TSVWG
Internet Draft
Intended status: Best Current Practice
Expires: November 2012

J. Touch
USC/ISI

May 30, 2012

Recommendations for Transport Port Uses
draft-ietf-tsvwg-port-use-00.txt

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), 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 November 30, 2012.

Copyright Notice

Abstract

This document provides recommendations to application and service designers on how to use the transport protocol port number space to help in its preservation. **NOTE THAT THIS CURRENT VERSION IS LARGELY AN OUTLINE OF ISSUES**.

Table of Contents

1. Introduction....2
2. Conventions used in this document....2
3. History....3
4. Current Port Use....4
5. What is a Port?....5
6. Conservation....6
7. How to Use Registered Ports....6
7.1. Do You Need a Port?....6
7.2. How Many Ports?....6
7.3. Picking a Port Number....7
7.4. Support for Security....7
7.5. Support for Future Versions....7
7.6. Transport Protocols....7
7.7. When to Register....7
7.8. Other Considerations....8
8. Recommendations for Future Allocation....8
9. Security Considerations....8
10. IANA Considerations....8
11. Conclusions....9
12. References....9
12.1. Normative References....9
12.2. Informative References....9
13. Acknowledgments....11

1. Introduction

(TBD)

2. Conventions used in this document

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 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

In this document, the characters ">>" preceding an indented line(s) indicates a compliance requirement statement using the key words listed above. This convention aids reviewers in quickly identifying or finding the explicit compliance requirements of this RFC.

3. History

The term 'port' was first used in RFC33 to describe a simplex communication path from a process [RFC33]. At a meeting described in RFC37, an idea was presented to decouple connections between processes and links that they use as paths, and thus to include source and destination socket identifiers in packets. RFC38 explains this in detail, in which processes might have more than one of these paths, and that more than one may be active at a time [RFC38]. As a result, there was the need to add a process identifier to the header of each message, so that the incoming data could be demultiplexed to the appropriate process. RFC38 further suggested that 32 bits would be used for these identifiers. RFC48 discusses the current notion of listening on a given port, but does not discuss how the issue of port determination [RFC48]. RFC61 notes that the challenge of knowing the appropriate port numbers is "left to the processes" in general, but introduces the concept of a "well-known" port for common services [RFC61].

RFC76 addresses this issue more constructively, proposing a "telephone book" by which an index would allow ports to be used by name, but still assumes that both source and destination ports are fixed by such a system [RFC76]. RFC333 suggests that the port pair, rather than an individual port, would be used on both sides of the connection for demultiplexing messages [RFC333]. This is the final view in RFC793 (and its predecessors, including IEN 112 [IEN112]), and brings us to their current meaning. RFC739 introduces the notion of generic reserved ports, used for groups of protocols, such as "any private RJE server" [RFC739]. Although the overall range of such ports was (and remains) 16 bits, only the first 256 (high 8 bits cleared) in the range were considered assigned.

RFC758 is the first to describe a list of such well-known ports, as well as describing ranges used for different purposes [RFC758]:

Binary	Octal	
0-63	0-77	Network Wide Standard Function
64-127	100-177	Hosts Specific Functions
128-223	200-337	Reserved for Future Use
224-255	340-377	Any Experimental Function

In RFC820, those range meanings disappeared, and a single list of assignments is presented [RFC820]. By RFC900, they appeared as decimal numbers rather than the octal ranges used previously [RFC900]. RFC1340 increased this range from 0..255 to 0..1023, and began to list TCP and UDP port assignments individually (although the assumption was, and remains, that once assigned a port applies to all transport protocols, including TCP, UDP, recently SCTP and DCCP, as well as ISO-TP4 for a brief period in the early 1990s) [RFC1340]. RFC1340 also established the Registered space of 1024-59151, though it notes that it is not controlled by the IANA at that point. The list provided by RFC1700 in 1994 remained the standard until it was declared replaced by an on-line version, as of RFC3232 in 2002 [RFC1700][RFC3232].

4. Current Port Use

The current IANA website (www.iana.org) indicates three ranges of port assignments:

Binary	Hex	
0-1023	0x03FF	Well-Known (a.k.a. 'system')
1024-49151	0x0300-0xBFFF	Registered (a.k.a. 'user')
49152-65535	0xC000-0xFFFF	Dynamic/Private

Well-known encompasses the range 0..1023. On some systems, use of these ports requires privileged access, e.g., that the process run as 'root', which is why these are referred to as 'system' ports. The ports from 1024..49151 denotes non-privileged services, known as 'registered'; because these ports do not run with special

privileges, they are often referred to as 'user' ports. Dynamic or Private ports are not registered through IANA.

Both Well-Known and Registered ports are registered through IANA, so both are sometimes called "registered ports". As a result, the term 'registered' is ambiguous, referring either to the entire range 0-49151 or to the user ports. Complicating matters further, 'system' ports do not always require special (i.e., 'root') privilege. Regardless, for clarity, throughout the remainder of this document we will refer to the port ranges as 'system', 'user', and 'private'.

5. What is a Port?

A port is a 16-bit number used for two distinct purposes:

- Demultiplexing transport connections within an end host
- Identifying a service

The first reason requires that each transport connection between a given pair of IP addresses use a different pair of ports, but does not require either coordination or registration of port use. It is the second reason that drives the need for a common registry.

Consider a user wanting to run a web server. That service could run on any port, provided that all clients knew what port to use to access that service at that host. Such information can be distributed out of band, e.g., in the URL, such as:

http:51509//www.example.com/

Ultimately, it's important to keep in mind that the correlation of a service with a port number is an agreement between the two endpoints of the connection only. The rest of the world might think that you're sending DNS packets on port 53, but you can run a web server on that port just fine, provided the server and client both decide that port 53 is for HTTP web server traffic.

Which brings us to the concept of a service. A service is the combination of ISO Layers 5-7 that represent an application protocol capability. For example www (port 80) is a service that uses HTTP as an application protocol, and provides a common web server. However, it is possible to use HTTP for other purposes, such as command and control. This is why some current service names (HTTP, e.g.) are a bit overloaded - they describe not only the application protocol, but a particular service.

IANA registers ports so that endpoints on the Internet do not need to pairwise, explicitly coordinate the meaning of their port numbers. This is the primary reason for registering ports with IANA - to have a common agreement between all endpoints on the Internet as to the meaning of a port.

Ports are used for other purposes as well, however. The other primary reason for registering ports with IANA is to simplify end system configuration, so individual installations do not need to coordinate their use of arbitrary ports. A similar reason is to simplify firewall management, so that a single, fixed firewall configuration can either permit or deny a service.

6. Conservation

(statistics of port allocations)

Ways to conserve, e.g., use service names (DNS SRV, TCP portnames, etc.), use portmapper, Bonjour, or other services for demuxing

7. How to Use Registered Ports

7.1. Do You Need a Port?

How to carefully use experimental ports (ref TCPM doc)

Reasons NOT to register a port, e.g.,

- not for a copy of an existing service
- not for anything a vanilla web client can connect to
- not for performance
- not for insecure versions of secure services (creates security hole)

Ports vs. SRV names

Reasons why only server ports are registered (not client)

7.2. How Many Ports?

Reasons NOT to have multiple ports (performance, etc.)

Techniques to reduce port use:

- When can you use a discovery service
- When can you use multiplexing
- When can you use handoff with in-band IDs

7.3. Picking a Port Number

Would you still want one if you can't pick the value?

Would you still want the UDP / TCP one if it didn't match the value for a previously assigned TCP / UDP one?

7.4. Support for Security

Why this is generally expected

Why this should/should not use a separate port (it's a performance issue, and performance would argue for multiple ports anyway, and ports are a limited resource)

TLS allows optional security

7.5. Support for Future Versions

Reasons NOT to include the version number in the name

7.6. Transport Protocols

UDP vs. TCP vs. others - and when the transport you lookup is not always the one you end up using

When/why you need multiples

When UDP is -disc

Caveats about using broadcast as discovery.

7.7. When to Register

What range to use before registering

When are you ready to register (basically when you have enough information to fill out the application)

Reasons NOT to squat

7.8. Other Considerations

Higher bar for system ports

Changing a name

Why aliases are bad and now deprecated

Providing enough information for IANA review, e.g., to avoid Internet congestion, fit in MTUs, deal with reordering, etc.

Provide enough information that's stand-alone; don't describe a protocol by a URL, e.g. - how to do a high-level description (what are we looking for?)

Why a heartbeat port MUST be on the same port as a service.

Relation of this doc to the IANA Port Experts review process (this is just a summary from the user/designer viewpoint, and is NOT binding to IANA or its Expert Review team)

8. Recommendations for Future Allocation

Abolish the distinction of system ports? BIG QUESTION HERE...

Why NOT to allocate ports or names for use as examples

9. Security Considerations

This document discusses ways to conserve port numbers, notably through encouraging demultiplexing within a single port. As such, there may be cases where two variants of a protocol - insecure and secure, are suggested to share the same port (e.g., HTTP and HTTPS, though currently those are assigned different ports).

This document reminds protocol designers that port numbers are not a substitute for security, and should not alone be used to avoid denial of service or firewall traffic, notably because their use is not regulated or authenticated.

10. IANA Considerations

The entirety of this document focuses on IANA issues, notably suggestions that help ensure the conservation of port numbers and provide useful hints for issuing informative requests thereof.

11. Conclusions

<Add any conclusions>

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

12.2. Informative References

[Hi95] Hickman, K., "The SSL Protocol", February 1995.

[IEN112] Postel, J., "Transmission Control Protocol", IEN 112, August 1979.

[RFC33] Crocker, S., "New Host-Host Protocol", RFC 33 February 1970.

[RFC37] Crocker, S., "Network Meeting Epilogue", RFC 37, March 1970.

[RFC38] Wolfe, S., "Comments on Network Protocol from NWG/RFC #36", RFC 38, March 1970.

[RFC48] Postel, J., S. Crocker, "Possible protocol plateau", RFC 48, April 1970.

[RFC61] Walden, D., "Note on Interprocess Communication in a Resource Sharing Computer Network", RFC 61, July 1970.

[RFC76] Bouknight, J., J. Madden, G. Grossman, "Connection by name: User oriented protocol", RFC 76, October 1970.

[RFC333] Bressler, R., D. Murphy, D. Walden. "Proposed experiment with a Message Switching Protocol", RFC 333, May 1972.

[RFC739] Postel, J., "Assigned numbers", RFC 739, November 1977.

[RFC758] Postel, J., "Assigned numbers", RFC 758, August 1979.

[RFC768] Postel, J., "User Datagram Protocol", RFC 768, August 1980.

[RFC793] Postel, J., "Transmission Control Protocol" RFC 793, September 1981

[RFC820] Postel, J., "Assigned numbers", RFC 820, August 1982.

[RFC900] Reynolds, J., J. Postel, "Assigned numbers", RFC 900, June 1984.

[RFC1122] Deering, S., "Host extensions for IP multicasting", RFC 1122, August 1989.

[RFC1340] Reynolds, J., J. Postel, "Assigned numbers", RFC 1340, July 1992.

[RFC1700] Reynolds, J., J. Postel, "Assigned numbers", RFC 1700, October 1994.

[RFC1918] Rekhter, Y., B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, "Address Allocation for Private Internets", RFC 1918, February 1996.

[RFC2616] Fielding, R., J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2780] Bradner, S., V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", RFC 2780, March 2000.

[RFC2817] Khare, R., S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC 2817, May 2000.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC3232] Reynolds, J. (Ed.), "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[RFC4340] Kohler, E., M. Handley, S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, March 2006.

[RFC4960] Stewart, R. (Ed.), "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5246] Dierks, T., E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

13. Acknowledgments

TBD

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Joe Touch
USC/ISI
4676 Admiralty Way
Marina del Rey, CA 90292-6695
U.S.A.

Phone: +1 (310) 448-9151
EMail: touch@isi.edu