URL of a web page in the printout's footer. The date assigned by the Internet Archive applies to the HTML file but not to image files linked therein. Thus images that appear on a page may not have been archived on the same date as the HTML file. Likewise, if a website is designed with "frames," the date assigned by the Internet Archive applies to the frameset as a whole, and not the individual pages within each frame.

6. Attached hereto as Exhibit A are true and accurate copies of printouts of the Internet Archive's records of the HTML files for the URLs and the dates specified in the footer of the printout.

7. I declare under penalty of perjury that the foregoing is true and correct.

DATE: 12/22/15

Christopher Butler

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

CALIFORNIA JURAT

See Attached Document.

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is atached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of San Francisco

Subscribed and sworn to (or affirmed) before me on this

22nd day of December, 2015, by

Christopher Butler,

proved to me on the basis of satisfactory evidence to be the person who appeared before me.

LINDA WONG
Commission # 2086421
Notary Public - California
San Francisco County
My Comm. Expires Oct 17, 2018

Signature: ______________________

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Case 1:16-cv-00453-RGA Document 502-1 Filed 03/08/18 Page 4 of 60 PageID #: 43118

NAT and Peer-to-peer networking

Peer-to-peer is a style of networking in which a group of computers communicate directly with each other, rather than through a central server. This is often used for multiplayer online games, such as Activision's Battlezone, to avoid the expense and delay of handling all that traffic at the server. However, this style of networking often has problems dealing with Network Address Translators (NATs). In this page, I describe a way to solve these problems. Products that use this technique now work properly through several commercial NATs.

The situation

The Internet is based on 32-bit IP (Internet Protocol) addresses, which means the theoretical maximum number of computers on the Internet is 4 billion or so. The practical limit is much lower, due to inefficiences in how IP addresses are used. In fact, the Internet may be only a few years away from running out of IP addresses.

As IP addresses become scarce, a technique known as Network Address Translation, or NAT, was developed to allow the use of a single IP address for a whole network of computers.

A NAT sits inbetween the public Internet and the network it serves, and works by rewriting IP addresses and port numbers in IP headers on the fly so the packets all appear to be coming from (or going to) the single public IP address of the NAT device instead of the actual source or destination.

NAT is now commonly employed in small home-office routers and in software used by consumers to connect several personal computers to a single cable modem. It is even used by some Internet Service providers.

(NAT is not the only possible solution; proxy servers are also commonly used, but require more configuration, and sometimes require custom client software. Eventually, we'll all switch to IPv6, which will have 128-bit addresses, and will solve the problem once and for all, but that's probably not going to be commonplace for many years.)

Some Protocols Aren't NAT-Friendly

Some applications send IP addresses or port numbers hidden inside their datapackets, where NAT can't properly rewrite them - so those applications don't work when you try to use them on computers behind NATs.

Some NATs, for security reasons, only allow incoming traffic from an outside address if an outgoing packet has already been sent to that outside address. This means that two people behind different NATs can't open up connections to each other in the usual way - ever!

The solution

Peer-to-peer protocols that wish to be NAT-friendly must be aware that any addresses they embed in their data packets may be invalid once the packets pass through the NAT, and compensate accordingly. One way to do it is as follows:

All traffic between the peers is done via a single UDP port. There is an address server which is not behind any NAT. Users connect to the address server first, and send it the IP address they think they have; the server notes both that address and the address it sees in the UDP header. The server then sends both addresses to the other peers. At this point, everyone knows everyone else's address(es).

To open up peer-to-peer connections, all old peers send a UDP packet to the new peer, and the new peer sends a UDP packet to each of the old peers. Since nobody knows at first whether they are behind the same NAT, the first packet is always sent to both the public and the private address.

This causes everyone's NAT to open up a bidirectional hole for the UDP traffic to go through. Once the first reply comes back from each peer, the sender knows which return address to use, and can stop sending to both addresses.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Compatibility Requirements

Above and beyond the basic NAT RFC, a NAT device that wants to support this scheme should have the following desirable property:

> *NATs should not change the number of UDP ports used by a stream of packets.*

For example, if a host behind a NAT sends a series of three packets from a single UDP port, the packets as relayed by the NAT should also appear to come from a single host and UDP port.

Draft RFC

I'm working on a draft RFC describing this technique in more detail. Contact me if you're interested.

Compatibility Test Results

I am testing the compatibility of this approach with several NAT implementations. Here are partial results:

Known Compatible NAT Implementations

- NAT1000 - fully compatible. Thanks to Nevod for their early help doing compatibility testing. They didn't need to change anything; the technique just plain worked with their NAT.
- SyGate - fully compatible. Although I had some wierd trouble with my network while testing SyGate, it seems to work fine in the most common configuration.
- NAT32 - the beta test version released Jan 5th, 1999 is fully compatible.
- Linux IP Masquerading - kernel 2.2.1 should work (though I haven't tested it since 2.2.0-pre6-ac2). See Juanjo's page for the patch for earlier 2.1 kernels. For 2.0 kernels, see the backport to kernel 2.0.36 by Glenn Lamb; Glenn's port makes it a configure-time option CONFIG_IP_MASQ_LOOSE_UDP, which is a nice touch.
- WinNAT - their current release works fine. They don't have a free trial version on their web site, but I hear they will in a few weeks.

NAT Implementations Soon to be Compatible

- Arescom Apex 1100 ISDN Router - Arescom has a firmware patch that fixes the problem, but it hasn't been released yet.
- Vicomsoft Softrouter Plus Vicom sent me a version that fixes the problem, but it hasn't been released yet. - Note: you may have to disable all native TCP bindings on the gateway machine except for one pointing to the inside ethernet adapter for this implementation to work. Be sure to read their doc all the way through before using their Setup Assistant.

Not yet known to be compatible

- Cisco IOS has a built-in NAT capability that might or might not be compatible. I'm talking with an engineer at Cisco, and we'll be running some tests soon.
- We have tested all the win32 software NATs we can get our hands on. We have not yet tested the NATs built into many small home office routers, nor the standalone NATs such as the SonicWall.

Not compatible

- Any pure proxy server solution, such as Wingate 2 or PPPShar, will not work properly. (Wingate 3 beta implements a proprietary form of HNAT, and does work properly.)

Discussion Area

I'd love to hear what other developers think about this technique, or about how Masq could be rewritten to reuse UDP ports

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.