Internet Engineering Task Force	A. Durand	
Internet-Draft	Juniper Networks	
Intended status: BCP	I. Gashinsky	
Expires: July 23, 2011	Yahoo! Inc.	
	D. Lee	
	Facebook, Inc.	
	S. Sheppard	
	ATT Labs	
	January 19, 2011	

TOC

Logging recommendations for Internet facing servers
draft-ietf-intarea-server-logging-recommendations-01

Abstract

In the wake of IPv4 exhaustion and deployment of IP address sharing techniques, this document recommends that Internet facing servers log port number and accurate timestamps in addition to the incoming IP address.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on July 23, 2011.

Copyright Notice

Table of Contents

---

1. Introduction

TOC

According to the most recent predictions, the global IPv4 address free pool at IANA will exhaust sometime in 2011. After that, service providers will have a hard time finding enough IPv4 global addresses to sustain product and subscriber growth. Due to the huge global existing infrastructure, both hardware and software, vendors and service providers must continue to support IPv4 technologies for the foreseeable future. As legacy applications and hardware are retired the reliance on IPv4 will diminish but this is a years long perhaps decades long process.

To maintain legacy IPv4 address support, service providers will have little choice but to share IPv4 global addresses among multiple customers. Techniques to do so are outside of the scope of this documents. All include some form of address translation/address sharing, being NAT44, NAT64 or DS-Lite.

The effects on the Internet of the introduction of those address sharing techniques have been documented in [I-D.ietf-intarea-shared-addressing-issues] (Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, “Issues with IP Address Sharing,” October 2010.).

Address sharing techniques come with their own logging infrastructure to track the relation between which original IP address and source port(s) were associated with which user and external IPv4 address at any given point in time. In the past to support abuse mitigation or public safety requests, the knowledge of the external global IP address

was enough to identify a subscriber of interest. With address sharing technologies, only providing information about the external public address associated with a session to a service provider is no longer sufficient information to unambiguously identify customers.
Note: this document provides recommendations for Internet facing servers logging incoming connections. Its does not provide any recommendations about logging on carrier-grade NAT or other address sharing tools.

---

2. Recommendations

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.) [RFC2119].
It is RECOMMENDED as best current practice that Internet facing servers logging incoming IP addresses also log:

- The source port number.
- A timestamp, preferably in UTC, accurate to the second, from a traceable time source (e.g. NTP).
- The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports.

Discussion: Carrier-grade NATs may have different policies to recycle ports, some implementations may decide to reuse ports almost immediately, some may wait several minutes before marking the port ready for reuse. As a result, servers have no idea how fast the ports will be reused and, thus, should log timestamps using a reasonably accurate clock. At this point the RECOMMENDED accuracy for timestamps is to the second or better. Representation of timestamps in UTC is preffered to localtime with UTC-offset or time zone as this extra information can be lost in the reporting chain.
Examples of Internet facing servers include, but are not limited to, web servers and email servers.
Although the deployment of address sharing techniques is not immediately foreseen in IPv6, the above recommendations apply to both IPv4 and IPv6, if only for consistency and code simplification reasons.
Discussions about data retention policies are out of scope for this document.
The above recommendation also applies to devices such as load-balancers logging incoming connections on behalf of actual servers.

3. ISP Considerations

TOC

ISP deploying IP address sharing techniques should also deploy a corresponding logging architecture to maintain records of the relation between customers identity and IP/port resources they utilize. However, recommendation on this topic are out of scope for this document.

4. IANA Considerations

TOC

None.

5. Security Considerations

TOC

In the absence of source port number and accurate timestamp, operators deploying any address sharing techniques will not be able to identify unambiguously customers when dealing with abuse or public safety queries.

6. References

TOC

6.1. Normative references

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

6.2. Informative references

TOC

[I-D.ietf-intarea-shared-addressing-issues]	Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, “Issues with IP Address Sharing,” draft-ietf-intarea-shared-addressing-issues-02 (work in progress), October 2010 (TXT).

Authors' Addresses

TOC

	Alain Durand
	Juniper Networks
	1194 North Mathilda Avenue
	Sunnyvale, CA 94089-1206
	USA
Email:	adurand@juniper.net
	Igor Gashinsky
	Yahoo! Inc.
	45 West 18th St.
	New York, NY 10011
	USA
Email:	igor@yahoo-inc.com
	Donn Lee
	Facebook, Inc.
	1601 S. California Ave.
	Palo Alto, CA 94304
	USA
Email:	donn@fb.com
	Scott Sheppard
	ATT Labs
	575 Morosgo Ave, 4d57
	Atlanta, GA 30324
	USA
Email:	Scott.Sheppard@att.com