Weave Message Format

Version 1.3
2020/06/28

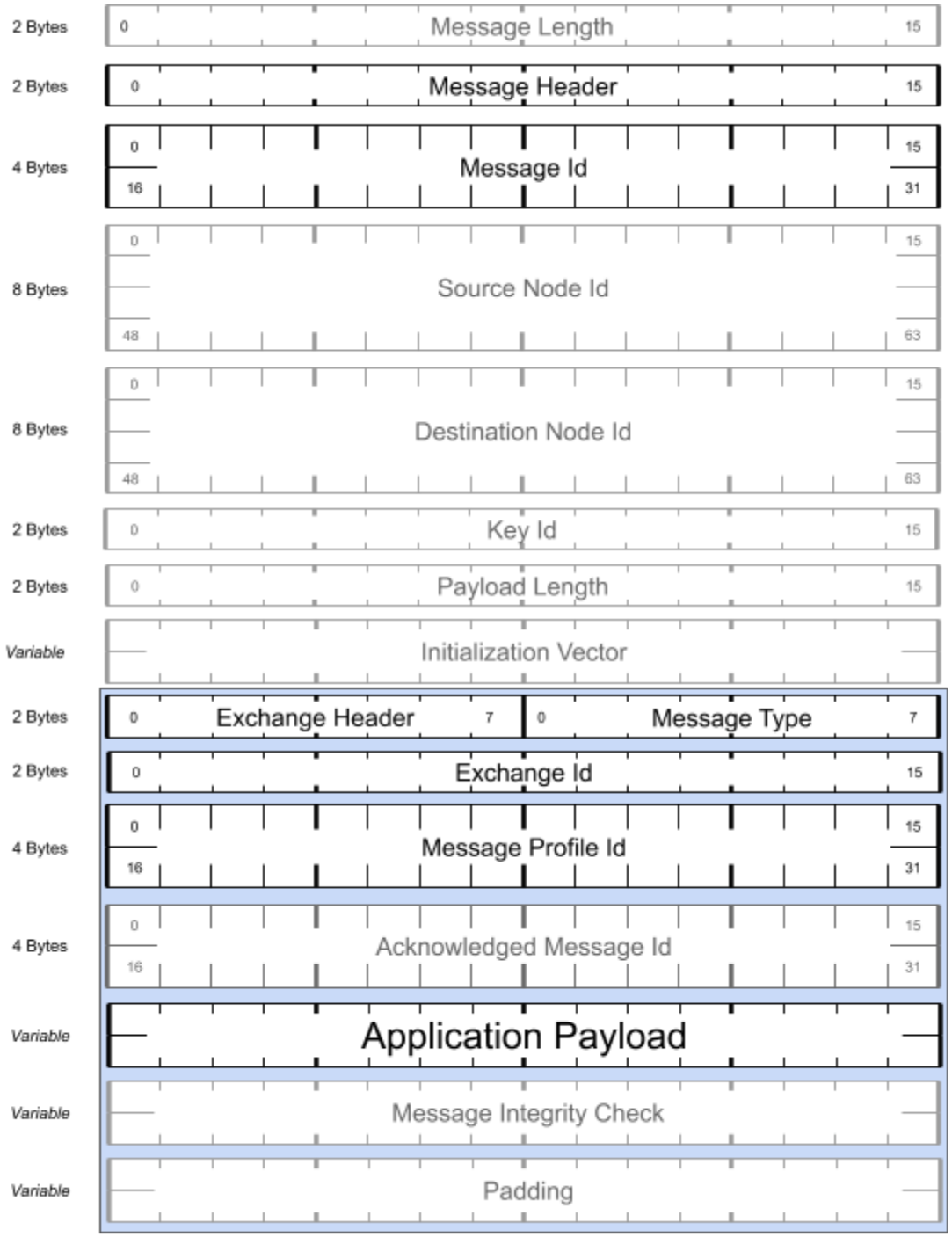
Introduction

This document describes the various encoded forms of a Weave message. There are two overall types of Weave message: a ***general Weave message*** and a ***tunneled IP packet message***. Both types of messages can be transmitted in encrypted and unencrypted form. The process of encrypting both types of message is the same, and messages of both types can be encrypted using the same keys.

General Message Format

General Weave messages are used by Weave applications to convey application-specific data and/or commands. General Weave messages contain a message profile id and type which identify both the semantic meaning of the message as well as the structure of any associated application payload data. General messages also convey an exchange id, which relates the message to a particular exchange (a.k.a. conversation) taking place between two nodes. Finally, certain types of general Weave messages can convey information that acknowledges the reception of an earlier message. This is used as part of the Weave Reliable Messaging protocol to provide guaranteed delivery of messages over unreliable transports.

General Weave messages are structured as follows.

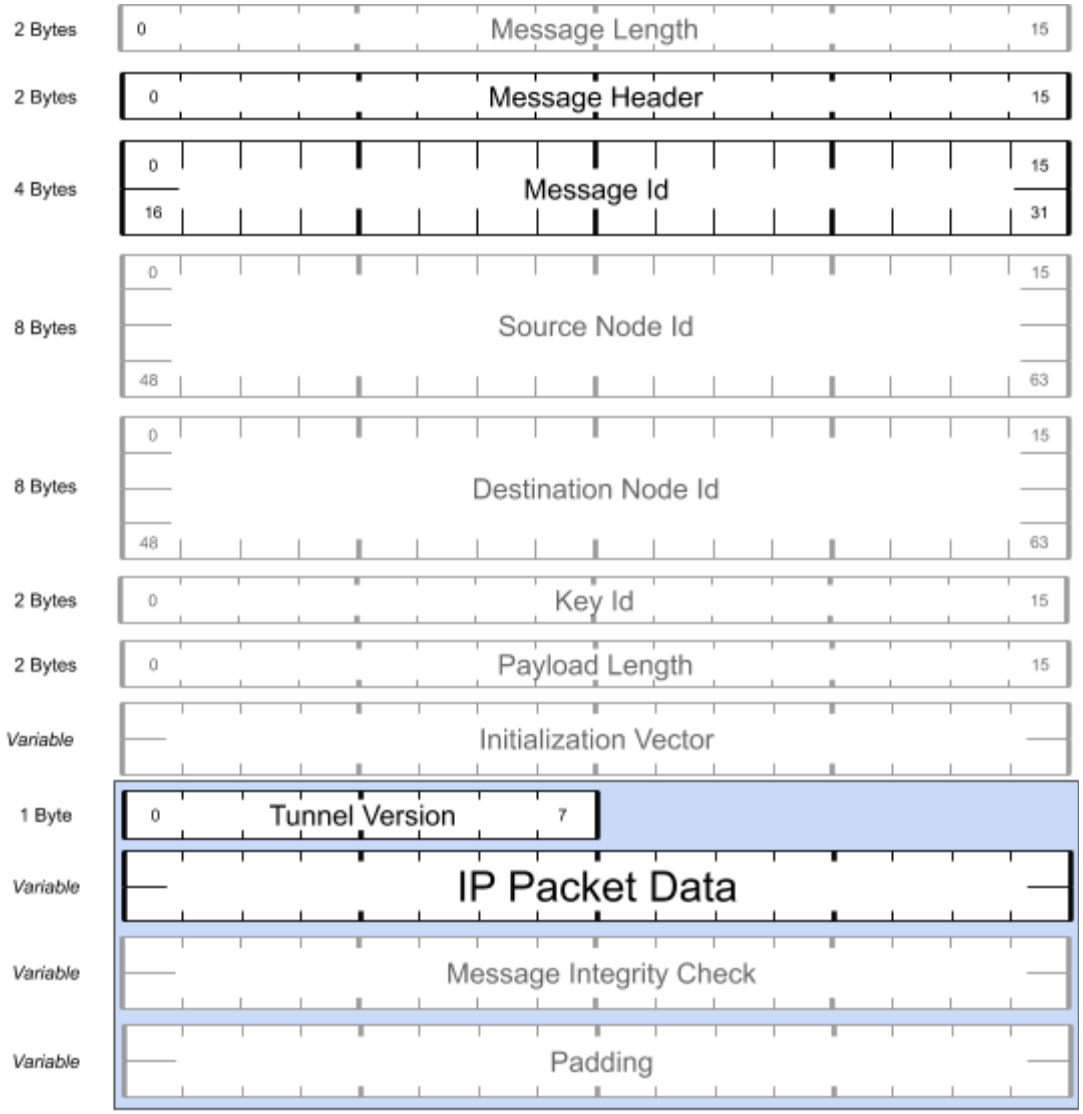


Grey denotes optional or conditional fields.
Blue denotes fields subject to encryption.

Tunneled IP Message Format

Tunneled IP packets encapsulate an encoded IP packet that is being transported between two Weave nodes. Tunneled IP packets can convey either IPv4 or IPv6 packets, although typically only the latter is used in practice. Tunneled IP packets forgo many of the application-specific headers present in a general Weave message, making them simpler in structure.

Weave messages that convey tunneled IP packets are structured as follows.



Grey denotes optional or conditional fields.
Blue denotes fields subject to encryption.

Weave messages containing tunneled IP packets have a similar format to general Weave messages. For all fields that are shared between the two formats, the structure and interpretation of those fields is the same as described for the general Weave message format.

Similarly, the process by which messages are encrypted and integrity checked are also the same, albeit with different inputs to the encryption/integrity process.

It is important to note that the contents of the contained IP packet have no bearing on the format or addressing of the tunneled IP Weave message that conveys it. In particular, the Source and Destination Node Id fields of a tunneled IP Weave message convey the node ids of the *tunneling agents* that are exchanging the tunneled IP message, and need not have any relationship to the source and destination IP addresses contained in the IP packet.

Similarly, in the case where the contained IP message is itself conveying another Weave message, the structure, encoding and encryption of the inner Weave message has no bearing on that of the outer tunneled IP Weave message. This implies, among other things, that a tunneled IP Weave message that is encrypted using a particular set of encryption keys, can convey a IP packet containing another Weave message that is encrypted using an entirely different set of keys.

Byte Ordering

All multi-byte integer fields are transmitted in little-endian order unless otherwise noted in the field description.

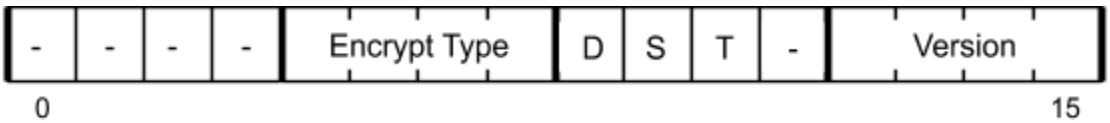
Field Descriptions

Message Length (16 bits)

An unsigned integer value specifying the overall length of the message in bytes, not including the size of the Message Length field itself. This field is only present when the message is being transmitted over a stream-oriented channel such as TCP. When transmitted over a message-oriented channel, the message length is conveyed by the underlying channel. For example, when transmitted over UDP, the message length is equal to the payload length of the UDP packet.

Message Header (16 bits)

An unsigned integer bit field containing the following subfields:



Version (4 bits, positions 12-15)

An unsigned integer specifying the version of the Weave Message format used to encode the message. Currently only two versions are defined:

1 -- Weave Message Format version 1
2 -- Weave Message Format version 2

All other values are reserved.

Note that the Version field conveys information solely about the structure of the Weave message itself, not about the structure of the application payload or the interpretation of the message's type. Thus, changes to how an application handles or interprets a message *do not* result in the creation of a new message format version number.

T Flag (1 bit, position 10)

A single bit field identifying whether the message is a general Weave message or tunneled IP packet message. A value of 0 indicates a general Weave message.

The value of the T Flag must be 0 if the Version subfield in the Message Header has a value less than 2.

S Flag (1 bit, position 9)

A single bit field indicating that the Source Node Id field is present.

D Flag (1 bit, position 8)

A single bit field indicating that the Destination Node Id field is present.

Encrypt Type (4 bits, positions 4-7)

An unsigned integer specifying the type of encryption/integrity checking applied to the message. The following values are defined:

0 -- No encryption / message integrity
1 -- AES-128-CTR encryption with HMAC-SHA-1 message integrity

All other values are reserved.

Note: All unused bits in the Message Header field are reserved and must be set to 0.

Message Id (32 bits)

An unsigned integer value uniquely identifying the message from the perspective of the sending node.

Source Node Id (64 bits)

A sequence of 8 bytes containing the EUI-64 identifier of the source node. Within the field, the bytes of the EUI-64 identifier are transmitted in an ascending index-value order, i.e. EUI[0], followed by EUI[1], EUI[2], etc.

The Source Node Id field is only present in a message when the S flag in the Message Header field is set to 1.

Destination Node Id (64 bits)

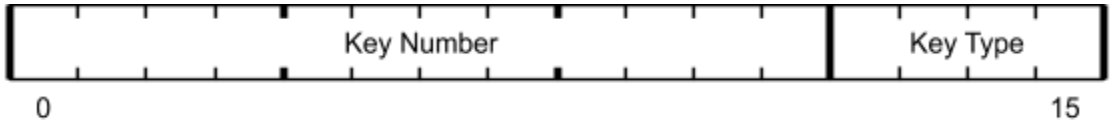
A sequence of 8 bytes containing the EUI-64 identifier of the destination node. Within the field, the bytes of the EUI-64 identifier are transmitted in an ascending index-value order, i.e. EUI[0], followed by EUI[1], EUI[2], etc.

The Destination Node Id field is only present in a message when the D flag in the Message Header field is set to 1.

Key Id (16 bits)

An unsigned integer value identifying the encryption/message integrity keys used encrypt the message. The Key Id field is only present when the Encryption Type field has a value other than 0.

The Key Id field contains the following subfields:



Key Type (4 bits, positions 12-15)

An unsigned integer value identifying the type of encryption/message integrity used to encrypt the message. The following types are defined:

1 -- A fabric key shared by multiple nodes in the fabric
2 -- A session key shared by a pair of nodes

All other values are reserved.

Key Number (12 bits)

An unsigned integer value identifying the particular key used to encrypt the message out of the set of available keys (either fabric or shared).

Payload Length (16 bits)

An unsigned integer value equal to the size in bytes of the Application Payload field. The Payload Length field is only present when the message is encrypted, and only when the selected encryption algorithm requires the use of message padding (e.g. block ciphers in CBC mode).

Note: At present, no encryption type is defined that requires the use of padding. Thus the Payload Length field is defined for future use only.

Initialization Vector (variable length)

A sequence of bytes containing the cryptographic initialization vector (IV) value used to encrypt the message. The Initialization Vector field is only present when the message is encrypted, and only when the selected encryption algorithm requires the use of an initialization vector. The length of the Initialization Vector field is implied by the type of encryption in use.

Note: At present, no encryption type is defined that requires the use of an IV. Thus the Initialization Vector field is defined for future use only.

Exchange Header (8 bits)

An unsigned integer bit field containing the following subfields:

I Flag (1 bit, position 0)

A single bit field indicating that the message was sent by the initiator of the exchange.

A Flag (1 bit, position 1)

A single bit field indicating that the message serves as an acknowledgement of a previous message received by the current message sender. The value of the A Flag *must* be 0 if the Version subfield in the Message Header has a value of 1.

R Flag (1 bit, position 2)

A single bit field indicating that the message sender wishes to receive an acknowledgement for the message. The value of the R Flag *must* be 0 if the Version subfield in the Message Header has a value of 1.

F Value (1 bit, position 4)

A single bit field reserved for compatibility with old protocol versions. The value of this bit must be set to 1.

Note: All unused bits in the Exchange Header field are reserved and must be set to 0.

Message Type (8 bits)

An unsigned integer value identifying the type of the message. The message type value is interpreted relative to the Weave profile specified in the Message Profile Id field.

Exchange Id (16 bits)

An unsigned integer value identifying the exchange to which the message belongs.

Message Profile Id (32 bits)

An unsigned integer value identifying the profile in which the message type is defined.

Acknowledged Message Id (32 bits)

An unsigned integer value containing the message id of a previous message that is being acknowledged by the current message. The Acknowledged Message Id field is only present when the Version subfield in the Message Header is 2 or greater and the A flag in the Exchange Header field is 1.

Application Payload (variable length)

A sequence of zero or more bytes containing the application data conveyed by the message. The length of the Application Payload field is given by the Payload Length field, when that field is present in the message. When the Payload Length field is not present, the length of the Application Payload field can be computed by taking the overall length of the message and subtracting the length of all other fields in the message.

Tunnel Version (8 bits)

An unsigned integer specifying the method by which the IP packet is encapsulated within the Weave Message. Currently only one value is defined:

1 -- Direct IP Encapsulation

All other values are reserved.

IP Packet Data (variable length)

A sequence of bytes containing an encoded IP packet. The length of the IP Packet Data field must correspond exactly to the length of the contained IP packet, as encoded in its header. The IP Packet Data field can contain either an IPv4 packet or an IPv6 packet. The type of packet can be distinguished by the IP version field encoded in the initial byte of the IP header. The IP packet may contain any valid IP protocol type including UDP, TCP, ICMP, etc.

Message Integrity Check (variable length)

A sequence of bytes containing the message integrity check value for the message. The length and byte order of the field depends on the integrity check algorithm in use. For HMAC-SHA-1, the field consists of 20 bytes in big-endian ordering.

The Message Integrity Check field is only present when the message is encrypted, i.e. when the Encryption Type field has a value other than 0.

Padding (variable length)

A sequence of bytes representing a cryptographic padding added to the message to make the encrypted portion of the message evenly divisible by the encryption block size. The Padding field is only present when the message is encrypted, and only when the selected encryption algorithm requires the use of message padding (e.g. block ciphers in CBC mode).

The contents of the padding field depend on the encryption algorithm used. The length (in bytes) of the Padding field can be calculated as follows:

```
encrypted_len = application_payload_len + message_integrity_check_len

if ((encrypted_len % block_len) > 0)
  padding_len = block_len - (encrypted_len % block_len)
else
  padding_len = 0
```

Note: At present, no encryption type is defined that requires the use of padding. Thus the Padding field is defined for future use only.

Message Overhead

The following table shows the message overhead in bytes for different configurations of a general Weave message. Common case configurations are highlighted in blue.

Transport	Encryption Type	Source/Dest Ids	Overhead
UDP	None	Not Included	14
UDP	None	Included	30
UDP	AES-128-CTR/HMAC-SHA-1	Not Included	36
UDP	AES-128-CTR/HMAC-SHA-1	Included	52
TCP	None	Not Included	16
TCP	None	Included	32
TCP	AES-128-CTR/HMAC-SHA-1	Not Included	38
TCP	AES-128-CTR/HMAC-SHA-1	Included	54

Revision History

Revision	Date	Description
1.0	2014/10/26	Initial revision
1.1	2015/10/08	Added description of Tunneled IP message format.
1.2	2016/02/13	Added Introduction section.
1.3	2020/06/28	Restructured section describing Tunneled IP messages. Added description of Tunnel Version field.