Network Working Group   G. Mirsky
Internet-Draft   ZTE Corp.
Updates: 5357 (if approved)   M. Perumal
Intended status: Standards Track   Ericsson
Expires: December 2, 2017   R. Foote
                                                            Nokia
                                                 L. M. Contreras
                                                       Telefonica
                                                         L. Jalil
                                                          Verizon
                                                     May 31, 2017

        UDP Port Allocation for the Receiver Port in Two-Way Active Measurement
                              Protocol (TWAMP)
                draft-mirsky-ippm-twamp-refl-registered-port-03

Abstract

   This document arguments and requests re-allocation of an UDP port
   number from the System Ports range for a Reflector in Two-Way Active
   Measurement Protocol (TWAMP). This document, if accepted, will be an
   update to the TWAMP Test protocol specified in RFC 5357.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

One particular compelling vision of the Two-Way Active Measurement
Protocol (TWAMP) [RFC5357] is widespread deployment of open servers
that would make IP Performance Metrics (IPPM) measurements a
commonplace. This is complemented by the proliferation of the
Internet of Things (IoT) devices, such as sensors, and the need for
obtaining IPPM measurements from those devices by the service
provider. IoT devices are often constrained by limited processing
power and memory and benefit from TWAMP Light, as defined in
Appendix I [RFC5357].

TWAMP Light provides a simple solution for devices to act as test
points in the network, by avoiding the need for the TWAMP-Control
protocol [RFC5357]. In the absence of TWAMP-Control, a registered
(default) UDP port that can be used as the Receiver Port for TWAMP-
Test will simplify configuration and management of the TWAMP-Light
test sessions.

This document requests re-allocation of the UDP port number from the
System Ports range [RFC6335] as Receiver Port for TWAMP-Test.

2. Requirements Language

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
[RFC2119].

3. **Impact to TWAMP-Control Protocol**

   Section 3.5 [RFC5357] describes in details the process of negotiating
   value of the Receiver Port. The Control-Client, acting on behalf of
   the Session-Sender, proposes the port number from the Dynamic Port
   range [RFC6335]:

      "The Receiver Port is the desired UDP port to which TWAMP-Test
      packets will be sent by the Session-Sender (the port where the
      Session-Reflector is asked to receive test packets). The Receiver
      Port is also the UDP port from which TWAMP-Test packets will be
      sent by the Session-Reflector (the Session-Reflector will use the
      same UDP port to send and receive packets)."

   But the proposed Receiver Port may be not available, e.g. being in
   use by other test session or another application. In this case:

      "... the Server at the Session-Reflector MAY suggest an alternate
      and available port for this session in the Port field. The
      Session- Sender either accepts the alternate port, or composes a
      new Session- Request message with suitable parameters. Otherwise,
      the Server uses the Accept field to convey other forms of session
      rejection or failure to the Control Client and MUST NOT suggest an
      alternate port; in this case, the Port field MUST be set to zero."

   The allocated TWAMP Receiver Port number Section 5 MAY be advertised
   by the Server. The Control Client that supports use of the allocated
   TWAMP Receiver Port MUST accept the port number advertised by the
   Server. If the Server does not support the allocated TWAMP Receiver
   Port, then it sends another Session-Request message with new
   parameters. Thus the deployment of the allocated TWAMP Receiver Port
   number is backward compatible with existing TWAMP-Control solutions
   that are based on [RFC5357]. At the same time, use of the UDP port
   number allocated from the User Port range [RFC6335] will help to
   avoid the situation when the Server finds the proposed port being
   already in use.

4. **Impact to TWAMP-Test Protocol**

   TWAMP-Test may be used to measure IP performance metrics in an Equal
   Cost Multipath (ECMP) environment. Though algorithms to balance IP
   flows among available paths had not been standardized, the most
   common is the Five-tuple that uses destination IP address, source IP
   address, protocol type, destination port number, and source port
   number. To attempt to monitor different paths in ECMP network is
   sufficient to variate only one of five parameters, e.g. the source
   port number. Thus, there will be no negative impact on ability to
   have concurrent TWAMP test sessions between the same test points to

monitor different paths in the ECMP network when using the allocated UDP port number as the Receiver Port.

The allocation of the TWAMP Receiver Port from the User Port Range [RFC6335] benefits TWAMP Light mode of the TWAMP-Test. The allocated UDP port number Section 5 may be used as default value for the Receiver Port to simplify configuration and management of the TWAMP-Light test sessions.

5. IANA Considerations

The Service Name and Transport Protocol Port Number Registry defined in [RFC6335].

[RFC5357] has been allocated UDP port 862 for TWAMP-Control protocol. IANA is requested to re-assign UDP port 862 as follows:

Servic e Name	Port Numb er	Trans port Proto col	Description	Semantics Definition	Referenc e
twamp- test	862	UDP	TWAMP-Test Receiver Port	Section 4	This document

Table 1: TWAMP Receiver Port

6. Security Considerations

The registered UDP port as the Receiver Port for TWAMP-Test may be used as target of denial-of-service (DoS) or used by man-in-the-middle (MitM) attack. To improve protection from the DoS following methods are recommended:

o filtering access to the TWAMP Receiver Port by access list;

o non-routable IPs outside of the domain for the TWAMP loopback.

MitM attack may try to modify the content of the TWAMP-Test packet thus altering measurement results. An implementation can use data consistency check to detect modification of data. In addition, it can use encryption of TWAMP-Test packets to prevent eavesdropping.

7. **Acknowledgments**

   TBD

8. **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>.

   [RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J.
              Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)",
              RFC 5357, DOI 10.17487/RFC5357, October 2008,
              <http://www.rfc-editor.org/info/rfc5357>.

   [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>.

Authors' Addresses

   Greg Mirsky
   ZTE Corp.

   Email: gregimirsky@gmail.com

   Muthu Arul Mozhi Perumal
   Ericsson
   Ferns Icon
   Doddanekundi, Mahadevapura
   Bangalore, Karnataka 560037
   India

   Email: p.muthu.arul.mozhi@ericsson.com

   Richard Foote
   Nokia

   Email: footer.foote@nokia.com

Luis M. Contreras
Telefonica

Email: luismiguel.contrerasmurillo@telefonica.com

Luay Jalil
Verizon

Email: luay.jalil@verizon.com