SRT Protocol Overview

IETF 107 [MOPS]

Maxim Sharabayko, PhD
Senior Software Developer | Haivision
maxsharabayko@haivision.com

What is SRT?

- A protocol on top of UDP (unicast)
- Content agnostic
- Bidirectional data transfer
- ARQ (ACK + NAK)
- FEC (Packet Filter API v1.4.0+)
- Connection bonding (v1.5.0)
- Stream multiplexing
- Secure (AES 128/192/256 Encryption)

SRT | SECURE RELIABLE TRANSPORT

> “*Enabling **low-latency video** contribution & distribution and **fast file transfer** over unpredictable networks.*”

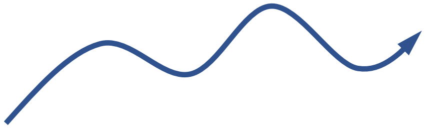
SRT Operation Modes

Message Mode

- Non-real-time
- File/message transfer
- Content agnostic
- Message interchange

Live Mode

- Real-time
- Live Streaming
- Content agnostic
- Latency management



Buffer Mode

- Non-real-time
- A single file transfer
- Content agnostic

SRT Use Cases

- Live video contribution/distribution
  - MPEG-TS, RTP, Elementary Stream, etc.
- File transfer
  - Files and segmented Streaming Formats like HLS and DASH
- Tunneling
  - TCP => SRT => TCP
  - RTP => SRT => RTP
  - HTTP => SRT => HTTP
- Messaging
  - Custom messages: chat, voice, etc.
  - Metadata
  - Control data

SRT Live Streaming

- Data Transmission Mode: “Live”
- A fixed end-to-end latency:
  - Network delay
  - Configurable receiver buffer delay
- Recovers source timing T_{SOURCE} : $T_{DELIVERY} >= T_{SOURCE} + T_{LATENCY}$
  - $T_{DELIVERY}$ – packet delivery time
  - T_{SOURCE} – packet source time
  - $T_{LATENCY}$ – end-to-end latency
- Drops too late packets

Pristine Quality

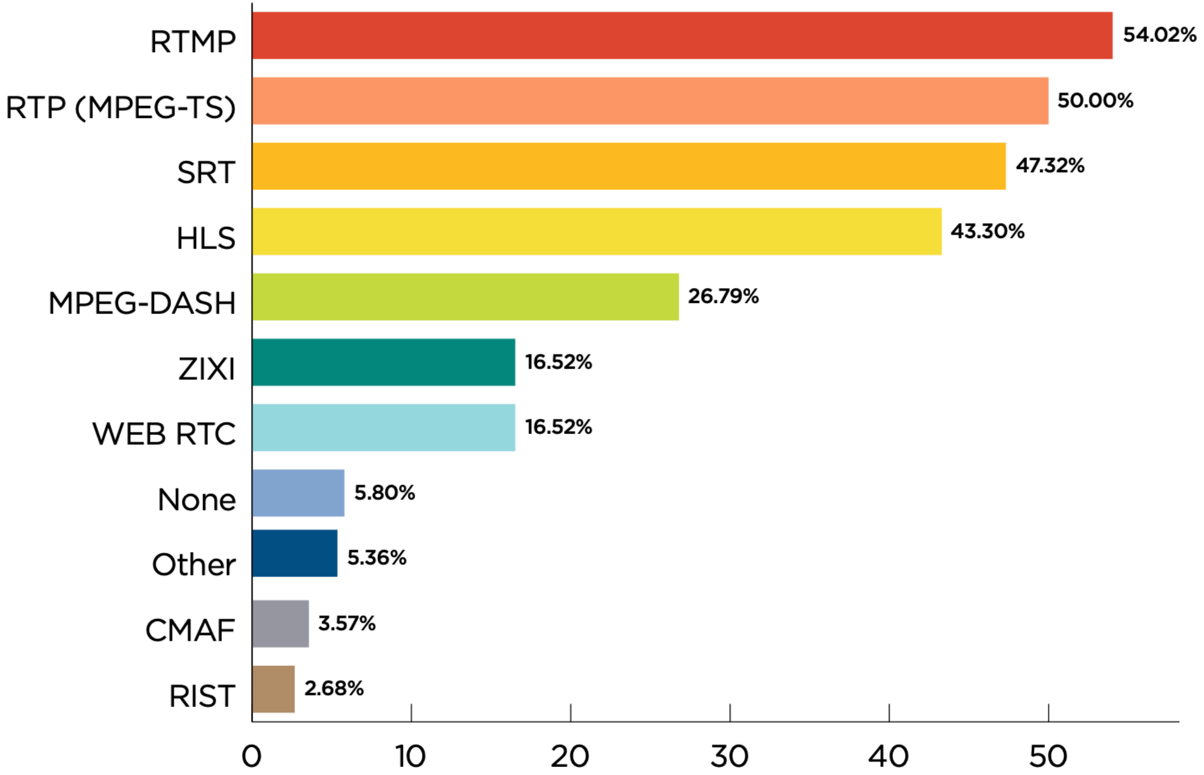
Protect against jitter, packet loss and bandwidth fluctuation, so your viewers get the best viewing experience.

Low Latency

Configurable control to deliver low latency video while overcoming network challenges.

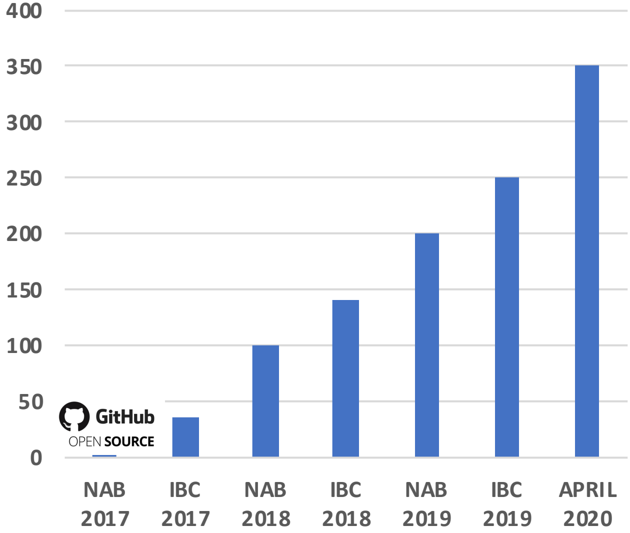
Why SRT?

Video Transport Protocol Usage Survey*



* Broadcast IP Transformation Report

SRT Alliance Member Companies



COMCAST, Microsoft, Haivision, AVID, grass valley, Alibaba Cloud
EUROVISION SERVICES, ENCOMPASS, harmonic, telestream, netinsight, TATA COMMUNICATIONS
BITMOVIN, IIJ, deluxe, Tencent腾讯, WOWZA media systems, RED BEE, JVC, BRIDGE TECHNOLOGIES
MediaKind, PERFORM, Imagine COMMUNICATIONS, Panasonic, ERICSSON, Cinegy, iStreamPlanet
Appear tv, sencore, ateme, TERADEK, ROHDE&SCHWARZ, AVIWEST, edgeware
pebble beach systems, brightcove, OOYALA, Limelight NETWORKS, matrox, StreamShark, KALTURA
sohonet, StreamGuys, Dacast, COLLABORA, Softvelum, anevia, amagi, NAGRA KUDELSKI

SRT Feature Matrix (Live Streaming over Public Networks)

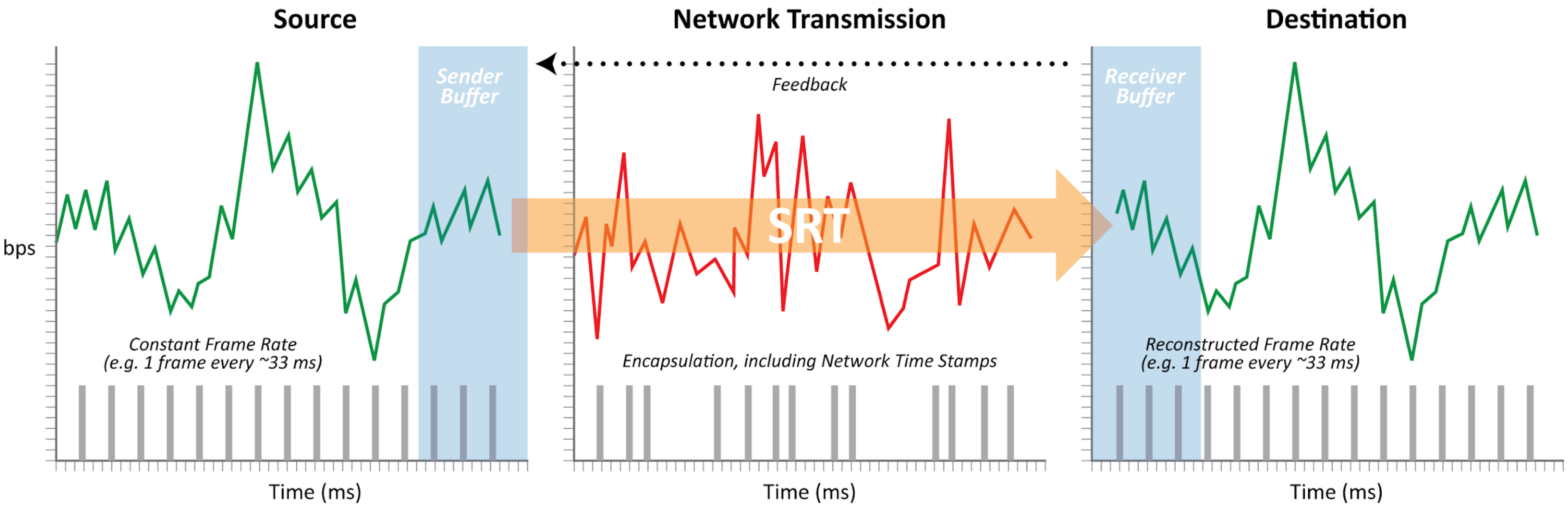
1. Connectivity
   - Firewall traversal ✓
   - NAT traversal ✗ (TODO?: RFC-8445 ICE)
   - Connection migration ✗ ?
   - Network switching ✗ ?
   - Connection Rejection Reason !
2. Access Control
   - User Authentication ✓ (username is not encrypted)
   - Resource Request ✓ (not encrypted)
   - Stream Definition ! (TODO: RFC-4566: SDP)
3. Security
   - Encryption: AES-CTR 128/192/256 ✓
   - Pre-shared password + PBKD2 ✓
   - TLS ✗ (Could be added?)
   - DTLS ! (potentially works)
4. Content delivery
   - Content agnostic ✓ (MPEG-TS, RTP, ES, …)
   - Stream multiplexing ✓
   - UDP unicast (bidirectional) ✓
   - UDP multicast ✗ (TODO?)
   - Loss recovery
     - ARQ (ACK, NAK, Retransmit) ✓
     - FEC ✓ (v1.4.0)
     - Connection bonding: broadcast ✓ (v1.5.0 in progress)
   - Packet reordering / jitter ✓
   - Varying latency (RTT) handling ✓
   - Too-late Packet Drop (real-time) ✓
   - Congestion control ✓ (to be improved)
   - Flow control ✓ (to be improved)
   - Network friendliness ✓ (to be improved)
5. Connection Bonding ✓ (v1.5.0 in progress)
   - Data duplication (broadcast)
   - Backup link
   - Smart link utilization (balancing)

Thank you!

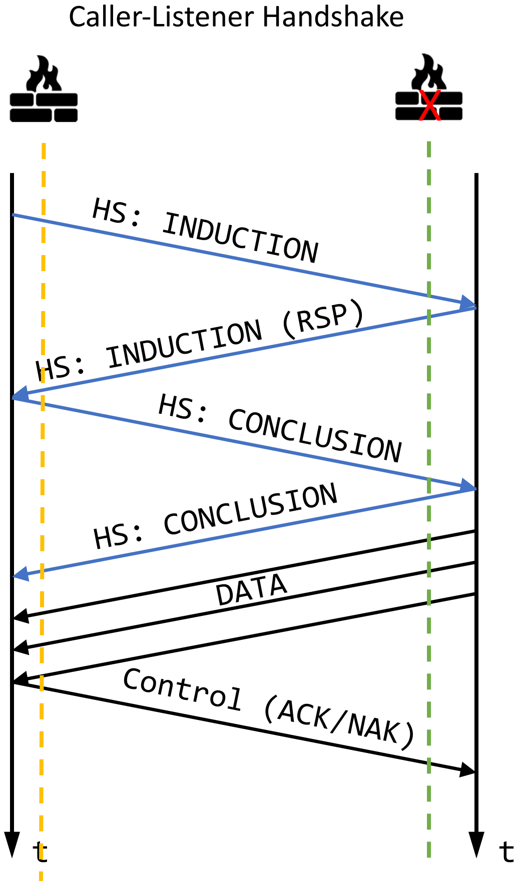
For more info:

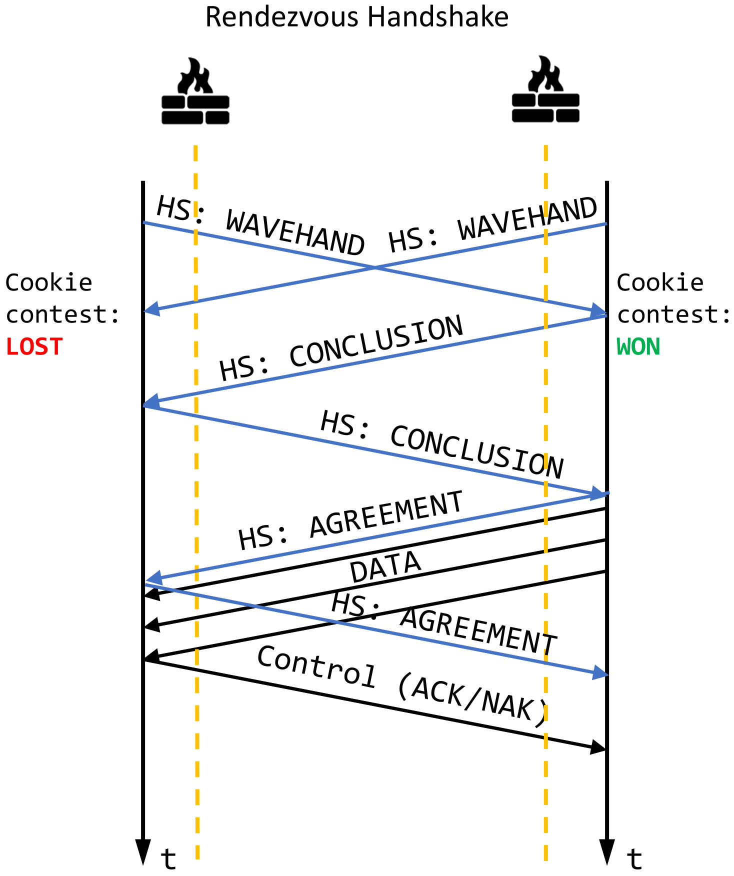
- SRT RFC Draft Proposal
  https://datatracker.ietf.org/doc/draft-sharabayko-mops-srt/
- SRT Technical Overview
  https://github.com/Haivision/srt/files/2489142/SRT_Protocol_TechnicalOverview_DRAFT_2018-10-17.pdf
- SRT Open-source Library
  https://github.com/Haivision/srt
- SRT Alliance
  https://www.srtalliance.org/
- SRT Slack Channel
  https://srtalliance.slack.com/

Live Stream Integrity & Timing



Connection Establishment





Firewall Friendly

Establish quality streams from event centers and unknown locations without IT involvement.

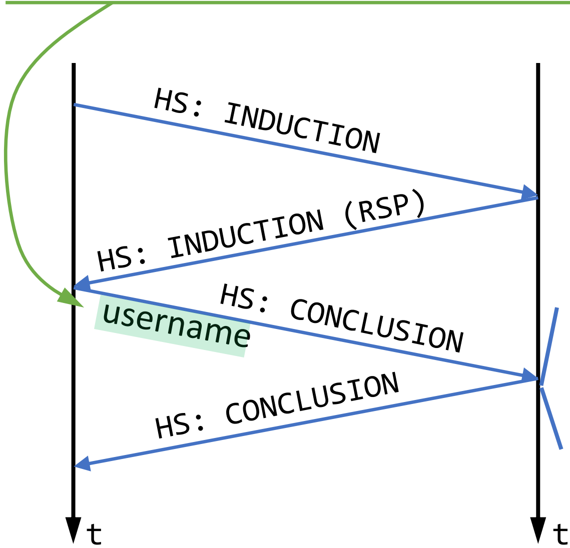
SRT Access Control

The Stream ID free-form value, but there is a recommended convention.

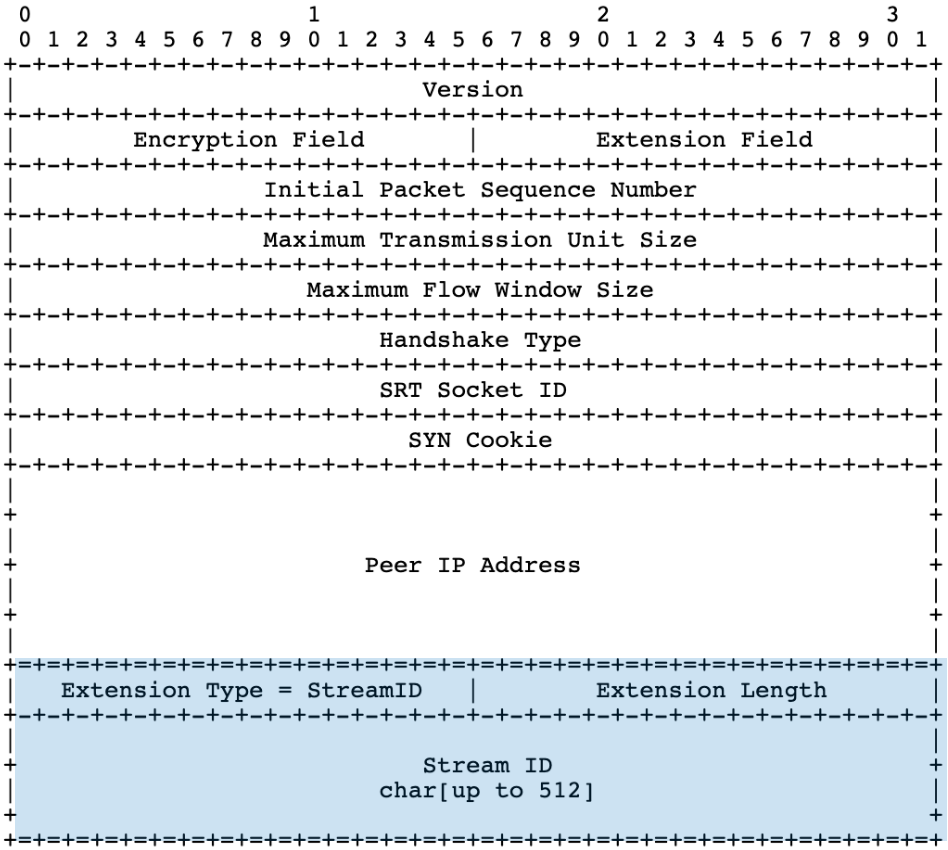
Example content:

requested resource ID

`#!::u=admin,r=ietf_107_srt_overview`



Tell SRT a user-unique **passphrase = F(username)** SRT rejects or accepts the connection



```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Version                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Encryption Field       |        Extension Field        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Initial Packet Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Maximum Transmission Unit Size                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Maximum Flow Window Size                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Handshake Type                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         SRT Socket ID                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           SYN Cookie                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                        Peer IP Address                        +
|                                                               |
+                                                               +
|                                                               |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
|   Extension Type = StreamID   |        Extension Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                           Stream ID                           +
|                        char[up to 512]                        |
+                                                               +
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

https://github.com/Haivision/srt/blob/master/docs/AccessControl.md

SRT Packets

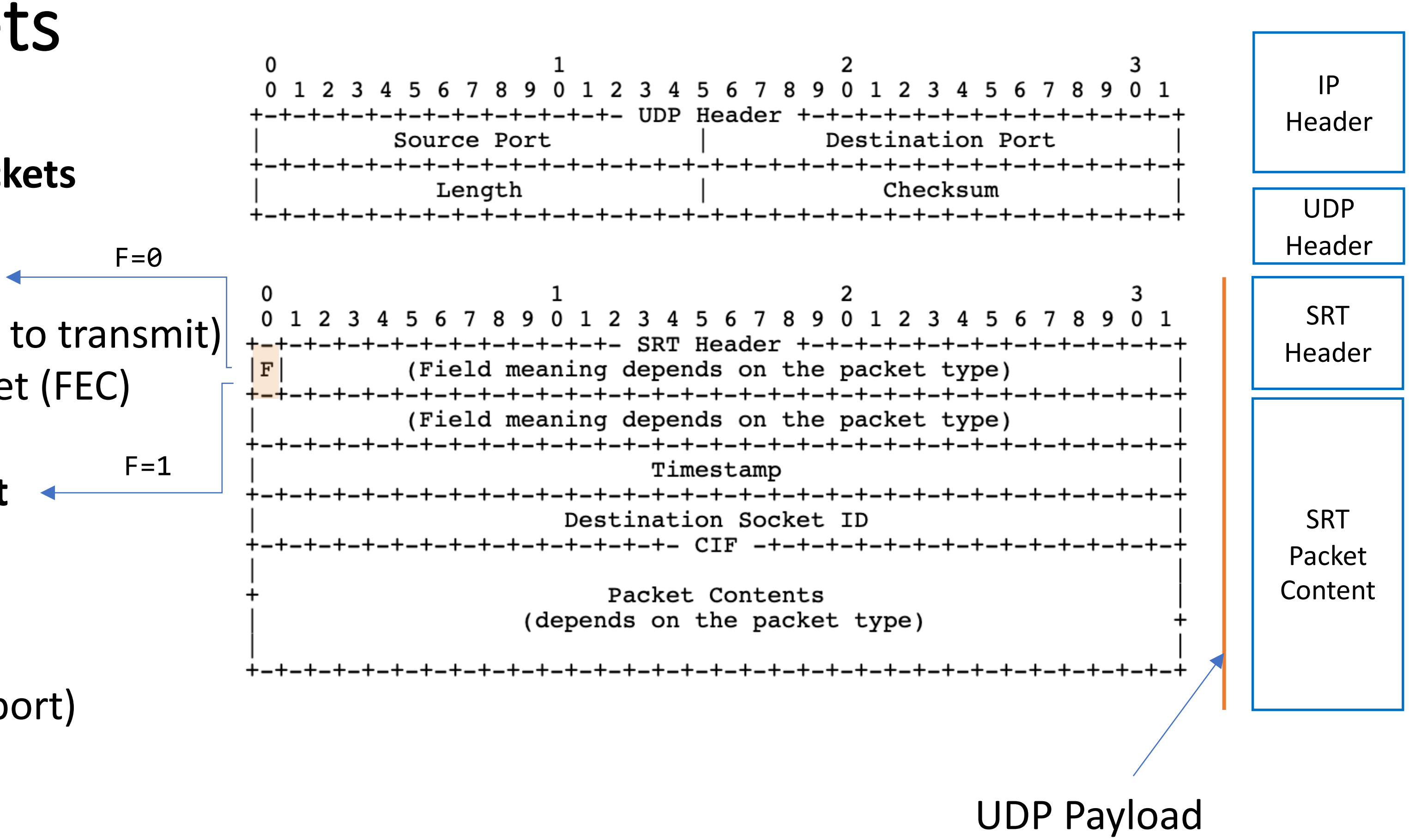
Types of SRT Packets

0: Data Packet

- Data (content to transmit)
- Filtering packet (FEC)

1: Control Packet

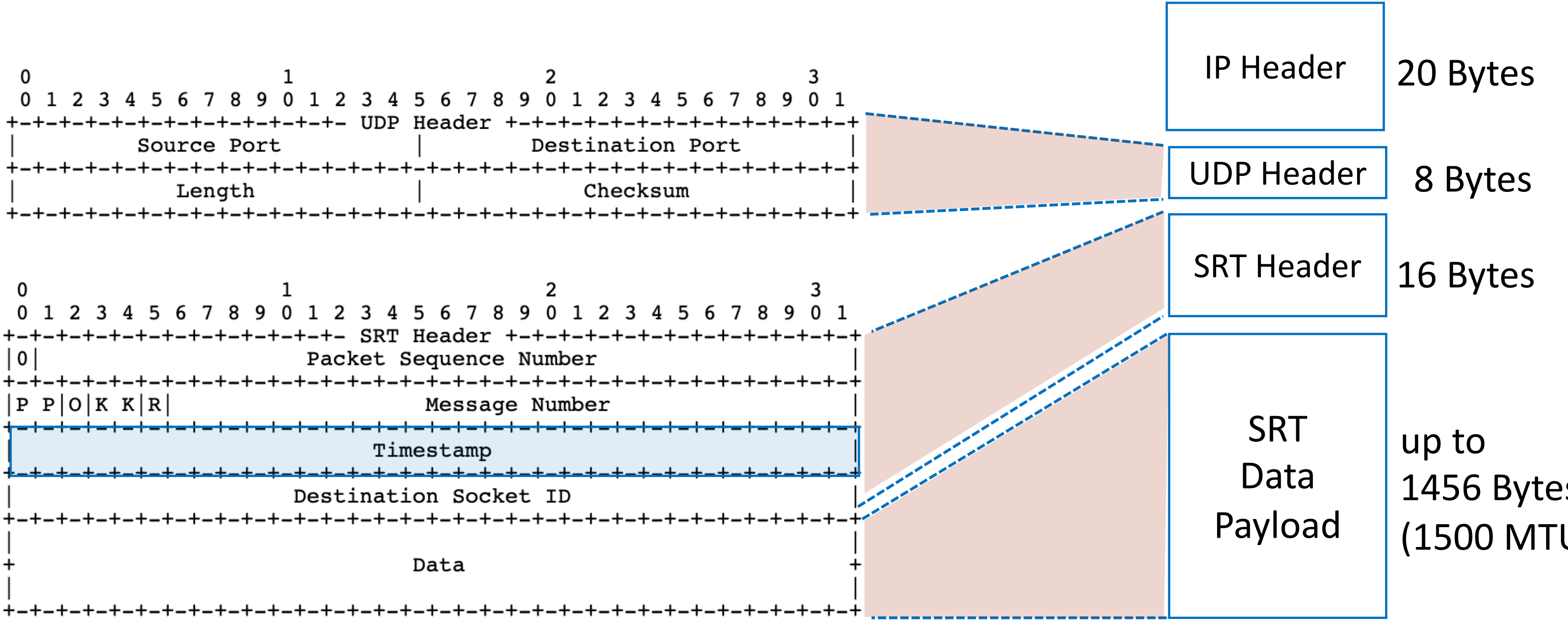
- HANDSHAKE
- KEEPALIVE
- ACK
- NAK (Loss Report)
- SHUTDOWN
- ACKACK



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

 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+- SRT Header +-+-+-+-+-+-+-+-+-+-+-+-+-+
|F|        (Field meaning depends on the packet type)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          (Field meaning depends on the packet type)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Socket ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- CIF -+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                        Packet Contents                        |
|                  (depends on the packet type)                 +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SRT Data Packet



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

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+- SRT Header +-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|                    Packet Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|P P|O|K K|R|                   Message Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Socket ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                              Data                             +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IP Header 20 Bytes

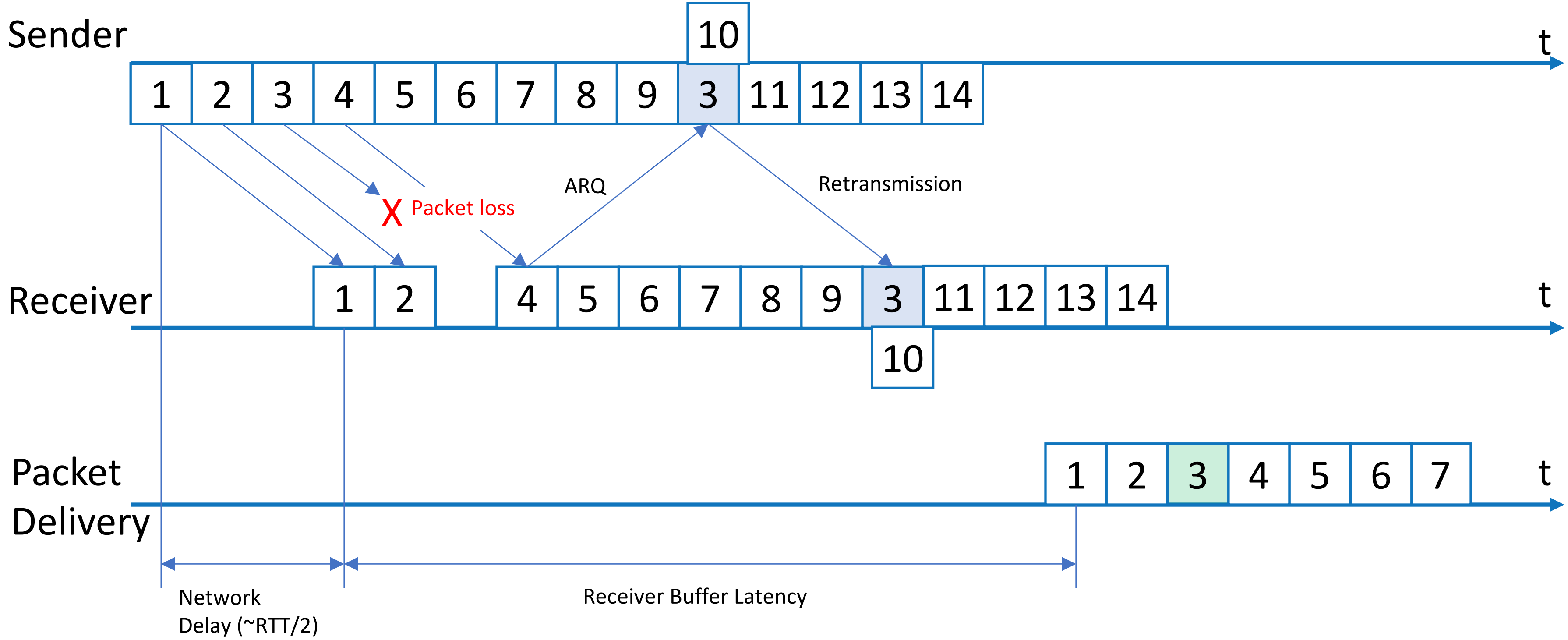
UDP Header 8 Bytes

SRT Header 16 Bytes

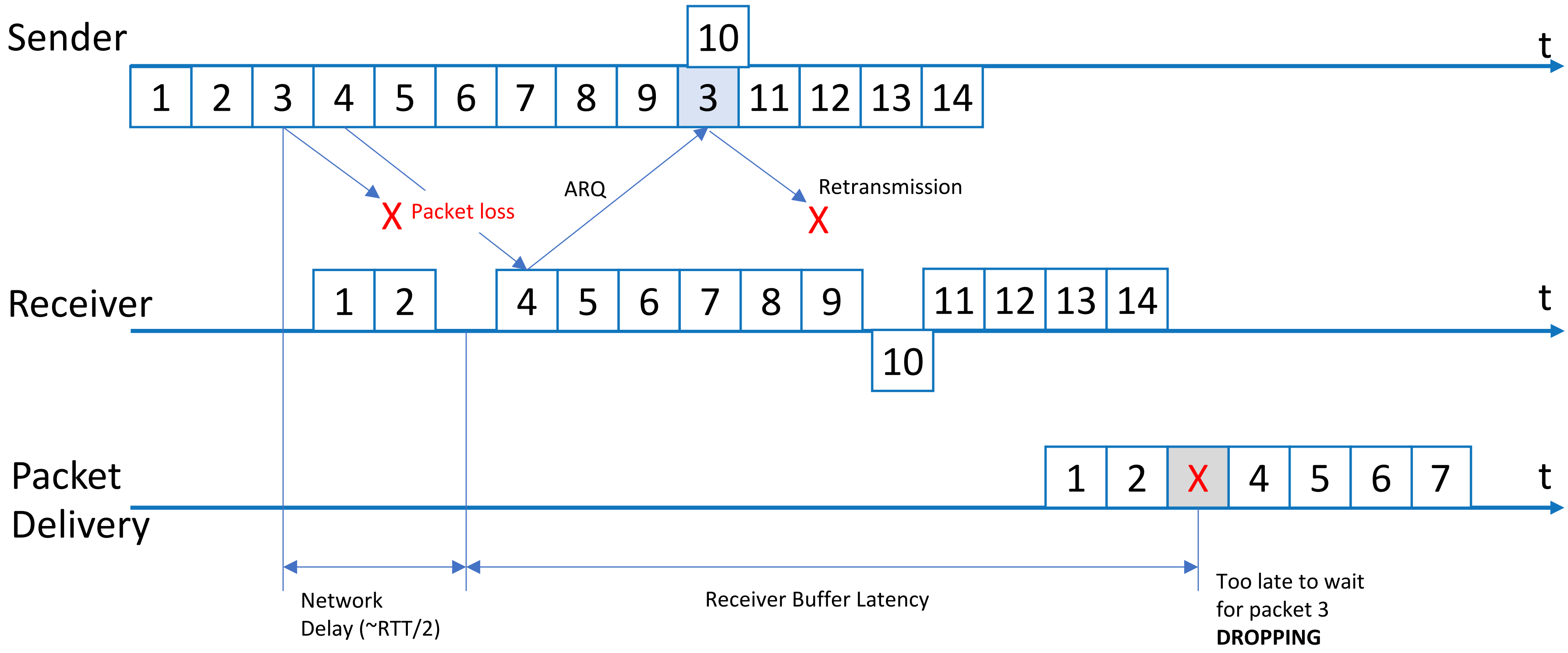
SRT Data Payload

up to
1456 Bytes
(1500 MTU

Timestamp Based Packet Delivery (TSBPD)



Too-Late Packet Drop (TL Packet Drop)



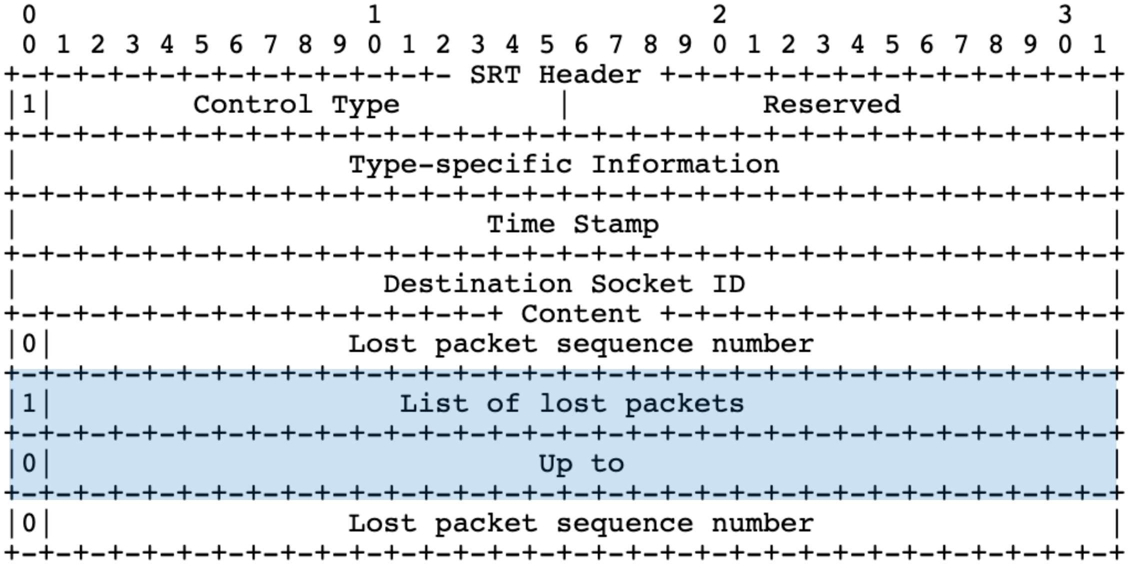
Negative Acknowledgement

Two types of loss reports:

- Loss-triggered NAK reports
- Periodic NAK reports

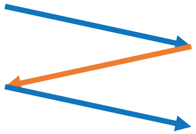
NAK packet can transmit:

- A single lost packet sequence number;
- A range of sequence numbers of lost packets.



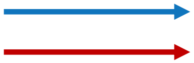
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- SRT Header +-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|        Control Type         |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Type-specific Information                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Time Stamp                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Socket ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ Content +-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|                 Lost packet sequence number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|                    List of lost packets                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|                            Up to                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|                 Lost packet sequence number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Packet Recovery Options



ARQ

- Loss-triggered NAK reports
- Periodic NAK reports



FEC

- Error correction packet
- Packet Filter API allows custom implementation

Bonded connections

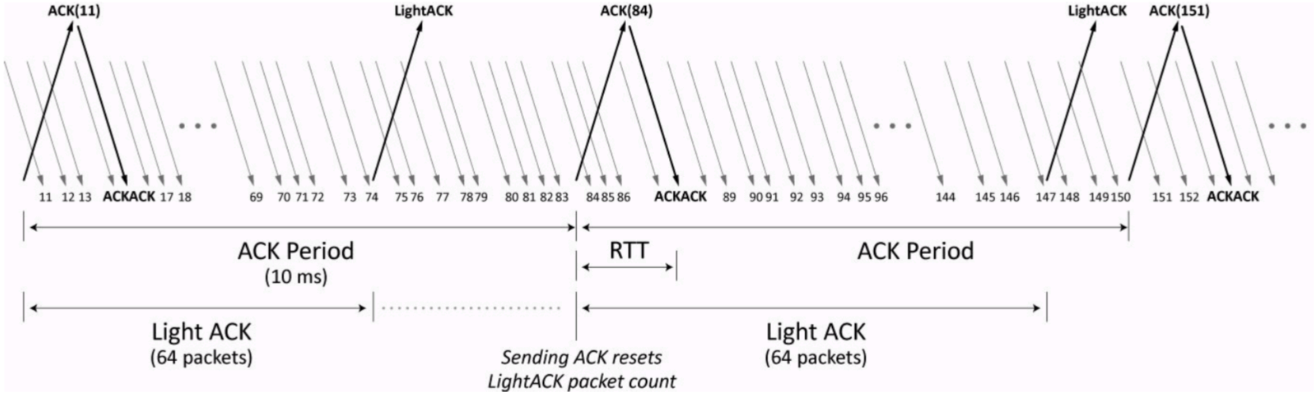
- Broadcast
- Main-backup
- Load balancing

Positive Acknowledgement

- Acknowledge received packet by its sequence number
- Lost packets block further ACK
- ACK is sent every 10 ms
- Additional info: RTT, Link Capacity, …
- Full ACK is sent every 10ms
- Light ACK is sent on every 64 pkts

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+- SRT Header +-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|         Control Type        |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Type-specific Information                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Time Stamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Socket ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- CIF -+-+-+-+-+-+-+-+-+-+-+-+-+
|            Last Acknowledged Packet Sequence Number           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              RTT                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          RTT variance                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Available Buffer Size                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Packets Receiving Rate                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Estimated Link Capacity                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Receiving Rate                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Light ACK



Congestion Control

Sender gets from the receiver:

- NAK packet to determine losses
- ACK packets (every 10 ms) to get updates on:
  - RTT
  - RTT variance
  - Estimated link capacity
  - Available receiver buffer
  - Receiving rate
- Congestion control can use this feedback to make decisions!

Stream Multiplexing and Bidirectional Transmission

Both peers know each other’s IP and **SRT Socket ID** to communicate with data and control packets in both directions.

Handshake Packet

Data Packet

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+- SRT Header +-+-+-+-+-+-+-+-+-+-+-+-+
|0|                    Packet Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|P P|O|K K|R|                   Message Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination Socket ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                              Data                             +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

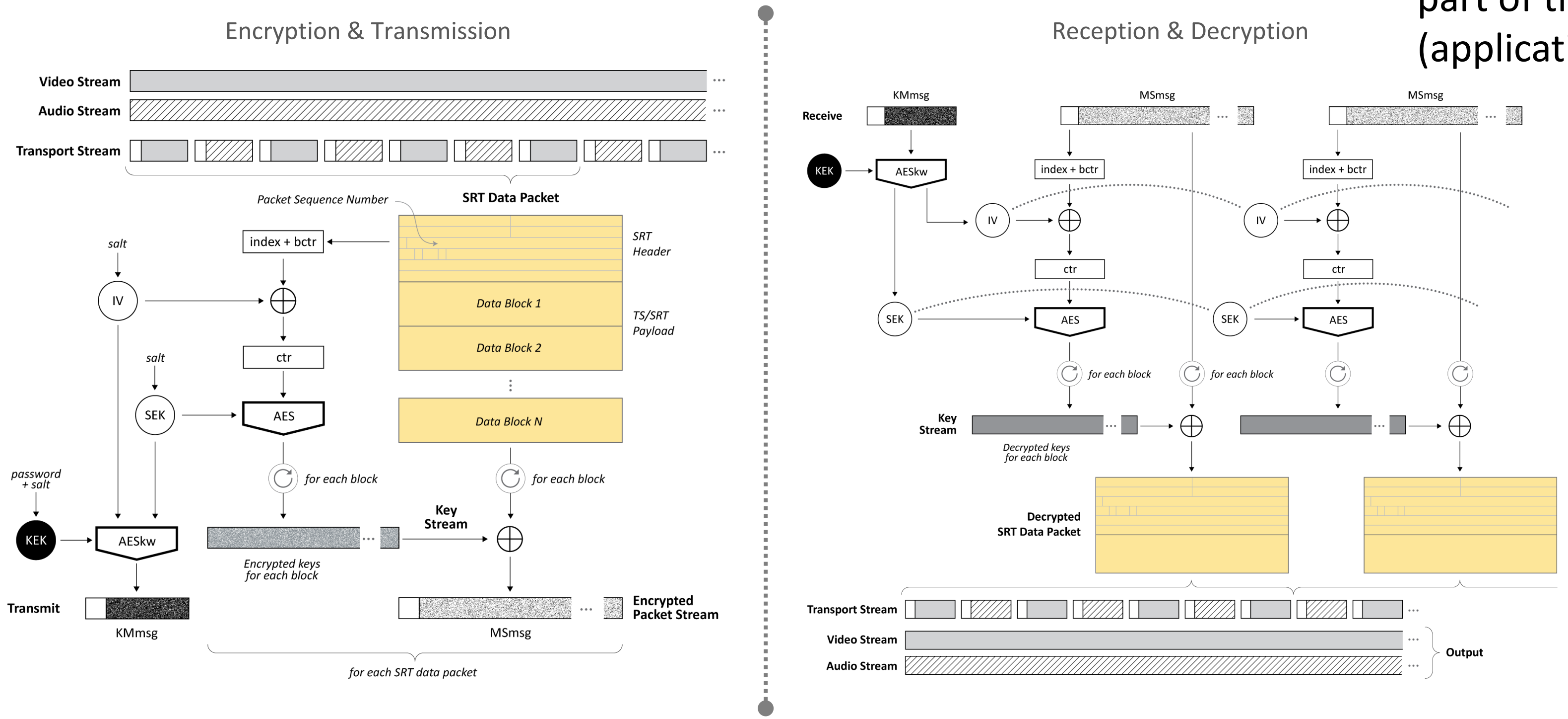
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Version                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Encryption Field       |        Extension Field        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Initial Packet Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Maximum Transmission Unit Size                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Maximum Flow Window Size                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Handshake Type                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         SRT Socket ID                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           SYN Cookie                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                        Peer IP Address                        +
|                                                               |
+                                                               +
|                                                               |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
|         Extension Type        |        Extension Length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                       Extension Contents                      +
|                                                               |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Security & Encryption

Refer to SRT Technical Overview

https://github.com/Haivision/srt/files/2489142/SRT_Protocol_TechnicalOverview_DRAFT_2018-10-17.pdf

- AES 128/192/256-bit encrypted
- Payload encrypted with cipher in AES-CTR mode
- Secret/pass-phrase is not part of the protocol (application layer)



Encryption & Transmission
Video Stream
Audio Stream
Transport Stream
Packet Sequence Number
SRT Data Packet
SRT Header
Data Block 1
Data Block 2
Data Block N
TS/SRT Payload
salt
index + bctr
IV
ctr
salt
SEK
AES
for each block
for each block
password + salt
KEK
AESkw
Key Stream
Encrypted keys for each block
Transmit
KMmsg
MSmsg
Encrypted Packet Stream
for each SRT data packet
Reception & Decryption
KMmsg
MSmsg
MSmsg
Receive
KEK
AESkw
index + bctr
index + bctr
IV
IV
ctr
ctr
SEK
SEK
AES
AES
for each block
for each block
Key Stream
Decrypted keys for each block
Decrypted SRT Data Packet
Transport Stream
Video Stream
Audio Stream
Output