                Recommendations on Using Assigned Transport Port Numbers

Abstract

   This document provides recommendations to designers of application
   and service protocols on how to use the transport protocol port
   number space and when to request a port assignment from IANA. It
   provides designer guidance to requesters or users of port numbers on
   how to interact with IANA using the processes defined in RFC 6335;
   thus, this document complements (but does not update) that document.
   It provides guidelines for designers regarding how to interact with
   the IANA processes defined in RFC 6335, thus serving to complement
   (but not update) that document.

Copyright Notice

Table of Contents

1. Introduction

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

   numbers. Note that this document provides information to potential
   port number applicants that complements the IANA process described in
   [RFC6335] (the sole document of BCP 165 before this document), but it
   does not change any of the port number assignment procedures
   described therein. Because they are thus so closely related, this
   document and RFC 6335 are now known together as BCP 165. This
   document is intended to address concerns typically raised during
   Expert Review (see [RFC5226]) of assigned port number applications,
   but it is not intended to bind those reviews. RFC 6335 also
   describes the interaction between port experts and port requests in
   IETF consensus documents. Authors of IETF consensus documents should
   nevertheless follow the advice in this document and can expect
   comment on their port requests from the port experts during IETF Last
   Call or at other times when review is explicitly sought.

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. Lowercase uses of these words are not to be
   interpreted as carrying significance described in RFC 2119.

   In this document, the characters ">>" preceding an indented line(s)
   indicates a statement using the key words listed above. This
   convention aids reviewers in quickly identifying or finding
   requirements for registration and recommendations for use of port
   numbers in this RFC.

3. History

   The term 'port' was first used in [RFC33] to indicate a simplex
   communication path from an individual process and originally applied
   to only the Network Control Program (NCP) connection-oriented
   protocol. 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 numeric source and destination socket

identifiers in packets. [RFC38] provides further detail, describing
how processes might have more than one of these paths and that more
than one path may be active at a time. As a result, there was the
need to add a process identifier to the header of each message so
that incoming messages could be demultiplexed to the appropriate
process. [RFC38] further suggests that 32-bit numbers be used for
these identifiers. [RFC48] discusses the current notion of listening
on a specific port number, but does not discuss the issue of port
number determination. [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 number for common
services.

[RFC76] proposes a "telephone book" by which an index will allow port
numbers to be used by name, but still assumes that both source and
destination port numbers are fixed by such a system. [RFC333]
proposes that a port number pair, rather than an individual port
number, be used on both sides of the connection for demultiplexing
messages. This is the final view in [RFC793] (and its predecessors,
including [IEN112]), and brings us to their current meaning.
[RFC739] introduces the notion of generic reserved port numbers for
groups of protocols, such as "any private RJE server" [RFC739].
Although the overall range of such port numbers 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 port numbers as being used for TCP
(previous RFCs all refer to only NCP). It includes a list of such
well-known port numbers, as well as describes ranges used for
different purposes:

```
   Decimal    Octal     Description
   ----------------------------------------------------------
   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 disappear, and a single list of
number assignments is presented. This is also the first time that
port numbers are described as applying to a connectionless transport
(e.g., UDP) rather than only connection-oriented transports.

By [RFC900], the ranges appear as decimal numbers rather than the
octal ranges used previously. [RFC1340] increases this range from
0-255 to 0-1023 and begins to list TCP and UDP port number
assignments individually (although the assumption was that once
assigned a port number applies to all transport protocols, including

TCP, UDP, recently Stream Control Transmission Protocol (SCTP) and
Datagram Congestion Control Protocol (DCCP), as well as ISO-TP4 for a
brief period in the early 1990s). [RFC1340] also establishes the
Registered range 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 online version, as of [RFC3232] in 2002.

4. Current Port Number Use

   RFC 6335 indicates three ranges of port number assignments:

       Binary   Hex

       0-1023   0x0000-0x03FF System (also Well-Known)
       1024-49151   0x0400-0xBFFF User (also Registered)
       49152-65535   0xC000-0xFFFF Dynamic (also Private)

   System (also Well-Known) encompasses the range 0-1023. On some
   systems, use of these port numbers requires privileged access, e.g.,
   that the process run as 'root' (i.e., as a privileged user), which is
   why these are referred to as System port numbers. The port numbers
   from 1024-49151 denotes non-privileged services, known as User (also
   Registered), because these port numbers do not run with special
   privileges. Dynamic (also Private) port numbers are not assigned.

   Both System and User port numbers are assigned through IANA, so both
   are sometimes called 'registered port numbers'. As a result, the
   term 'registered' is ambiguous, referring either to the entire range
   0-49151 or to the User port numbers. Complicating matters further,
   System port numbers do not always require special (i.e., 'root')
   privilege. For clarity, the remainder of this document refers to the
   port number ranges as System, User, and Dynamic, to be consistent
   with IANA process [RFC6335].

5. What is a Port Number?

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

   o Demultiplexing transport endpoint associations within an end host

   o Identifying a service

   The first purpose requires that each transport endpoint association
   (e.g., TCP connection or UDP pairwise association) using a given
   transport between a given pair of IP addresses use a different pair
   of port numbers, but it does not require either coordination or

registration of port number use. It is the second purpose that
drives the need for a common registry.

Consider a user wanting to run a web server. That service could run
on any port number, provided that all clients knew what port number
to use to access that service at that host. Such information can be
explicitly distributed -- for example, by putting it in the URI:

   http://www.example.com:51509/

Ultimately, the correlation of a service with a port number is an
agreement between just the two endpoints of the association. A web
server can run on port number 53, which might appear as DNS traffic
to others but will connect to browsers that know to use port number
53 rather than 80.

As a concept, a service is the combination of ISO Layers 5-7 that
represents an application-protocol capability. For example, www
(port number 80) is a service that uses HTTP as an application
protocol and provides access to a web server [RFC7230]. However, it
is possible to use HTTP for other purposes, such as command and
control. This is why some current services (HTTP, e.g.) are a bit
overloaded -- they describe not only the application protocol, but a
particular service.

IANA assigns port numbers so that Internet endpoints do not need
pairwise, explicit coordination of the meaning of their port numbers.
This is the primary reason for requesting port number assignment by
IANA -- to have a common agreement between all endpoints on the
Internet as to the default meaning of a port number, which provides
the endpoints with a default port number for a particular protocol or
service.

Port numbers are sometimes used by intermediate devices on a network
path, either to monitor available services, to monitor traffic (e.g.,
to indicate the data contents), or to intercept traffic (to block,
proxy, relay, aggregate, or otherwise process it). In each case, the
intermediate device interprets traffic based on the port number. It
is important to recognize that any interpretation of port numbers --
except at the endpoints -- may be incorrect, because port numbers are
meaningful only at the endpoints. Further, port numbers may not be
visible to these intermediate devices, such as when the transport
protocol is encrypted (as in network- or link-layer tunnels) or when
a packet is fragmented (in which case only the first fragment has the
port number information). Such port number invisibility may
interfere with these capabilities, which are implemented inside the
network and based on a port number.

Port numbers can also be used for other purposes. Assigned port numbers can simplify end-system configuration, so that individual installations do not need to coordinate their use of arbitrary port numbers. Such assignments may also have the effect of simplifying firewall management, so that a single, fixed firewall configuration can either permit or deny a service that uses the assigned ports.

It is useful to differentiate a port number from a service name. The former is a numeric value that is used directly in transport protocol headers as a demultiplexing and service identifier. The latter is primarily a user convenience, where the default map between the two is considered static and resolved using a cached index. This document focuses on the former because it is the fundamental network resource. Dynamic maps between the two, i.e., using DNS SRV records, are discussed further in Section 7.1.

6. Conservation

   Assigned port numbers are a limited resource that is globally shared by the entire Internet community. As of 2014, approximately 5850 TCP and 5570 UDP port numbers had been assigned out of a total range of 49151. As a result of past conservation, current assigned port use is small and the current rate of assignment avoids the need for transition to larger number spaces. This conservation also helps avoid the need for IANA to rely on assigned port number reclamation, which is practically impossible even though procedurally permitted [RFC6335].

   IANA aims to assign only one port number per service, including variants [RFC6335], but there are other benefits to using fewer port numbers for a given service. Use of multiple assigned port numbers can make applications more fragile, especially when firewalls block a subset of those port numbers or use ports numbers to route or prioritize traffic differently. As a result:

   >> Each assigned port requested MUST be justified by the applicant as an independently useful service.

6.1. Guiding Principles

   This document provides recommendations for users that also help conserve assigned port number space. Again, this document does not update [RFC6335] (originally the sole document of BCP 165), which describes the IANA procedures for managing assigned transport port numbers and services, but rather augments it by now becoming part of BCP 165 (i.e., BCP 165 now refers to both documents together). Assigned port number conservation is based on a number of basic principles:

   o A single assigned port number can support different functions over
      separate endpoint associations, determined using in-band
      information. An FTP data connection can transfer binary or text
      files, the latter translating line-terminators, as indicated in-
      band over the control port number [RFC959].

   o A single assigned port number can indicate the Dynamic port
      number(s) on which different capabilities are supported, as with
      passive-mode FTP [RFC959].

   o Several existing services can indicate the Dynamic port number(s)
      on which other services are supported, such as with Multicast DNS
      (mDNS) and portmapper [RFC1833] [RFC6762] [RFC6763].

   o Copies of some existing services can be differentiated using in-
      band information (e.g., URIs in the HTTP Host field and TLS Server
      Name Indication extension) [RFC7230] [RFC6066].

   o Services requiring varying performance properties can already be
      supported using separate endpoint associations (connections or
      other associations), each configured to support the desired
      properties. For example, a high-speed and low-speed variant can
      be determined within the service using the same assigned port.

   Assigned port numbers are intended to differentiate services, not
   variations of performance, replicas, pairwise endpoint associations,
   or payload types. Assigned port numbers are also a small space
   compared to other Internet number spaces; it is never appropriate to
   consume assigned port numbers to conserve larger spaces such as IP
   addresses, especially where copies of a service represent different
   endpoints.

6.2. Firewall and NAT Considerations

   Ultimately, port numbers indicate services only to the endpoints, and
   any intermediate device that assigns meaning to a value can be
   incorrect. End systems might agree to run web services (HTTP) over
   port number 53 (typically used for DNS) rather than port number 80,
   at which point a firewall that blocks port number 80 but permits port
   number 53 would not have the desired effect. Nonetheless, assigned
   port numbers are often used to help configure firewalls and other
   port-based systems for access control.

   Using Dynamic port numbers, or explicitly indicated port numbers
   indicated in-band over another service (such as with FTP) often
   complicates firewall and NAT interactions [RFC959]. FTP over
   firewalls often requires direct support for deep-packet inspection
   (to snoop for the Dynamic port number for the NAT to correctly map)

or passive-mode FTP (in which both connections are opened from the
client side).

7. Considerations for Requesting Port Number Assignments

   Port numbers are assigned by IANA by a set of documented procedures
   [RFC6335]. The following section describes the steps users can take
   to help assist with responsible use of assigned port numbers and with
   preparing an application for a port number assignment.

7.1. Is a port number assignment necessary?

   First, it is useful to consider whether a port number assignment is
   required. In many cases, a new number assignment may not be needed.
   The following questions may aid in making this determination:

   o Is this really a new service or could an existing service suffice?

   o Is this an experimental service [RFC3692]? If so, consider using
      the current experimental ports [RFC2780].

   o Is this service independently useful? Some systems are composed
      from collections of different service capabilities, but not all
      component functions are useful as independent services. Port
      numbers are typically shared among the smallest independently
      useful set of functions. Different service uses or properties can
      be supported in separate pairwise endpoint associations after an
      initial negotiation, e.g., to support software decomposition.

   o Can this service use a Dynamic port number that is coordinated
      out-of-band? For example:

      o By explicit configuration of both endpoints.

      o By internal mechanisms within the same host (e.g., a
         configuration file, indicated within a URI or using
         interprocess communication).

      o Using information exchanged on a related service: FTP [RFC959],
         SIP [RFC3261], etc.

      o Using an existing port discovery service: portmapper [RFC1833],
         mDNS [RFC6762] [RFC6763], etc.

There are a few good examples of reasons that more directly suggest
that not only is a port number assignment not necessary, but it is
directly counter-indicated:

o Assigned port numbers are not intended to differentiate
   performance variations within the same service, e.g., high-speed
   versus ordinary speed. Performance variations can be supported
   within a single assigned port number in context of separate
   pairwise endpoint associations.

o Additional assigned port numbers are not intended to replicate an
   existing service. For example, if a device is configured to use a
   typical web browser, then the port number used for that service is
   a copy of the http service that is already assigned to port number
   80 and does not warrant a new assignment. However, an automated
   system that happens to use HTTP framing -- but is not primarily
   accessed by a browser -- might be a new service. A good way to
   tell is to ask, "Can an unmodified client of the existing service
   interact with the proposed service?". If so, that service would
   be a copy of an existing service and would not merit a new
   assignment.

o Assigned port numbers not intended for intra-machine
   communication. Such communication can already be supported by
   internal mechanisms (interprocess communication, shared memory,
   shared files, etc.). When Internet communication within a host is
   desired, the server can bind to a Dynamic port that is indicated
   to the client using these internal mechanisms.

o Separate assigned port numbers are not intended for insecure
   versions of existing (or new) secure services. A service that
   already requires security would be made more 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 number assignment. This can be necessary
   when the existing service is not backward-compatible with security
   enhancements, such as the use of TLS [RFC5246] or DTLS [RFC6347].

o Assigned port numbers are not intended for indicating different
   service versions. Version differentiation should be handled in-
   band, e.g., using a version number at the beginning of an
   association (e.g., connection or other transaction). This may not
   be possible with legacy assignments, but all new services should
   incorporate support for version indication.

Some services may not need assigned port numbers at all, e.g., SIP
allows voice calls to use Dynamic ports [RFC3261]. 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 [RFC6762] [RFC6763]. In such cases, users can more easily
request an 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 or
other associations. Clients, i.e., hosts that initiate connections
or other associations, typically refer to those assigned port numbers
but do not need port number assignments for their endpoint.

Finally, an assigned port number is not a guarantee of exclusive use.
Traffic for any service might appear on any port number, due to
misconfiguration or deliberate misuse. Application and service
designers are encouraged to validate traffic based on its content.

7.2. How many assigned port numbers are necessary?

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

Such techniques include:

o Use of a discovery service, either a shared service (mDNS) or a
   discovery service for a given system [RFC6762] [RFC6763].

o Multiplex packet types using in-band information, either on a per-
   message or per-connection basis. Such demultiplexing can even
   hand off different messages and connections among different
   processes, such as is done with FTP [RFC959].

There are some cases where NAT and firewall traversal are
significantly improved by having an assigned port number. Although
NAT traversal protocols supporting automatic configuration have been
proposed and developed (e.g., Session Traversal Utilities for NAT
(STUN) [RFC5389], Traversal Using Relays around NAT (TURN) [RFC5766],
and Interactive Connectivity Establishment (ICE) [RFC5245]), not all
application and service designers can rely on their presence as of
yet.

In the past, some services were assigned multiple port numbers or
sometimes fairly large port ranges (e.g., X11). This occurred for a
variety of reasons: port number conservation was not as widely
appreciated, assignments were not as ardently reviewed, etc. This no
longer reflects current practice and such assignments are not
considered to constitute a precedent for future assignments.

7.3. Picking an Assigned 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 number 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 an assignment be acceptable if IANA picked the
   port number value? Would a TCP (or other transport protocol) port
   number assignment be useful by itself? If so, a port number can be
   assigned to a service for one transport protocol where it is already
   (or can be subsequently) assigned to a different service for other
   transport protocols.

   The most critical issue in picking a number is selecting the desired
   range, i.e., System versus User port numbers. The distinction was
   intended to indicate a difference in privilege; originally, System
   port numbers required privileged ('root') access, while User port
   numbers did not. That distinction has since blurred because some
   current systems do not limit access control to System port numbers
   and because some System services have been replicated on User numbers
   (e.g., IRC). Even so, System port number assignments have continued
   at an average rate of 3-4 per year over the past 7 years (2007-2013),
   indicating that the desire to keep this distinction continues.

   As a result, the difference between System and User port numbers
   needs to be treated with caution. Developers are advised to treat
   services as if they are always run without privilege.

   Even when developers seek a System port number assignment, it may be
   very difficult to obtain. System port number assignment requires
   IETF Review or IESG Approval and justification that both User and
   Dynamic port number ranges are insufficient [RFC6335]. Thus, this
   document recommends both:

   >> Developers SHOULD NOT apply for System port number assignments
   because the increased privilege they are intended to provide is not
   always enforced.

>> System implementers SHOULD enforce the need for privilege for
processes to listen on System port numbers.

At some future date, it might be useful to deprecate the distinction
between System and User port numbers altogether. Services typically
require elevated ('root') privileges to bind to a System port number,
but many such services go to great lengths to immediately drop those
privileges just after connection or other association establishment
to reduce the impact of an attack using their capabilities. Such
services might be more securely operated on User port numbers than on
System port numbers. Further, if System port numbers were no longer
assigned, as of 2014 it would cost only 180 of the 1024 System values
(17%), or 180 of the overall 49152 assigned (System and User) values
(<0.04%).

7.4. Support for Security

Just as a service is a way to obtain information or processing from a
host over a network, a service can also be the opening through which
to compromise that host. Protecting a service involves security,
which includes integrity protection, source authentication, privacy,
or any combination of these capabilities. Security can be provided
in a number of ways, and thus:

>> New services SHOULD support security capabilities, either directly
or via a content protection such as TLS [RFC5246] or Datagram TLS
(DTLS) [RFC6347], or transport protection such as the TCP-AO
[RFC5925]. Insecure versions of new or existing secure services
SHOULD be avoided because of the new vulnerability they create.

Secure versions of legacy services that are not already security-
capable via in-band negotiations can be very useful. However, there
is no IETF consensus on when separate ports should be used for secure
and insecure variants of the same service [RFC2595] [RFC2817]
[RFC6335]. The overall preference is for use of a single port, as
noted in Section 6 of this document and Section 7.2 of [RFC6335], but
the appropriate approach depends on the specific characteristics of
the service. As a result:

>> When requesting both secure and insecure port assignments for the
same service, justification is expected for the utility and safety of
each port as an independent service (Section 6). Precedent (e.g.,
citing other protocols that use a separate insecure port) is
inadequate justification by itself.

It's also important to recognize that port number assignment is not itself a guarantee that traffic using that number provides the corresponding service or that a given service is always offered only on its assigned port number. Port numbers are ultimately meaningful only between endpoints and any service can be run on any port. Thus:

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

Applications for a new service that requires both a secure and insecure port may be found, on Expert Review, to be unacceptable, and may not be approved for allocation. Similarly, an application for a new port to support an insecure variant of an existing secure protocol may be found unacceptable. In both cases, the resulting security of the service in practice will be a significant consideration in the decision as to whether to assign an insecure port.

7.5. Support for Future Versions

Requests for assigned port numbers are expected to support multiple versions on the same assigned port number [RFC6335]. Versions are typically indicated in-band, either at the beginning of a connection or other association or in each protocol message.

>> Version support SHOULD be included in new services rather than relying on different port number assignments for different versions.

>> Version numbers SHOULD NOT be included in either the service name or service description, to avoid the need to make additional port number assignments for future variants of a service.

Again, the assigned 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 in new requests.

7.6. Transport Protocols

IANA assigns port numbers specific to one or more transport protocols, typically UDP [RFC768] and TCP [RFC793], but also SCTP [RFC4960], DCCP [RFC4340], and any other standard transport protocol. Originally, IANA port number assignments were concurrent for both UDP and TCP, and other transports were not indicated. However, to conserve the assigned port number space and to reflect increasing use of other transports, assignments are now specific only to the transport being used.

In general, a service should request assignments for multiple
transports using 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. For example, the UDP variant of a service might add
sequence numbers and the TCP variant of the same service might add
in-band message delimiters. This document does not describe the
appropriate selection of a transport protocol for a service.

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

When the services differ, it may be acceptable or preferable to use
the same port number, but the service names and descriptions should
be different for each transport/service pair, reflecting the
differences in the services. For example, 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 (e.g., via a unicast, broadcast, or multicast
test message) [RFC1122]. IANA has, for several years, used the
suffix "-disc" in service names to distinguish discovery services,
such as are used to identify endpoints capable of a given service.

>> Names of discovery services SHOULD use an identifiable suffix; the
suggestion is "-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 (over IPv4)
because IP routers do not forward "all nodes" broadcasts (all 1's,
i.e., 255.255.255.255 for IPv4) and have not been required to support
subnet-directed broadcasts since 1999 [RFC1812] [RFC2644].

This issue is relevant only for IPv4 because IPv6 does not support
broadcast.

>> UDP over IPv4 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, as summarized in Table 1 in [RFC5405]. In addition, the
following recommendations apply to service design:

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

>> Services SHOULD NOT use UDP as a performance enhancement over TCP,
e.g., 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. IANA applications typically take up to a few weeks to
process, with some complex cases taking up to a month. The process
typically involves a few exchanges between the IANA Ports Expert
Review team and the applicant.

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. The application should be complete and
not refer solely to an Internet-Draft, RFC, website, or any other
external documentation.

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 assigned port
numbers prior their assignment by IANA.

>> Users MUST NOT deploy implementations that default to using the
experimental System port numbers (1021 and 1022 [RFC4727]) outside a
controlled environment where they can be updated with a subsequent
assigned port [RFC3692].

Deployments that use unassigned port numbers before assignment
complicate IANA management of the port number space. Keep in mind
that this recommendation protects existing assignees, users of
current services, and applicants for new assignments; it helps ensure
that a 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. Waiting for
an official IANA assignment reduces the chance that an assignment
request will conflict with another deployed service.

Applications made through Internet-Draft posting or RFC publication
(in any stream) typically use a placeholder ("PORTNUM") in the text,
and implementations 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, which
is tracked by the RFC Editor. When a document has been approved for
publication, that request is forwarded to IANA for handling. IANA
will make the new assignment accordingly. At that time, IANA may
also request that the applicant fill out the application form on
their website, e.g., when the RFC does not directly address the
information expected as per [RFC6335]. "Early" assignments can be
made when justified, e.g., for early interoperability testing,
according to existing process [RFC7120] [RFC6335].

>> Users writing specifications SHOULD use symbolic names for port
numbers and service names until an IANA assignment has been
completed. Implementations SHOULD use experimental port numbers
during this time, but those numbers MUST NOT be cited in
documentation except as interim.

7.8. Squatting

"Squatting" describes the use of a number from the assignable range
in deployed software without IANA assignment for that use, regardless
of whether the number has been assigned or remains available for
assignment. It is hazardous because IANA cannot track such usage and
thus cannot avoid making legitimate assignments that conflict with
such unauthorized usage.

Such "squatted" port numbers remain unassigned, and IANA retains the
right to assign them when requested by other applicants. Application
and service designers are reminded that is never appropriate to use
port numbers that have not been directly assigned [RFC6335]. In
particular, any unassigned code from the assigned ranges will be
assigned by IANA, and any conflict will be easily resolved as the
protocol designer's fault once that happens (because they would not
be the assignee). This may reflect in the public's judgment on the
quality of their expertise and cooperation with the Internet
community.

Regardless, there are numerous services that have squatted on such
numbers that are in widespread use. Designers who are using such
port numbers are encouraged to apply for an assignment. Note that
even widespread de facto use may not justify a later IANA assignment
of that value, especially if either the value has already been
assigned to a legitimate applicant or if the service would not
qualify for an assignment of its own accord.

7.9. Other Considerations

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

   Assigned port numbers are not intended to be changed; this includes
   the corresponding service name. 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 assigned port number,
   are no longer considered appropriate [RFC6335].

8. Security Considerations

   This document focuses on the issues arising when designing services
   that require new port assignments. Section 7.4 addresses the
   security and security-related issues of that interaction.

   When designing a secure service, the use of TLS [RFC5246], DTLS
   [RFC6347], or TCP-AO [RFC5925] mechanisms that protect transport
   protocols or their contents is encouraged. It may not be possible to
   use IPsec [RFC4301] in similar ways because of the different
   relationship between IPsec and port numbers and because applications
   may not be aware of IPsec protections.

   This document reminds application and service designers that port
   numbers do not protect against denial-of-service attack or guarantee
   that traffic should be trusted. Using assigned numbers for port
   filtering isn't a substitute for authentication, encryption, and
   integrity protection. The port number alone should not be used to
   avoid denial-of-service attacks or to manage firewall traffic because
   the use of port numbers is not regulated or validated.

   The use of assigned port numbers is the antithesis of privacy because
   they are intended to explicitly indicate the desired application or
   service. Strictly, port numbers are meaningful only at the
   endpoints, so any interpretation elsewhere in the network can be
   arbitrarily incorrect. However, those numbers can also expose
   information about available services on a given host. This
   information can be used by intermediate devices to monitor and

intercept traffic as well as to potentially identify key endpoint
software properties ("fingerprinting"), which can be used to direct
other attacks.

9. IANA Considerations

The entirety of this document focuses on 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,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC2780] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For
              Values In the Internet Protocol and Related Headers", BCP
              37, RFC 2780, DOI 10.17487/RFC2780, March 2000,
              <http://www.rfc-editor.org/info/rfc2780>.

   [RFC3692] Narten, T., "Assigning Experimental and Testing Numbers
              Considered Useful", BCP 82, RFC 3692,
              DOI 10.17487/RFC3692, January 2004,
              <http://www.rfc-editor.org/info/rfc3692>.

   [RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4,
              ICMPv6, UDP, and TCP Headers", RFC 4727,
              DOI 10.17487/RFC4727, November 2006,
              <http://www.rfc-editor.org/info/rfc4727>.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246,
              DOI 10.17487/RFC5246, August 2008,
              <http://www.rfc-editor.org/info/rfc5246>.

   [RFC5405] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines
              for Application Designers", BCP 145, RFC 5405,
              DOI 10.17487/RFC5405, November 2008,
              <http://www.rfc-editor.org/info/rfc5405>.

   [RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP
              Authentication Option", RFC 5925, DOI 10.17487/RFC5925,
              June 2010, <http://www.rfc-editor.org/info/rfc5925>.

   [RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S.
              Cheshire, "Internet Assigned Numbers Authority (IANA)
              Procedures for the Management of the Service Name and
              Transport Protocol Port Number Registry", BCP 165, RFC
              6335, DOI 10.17487/RFC6335, August 2011,
              <http://www.rfc-editor.org/info/rfc6335>.

   [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer
              Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347,
              January 2012, <http://www.rfc-editor.org/info/rfc6347>.

10.2. Informative References

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

   [RFC33]   Crocker, S., "New Host-Host Protocol", RFC 33,
              DOI 10.17487/RFC0033, February 1970,
              <http://www.rfc-editor.org/info/rfc33>.

   [RFC37]   Crocker, S., "Network Meeting Epilogue, etc", RFC 37,
              DOI 10.17487/RFC0037, March 1970,
              <http://www.rfc-editor.org/info/rfc37>.

   [RFC38]   Wolfe, S., "Comments on Network Protocol from NWG/RFC
              #36", RFC 38, DOI 10.17487/RFC0038, March 1970,
              <http://www.rfc-editor.org/info/rfc38>.

   [RFC48]   Postel, J. and S. Crocker, "Possible protocol plateau",
              RFC 48, DOI 10.17487/RFC0048, April 1970,
              <http://www.rfc-editor.org/info/rfc48>.

   [RFC61]   Walden, D., "Note on Interprocess Communication in a
              Resource Sharing Computer Network", RFC 61,
              DOI 10.17487/RFC0061, July 1970,
              <http://www.rfc-editor.org/info/rfc61>.

   [RFC76]   Bouknight, J., Madden, J., and G. Grossman, "Connection by
              name: User oriented protocol", RFC 76,
              DOI 10.17487/RFC0076, October 1970,
              <http://www.rfc-editor.org/info/rfc76>.

   [RFC333]   Bressler, R., Murphy, D., and D. Walden, "Proposed
              experiment with a Message Switching Protocol", RFC 333,
              DOI 10.17487/RFC0333, May 1972,
              <http://www.rfc-editor.org/info/rfc333>.

   [RFC739]   Postel, J., "Assigned numbers", RFC 739,
              DOI 10.17487/RFC0739, November 1977,
              <http://www.rfc-editor.org/info/rfc739>.

   [RFC758]   Postel, J., "Assigned numbers", RFC 758,
              DOI 10.17487/RFC0758, August 1979,
              <http://www.rfc-editor.org/info/rfc758>.

   [RFC768]   Postel, J., "User Datagram Protocol", STD 6, RFC 768,
              DOI 10.17487/RFC0768, August 1980,
              <http://www.rfc-editor.org/info/rfc768>.

   [RFC793]   Postel, J., "Transmission Control Protocol", STD 7, RFC
              793, DOI 10.17487/RFC0793, September 1981,
              <http://www.rfc-editor.org/info/rfc793>.

   [RFC820]   Postel, J., "Assigned numbers", RFC 820,
              DOI 10.17487/RFC0820, August 1982,
              <http://www.rfc-editor.org/info/rfc820>.

   [RFC900]   Reynolds, J. and J. Postel, "Assigned Numbers", RFC 900,
              DOI 10.17487/RFC0900, June 1984,
              <http://www.rfc-editor.org/info/rfc900>.

   [RFC959]   Postel, J. and J. Reynolds, "File Transfer Protocol", STD
              9, RFC 959, DOI 10.17487/RFC0959, October 1985,
              <http://www.rfc-editor.org/info/rfc959>.

   [RFC1122] Braden, R., Ed., "Requirements for Internet Hosts -
              Communication Layers", STD 3, RFC 1122,
              DOI 10.17487/RFC1122, October 1989,
              <http://www.rfc-editor.org/info/rfc1122>.

   [RFC1340] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1340,
              DOI 10.17487/RFC1340, July 1992,
              <http://www.rfc-editor.org/info/rfc1340>.

   [RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1700,
              DOI 10.17487/RFC1700, October 1994,
              <http://www.rfc-editor.org/info/rfc1700>.

   [RFC1812] Baker, F., Ed., "Requirements for IP Version 4 Routers",
              RFC 1812, DOI 10.17487/RFC1812, June 1995,
              <http://www.rfc-editor.org/info/rfc1812>.

   [RFC1833] Srinivasan, R., "Binding Protocols for ONC RPC Version 2",
              RFC 1833, DOI 10.17487/RFC1833, August 1995,
              <http://www.rfc-editor.org/info/rfc1833>.

   [RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC
              2595, DOI 10.17487/RFC2595, June 1999,
              <http://www.rfc-editor.org/info/rfc2595>.

   [RFC2644] Senie, D., "Changing the Default for Directed Broadcasts
              in Routers", BCP 34, RFC 2644, DOI 10.17487/RFC2644,
              August 1999, <http://www.rfc-editor.org/info/rfc2644>.

   [RFC2817] Khare, R. and S. Lawrence, "Upgrading to TLS Within
              HTTP/1.1", RFC 2817, DOI 10.17487/RFC2817, May 2000,
              <http://www.rfc-editor.org/info/rfc2817>.

   [RFC3232] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced
              by an On-line Database", RFC 3232, DOI 10.17487/RFC3232,
              January 2002, <http://www.rfc-editor.org/info/rfc3232>.

   [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
              A., Peterson, J., Sparks, R., Handley, M., and E.
              Schooler, "SIP: Session Initiation Protocol", RFC 3261,
              DOI 10.17487/RFC3261, June 2002,
              <http://www.rfc-editor.org/info/rfc3261>.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
              Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
              December 2005, <http://www.rfc-editor.org/info/rfc4301>.

   [RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram
              Congestion Control Protocol (DCCP)", RFC 4340,
              DOI 10.17487/RFC4340, March 2006,
              <http://www.rfc-editor.org/info/rfc4340>.

   [RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol",
              RFC 4960, DOI 10.17487/RFC4960, September 2007,
              <http://www.rfc-editor.org/info/rfc4960>.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              DOI 10.17487/RFC5226, May 2008,
              <http://www.rfc-editor.org/info/rfc5226>.

   [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment
              (ICE): A Protocol for Network Address Translator (NAT)
              Traversal for Offer/Answer Protocols", RFC 5245,
              DOI 10.17487/RFC5245, April 2010,
              <http://www.rfc-editor.org/info/rfc5245>.

   [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing,
              "Session Traversal Utilities for NAT (STUN)", RFC 5389,
              DOI 10.17487/RFC5389, October 2008,
              <http://www.rfc-editor.org/info/rfc5389>.

   [RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using
              Relays around NAT (TURN): Relay Extensions to Session
              Traversal Utilities for NAT (STUN)", RFC 5766,
              DOI 10.17487/RFC5766, April 2010,
              <http://www.rfc-editor.org/info/rfc5766>.

   [RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS)
              Extensions: Extension Definitions", RFC 6066,
              DOI 10.17487/RFC6066, January 2011,
              <http://www.rfc-editor.org/info/rfc6066>.

   [RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762,
              DOI 10.17487/RFC6762, February 2013,
              <http://www.rfc-editor.org/info/rfc6762>.

   [RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service
              Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,
              <http://www.rfc-editor.org/info/rfc6763>.

   [RFC7120] Cotton, M., "Early IANA Allocation of Standards Track Code
              Points", BCP 100, RFC 7120, DOI 10.17487/RFC7120, January
              2014, <http://www.rfc-editor.org/info/rfc7120>.

   [RFC7230] Fielding, R., Ed., and J. Reschke, Ed., "Hypertext
              Transfer Protocol (HTTP/1.1): Message Syntax and Routing",
              RFC 7230, DOI 10.17487/RFC7230, June 2014,
              <http://www.rfc-editor.org/info/rfc7230>.

Acknowledgments

Author's Address

   Joe Touch
   USC/ISI
   4676 Admiralty Way
   Marina del Rey, CA 90292-6695
   United States

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