Appendix C

TRUMP Protocol Headers

TRUMP is a transport protocol which provides for the reliable delivery of data across an unreliable packet-switched network. Chapter 5 gives a feature-oriented examination of the TRUMP transport protocol. This appendix describes a proposed set of TRUMP headers for use in an IPv6 network.

In the following section, all fields are unsigned integers or, if single bits, boolean flags. All multi-octet fields in TRUMP's headers are stored in big-endian format. All diagrams are 4 octets wide. For fields where not all the possible values are enumerated, the undefined values are currently invalid and reserved for future use. Fields that are described as 'unused' should be set to all bits off.

The first 64 bits of each TRUMP header are nearly identical for all packet types, and are shown in the following figure. A description of each field follows.

<table>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>3</td><td>3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3">QOS</td><td colspan="3">Pkt Type</td><td colspan="8">Error Number</td><td colspan="2">Un used</td><td>F</td><td>L</td><td>A</td><td>O</td><td>Y</td><td>X</td><td colspan="4">Unused</td><td colspan="4">Frag #</td></tr>
</table>

Figure 68: First 32 bits in TRUMP Headers

Next Hdr Part of the IPv6 header specification, described in [Stallings 96].

Hdr Extension Length Part of the IPv6 header specification, described in [Stallings 96].

Version The version of the transport protocol. The current TRUMP version is 2. Future versions of TRUMP will have higher version numbers.

Packet Encoding The encoding of the packet from the **Connection Number** field onwards. This is predominately used to allow for encryption of transport protocol packets. Currently, only two values out of the sixteen possible are defined:

- **0** The header and data are in plain-text.
- **1** The header (with the exception of the first four fields) and data are encrypted in DES block mode, using a key negotiated by the source and destination endpoints. The method of key negotiation is not a part of the TRUMP protocol. The checksum is not encrypted, and is set to the checksum of the whole packet after encryption.

Connection Number Currently, this field is not used and reserved. In future versions of TRUMP, it will hold a number that uniquely identifies the (source, destination, source port, destination port) tuple.

Port Size Identifies the size of the endpoint identifiers. The four possible values are:

- **0** Endpoint identifiers are 0 bits in size.
- **1** Endpoint identifiers are 16 bits in size.
- **2** Endpoint identifiers are 32 bits in size.
- **3** Endpoint identifiers are 64 bits in size.

The latter two are designed for use in distributed systems, where large integers can be used to store such things as object descriptors and capabilities.

Quality of Service Used in **SETUP** packets and in **DATA** packets where the **Y** bit is set. The field is invalid at any other time, and must be set to all bits off. The field holds the requested quality of service for the connection. Two values are currently defined:

- **0** Reliable. The destination sends ACKs and the source retransmits.
- **1** Time-sensitive. The destination sends ACKs but the source does not retransmit lost data.

Packet Type The type of packet. Five values are currently defined:

- **0** A SETUP packet.
- **1** A DATA packet.
- **2** An ACK packet.
- **3** A SACK packet.
- **4** A TEARDOWN packet.

Error Indication of any error that has occurred. This field is only valid for a SACK packet, and must be set to all bits off in any other packet. Defined values are given below.

Bits 50 to 55 are used to hold bit fields for particular packet types. The fields shown are described below. Refer to the rest of this section for details of the other fields in each packet type.

A – Return ACK Immediately Used in **DATA** packets. If set, the destination must return an ACK packet for this DATA packet immediately. This field is illegal in other packets.

O – Last segment Used in **DATA** packets. If set, the segment in the DATA packet is the last in the message. This field is illegal in other packets.

Y – DATA is Implicit SETUP Used in **DATA** packets. If set, the DATA packet holds the first segment of the message, and is an implicit SETUP. The QOS field is not valid in a DATA packet if this is not set. This field is illegal in other packets.

X – Explicit Teardown Used in **SETUP** and **SACK** packets. If set, the source must perform an explicit connection teardown. This field is illegal in other packets.

In addition, there are fields in each **DATA** packet that are used if a source must fragment a segment.

F – Segment is a Fragment If set, the segment is a fragment of another segment. The segment sequence number is the same as the original segment. This field is illegal in non-DATA packets.

L – Last Fragment If set, the segment is the last fragment of another segment. This field is illegal in non-DATA packets.

Fragment Number The fragment number of the given fragment. If **F** is not set, this field is invalid. This field is illegal in non-DATA packets.

C.1 Connection Setup

Explicit connection setup in TRUMP is performed by transmission of a **SETUP** packet from source to destination, acknowledged by a **SACK** from destination to source. This exchange passes the message identification, source and destination port, and type of connection teardown to the destination, and returns flow control information or a connection failure error to the source.

The **SETUP** packet has the fields as shown in the following figure.

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3">QOS</td><td colspan="3">SETUP</td><td colspan="8">Unused</td><td colspan="7">Unused</td><td colspan="1">X</td><td colspan="8">Unused</td></tr>
<tr><td colspan="32">Destination Port</td></tr>
<tr><td colspan="32">Source Port</td></tr>
<tr><td colspan="32">Initial Segment Sequence Number</td></tr>
<tr><td colspan="32">Checksum</td></tr>
</table>

Figure 69: Connection Setup Packet

Destination Port The TRUMP destination port of the connection.

Source Port The TRUMP source port of the connection.

Initial Segment Sequence Number The first segment in the message will have this sequence number.

Checksum A 32-bit checksum calculated over the fields in the packet. This is calculated using the algorithm described in [Fletcher 82].

In all TRUMP packets, the **Source Port** and **Destination Ports** are variable-sized, from zero- to 64-bits. The figures shown above and following give packets where these fields are 32-bits in size.

C.2 Special Acknowledgment

Explicit connection setup in TRUMP is acknowledged by a **SACK** packet. This packet is also used to abnormally terminate a message transmission (i.e an established connection).

The **SACK** packet has the fields as shown in the following figure.

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3">Unused</td><td colspan="3">SACK</td><td colspan="8">Error Number</td><td colspan="7">Unused</td><td>X</td><td colspan="8">Unused</td></tr>
<tr><td colspan="32">Destination Port</td></tr>
<tr><td colspan="32">Source Port</td></tr>
<tr><td colspan="32">Initial Segment Sequence Number</td></tr>
<tr><td colspan="32">Checksum</td></tr>
</table>

Figure 70: Special Acknowledgment Packet

The **SACK** packet has the following extra fields:

Error Indication of any error that has occurred. Defined values are:

- **00** No error has occurred.
- **01** The destination port doesn't exist.
- **02** The destination port is currently unavailable.
- **03** The source port doesn't have enough privileges for the connection.
- **04** The source machine doesn't have enough privileges for the connection.
- **05** The destination port has been destroyed.
- **06** The destination cannot continue the connection.
- **07** The destination TRUMP implementation cannot cope with the requested port size.
- **08** The destination TRUMP implementation cannot cope with the requested encryption scheme.
- **09** The destination TRUMP implementation cannot cope with the requested quality of service.
- **10** The last packet from the source had a port size different than that specified in the initial **SETUP** packet.

Destination Port The TRUMP destination port of the connection.

Source Port The TRUMP source port of the connection.

Checksum A 32-bit checksum calculated over the fields in the packet. This is calculated using the algorithm described in [Fletcher 82].

C.3 Data Transmission

The **DATA** packet is used to transport data from the source to the destination.

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3">QOS</td><td colspan="3">DATA</td><td colspan="8">Unused</td><td colspan="2">Un used</td><td>F</td><td>L</td><td>A</td><td>O</td><td>Y</td><td>X</td><td colspan="4">Unused</td><td colspan="4">Frag #</td></tr>
<tr><td colspan="32">Destination Port</td></tr>
<tr><td colspan="32">Source Port</td></tr>
<tr><td colspan="32">Segment Sequence Number</td></tr>
<tr><td colspan="32">Data</td></tr>
<tr><td colspan="32">Checksum</td></tr>
</table>

Figure 71: Data Transmission Packet

The **DATA** packet has the following extra fields:

Destination Port The TRUMP destination port of the connection.

Source Port The TRUMP source port of the connection.

Segment Sequence Number The sequence number of the segment in the DATA field.

Data The actual payload of the packet, a TRUMP message segment.

Checksum A 32-bit checksum calculated over the fields in the packet. This is calculated using the algorithm described in [Fletcher 82].

C.4 Data Acknowledgment

The **ACK** packet is used to acknowledge data from the source.

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3"></td><td colspan="3">ACK</td><td colspan="8">Highest Seq #</td><td colspan="16">Selective Acknowledgment Bitmap</td></tr>
<tr><td colspan="32">Destination Port</td></tr>
<tr><td colspan="32">Source Port</td></tr>
<tr><td colspan="32">Segment Sequence Number</td></tr>
<tr><td colspan="32">Flow Rate</td></tr>
<tr><td colspan="32">Checksum</td></tr>
</table>

Figure 72: Data Acknowledgment Packet

The **ACK** packet has the following extra fields:

Destination Port The TRUMP destination port of the connection.

Source Port The TRUMP source port of the connection.

Segment Sequence Number The sequence number of the first segment being acknowledged by this packet.

ACK Bitmap The bitmap that selectively acknowledges up to 16 segments. Assume the Segment Sequence Number is N. If segment S was received correctly, bit 2^{S-N} is set on; otherwise, it is set to zero.

Highest Sequence Number The highest sequence number H positively or negatively received in the bitmap, relative to the Segment Sequence Number N. Sequence numbers $> N + H$ are not acknowledged in the bitmap.

Flow Rate The highest bit rate of segment transmission by the source which will not cause buffer overflows in the destination.

Checksum A 32-bit checksum calculated over the fields in the packet. This is calculated using the algorithm described in [Fletcher 82].

C.5 Connection Termination

The **TEARDOWN** packet is used to explicitly close a finished message (i.e a completed connection). This allows the destination to remove data structures that it might have kept in order to detect delayed, out of sequence, or duplicate packets.

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Next Header</td><td colspan="8">Hdr Ext Len</td><td colspan="4">Version</td><td colspan="4">Pkt Encoding</td><td colspan="8">Connection #</td></tr>
<tr><td colspan="2">Port Size</td><td colspan="3">Unused</td><td colspan="3">Teardown</td><td colspan="24">Unused</td></tr>
<tr><td colspan="32">Destination Port</td></tr>
<tr><td colspan="32">Source Port</td></tr>
<tr><td colspan="32">Checksum</td></tr>
</table>

Figure 73: Connection Close Packet

The **TEARDOWN** header has the following fields:

Destination Port The TRUMP destination port of the connection.

Source Port The TRUMP source port of the connection.

Checksum A 32-bit checksum calculated over the fields in the packet. This is calculated using the algorithm described in [Fletcher 82].