**DEFAULT Packet**

| Offsets | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 0 | 0 | Version | | | | Type | | | | Flags | | | | | | | | Sequence ID | | | | | | | | | | | | | | | |
| 4 | 32 | Fragment ID* | | | | | | | | Fragment Number* | | | | | | | | Init Vector* | | | | | | | | | | | | | | | |
| 8 | 64 | Checksum Hash* | | | | | | | | | | | | | | | | Data* | | | | | | | | | | | | | | | |

**ACK Packet**

| Offsets | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 8 | 64 | Default Packet Headers | | | | | | | | | | | | | | | | ACK ID | | | | | | | | | | | | | | | |
| 12 | 96 | ACK Bits | | | | | | | | | | | | | | | | Data* | | | | | | | | | | | | | | | |

**AUTH Packet**

| Offsets | Octet | 0 | | | | | | | | 1 | | | | | | | | 2 | | | | | | | | 3 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Octet | Bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 8 | 64 | Default Packet Headers | | | | | | | | | | | | | | | | Reserved | | | | | | | | EC Public Key Size (E) | | | | | | | |
| 12 | 96 | EC Public Key | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | ... | ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10+E | 80+E | EC Public Key | | | | | | | | | | | | | | | | Certificate Size (C)* | | | | | | | | | | | | | | | |
| 14+E | 168+E | Certificate* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | ... | ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12+C+E | 96+C+E | Certificate* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Not required

Note: **C** and **B** are in bytes

| Types | |
|---|---|
| **Type** | **Enum** |
| DEFAULT | 0 |
| ACK | 1 |
| AUTH | 2 |
| RESERVED | 3..15 |

| Flags | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octet** | 1 | | | | | | | |
| **Bit** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Flag** | RELIABLE | FRAG | COMPRESSED | ENCRYPTED | CHECKSUM | RESERVED | | |

### Default Packet Spec

| Field | Size | Required | Required Flags | Notes |
|---|---|---|---|---|
| Version | 4 | 1 | | Version number. 0 (zero) for all development. |
| Type | 4 | 1 | | See Types. |
| Flags | 8 | 1 | | See Flags. |
| Sequence ID | 16 | 1 | | Packet identifcation number set by the sender. |
| Fragment ID* | 8 | 0 | FRAG | Possition in reassambled packed. |
| Fragment Number* | 8 | 0 | FRAG | Total number of fragmented packed. |
| Init Vector* | 16 | 0 | ENCRYPT | Init vector for use when decrypting. |
| Checksum Hash* | 16 | 0 | CHECKSUM | CRC-32 checksum. |
| *Data** | | 0 | | Data can be length 0..1000 bytes. |

### ACK Packet Spec

| Field | Size | Required | Required Flags | Notes |
|---|---|---|---|---|
| Default Packet Headers | 36-80 | 1 | | See Default Packet Spec. |
| ACK ID | 16 | 1 | | The Sequnce ID (see Default Packet Spec) of a packet with RELIABLE (see flags). |
| ACK Bits | 16 | 1 | | A record of the local ACK Bits i.e. a full record of all ACKed packets. |
| *Data** | | 0 | | Data can be length 0..1000 bytes. |

### AUTH Packet Spec

| Field | Size | Required | Required Flags | Notes |
|---|---|---|---|---|
| Default Packet Headers | 36-80 | 1 | | See Default Packet Spec. |
| Reserved | 8 | 1 | | For padding. |
| EC Public Key Size (**E**) | 8 | 1 | | Size of EC Public Key in *bytes* . |
| EC Public Key | E | 1 | | Senders Public Eliptic Curve Key (for generating session key). |
| Certificate Size (**C**)* | 16 | 0 | | Size of Certificate in *bytes* . |
| Certificate* | C | 0 | | Senders Certificate (for identiy validation). |

*Not required

Note: **C** and **B** are in bytes