TSVWG
Internet Draft
Intended status: Best Current Practice
Expires: August 2013

J. Touch
USC/ISI

February 25, 2013

# Recommendations for Transport Port Uses
# draft-ietf-tsvwg-port-use-01.txt

## Status of this Memo



## 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.

Table of Contents



## 1. Introduction

This document provides information and advice to system designers on the use of transport port numbers and services. It provides a detailed historical background of the evolution of transport port numbers and their multiple meanings. It also provides specific recommendations on how to use assigned ports.

## 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 assigned through IANA.

Both Well-Known and Registered ports are assigned 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 [RFC2616]. 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 assigns 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 requesting assigned 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 requesting assigned 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

Ports are a scarce resource that are globally shared by the entire Internet community. As a result, every attempt should be made to conserve ports and request only those that are absolutely necessary.

There are a variety of ways that systems can conserve port numbers:

- A single assigned port number can provide access to different capabilities over different connections (or equivalent, e.g., for UDP [RFC768]), using in-band information.

- A single assigned port can indicate the dynamic port(s) on which different capabilities are supported.

- An existing service can indicate the dynamic port(s) on which services are supported, such as with mDNS and portmapper [RFC6762] [RFC6763].

- Copies of an existing service can be differentiated by using different IP addresses (even on the same host).

- Copies of some existing services can be differentiated using in-band information (e.g., HTTP).

- Different performance requirements or capabilities can already be supported using different connections or endpoint associations.

The key observation is that port numbers are intended to differentiate services, not performance, replicas, connections, or payload types. Port numbers are a very small space, so it is never appropriate to consume port numbers to save larger spaces, such as IP addresses.

Others have noted "think twice about modifying TCP, then don't" [RFC1263]. In this case, similar advice might be:

- Think twice before asking for a port, then try not to.
- If you need more than one port assignment, revise your architecture until you can get by with only one, or, preferably, none.

## 7. How to Use Assigned Ports

The following section describes the steps users can take to help assist with the use of assigned ports.

### 7.1. Do You Need a Port?

First, ask whether you really need a port assignment. In many cases, a new assignment may not be needed, for example:

- Is this really a new service, or can you use an existing service?
- Is this an experimental service [RFC3692]? If so, consider using the current experimental ports [RFC2780]
- Can this service use a dynamic port that is coordinated out-of-band, e.g.:
  - By explicit configuration of both endpoints.
  - By shared information within the same host (e.g., a configuration file).
  - Using an existing port discovery service: portmapper, mDNS, etc. [RFC6762] [RFC6763]

There are a few good examples of reasons that more directly suggest that not only is a port not necessary, but it is directly counterindicated:

- Ports are not for performance. Performance enhancement can occur within separate connections.

- Additional ports are not to replicate an existing service. For example, if you have a device that is configured using a web browser, that is a copy of HTTP port 80, and does not warrant a new assignment. However, if you develop an automated system that happens to use HTTP framing, that could be a new service. A good way to tell is "can an unmodified client of the existing service interact with your service"? If so, that would be a copy, and should not request a new assignment.

- Ports are not for insecure versions of existing secure services. Consider that a service that includes required security would be made vulnerable by having the same capability accessible without security.

  Note that the converse is different, i.e., it can be useful to create a new, secure service that replicates an existing insecure service on a new port assignment. This can be necessary when the existing service is not backward-compatible with security enhancements, such as the use of TLS or SSL [Hi95] [RFC5246].

Some users may not need assigned port numbers at all. Some systems can register services in the DNS, using SRV entries. These services can be discovered by a variety of means, including mDNS, or via direct query. In such cases, users can more easily request a SRV name, which are assigned first-come, first-served from a much larger namespace.

IANA assigns port numbers, but this assignment is typically used only for servers, i.e., the host that listens for incoming connections. Clients, i.e., hosts that initiate connections, typically refer to those assigned ports but do not need port assignments for their endpoint.

### 7.2. How Many Ports?

As noted earlier, systems might require a single port assignment, but rarely require multiple ports. There are a variety of known ways to reduce port use. Although some may be cumbersome or inefficient, they are always preferable to consuming additional ports.

Such techniques include:

- Use of a discovery service, either a shared service (mDNS), or a discovery service for a given system

- Multiplex packet types using in-band information, either on a per-message or per-connection basis. Such demultiplexing can even hand-off connections among different processes.

There are some cases where it is still important to have assigned port numbers, largely to traverse either NATs or firewalls. Although automatic configuration protocols have been proposed and developed, system designers cannot yet their presence.

### 7.3. Picking a Port Number

Given a demonstrated need for a port number assignment, the next question is how to pick the desired port number. An application for a port assignment does not need to include a desired port number; in that case, IANA will select from those currently available.

Users should consider whether the requested port number is important. For example, would you accept an assignment if IANA picked the value? Would you want a TCP port number assignment if the corresponding UDP one were unavailable (assuming your service needed only a TCP port) [RFC793]?

The most critical issue in picking a number is selecting the desired range, i.e.., system vs. user ports. The distinction was intended to indicate a difference in privilege; system ports required privileged ('root') access, while user ports did not. That distinction has blurred because some current systems do not limit access control to system ports, and because some system services have been replicated on user numbers (e.g., IRC). Even so, system port assignments have continued at an average rate of 3-4 per year over the past 6 years (2007-2012), indicating that the desire to keep this distinction continues.

As a result, we recommend that the different between user and system ports be treated with caution. Developers are advised to treat services as if they are always run without privilege. As a result:

>> Developers SHOULD NOT apply for system ports because the increased privilege they provide is not always enforced.

>> System implementers SHOULD enforce the need for privilege for processes to listen on system ports.

At some future date, it might be useful to deprecate the distinction between system and user ports altogether, but merely avoiding system ports would potentially waste only approximately 180 of 1024 values (17%).

### 7.4. Support for Security

Services represent a potential system vulnerability. Given the current state of cybersecurity in the Internet, we recommend that:

>> New services SHOULD support security, either directly or via a secure transport such as TLS [RFC5246].

>> Insecure versions of new secure services SHOULD be avoided because of the vulnerability they create.

>> Security SHOULD NOT rely on port number distinctions alone; every service, whether secure or not, SHOULD expect to be attacked.

There is debate as to how to secure legacy insecure services [RFC6335]. Some argue that secure variants should share the existing port assignment, such that security is enabled on a per-connection basis [RFC2817]. Others argue that security should be supported on a new port assignment and be enabled by default. IANA currently permits either approach.

Optional security can penalize performance, requiring additional round-trip exchanges before a connection can be established. As we discussed earlier, ports are a critical resource and it is inappropriate to consume assignments to increase performance.

Note however that a new service might not be eligible for IANA assignment of both an insecure and a secure variant of the same service, and similarly IANA might be skeptical of an assignment for an insecure port for a secure service. In both cases, security of the service is compromised by adding the insecure port assignment.

### 7.5. Support for Future Versions

Current IANA assignments are expected to support versioning [RFC6335]. Versions are typically indicated in-band, either at the beginning of a connection or association, or in each protocol message.

>> Version support SHOULD be included in new services.

>> Version numbers SHOULD NOT be included in either the service name or service description.

Again, the port number space is far too limited to be used as an indicator of protocol version or message type. Although this has happened in the past (e.g., for NFS), it should be avoided.

### 7.6. Transport Protocols

IANA assigns port numbers specific to one or more transport protocols, typically UDP and TCP, but also SCTP, DCCP, and any other standard transport protocol [RFC4340] [RFC4960]. Originally, IANA port assignments were made for both UDP and TCP together; other transports were not indicated. However, to conserve space, and to reflect increasing use of other transports, assignments are now specific only to the transport requested.

In general, a service should request assignments for multiple transports the same service name and description on the same port number only when they all reflect essentially the same service. Good examples of such use are DNS and NFS, where the difference between the UDP and TCP services are specific to supporting each transport. E.g., the UDP variant of a service might add sequence numbers, and the TCP variant of the same service might add in-band message delimiters.

>> Service names and descriptions for multiple transport port assignments SHOULD match only when they describe the same service, with the exception of enhancements for each supported transport.

When the services differ, their service names and descriptions should reflect that difference. E.g., if TCP is used for the basic control protocol and UDP for an alarm protocol, then the services might be "name-ctl" and "name-alarm". A common example is when TCP is used for a service, and UDP is used to determine whether that service is active (via a multicast test message) [RFC1122]. The following convention has been used by IANA for several years to indicate this case:

>> When UDP is used for multicast discovery of an active TCP service, the UDP service name SHOULD end in "-disc".

Some services are used for discovery, either in conjunction with a TCP service, or as a stand-alone capability. Such services will be more reliable when using multicast rather than broadcast, because IP routers do not forward "all nodes" (all 1's, i.e., 255.255.255.255 for IPv4) broadcasts, and are have not been required to support subnet-directed broadcasts since 1999 [RFC1812] [RFC2644].

>> UDP multi-host services SHOULD use multicast rather than broadcast.

Designers should be very careful in creating services over transports that do not support congestion control or error recovery,

notably UDP. There are several issues that should be considered in such cases:

>> UDP services SHOULD be bandwidth limited, using only nominal network capacity. Users should keep in mind that "nominal" may vary depending on the deployment environment, and may be very low.

>> UDP services that use multipoint communication SHOULD be scalable, and SHOULD NOT rely solely on the efficiency of multicast transmission for scalability.

>> UDP services SHOULD include congestion detection and backoff.

>> UDP SHOULD NOT be used as a performance enhancement over TCP, i.e., to circumnavigate TCP's congestion control.

### 7.7. When to Request an Assignment

Assignments are typically requested when a user has enough information to reasonably answer the questions in the IANA application. An application needs to include a description of the service, as well as to address key questions designed to help IANA determine whether the assignment is justified.

Services that are independently developed can be requested at any time, but are typically best requested in the last stages of design and initial experimentation, before any deployment has occurred that cannot easily be updated.

>> Users MUST NOT deploy implementations that use ports prior their assignment by IANA.

Deployments that use ports before deployment complicate IANA management of the port space. Keep in mind that this recommendation protects both other parties and you; it helps ensure that your desired number and service name are available when assigned. The list of currently unassigned numbers is just that - *currently* unassigned. It does not reflect pending applications, nor applications that might arrive before yours. Waiting for an official IANA assignment reduces the chance that your assignment will conflict with another deployed service.

Applications made through Internet Draft / RFC publication typically use a placeholder ("PORTNUM") in the text, and use an experimental port number until a final assignment has been made [RFC6335]. That assignment is initially indicated in the IANA Considerations section of the document, and is tracked by the RFC Editor. When the RFC

reaches the last stages of publication, that request is forwarded to IANA for handling. At that time, IANA typically requests that the applicant fill out the application form on their website, because not every protocol document addresses the information required. Using this single application process also ensures that IANA has complete information even if the RFC publication is interrupted. For this reason as well, the application should be complete and not refer solely to the Internet Draft, RFC, a website, or any other external documentation.

>> Users writing specifications SHOULD use symbolic names for port numbers and service names until an IANA assignment has been completed.

### 7.8. Other Considerations

There are a few other points worth mentioning, which are summarized in this section.

As noted earlier, system ports should be used sparingly, and it is better to avoid them altogether. This avoids the potentially incorrect assumption that the service on such ports run in a privileged mode.

Port names and numbers are not intended to be changed. Once deployed, it can be very difficult to recall every implementation, so the assignment should be retained. However, in cases where the current assignee of a name or number has reasonable knowledge of the impact on such uses, and is willing to accept that impact, the name or number of an assignment can be changed [RFC6335]

Aliases, or multiple service names for the same port number, are no longer considered appropriate [RFC6335].

## 8. 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) [RFC2818].

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.

## 9. 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.

## 10. References

### 10.1. Normative References

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

### 10.2. 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.

[RFC1263] O'Malley, S., L. Peterson, "TCP Extensions Considered Harmful", RFC 1263, October 1991.

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

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

[RFC1812] Baker, F. (Ed.), "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[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.

[RFC2644] Senie, D., "Changing the Default for Directed Broadcasts in Routers", RFC 2644, August 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.

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3962, Jan. 2004.

[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.

[RFC6335] Cotton, M., L. Eggert, J. Touch, M. Westerlund, S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", RFC 6335, August 2011.

[RFC6762] Cheshire, S., M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] Cheshire, S., M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

## 11. 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