Structured Specifications in IETF Documents

Stephen McQuistin
Colin Perkins

HotRFC @ IETF 103
ASCII packet diagrams are useful

TCP Header Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Source Port | Destination Port |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Sequence Number |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Acknowledgment Number |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Data | U|A|P|R|S|F|
| Offset| Reserved |R|C|S|S|Y|I| Window |
| | | G|K|H|T|N|N |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Checksum | Urgent Pointer |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| Options | Padding |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
| data |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-

Note that one tick mark represents one bit position.

Figure 3.

Source Port: 16 bits
The source port number.

Destination Port: 16 bits
The destination port number.
ASCII packet diagrams are useful

Note that one tick mark represents one bit position.

TCP Header Format

Source Port: 16 bits
The source port number.

Destination Port: 16 bits
The destination port number.
4.2. Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be used by either 1) a DHCPv6 relay agent that uses a non-DHCP UDP port (not 547) communicating with the IPv6 server and the upstream relay agent or 2) an IPv6 relay agent that detects the use of a non-DHCP UDP port (not 547) by a downstream relay agent.

The format of the "Relay Source Port Option" is shown below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Option-Code: OPTIONS_RELAY_PORT | Option-Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Downstream Source Port |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where:

- Option-Code: OPTION_RELAY_PORT. 16-bit value, 135.
- Option-Length: 16-bit value to be set to 2.
- Downstream Source Port: 16-bit value. To be set by the IPv6 relay either to the downstream relay agent's UDP source port used for the UDP packet, or to zero if only the local relay agent uses the non-DHCP UDP port (not 547).

Note that one tick mark represents one bit position.

Figure 3.

Source Port: 16 bits
The source port number.

Destination Port: 16 bits
The destination port number.
4.2. Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be
inserted into an option by either 1) a DHCPv6 relay agent that uses a non-DHCP UDP port
in communicating with the IPv6 server and the upstream relay agent,
or 2) an IPv6 relay agent that detects the use of a non-DHCP UDP port
(not 547) by a downstream relay agent.

A user of the "Relay Source Port Option" is shown below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Port | Destination Port |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Length | Checksum |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

User Datagram Header Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>16 bits; the source port number</td>
</tr>
<tr>
<td>Destination Port</td>
<td>16 bits; the destination port number</td>
</tr>
<tr>
<td>Length</td>
<td>8 bits; the length of the user datagram including the header and the data (This means the minimum value of the length is eight.)</td>
</tr>
<tr>
<td>Checksum</td>
<td>16 bits; the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.</td>
</tr>
</tbody>
</table>

Source Port is an optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

Destination Port has a meaning within the context of a particular internet destination address.

Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)

Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

The pseudo header conceptually prefixed to the UDP header contains the source address, the destination address, the protocol, and the UDP length. This information gives protection against misrouted datagrams. This checksum procedure is the same as is used in TCP.
4.2. Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be
sent by either 1) a DHCPv6 relay agent that uses a non-DHCP UDP port
to communicate with the IPv6 server and the upstream relay
2) an IPv6 relay agent that detects the use of a non-DHCP (not 547)
by a downstream relay agent.

The format of the "Relay Source Port Option" is shown below:

```
0 1 2 3
+---------+---------+
| Source Port | Destination Port |
+---------+---------+
| Length | Checksum |
+---------+---------+
| Data |
+---------+
```

4.1. Availability SCSI-TLV

The Generalized SCSI is defined in [RFC8258]. This document defines
a new type of Generalized SCSI-TLV called the Availability SCSI-TLV.
The Availability SCSI-TLV can be included one or more times. The
following format:

```
0 1 2
+---------+---------+---------+
| Type | Length |
+---------+---------+
| Availability level |
+---------+
| LSP Bandwidth at Availability level n |
+---------+
```

Type: 0x000A, 16 bits
Length: 2 octets (16 bits)
Availability level: 32 bits

This field is a binary32-format floating-point number as defined by [IEEE754-2008]. The bytes are transmitted in network order; that is, the byte containing the sign bit is transmitted first. This field describes the decimal value of the availability guarantee of the Switching Capability Interface Switching Capability Descriptor object [RFC4201]. The value MUST be less than 1. The Availability level field is usually expressed as the value 0.99/0.999/0.9999/0.99999/...
4.2. Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be present when either:

1. a DHCPv6 relay agent that uses a non-DHCP UDP port (e.g., port 547) communicating with the IPv6 server and the upstream relay agent.
2. an IPv6 relay agent that detects the use of a non-DHCP port (not 547) by a downstream relay agent.

The format of the "Relay Source Port Option" is shown below:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

User Datagram Header Format

### Fields

- **Source Port**: An optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

- **Destination Port**: Has a meaning within the context of a particular internet destination address.

Following is the format of the MRT Capability Parameter:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

The following TLV format is used to encode the MRT Capability parameter, and the sum of all the TPDU Lengths included in the message, and the reserved bit. The capability contains the MRT capability TLV and the UDP payload. The following is the structure:

- **Type**: Contains the reserved bit, the MRT Capability (0x050E), and the reserved bit.
- **Length**: 2 octets (16 bits)
- **Availability level**: 32 bits

This field is a binary32-format floating-point number as defined by [IEEE754-2008]. The bytes are transmitted in network order; that is, the byte containing the sign bit is transmitted first. This field describes the decimal value of the availability guarantee of the Switching Capability Interface Switching Capability Descriptor object (RFC4201). The value MUST be less than 1. The Availability level field is usually expressed as the value 0.99/0.999/0.9999/0.99999.
4.2. Relay Source Port Option for DHCPv6

The Relay Source Port Option is a new DHCPv6 option. It MUST be used in either 1) a DHCPv6 relay agent that uses a non-DHCP UDP portumber communicating with the IPv6 server and the upstream relay or 2) an IPv6 relay agent that detects the use of a non-DHCP (not 547) by a downstream relay agent.

The format of the "Relay Source Port Option" is shown below:

- **Source Port**
- **Destination Port**
- **Length**
- **Checksum**
- **Data**

2. ICMP Extended Echo Request

The ICMP Extended Echo Request message is defined for both ICMPv4 and ICMPv6. Like any ICMP message, the ICMP Extended Echo Request message is encapsulated in an IP header. The ICMPv4 version of the Extended Echo Request message is encapsulated in an IPv4 header, while the ICMPv6 version is encapsulated in an IPv6 header.

Figure 1 depicts the ICMP Extended Echo Request message.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
U|F| MRT Capability (0x050F)
S| Reserved   |
+------------------
<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Sequence Number</td>
<td>Reserved</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>ICMP Extension Structure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure 1: ICMP Extended Echo Request Message**

**IP Header fields:**

- **Source Address:** The Source Address identifies the probing interface. It MUST be a valid IPv4 or IPv6 unicast address.
- **Destination Address:** The Destination Address identifies the proxy interface. It MUST be a unicast address.

**ICMP fields:**

- **Type:** Extended Echo Request. The value for ICMPv4 is 42. The value for ICMPv6 is 160.
- **Code:** MUST be set to 0 and MUST be ignored upon receipt.
The FEC type for the P2MP PW Upstream FEC Element is encoded as follows:

```
 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
P2MP PW Up=0xB2|C| PW Type | PW Info Length |
| AGI Type | AGI Length | AGI Value |
| ~ | AGI Value (contd.) | ~ |
| SAI| SAI Length | SAI Value |
| ~ | SAI Value (contd.) | ~ |
PMSI Tunnel Typ|PMSI TT Length | |
| ~ | Transport LSP ID | ~ |
| ~ | Optional Parameters | ~ |
```

Figure 2: P2MP PW Upstream FEC Element

* P2MP PW Up:

  8-bit representation for the P2MP PW Upstream FEC type.

* C bit:

  A value of 1 or 0 indicating whether a control word is present or absent for the P2MP PW.

---

Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be included in one of two cases:

1. A DHCPv6 relay agent that uses a non-DHCP UDP port number communicating with the IPv6 server and the upstream relay agent.
2. An IPv6 relay agent that detects the use of a non-DHCP-based P2MP PW (not 547) by a downstream relay agent.

The format of the "Relay Source Port Option" is shown below:

```
| 3  | 2  | 1  | 0  |
| 0  | 1  | 2  | 3  |
| 8  | 9  | 0  | 1  |
```

---

4.1. Availability CS-TLV

This TLV is defined in [RFC8258]. This document defines an additional CS-TLV called the Availability CS-TLV, which can be included one or more times.

```
| 0  | 1  | 2  | 3  |
| 2  | 3  | 4  | 5  |
| 6  | 7  | 8  | 9  |
| 0  | 1  | 2  | 3  |
| 4  | 5  | 6  | 7  |
| 8  | 9  | 0  | 1  |
```

---

Echo Request Message

This message is used by the client to test the reachability of another node on the Internet. The client sends the message and waits for a reply. If no reply is received, the client may send the message again or try another protocol. The message is formatted as follows:

```
| 0  | 1  | 2  | 3  |
| 4  | 5  | 6  | 7  |
| 8  | 9  | 0  | 1  |
```

---

ICMP fields:

- Destination Address: The Destination Address identifies the proxy interface. It MUST be a valid IPv4 or IPv6 unicast address.
- Code: MUST be set to 0 and MUST be ignored upon receipt.
- Type: Extended Echo Request. The value for ICMPv4 is 42. The value for ICMPv6 is 160.
The FEC type for the P2MP PW Upstream FEC Element is encoded as follows:

```
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
P2MP PW Up=0x82[C]
PW Type | PW Info Length
AGI Type | AGI Length | AGI Value
~
AGI Value (contd.)
~
AII Type | SAII Length | SAII Value
~
SAII Value (contd.)
~
PMSI Tunnel Typ | PMSI TT Length
```

**Figure 2: P2MP PW Upstream FEC Element**

- **P2MP PW Up:**
  8-bit representation for the P2MP PW Upstream FEC type.

- **C bit:**
  A value of 1 or 0 indicating whether a control word is present or absent for the P2MP PW.

### 3.2. Message Format

The CoAP message format defined in [RFC7252], as shown in Figure 3, relies on the datagram transport (UDP, or DTLS over UDP) for keeping the individual messages separate and for providing length information.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
| Ver | T | TKL | Code | Message ID |
+-----+---+-----+------+
| Token (if any, TKL bytes) ... |
| Options (if any) ... |
| Payload (if any) ... |
```

**Figure 3: CoAP Message Format as Defined in RFC 7252**

The message format for CoAP over TCP is very similar to the format specified for CoAP over UDP. The differences are as follows:

- **Since the underlying TCP connection provides retransmissions and deduplication, there is no need for the reliability mechanisms provided by CoAP over UDP.** The Type (T) and Message ID fields in the CoAP message header are elided.

- **The Version (Vers) field is elided as well.** In contrast to the message format of CoAP over UDP, the message format for CoAP over TCP uses a constant version number, which is not included in the message header.

---

As documented in [RFC8258], this document describes the MRT Capability TLV and the Availability SCST-TLV called the Availability SCST-TLV. The message format is defined for both ICMPv4 and ICMPv6.
The FEC type for the P2MP PW Upstream FEC Element is encoded as follows:

\[
\begin{array}{cccccccccccccccc}
0 & 1 & 2 & 3 \\
\hline
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 \\
| P2MP PW Up=0x82[C] | PW Type | PW Info Length | AGI Type | AGI Length | AGI Value | AGI Value (contd.) | \\
| AII Type | AII Length | AII Value | AII Value (contd.) | \\
| PMSI Tunnel Typ | PMSI TT Length | Transport LSP ID | Optional Parameters | \\
\end{array}
\]

Figure 2: P2MP PW Upstream FEC Element

* P2MP PW Up:

8-bit representation for the P2MP PW Upstream FEC type.

* C bit:

A value of 1 or 0 indicating whether a control word is present or absent for the P2MP PW.

The unknown TLV bit MUST be a 1. As indicated in Section 3 of [RFC5561], it is used to recognize the MRT Capability TLV and to process the rest of the messages.

The forward unknown TLV bit MUST be a 0. The TE (Transport) interface. It MUST be a V bit.

ICMP fields:

- Type: Extended Echo Request value for ICMPv6 is 160.
- Code: MUST be set to 0 and
- Message ID:

Many variations with subtle differences.

Relay Source Port Option for DHCPv6

The "Relay Source Port Option" is a new DHCPv6 option. It MUST be either 1) a DHCPv6 relay agent that uses a non-DHCP UDP port communicating with the IPv6 server and the upstream relay or 2) an IPv6 relay agent that detects the use of a non-DHCP (not 547) by a downstream relay agent.

Figure of the "Relay Source Port Option" is shown below:

```
+-------------------+
| 1 | 2 | 3 | 4 |
+-------------------+
```

Section 4.1. Available GSLAT TLV

This document defines a new TLV called the Availability GSLAT TLV which can be included one or more times.

3.2. Message Format

The CoAP message format defined in [RFC7252], as shown in Figure 3, is used for transport (UDP, or DTLS over UDP) for keeping a separate and for providing length.

Figure 3: CoAP Message Format as Defined in RFC 7252

The message format for CoAP over TCP is very similar to the format specified for CoAP over UDP. The differences are as follows:

- Since the underlying TCP connection provides retransmissions and deduplication, there is no need for the reliability mechanisms provided by CoAP over UDP. The Type (T) and Message ID fields in the CoAP message header are elided.
- The Version (Vers) field is elided as well. In contrast to the message format of CoAP over UDP, the message format for CoAP over TCP does not contain the Version field.
Parsing packet diagrams

• Subtle differences in structure and English prose make parsing packet diagrams difficult

• But many benefits if we can parse them: can generate parser code, perform continuous integration → better standards

• Many efforts to introduce structured descriptions: ABNF, ASN.1, TLS presentation language, ..

• Clusters of adoption → need a broad framework, not another description language
Discussion

• Help us understand: what are the technical and social obstacles to adoption of structured languages?

• Work is part of a broader project on improving the standards process using structured languages and formal methods

• Stephen McQuistin
  sm@smcquistin.uk

• Colin Perkins
  csp@csperkins.org