Traceroute and Ping Message Extension
draft-shen-traceroute-ping-ext-00

Abstract

This document specifies an extension to traceroute and ping messages that allows the 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 probe sender is interested to receive from one or more nodes via the traceroute and ping replies. This extension supports UDP, TCP and ICMP types of traceroute and ping probes.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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 March 26, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document.
publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Specification of Requirements .................................. 3
2. Introduction ....................................................... 3
3. Motivation ......................................................... 3
4. Probe Message Extension ........................................... 4
   4.1. Probe Structure ............................................... 4
       4.1.1. Probe Common Header .................................... 4
       4.1.2. Probe TLV ............................................... 5
           4.1.2.1. Probe Authentication TLV ........................... 5
           4.1.2.2. Probe Information-Request TLV ..................... 7
   4.2. Probe Extension Offset Field ................................. 7
       4.2.1. UDP Messages ............................................. 8
       4.2.2. TCP Messages ............................................ 8
       4.2.3. ICMP Messages .......................................... 8
       4.2.4. Implementation Discussion .............................. 8
5. Implementation and Operation Considerations ....................... 9
   5.1. Traceroute and Ping Probe Sender ............................. 9
   5.2. Traceroute and Ping Probe Receiver ............................ 9
6. Security Considerations ........................................... 10
7. IANA Considerations .............................................. 10
8. Acknowledgements ................................................. 10
9. References ........................................................ 11
   9.1. Normative References ....................................... 11
   9.2. Informative References .................................... 11

Authors’ Addresses .................................................. 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 and Ping are tools widely used in the diagnosis of network problems. This document proposes the mechanism in which the source probe packets can be authenticated by the intermediate and the destination nodes. It also specifies the mechanism for specific information in the traceoute and ping replies the source is interested to get. This mechanism gives operators more secure ways of performing network management and troubleshooting tasks. It applies to both IPv4 and IPv6 networks.

This document applies to most type of traceroute and ping probe packets including UDP [RFC0768], TCP [RFC0793] and ICMP/ICMPv6 [RFC0792] [RFC4443] types. The ICMP/ICMPv6 reply messages responding to those probes are not part of this specification.

This document defines an extension for traceroute and ping probe messages to optionally include authentication signature. The intermediate and destination nodes can authenticate the sender of the traceroute or ping packet before providing the requested information in the ICMP response. This document also includes an Information-Request TLV for the traceroute/ping extension. This TLV specifies the types of information the sender expects to be included in the traceroute/ping response (i.e., in the ICMP message elicited by the traceroute/ping packet and generated by the intermediate or destination node or nodes).

This specification is evolved from the UDP Traceroute Extension document [I-D.shen-udp-traceroute-ext].

3. Motivation

Although one may employ a rudimentary control mechanism to limit the trusted senders by defining on every router the access control lists specifying source addresses of the traceroute and ping 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.
The ICMP reply messages has been extended to support multi-part message inside ICMP [RFC4884]. Some of the applications [RFC5837] [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/ping probes due to security or policy reasons by using this mechanism described in this document.

4. Probe Message Extension

This proposed extension is to define a probe data structure which resides within UDP/TCP/ICMP data field; and to reserve the lowest 4 bits inside a 16-bit field within UDP/TCP/ICMP headers to indicate the extension structure offset location.

In most of the traceroute implementation, there is some private data in probe messages used by traceroute applications. With this "extension offset" defined, the applications can continue to use those private data while supporting this probe extension in a deterministic way. This extension applies to both traceroute and ping applications.

4.1. Probe Structure

The probe structure starts in UDP/TCP/ICMP data field location from 0 to 56 octets specified in the "extension offset", see Section 4.2, in 32-bit boundary. It MUST have exactly one probe common header followed by zero or more probe TLVs.

4.1.1. Probe Common Header

The Common Header is a 8 octets structure has the following format:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Version |        Length         |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Magic-Number (0x54726163)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 probe 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 probe 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.

4.1.2. Probe TLV

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

```
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------+
|                      Type                     |    Length     |
|-----------------------------------------------|
+-----------------------------------------------+
|                                             |      Value    |
|                                             |                |
|                                             |                |
+-----------------------------------------------+
```

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.

4.1.2.1. Probe 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 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/ping 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/TCP/ICMP header and probe 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.

4.1.2.2. Probe Information-Request TLV

The Information-Request TLV has the following format:

```
  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 probe sender is interested. The bit number ranges from the right most bit to the left most bit. Currently defined as the following:

<table>
<thead>
<tr>
<th>Bit Number</th>
<th>Information Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>MPLS label related attributes</td>
</tr>
<tr>
<td>1</td>
<td>Interface related attributes</td>
</tr>
<tr>
<td>2</td>
<td>IP/IPv6 address related attributes</td>
</tr>
<tr>
<td>3</td>
<td>Routing Instance related attributes</td>
</tr>
<tr>
<td>4</td>
<td>Nexthop(s) related attributes</td>
</tr>
<tr>
<td>5</td>
<td>Device role related attributes</td>
</tr>
</tbody>
</table>

4.2. Probe Extension Offset Field

This probe "extension offset" field is defined as the lowest nibble within a 16-bit field, and it specifies the position at which the probe extension data structure begins. The value represents 32-bit words ranges from 0x0 to 0xF, with value 0xF as reserved. Thus the position of the probe data structure can start from 0 to 56 octets inside TCP, UDP or ICMP data field. The probe "extension offset" field value 0xF indicates there is no probe data structure inside the message data field.

The probe "extension offset" field is defined as the following:
Ext-Off: 4 bits. The value (Ext-Off) represents the probe data structure start position in 32-bit words. The Ext-Off value 0xF is reserved.

The rest of the 12 bits out of this 16-bit field is not changed by this proposal. For application usage detail in terms of different traceroute/ping probe types, see Section 4.2.4.

4.2.1. UDP Messages

In the UDP traceroute/ping probe case, this 16-bit field is the UDP source port field in UDP header [RFC0768]. The "Ext-Off" specifies the probe extension structure start location inside UDP data field.

4.2.2. TCP Messages

In the TCP traceroute/ping probe case, this 16-bit field is the TCP source port field in TCP header [RFC0793]. The "Ext-Off" specifies the probe extension structure start location inside TCP data field.

4.2.3. ICMP Messages

In the ICMP traceroute/ping probe case, this 16-bit field is the "Identifier" field of ICMP type 8 structure [RFC0792]. The "Ext-Off" specifies the probe extension structure start location inside ICMP data field of the type 8 (ICMP echo request) message.

4.2.4. Implementation Discussion

In the majority of today’s traceroute implementations, the application process identifier (process-ID) is used as the UDP source port for UDP type of traceroute probe; in TCP implementation, the process-ID is used as the TCP source port for traceroute probe; and the process-ID is also used as the ICMP Identifier of ICMP type 8 message. With this extension, an implementation can use the highest 12-bits of the source port field for UDP/TCP header and ID field for ICMP type 8 message to encode this process information since the lowest 4-bits are now reserved for the probe "extension offset".

Ping implementation is similar to traceroute, it either uses the process-ID or an internally generated number inside the ICMP echo request ID field and in UDP/TCP source port field. An implementation
now can use the highest 12-bits of the field and leave the lowest 4-bits for the probe extension.

5. Implementation and Operation Considerations

There is no change in this extension for the normal traceroute/ping implementation and operation except for reserving the lowest 4 bits in the UDP/TCP source port field and ICMP Id field of type 8 message. The implementations for the sender can use the same semantics with this 16-bit field; and it makes no difference to the receivers if they don’t support this extension.

5.1. Traceroute and Ping Probe Sender

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

5.2. Traceroute and Ping Probe Receiver

When the traceroute/ping probe receiver, the intermediate and destination node, processes the incoming probe, it MAY check the Probe 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 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 probe "extension offset" value is not 0xF, the probe 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 probe structure. It MUST perform the checksum to verify the probe 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 probes are from trusted peer networks.

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

Even if the authentication fails, the receiver MAY still send the
regular ICMP echo reply back to the sender, without the requested or internal information, as if this probe extension is not supported.

6. Security Considerations

This extension enhances the security of traceroute and ping operation in a backwards-compatible fashion. The mechanism allows the receiver to verify the sender of the traceroute/ping 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/ping 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 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 deters 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 traceroute/ping packet is sent over a NAT.

7. IANA Considerations

The Probe Extension contains probe TLVs. IANA should establish a registry of Probe 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 Probe Info-Request Bits. This document defines bits 0 - 5 in Section 4.1.2.2. Bits 6-29 are allocated through Expert Review. Bits 30 - 31 are reserved for private use.

8. Acknowledgements

Many thanks to Dan Wing and Tony Li, for their insightful comments
9. References

9.1. Normative References


9.2. Informative References


[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an


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
Alia K. Atlas
BT

Email: alia.atlas@bt.com