TSVWG
Internet Draft
Updates: 4727
Intended status: Standards Track
Expires: November 2025

J. Touch
Independent Consultant

May 18, 2025

User Ports for Experiments
draft-ietf-tsvwg-usr-exp-10.txt

Abstract

This document defines user ports for experiments using transport protocols. It describes the use of experiment identifiers to enable shared use of these user ports. It also updates RFC 4727 to recommend the use of these experimental identifiers for the system ports for experiments in the same manner.

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.

The list of current Internet-Drafts can be accessed at https://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

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 November 18, 2025.

Table of Contents

1. Introduction

Various network codepoints have been allocated for experimental use, including those for IPv4 [RFC791], IPv6 [RFC8200], ICMPv4 [RFC792], ICMPv6 [RFC4443], UDP [RFC768], and TCP [RFC9293]. These include transport protocol port numbers 1021 and 1022, using the service names "EXP1" and "EXP2" [RFC4727].

There has always been an expectation that experiments needing privileged (system) ports use these assignments and unprivileged ports use those from the dynamic range [RFC6335][RFC7605]. However, dynamic ports can be difficult to reserve in some systems or blocked from traversing some firewalls. As a consequence, there is a need for non-privileged, non-dynamic ports - i.e., user ports - for experiments.

This document reserves user ports for experimentation and describes the use of experiment identifiers to differentiate shared use of these ports for concurrent experiments. This document also creates a

PExID registry, in addition to the IANA service names and ports registry [SP-reg], to reduce the potential that experimental uses of PExIDs that could be tested in the public Internet might interfere with each other.

This document updates RFC 4727 by adding the following text to section 1:

> "[IANA-THIS-RFC] defines PExIDs that are that are recommended for services that might not qualify for a port assignment per current requirements in [RFC6335] and [RFC7605] because they are either short-term or need more than one port number during development (see Sec. 7.1 of [RFC7605])."

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. User Ports for Experiments

The system, user, and dynamic port ranges vary in their properties [RFC7605]. System ports often include privileged access, sometimes known as ’root’. Dynamic ports are used as client ports when establishing associations with services on registered ports. User ports have neither privilege nor the risk of use by other connections. User ports are also more likely to allow configuration to pass through firewalls, where system and dynamic ports can be difficult to ’un-block’.

This document registers USR-EXP1 and USR-EXP2 for user port experiments, using port numbers #UPORT1 and #UPORT2. These ports are assigned from the user range, allowing non-privileged experiments without the need to use ports from the dynamic range. They are intended to complement the system ports already assigned for experimental use [RFC4727].

4. Protocol Experiment Identifiers (PExIDs)

This document also creates a registry for port experiment identifiers (PExIDs), in the same manner as the registry created for shared TCP option experiments [RFC6994][TCP-reg]. These PExIDs are intended for services that might not qualify for a port assignment per current requirements in [RFC6335] and [RFC7605] because they are

either short-term or need more than one port number during development (see Sec. 7.1 of [RFC7605]). Such is the case for student projects that operate over the public Internet and/or across firewalls. Additionally, although selection of a random PExID might suffice, the bar for PExID registration is low (first-come, first served) and encouraged.

The PExID approach is inspired by the ExID method for sharing experimental option codepoints, originally developed for TCP [RFC6994] and later applied to UDP [TH25]. That method could be applied here, but requires OS support, whereas the PExID is used in the data path and requires no OS modification. This method could be applied to sharing other codepoints, e.g., protocol options and codes, but that is outside the scope of this document.

Experimenters are encouraged to register PExIDs with IANA and to include them at the beginning of their transport data, i.e., at the front of each separate message or byte stream, as a 32-bit unsigned integer in network standard byte order. The use of PExIDs helps differentiate experiments without the need for additional port assignments.

This document also encourages the use of these PExIDs for experiments using existing experiment ports, i.e., system ports EXP1 and EXP2.

PExIDs differentiate experiments but are not intended to be specific to a given experiment port, whether system or user, so a single registration is used for all experiment ports. It is the responsibility of the experimenter to determine which port(s) each experiment uses.

The remainder of this document focuses on the issues associated with using PExIDs.

5. Using PExIDs in Transport Protocols

PExIDs differentiate use of the experiment transport ports, both for TCP as previously assigned [RFC4727] and for other transports as defined in this document.

PExIDs are intended to be placed in network-standard byte order at the beginning of each independent transport data payload.

For connection-oriented transport protocols, such as TCP [RFC9293], SCTP [RFC9260], and DCCP [RFC4340], the PExID is typically sent once for each connection at the beginning of the user transfer and echoed

upon receipt, enabling both ends to confirm the experiment for the connection's socket pair. That socket pair is then associated with the experiment identified by that PExID for the duration of the connection.

For connectionless transport protocols, such as UDP [RFC768], the PExID is typically included at the beginning of every message in both directions.

In most cases, the PExID is sent as user data. SCTP is one exception, because of its Payload Protocol Identifier (PPID), as discussed further in Section 5.1. Alternately, PExID can be confirmed during the connection or security handshake or other transport header, as discussed in Section 5.2. In other cases, the PExID can be transferred elsewhere in the data stream, as specified by the user application.

Two endpoints can engage in multiple experiments using the same experimental port number and transport protocol. In such cases, users are expected to support demultiplexing of those different experiments using the PExID.

5.1. SCTP and DCCP PExID Use

SCTP and DCCP connections can use self-assigned Private service codes, which provide experimental-use identification [RFC4340][RFC5595]. There is thus no need to use PExIDs to differentiate experiments on the same port number. PExIDs can be used in addition to those codes if desired, notably in developing a single application-layer solution for multiple transport protocols.

SCTP also includes a Payload Protocol Identifier (PPID), which identifies the information within each user message. PPIDs are assigned on a first-come, first-served (FCFS) basis and are abundant (2^32 codepoints), so there is no need for a separate experimental-use PPID. The PExID differentiate shared use of the user experimental port number and thus serves a different purpose than the PPID; both can be used together or separately for SCTP.

Because SCTP supports multiple concurrent streams, it is useful for experiments using PExIDs to be identified in a particular stream before proceeding with other streams, to avoid excessive buffering. For SCTP using only PExIDs for that purpose, users SHOULD send the PExID ordered and reliably as the first user message using PPID of #PPID1 in stream 0 (the default stream). Until the PExID user message is echoed back on stream 0, user messages on stream 0 SHOULD be sent ordered and the user SHOULD avoid transmitting user messages

on other streams. The echoed user message SHOULD use the PPID of #PPID1 assigned for this purpose. That PExID user message MUST contain only the PExID as a 32-bit unsigned integer in network standard byte order.

5.2. PExID Coordination During State Negotiation

For stateful associations, the PExID can be indicated during the initial state negotiation of the transport or security protocol. For TCP, SCTP, DCCP, QUIC [RFC9000], these could be indicated using parameters of the initial connection handshake, e.g, as transport options. For UDP, a similar mechanism could be used on each packet if UDP options are supported [TH25]. In all cases (TCP, SCTP, DCCP, QUIC, UDP), no option type is currently assigned for this purpose. Additionally, these options would be available only after assigned and deployed, whereas the mechanism defined here is available without needing any OS modification.

A similar mechanism is available within both TLS and DTLS, providing extensions to negotiating additional security association parameters [RFC8446][RFC9147]. In both protocols, the PExID could be sent in ClientHello requests and echoed in ServerHello responses, although for these protocols the extension would require two fields (because such fields carry only 16 bits of content and two are needed for the 32-bit PExID).

In all the above cases, the details of such a mechanism are outside the scope of this document and would require additional IANA codepoint assignments. They are not generally anticipated because such mechanisms are more difficult to deploy, hampering the very experimentation this mechanism is intended to foster.

6. PExID Interactions with Other Protocols and Mechanisms

PExIDs help differentiate different uses of the same experimental transport port number using data outside the transport header, and thus would not be supported by existing NATs, firewalls, deep-packet inspectors (DPIs), or service function chaining [RFC7665]. These devices would need to be modified to detect the PExID, either at the beginning of the connection (for connection-oriented uses) or within each data payload (for connectionless uses).

Some methods to traverse tunnels are also affected by the use of PExIDs. STUN uses a method similar to PExIDs in its in-band message identifier [RFC8489]. These identifiers begin with a 32-bit field first two bits are "00", followed by a type and length, followed by a 32-bit ’magic number’ of 0x2112A442, followed by a 96-bit

transaction identifier. PExIDs are similar to the transaction identifier, but would occur earlier in the data stream.

The TURN mechanism for NAT traversal does not interact with use of PExIDs [RFC8656]. The STUN mechanism can be used concurrent with PExIDs if the PExIDs are selected where the two highest bits are something other than "00" (as required in STUN messages). Because not all service or protocols are intended to be used concurrent with STUN, this restricting should not be a concern.

Some protocols use "magic bytes" to identify streams and/or messages. PExIDs are a specific interpretation of the first for magic bytes of each stream or message to demultiplex shared use of the experimental transport ports, thus they would not necessarily be compatible with other concurrent use of magic bytes.

7. Security Considerations

The creation of new ports for experiment purposes does not create any new security considerations. At best, it potentially reduces the use of privileged system ports for such experiments, which avoids the associated risk of unnecessary privileged access.

Like conventional transport protocol port numbers, PExIDs can be used for DPI to identify services and protocols (see Sec. 5.3.1 of [RFC6973]). When such information is intended to be protected or private, it can be sent as user data inside an encrypted stream or message, e.g., as user data in TCP/TLS or UDP/DTLS.

PExIDs are not supported by existing firewalls, DPI devices, IPsec traffic selectors or other systems that demultiplex or identify traffic using transport port numbers. Traffic using the same transport port numbers would be treated the same if the PExID were not included in the filter, which could either inadvertently admit or deny access. Care should be taken when to avoid PExID use with the same experimental port number when different filtering is expected.

Experimenters are encouraged to include security in any new experiment, regardless of port (per Section 7.4 of [RFC7605]).

8. IANA Considerations

This document hereby requests the assignment of two user ports for experimental purposes below. IANA is asked to replace instances of #UPORT1 and #UPORT2 throughout this document based on the actual

allocation. This paragraph is intended to be removed prior to final publication.

This document also hereby requests the assignment of the SCTP PPID "PEXID" for use in association with these port numbers. IANA is asked to replace instances of #PPID1 throughout this document based on the actual allocation. This paragraph is intended to be removed prior to final publication.

IANA has assigned the following user ports for experiments:

Service Name	USR-EXP1
Transport Protocol(s)	TCP, UDP, DCCP, and SCTP
Assignee	IESG
Contact	IETF Chair
Description	RFC[TBD-rfc]-style Experiment
Reference	RFC [TBD-rfc]
Port Number	#UPORT1 (requesting 1031)
Service Code	none - use private use service codes
Known Unauthorized Uses	none
Assignment Notes	Intended for use with PExIDs only

And:

Service Name	USR-EXP2
Transport Protocol(s)	TCP, UDP, DCCP, and SCTP
Assignee	IESG
Contact	IETF Chair
Description	RFC[TBD-rfc]-style Experiment
Reference	RFC [TBD-rfc]
Port Number	#UPORT2 (requesting 1032)

Service Code	none - use private use service codes
Known Unauthorized Uses	none
Assignment Notes	Intended for use with PExIDs only

IANA has assigned the following SCTP Payload Protocol Identifier (PPID) for experiments associated with these port numbers:

SCTP PPID #PPID1

This document directs IANA to create a "Port Experimental Option Experiment Identifiers (PExIDs)" registry linked under the IANA ports registry [SP-reg], using the same format and structure as the TCP option ID registry [TCP-reg]. The registry records PExIDs as 32-bit unsigned integers, including a brief description, document pointer if available, assignee name, and e-mail contact for each entry. Once registered, PExIDs can be used with either the system (EXP1, EXP2) or user (USR-EXP1, USR-EXP2) ports and with any transport protocol. This registry has no initial entries.

Entries are assigned on a First Come, First Served (FCFS) basis [RFC8126]. IANA will also record known duplicate uses to assist the community in both debugging assigned uses as well as correcting unauthorized duplicate uses.

IANA should impose no requirements on making a registration request other than indicating the desired codepoint and providing a point of contact. A short description or acronym for the use is desired but not required.

9. References

9.1. Normative References

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

[RFC4727] Fenner, B., "Experimental Values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers," RFC 4727, Nov. 2026.

[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, Aug. 2011.

[RFC6994] Touch, J., "Shared Use of Experimental TCP Options," RFC 6994, Aug. 2013.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, June 2017.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

9.2. Informative References

[RFC768] Postel, J., "User Datagram Protocol," STD 6, RFC 768, Aug. 1980.

[RFC791] Postel, J., "Internet Protocol," STD 5, RFC 791, Sep. 1981.

[RFC792] Postel, J., "Internet Control Message Protocol," STD 5, RFC 792, Sep. 1981.

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

[RFC4443] Conta, A., Deering, S., and M. Gupta, (Ed.), "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," STD 89, RFC 4443, Mar. 2006.

[RFC5595] Fairhurst, G., "The Datagram Congestion Control Protocol (DCCP) Service Codes", RFC 5595, September 2009.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

[RFC7605] Touch, J., "Recommendations on Using Assigned Transport Port Numbers," BCP 165, RFC 7605, Aug. 2015.

[RFC7665] Halpern, J., Ed., and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, October 2015.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," STD 86, RFC 8200, Jul. 2017.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol VerREsion 1.3", RFC 8446, Aug. 2018.

[RFC8489] Petit-Huguenin, M., Salgueiro, G., Rosenberg, J., Wing, D., Mahy, R., and P. Matthews, "Session Traversal Utilities for NAT (STUN)", RFC 8489, February 2020.

[RFC8656] Reddy, T., Ed., Johnston, A., Ed., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 8656, February 2020,

[RFC9000] Iyengar, J., Ed., and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, May 2021.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, April 2022.

[RFC9260] Stewart, R. (Ed.), "Stream Control Transmission Protocol," RFC 9260, Sep. 2007.

[RFC9293] Eddy, W. (Ed.), "Transmission Control Protocol (TCP), Aug. STD 7, RFC 9293, 2022.

[SP-reg] Service Name and Transport Protocol Port Number Registry, https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[TCP-reg] TCP Option ID registry, https://www.iana.org/assignments/tcp-parameters/tcp-parameters.xhtml#tcp-exids

[TH25] Touch, J, C. Heard (Ed.), "Transport Options for UDP", draft-ietf-tsvwg-udp-options, Mar. 2025.

10. Acknowledgments

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

Authors' Addresses

Joe Touch
Manhattan Beach, CA 90266 USA
Phone: +1 (310) 560-0334
Email: touch@strayalpha.com