On-demand Continuity Check (CC) and Connectivity Verification (CV) for Overlay Networks
draft-ooamdt-rtgwg-demand-cc-cv-01

Abstract

This document defines Overlay Echo Request and Echo Reply that enable on-demand Continuity Check, Connectivity Verification among other operations in overlay networks.

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 April 27, 2017.
1. Introduction

Operations, Administration, and Maintenance (OAM) toolset provides methods for fault management and performance monitoring in each layer of the network, in order to improve their ability to support services with guaranteed and strict Service Level Agreements (SLAs) while reducing operational costs.
1.1. Conventions used in this document

1.1.1. Terminology

Term "Overlay OAM" used in this document interchangeably with longer version "set of OAM protocols, methods and tools for Overlay networks". And "Overlay ping" is used interchangeably with longer version Overlay Echo Request/Reply.

CC Continuity Check

CV Connectivity Verification

FM Fault Management

Geneve Generic Network Virtualization Encapsulation

GUE Generic UDP Encapsulation

MPLS Multiprotocol Label Switching

NVO3 Network Virtualization Overlays

OAM Operations, Administration, and Maintenance

SFC Service Function Chaining

SFP Service Function Path

VXLAN Virtual eXtensible Local Area Network

VXLAN-GPE Generic Protocol Extension for VXLAN

1.1.2. 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].

2. On-demand Continuity Check and Connectivity Verification

The format of the Echo Request/Echo Reply control packet is to support ping and traceroute functionality in overlay networks

Figure 1 resembles the format of MPLS LSP Ping [RFC4379] with some exceptions.
The interpretation of the fields is as following:

The Version reflects the current version. The version number is to be incremented whenever a change is made that affects the ability of an implementation to correctly parse or process control packet.

The Global Flags is a bit vector field.

The Message Type filed reflects the type of the packet. Value TBA2 identifies Echo Request and TBA3 - Echo Reply.

The Reply Mode defines the type of the return path requested by the sender of the Echo Request.

Return Codes and Subcodes can be used to inform the sender about result of processing its request.

The Sender’s Handle is filled in by the sender, and returned unchanged by the receiver in the Echo Reply.

The Sequence Number is assigned by the sender and can be (for example) used to detect missed replies.

TLVs (Type-Length-Value tuples) have the two octets long Type field, two octets long Length field that is length of the Value field in octets.
2.1. Overlay Echo Request Transmission

Overlay Echo Request control packet MUST use the appropriate encapsulation of the monitored overlay network. Overlay network encapsulation MUST identify Echo Request as OAM packet. Overlay encapsulation uses different methods to identify OAM payload [I-D.ietf-nvo3-vxlan-gpe], [I-D.ietf-nvo3-gue], [I-D.ietf-nvo3-geneve], [I-D.ietf-sfc-nsh],[I-D.ietf-bier-mpls-encapsulation]. Overlay network’s header MUST be immediately followed by the Overlay OAM Header [I-D.oamdt-rtgwg-ooam-header]. Message Type field in the Overlay OAM Header MUST be set to Overlay Echo Request value (TBA2).

Value of the Reply Mode field MAY be set to:

- Do Not Reply (TBA4) if one-way monitoring is desired. If Echo Request is used to measure synthetic packet loss, the receiver MAY report loss measurement results to a remote node.
- Reply via an IPv4/IPv6 UDP Packet (TBA5) value likely will be the most used.
- Reply via Application Level Control Channel (TBA6) value if the overlay network MAY have bi-directional paths.
- Reply via Specified Path (TBA7) value in order to enforce use of the particular return path specified in the included TLV to verify bi-directional continuity and also increase robustness of the monitoring by selecting more stable path.

2.2. Overlay Echo Request Reception

2.3. Overlay Echo Reply Transmission

The Reply Mode field directs whether and how the Echo Reply message should be sent. The sender of the Echo Request MAY use TLVs to request that corresponding Echo Reply be sent using the specified path. Value TBA3 is referred as "Do not reply" mode and suppresses transmission of Echo Reply packet. Default value (TBA5) for the Reply mode field requests the responder to send the Echo Reply packet out-of-band as IPv4 or IPv6 UDP packet. [Selection of destination and source IP addresses and UDP port numbers to be provided in the next update.]
2.4. Overlay Echo Reply Reception

3.  IANA Considerations

3.1. Overlay Echo Request/Echo Reply Type

IANA is requested to assign new type from the Overlay OAM Protocol Types registry as follows:

```
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBA1</td>
<td>Overlay Echo Request/Echo Reply</td>
<td>This document</td>
</tr>
</tbody>
</table>
```

Table 1: Overlay Echo Request/Echo Reply Type

3.2. Overlay Ping Parameters

IANA is requested to create new Overlay Echo Request/Echo Reply Parameters registry.

3.3. Overlay Echo Request/Echo Reply Message Types

IANA is requested to create in the Overlay Echo Request/Echo Reply Parameters registry the new sub-registry Message Types. All code points in the range 1 through 191 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC5226] and assign values as follows:

```
<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>TBA2</td>
<td>Overlay Echo Request</td>
<td>This document</td>
</tr>
<tr>
<td>TBA3</td>
<td>Overlay Echo Reply</td>
<td>This document</td>
</tr>
<tr>
<td>TBA3+1-191</td>
<td>Unassigned</td>
<td>IETF Review</td>
</tr>
<tr>
<td>192-251</td>
<td>Unassigned</td>
<td>First Come First Served</td>
</tr>
<tr>
<td>252-254</td>
<td>Unassigned</td>
<td>Private Use</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>
```

Table 2: Overlay Echo Request/Echo Reply Message Types
3.4. Overlay Echo Reply Modes

IANA is requested to create in the Overlay Echo Request/Echo Reply Parameters registry the new sub-registry Reply Modes All code points in the range 1 through 191 in this registry shall be allocated according to the "IETF Review" procedure as specified in [RFC5226] and assign values as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td>This document</td>
</tr>
<tr>
<td>TBA4</td>
<td>Do Not Reply</td>
<td>This document</td>
</tr>
<tr>
<td>TBA5</td>
<td>Reply via an IPv4/IPv6 UDP Packet</td>
<td>This document</td>
</tr>
<tr>
<td>TBA6</td>
<td>Reply via Application Level Control Channel</td>
<td>This document</td>
</tr>
<tr>
<td>TBA7</td>
<td>Reply via Specified Path</td>
<td>This document</td>
</tr>
<tr>
<td>TBA7+1-191</td>
<td>Unassigned</td>
<td>IETF Review</td>
</tr>
<tr>
<td>192-251</td>
<td>Unassigned</td>
<td>First Come First Served</td>
</tr>
<tr>
<td>252-254</td>
<td>Unassigned</td>
<td>Private Use</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Overlay Echo Reply Modes

4. Security Considerations

Overlay EchoRequest/Replay operates within the domain of the overlay network and thus inherits any security considerations that apply to the use of that overlay technology and, consequently, underlay data plane. Also, the security needs for Overlay Echo Request/Reply are similar to those of ICMP ping [RFC0792], [RFC4443] and MPLS LSP ping [I-D.ietf-mpls-rfc4379bis].

There are at least three approaches of attacking a node in the overlay network using the mechanisms defined in the document. One is a Denial-of-Service attack, by sending Overlay ping to overload a node in the overlay network. The second may use spoofing, hijacking, replaying, or otherwise tampering with Overlay Echo Requests and/or Replies to misrepresent, alter operator’s view of the state of the overlay network. The third is an unauthorized source using an Overlay Echo Request/Reply to obtain information about the overlay and/or underlay network.
To mitigate potential Denial-of-Service attacks, it is RECOMMENDED that implementations throttle the Overlay ping traffic going to the control plane.

Replay and spoofing attacks involving faking or replaying Overlay Echo Reply messages would have to match the Sender’s Handle and Sequence Number of an outstanding Overlay Echo Request message which is highly unlikely. Thus the non-matching replay would be discarded. But since “even a broken clock is right twice a day” implementations MAY use Timestamp control block [I-D.ooamdt-rtgwg-ooam-header] to validate the TimeStamp Sent by requiring an exact match on this field.

To protect against unauthorized sources trying to obtain information about the overlay and/or underlay an implementation MAY check that the source of the Echo Request is indeed part of the overlay domain.

5. Acknowledgement

TBD

6. References

6.1. Normative References

[I-D.ietf-bier-mpls-encapsulation]

[I-D.ietf-nvo3-geneve]

[I-D.ietf-nvo3-gue]

[I-D.ietf-nvo3-vxlan-gpe]
6.2. Informative References

[I-D.ietf-mpls-rfc4379bis]


Authors’ Addresses

Greg Mirsky

Email: gregimirsky@gmail.com