UDP Traceroute Message Extension
draft-shen-udp-traceroute-ext-01

Abstract

This document specifies an extension to UDP traceroute messages that allows the UDP traceroute probe packets to be authenticated by the intermediate nodes and the destination node. This extension can also include requests for node specific information that the sender is interested to receive from one or more nodes via the traceroute replies.
Table of Contents

1. Specification of Requirements .......................... 3
2. Introduction ............................................. 3
3. UDP Traceroute Message Extension ....................... 4
   3.1. Original Length Field .............................. 4
   3.2. UDP Traceroute Structure .......................... 4
   3.2.1. Traceroute Common Header ....................... 4
   3.2.2. Traceroute TLV .................................. 5
       3.2.2.1. Traceroute Authentication TLV .......... 6
       3.2.2.2. Traceroute Information-Request TLV .... 7
4. Implementation and Operation Considerations .......... 8
   4.1. Traceroute Probe Sender ........................... 8
   4.2. Traceroute Probe Receiver .......................... 8
5. Security Considerations ................................ 9
6. IANA Considerations .................................... 9
7. Acknowledgements ....................................... 9
8. Normative References .................................. 10

Authors’ Addresses ....................................... 10
Intellectual Property and Copyright Statements ............ 12
1. Specification of Requirements

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 [RFC2119].

2. Introduction

Traceroute is a tool widely used in the diagnosis of network problems. Majority of the traceroute tools are implemented by sending out UDP [RFC0768] probe messages and receiving ICMP messages.

Internet Control Message Protocol (ICMP/ICMPv6) [RFC0792] [RFC4443] has been extended to support multi-part message inside ICMP [RFC4884]. Some of the applications [I-D.atlas-icmp-unnumbered] [RFC4950] [I-D.shen-icmp-routing-inst] are designed mainly for internal network troubleshooting by network operators. Network providers may want to limit those applications only to trusted senders of traceroute probes due to security or policy reasons.

Although one may employ a rudimentary control mechanism to limit the trusted senders by defining access control lists specifying IPv4/IPv6 source addresses of the UDP traceroute message, such mechanism is deemed configuration intensive, static, and error-prone. Moreover, such mechanism would be susceptible to address spoofing. Additionally, such mechanism does not provide the sender with dynamic control of the different kind of extensions to be requested.

This document defines an extension for UDP traceroute messages to optionally include authentication signature. The intermediate and destination nodes can authenticate the sender of the traceroute packet before providing the requested information in the traceroute response.

This document also includes an Information-Request TLV for the traceroute extension. This TLV specifies the types of information the sender expects to be included in the traceroute response (i.e., in the ICMP message elicited by the UDP packet and generated by the intermediate or destination node or nodes).

This extension is backwards compatible with the existing Internet traceroute mechanism, and it is applied to both IPv4 and IPv6 networks.

This extension is applicable to only the UDP type of traceroute probe, similar scheme might be used with other types of traceroute probe and it is outside the scope of this document.
3. UDP Traceroute Message Extension

This proposed extension is to reserve the lowest 4 bits in the UDP source port field, and a traceroute structure within UDP data field.

3.1. Original Length Field

This "original length" field is defined as the lowest nibble of the UDP source port field, and specifies the position at which the traceroute data structure begins. The value represents 32-bit words ranges from 0x0 to 0xF, with value 0xF as reserved. Thus the position of the traceroute data structure can start from 0 to 56 octets inside UDP data field. The "original length" field value 0xF indicates there is no traceroute data structure inside the UDP data field.

The "original length" field is defined within UDP "source port" as the following:

```
    +--------+-+-++-
    |        |Ori-Len|
    +--------+-+-++-

Ori-Len: 4 bits. The value (Ori-Len) represents the traceroute data structure start position in 32-bit words. The Ori-Len value 0xF is reserved.
```

3.2. UDP Traceroute Structure

The UDP traceroute structure starts in UDP data field location from 0 to 56 octets specified in the "original length" in 32-bit boundary. It MUST have exactly one traceroute common header followed by one or more UDP traceroute TLVs.

3.2.1. Traceroute Common Header

The Common Header is a 8 octets structure has the following format:
The fields of the Common Header are defined as follows:

Version: 4 bits. It is defined as 1 in this document.

Length: 12 bits. The total length of the traceroute data structure specifying number of 32-bit words (includes the common header and all the TLVs).

Checksum: 16 bits. The one’s complement of the one’s complement sum of the traceroute data structure, with the checksum field replaced by zero for the purpose of computing the checksum.

Magic Number: 32 bits. It is defined as Hex value of 0x54726163 in this document. This is used mainly for structure identification of this extension version.

3.2.2. Traceroute TLV

Traceroute TLVs (Type-Length-Value tuples) have the following format:

Type: 16 bits.

Length: 16 bits. length of the Value field in octets.
Value: depends on the Type. It is zero padded to align to a 4-octet boundary.

This document defines two TLVs below.

3.2.2.1. Traceroute Authentication TLV

This TLV carries the HMAC authentication related information. It verifies both the data integrity and the authenticity of the entire message. This TLV has the following format:

```
  0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 1 (Authentication)   |       Length (variable)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Auth Type                 |    Key ID     | Auth Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                     Auth Data (Variable)                      |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Auth Type: 16 bits. The following values are proposed:

* Type=0 signifies no authentication

* Type=1 signifies simple password based authentication.

* Type=2 signifies Cryptographic authentication.

Please note that the above type values are in line with IANA allocated values for other protocols (e.g., OSPF).

Key ID: 8 bits. This allows multiple secret keys to be active simultaneously. Using Key IDs makes the key rollover convenient. Each secret key must be associated with the hash algorithm. This may be done through provisioning on each node.

Auth Data Len: 8 bits. This specifies the length of the authentication data (and allows for the support of current and future authentication schemes).
Auth Data: Variable length. This field carries the result (e.g., HMAC code) of the HMAC algorithm applied over the entire traceroute IP/IPv6 packet. When the Auth data is calculated, the shared key is stored in this field, and the checksum fields in the IP header, UDP header and traceroute common header are set to zero. The result of the algorithm is placed in the Auth Key field. The following lists algorithms that could be commonly supported:

* HMAC-MD5
* HMAC-SHA1
* HMAC-SHA2 variants (e.g., 224, 256, 384, 512, etc.)

At least HMAC-MD5 and HMAC-SHA1 algorithms should be supported on all the nodes compliant with this specification.

3.2.2.2. Traceroute Information-Request TLV

The Information-Request TLV has the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type = 2 (Info-Req)       |          Length = 4           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Info Request                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Info-Req: 32 bits. This bitflag field lists the request items the traceroute sender is interested. The bit number ranges from the right most bit to the left most bit. Currently defined as the following:
Bit Number Information Item
0  MPLS label related attributes
1  Interface related attributes
2  IP/IPv6 address related attributes
3  Routing Instance related attributes

4. Implementation and Operation Considerations

There is no change in this extension for the normal traceroute implementation and operation except for reserving the lowest 4 bits in the UDP source port field. The implementations for the sender can use the same semantics with the UDP source port; and it makes no difference to the receivers if they don’t support this extension.

4.1. Traceroute Probe Sender

The sender supports this extension MAY include the Traceroute structure in it’s UDP probe to specify the request types and authentication key. The sender SHOULD set the "original length" value to 0xF if there is no Traceroute structure present inside the UDP probe. The sender MAY request one or multiple types of information defined in the traceroute "Info-Req" TLV.

4.2. Traceroute Probe Receiver

When the traceroute probe receiver, the intermediate and destination node, processes the UDP probe, it MAY check the UDP Traceroute structure to verify if the sender is from an authenticated host and to see what types of information it requested. This check is only needed when the receiver tries to authenticate the UDP probe sender, or when the receiver is formatting the ICMP and ICMPv6s that support multi-part messages and it has certain internal information that can be included in the ICMP packets.

If the "original length" value is not 0xF, UDP traceroute structure may be present. The receiver MUST verify the integrity of the data structure by examining the "version" field, the Magic-Number value, and the length of the structure. It MUST perform the checksum to verify the data structure. If the authentication TLV is present and the local policy requires it to perform the verification, the receiver MUST use it’s locally stored shared key to validate the checksum in the TLV. Multiple Authentication Keys can be used which can be useful in the case the UDP probes are from trusted peer networks.

If the "Info-Req" TLV is included, the receiver SHOULD fetch the related information when formating the ICMP packets, but MUST NOT
include information that has the corresponding bitflag cleared.

5. Security Considerations

This extension enhances the security of traceroute operation in a backwards-compatible fashion. The mechanism allows the receiver to verify the sender of the UDP traceroute packet such that certain sensitive interface and network related information can be supplied in the internal network or across trusted networks.

The use of Cryptographic authentication (i.e., an Auth Type value of 2) allows for a strong authentication mechanism since the keys cannot be discerned by intercepting the packets. The proposed Keyed authentication does not prevent replay attacks. However, in the case of replay attacks, since the packet source IP/IPv6 address of the traceroute probe can not be changed, there is no easy way for the attacker to retrieve the ICMP messages.

A router needs to protect against purposefully-bogus UDP Traceroute packets with extensions that fail the authentication, as a high rate of messages can require significant processing time. [RFC1812] specifies how rate-limiting is applied to the generation of ICMP messages, and this rate-limiting deterrs the threat when applied before checking the Authentication. Additionally, when using Cryptographic authentication, the HMAC includes the source IP address, which means the HMAC will not validate if the UDP packet is sent over a NAT.

6. IANA Considerations

The UDP Traceroute Extension contains traceroute TLVs. IANA should establish a registry of UDP Traceroute Extension Types. This document defines Type 1 and Type 2 for authentication and information-request. Types 3-0xF6 are allocated through Expert Review [RFC5226]. Types 0xF7 to 0xFF are reserved for private use.

IANA should also establish a registry for UDP Traceroute Info-Request Bits. This document defines bits 0 - 3 in section 3.2.2.2. Bits 4-29 are allocated through Expert Review. Bits 30 - 31 are reserved for private use.

7. Acknowledgements

Many thanks to Dan Wing, for his insightful comments and valuable suggestions regarding this document.
8. Normative References

[I-D.atlas-icmp-unnumbered]

[I-D.shen-icmp-routing-inst]


Authors’ Addresses

Naiming Shen
Cisco Systems, Inc.
225 West Tasman Drive
San Jose, CA  95134
USA

Email: naiming@cisco.com

Carlos Pignataro
Cisco Systems, Inc.
7200 Kit Creek Road
Research Triangle Park, NC  27709
USA

Email: cpignata@cisco.com

Rajiv Asati
Cisco Systems, Inc.
7025 Kit Creek Road
Research Triangle Park, NC  27709
USA

Email: rajiva@cisco.com

Enke Chen
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA  95134
USA

Email: enkechen@cisco.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.