Reliable Internet Stream Transport Main Profile Description

Adi Rozenberg
VideoFlow Ltd.
Ciro A. Noronha, Ph.D.
Cobalt Digital Inc

Agenda

- RIST Timeline
- What is Available in Simple Profile
- Overview of Main Profile Features
  - Tunneling and Multiplexing
  - Security
  - Bandwidth Optimization
  - Support for high bitrate/high latency links
- Interop tests
- Application examples

RIST Timeline

- February 2017: RIST AG is created during VidTrans
- April 2017: First face-to-face meeting at NAB
- April 2018: First draft of Simple Profile approved during face-to-face meeting at NAB
- May 2018: Interop demo during VSF May Meeting at Cisco in San Jose, CA
- July 2018: Second draft of Simple Profile approved and implemented
- September 2018: Public Interop demo at IBC
- October 2018: RIST Simple Profile published as VSF TR-06-1
- April 2019: Public Interop demo at NAB (commercial products)
- September 2019: Main Profile draft approved and demonstrated at IBC (to be published as VSF TR-06-2)

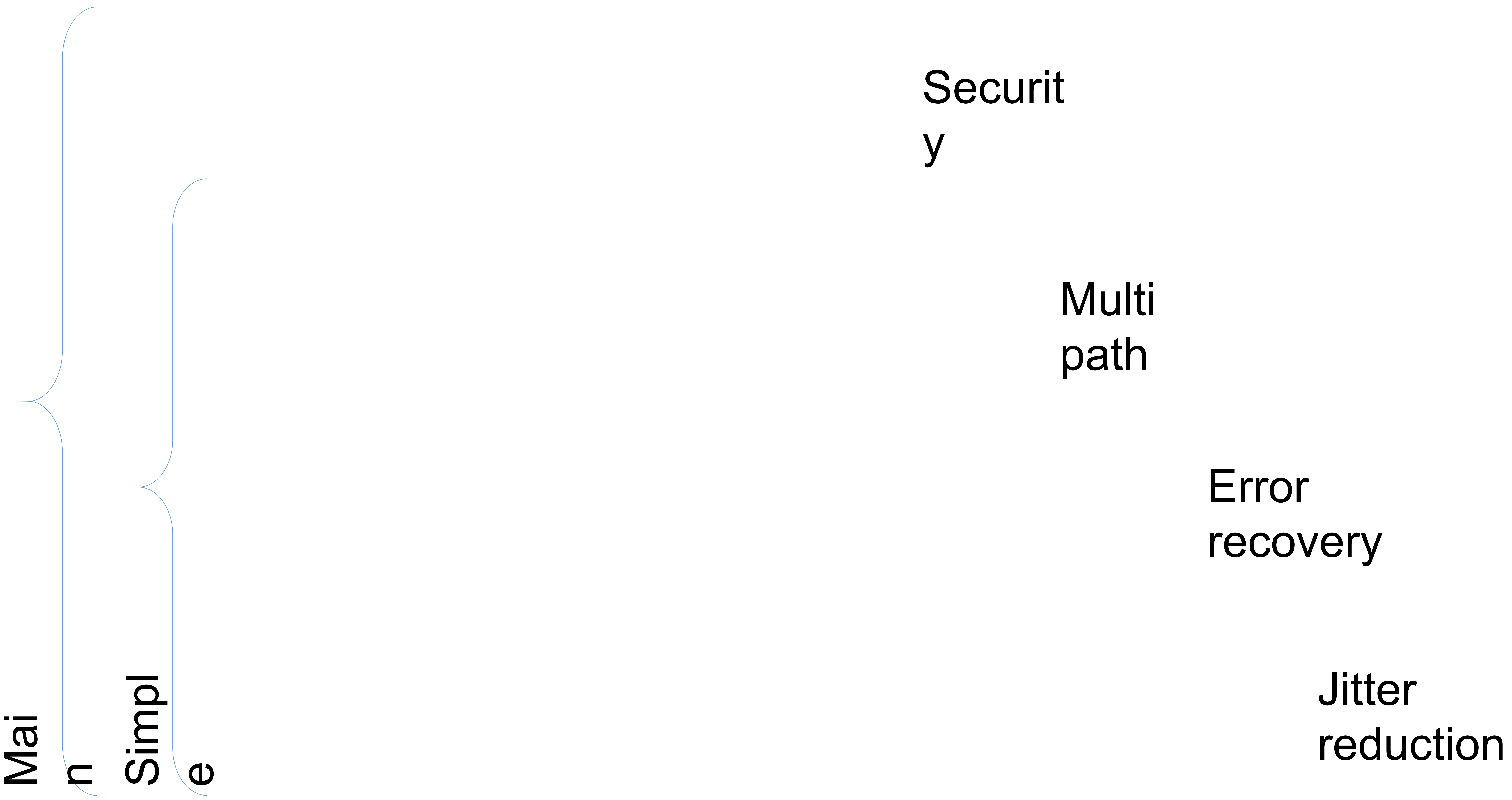
What's in RIST Simple Profile?

- Basic compatibility with non-RIST systems using RTP
- Top of the line packet loss recovery using NACK-based ARQ
  - Bandwidth efficient
  - Tunable tradeoff between latency and protection
- Multi-link support
  - Bonding: combine multiple links to achieve higher bandwidth
  - Seamless Switching: send streams through redundant paths to protect against network failures
- Multicast Support
- SMPTE 2022-1/2 FEC native support

VideoFlow

VSF
VIDEO SERVICES FORUM

The foundation of reliable streaming



Mai
n

Simpl
e

Securit
y

Multi
path

Error
recovery

Jitter
reduction

What is coming with Main Profile

- Use tunneling over UDP connection
  - Use a tunnel to deliver native multicast or unicast
- Encryption
  - Protect high-value streams in flight on the Internet
- Authentication
  - Make sure that the other endpoint is who you think they are
- Simplify Firewall Configuration
  - Use of a single connection to deliver egress and ingress simultaneously
  - One UDP port in, with less work for IT
- Provide optional in-band control
  - Technician can “ride” the connection back and manage the equipment
- Support scenarios with high (bitrate x latency) conditions
- Extract further bandwidth optimization
  - Don’t transmit NULL packets, re-create them on the other side

Tunneling and Multiplexing

- Purpose: combine one or more Simple Profile flows, plus optional arbitrary data traffic, into a single network flow using UDP
- Advantages:
  - Only one UDP port needs to be configured in the firewall, regardless of the number of flows
  - Only one encryption session is required to protect the whole set of streams and data
  - Session can be initiated from either tunnel endpoint
  - Tunnel is bidirectional
  - The same infrastructure can be optionally used for in-band control
    - SNMP, Web, or any other management traffic

Tunneling Technology in RIST

- RIST has selected GRE over UDP (RFC 8086) for tunneling
- Two modes:
  - **Full Datagram Mode:**
    - A complete (layer-3) IP packet is encapsulated
    - Supports end-to-end transport of addresses and ports
    - Supports end-to-end transport of any IP packets (for in-band control and generic routing)
    - Overhead: 32 bytes (2.4% over a 7-TS RTP packet)
  - **Reduced Overhead Mode:**
    - Includes only UDP source/destination ports
    - Supports only RIST streams – destination is the endpoint
    - Overhead: 8 bytes (0.6% over a 7-TS RTP packet)

RIST main Profile message sizes

Encapsulation header

RIST packet / Non RIST packet

PSK mode Full datagram + Sequence + key

IP header | UDP header 8B | GRE header 12B | IP header 20B | UDP header | RTP Packet | Any Packet

Full datagram + Sequence

IP header | UDP header 8B | GRE header 8B | IP header 20B | UDP header | RTP Packet | Any Packet

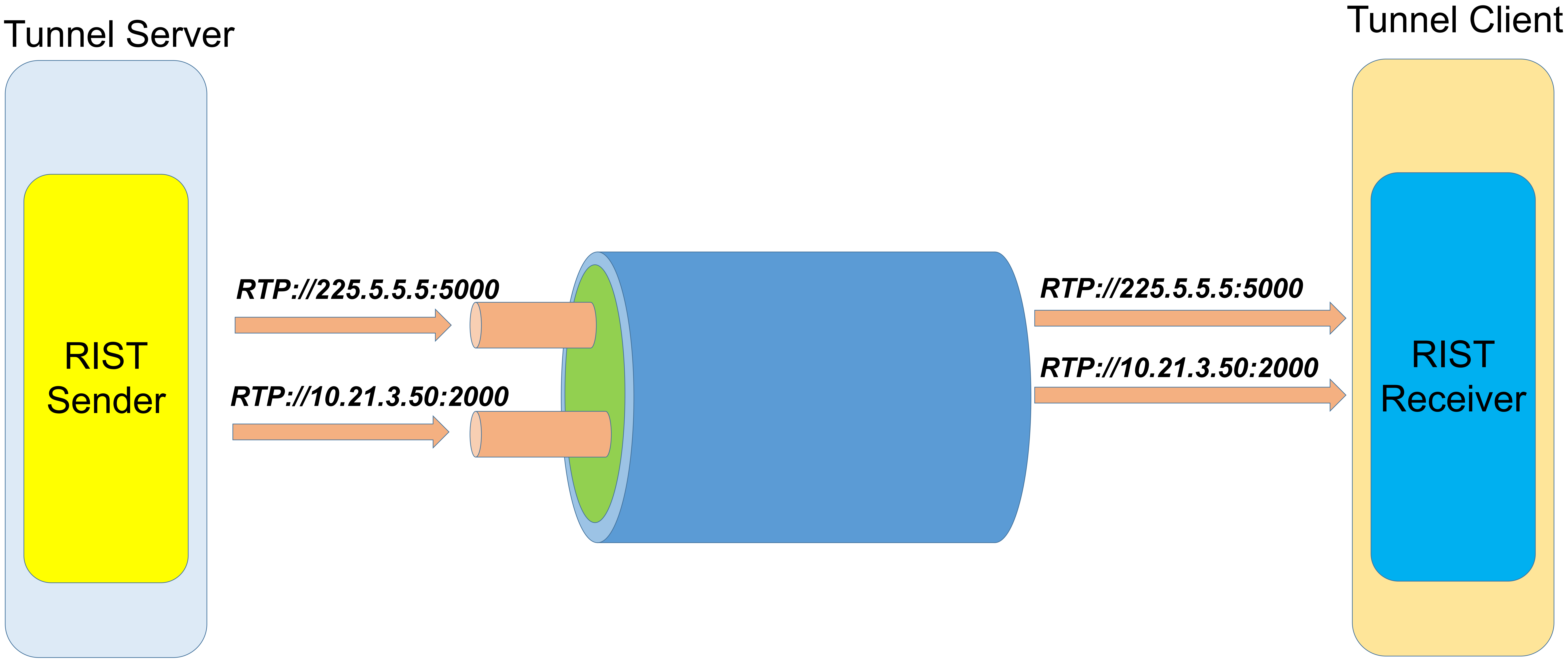
Full datagram

IP header | UDP header 8B | GRE header 4B | IP header 20B | UDP header | RTP Packet | Any Packet

Reduce datagram

IP header | UDP header 8B | GRE header 4B | UDP header | RTP Packet

Tunnel Example: Unicast/Multicast Mix

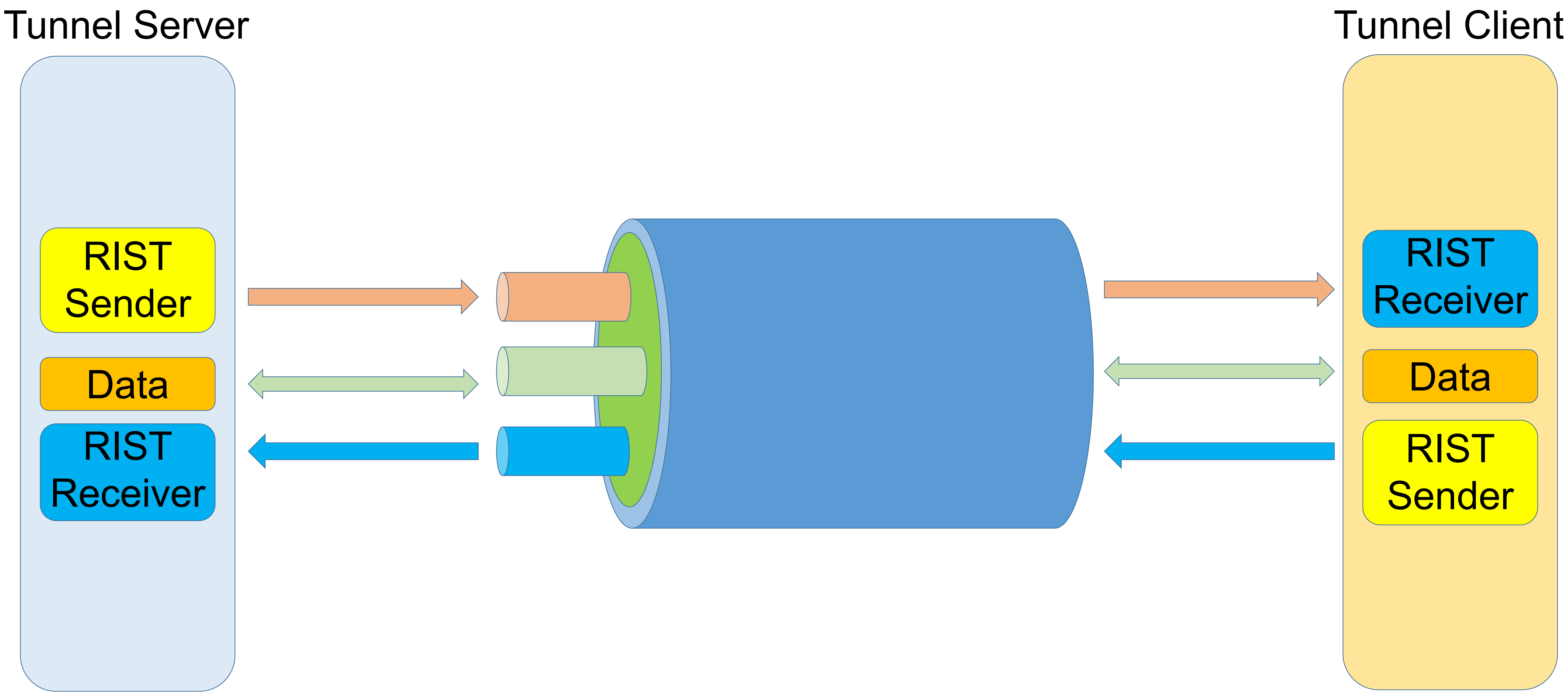


- Connection is initiated by RIST Receiver Side
  - This is not supported in Simple Profile!
- Two independent streams are sent

VideoFlow

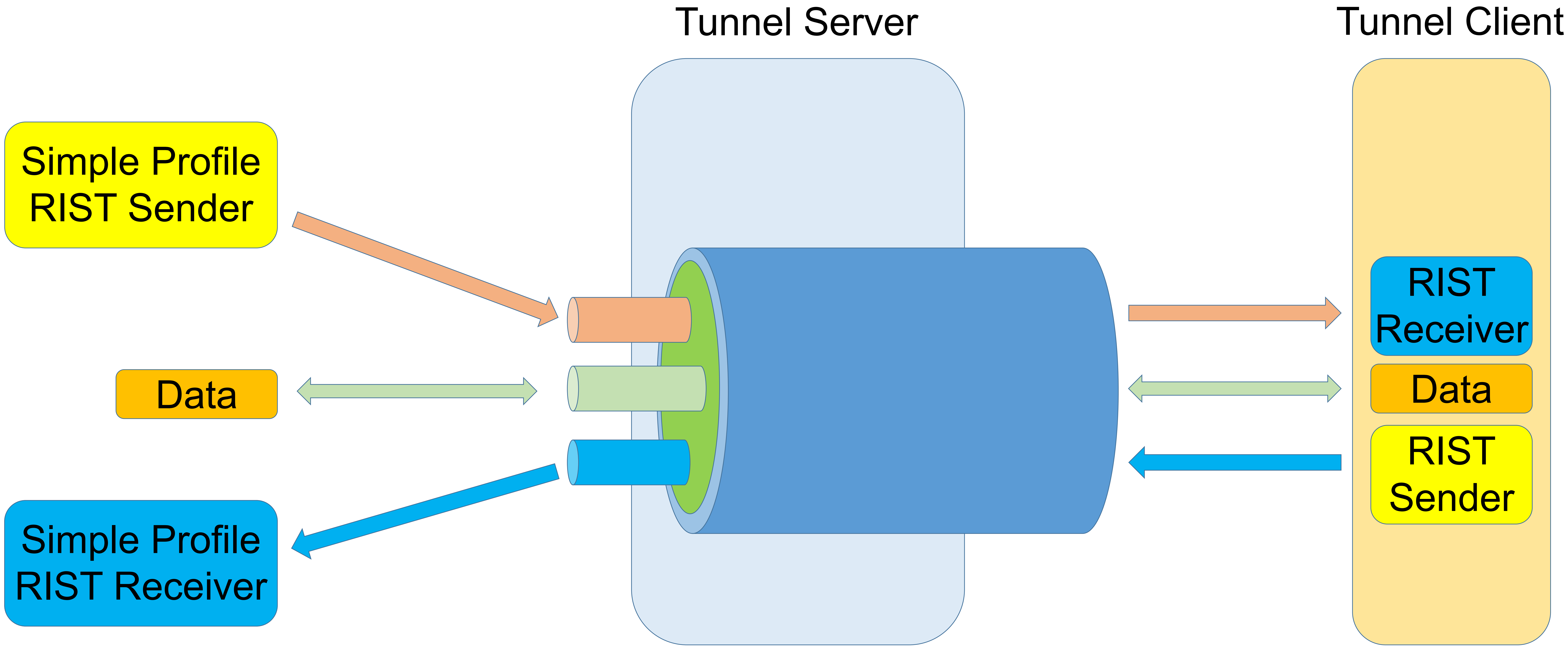
VSF VIDEO SERVICES FORUM

Tunnel Example: Bidirectional Plus Data

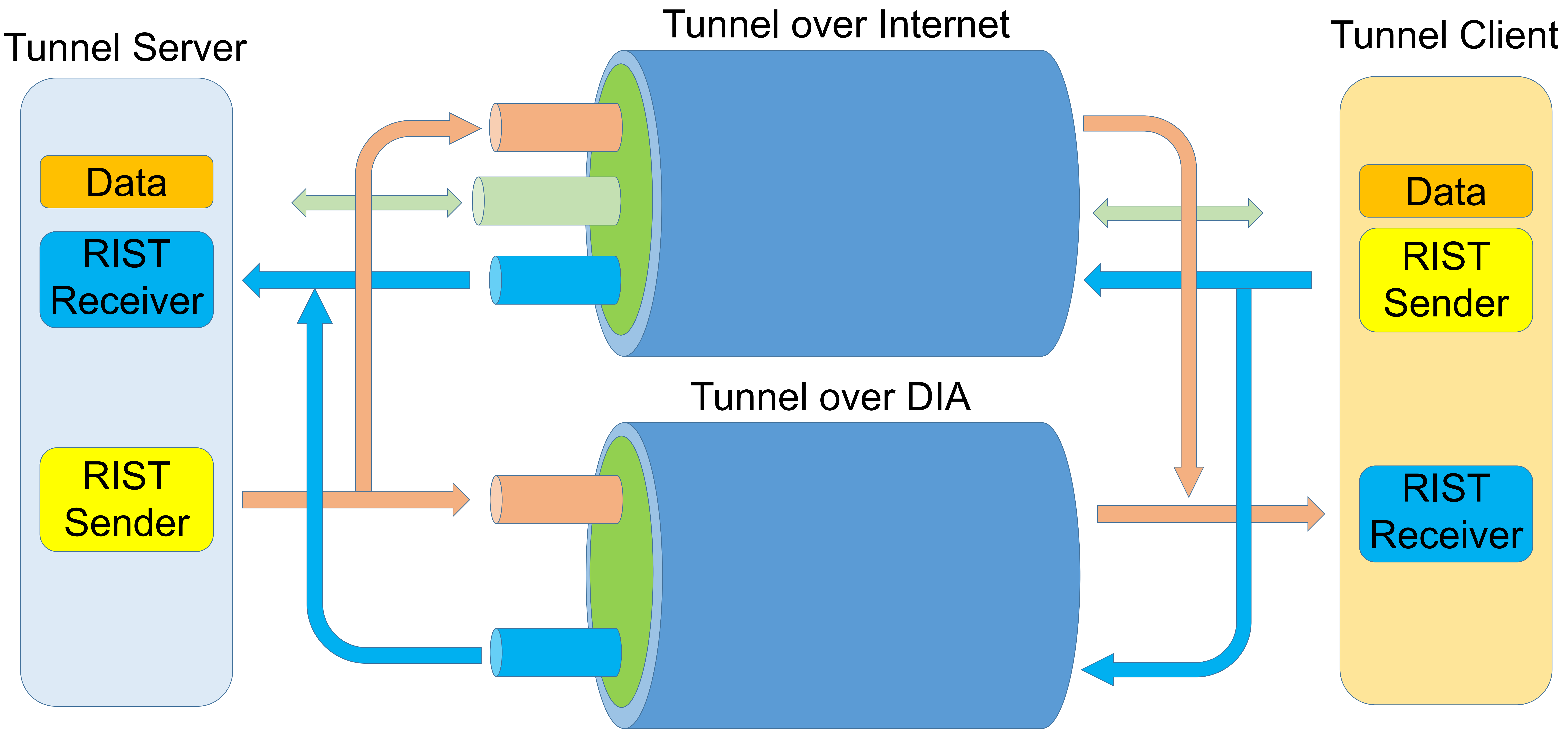


- Tunnel Client starts the connection
- Streams are sent in both directions
- Data is sent in both directions (remote management)

Tunnel Example: Smart Gateway



Tunnel Example: Bonded Tunnels



Optional Tunnel Negotiation

Tunnel Client
Tunnel Server
JSON Keep Alive:
JSON Keep Alive:

```
"tunnelIP": "10.0.0.2",
 "remoteIP": "10.0.0.3",
 "excludedIP": ["192.168.1.0/24",
"10.10.10.0/25"],
"routing": true,
 "pskRotation": 600,
 "vendor":
    {   “Implementation":
      {      "version": "2.3.5",
        "product": “HEVC ENCODER",
       "vendorName": “COBALT INC." )),
```

```
"tunnelIP": "10.0.0.3",
 "remoteIP": "10.0.0.2",
 "excludedIP": ["192.168.1.0/24",
"10.10.10.0/25"],
"routing": true,
 "pskRotation": 600,
 "vendor":
    {   “implementation":
      {      "version": “4.0.5",
        "product": “DIGITAL VIDEO GATEWAY",
       "vendorName": “VIDEO-FLOW.LTD." )),
```

Content Protection: Encryption

- Valuable content must be protected while traveling on the Internet
  - In many cases, this is a contractual requirement
  - Solution: encrypt the content!
- Different parts of the world have varying legal constraints in what is allowed for encryption
  - There is no “one size fits all” solution
  - Multiple options need to be provided
- Any solution must have the possibility of a fallback
  - Content needs to go on air “right now”
- Fixed-key operation must also be supported
  - One-to-many scenarios

Authentication

- Make sure that the endpoint you are talking to is who you think they are!
- Some scenarios:
  - Reporter transmitting from the field
    - Publishing point is open on the Internet
    - Is it really him/her?
  - Remote feed going on-air
    - Publishing point is open on the Internet
    - Can someone hijack this and push their own content?
- Endpoints need to (optionally) be authenticated!

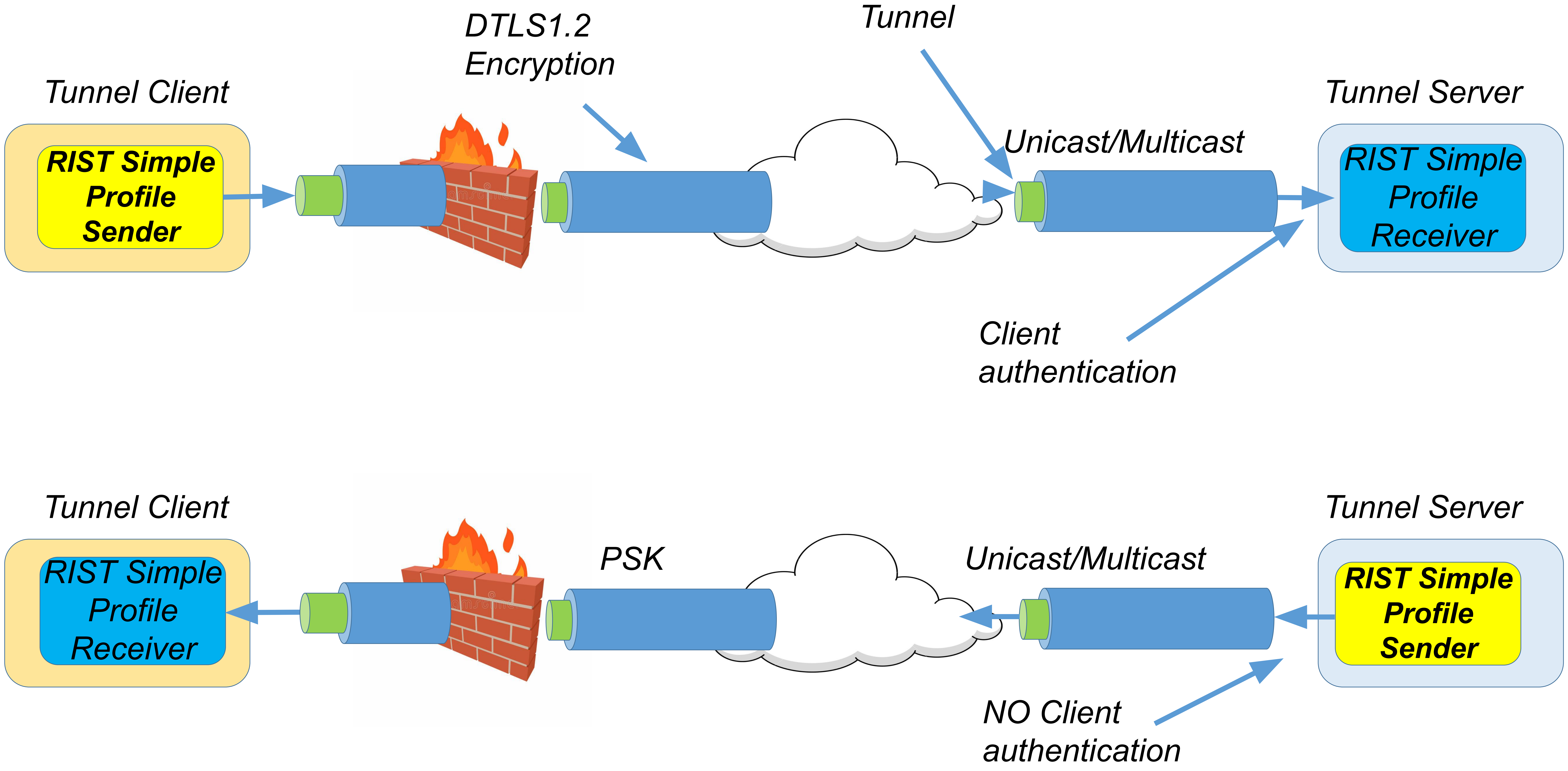
DTLS encryption

- RIST selected the Datagram Transport Layer Security (DTLS) technology for both encryption and authentication
- Advantages:
  - Datagram (UDP) version of the TLS technology already used in the Internet
  - Mature and well-vetted
  - Ability to select multiple cyphers to match requirements
    - RIST defines a minimum list that all vendors must support
    - Vendors are free to add other cyphers
- DTLS is applied to the tunnel

DTLS required Cypher Suites

- A subset of cypher suites has been selected, and all vendors must support them
- These include:
  - AES 128
  - AES 256
  - No Encryption (for testing or **optional** fallback)
- Good compromise between encryption strength and ability to adhere to local legal requirements
- Individual vendors are free to add to the list

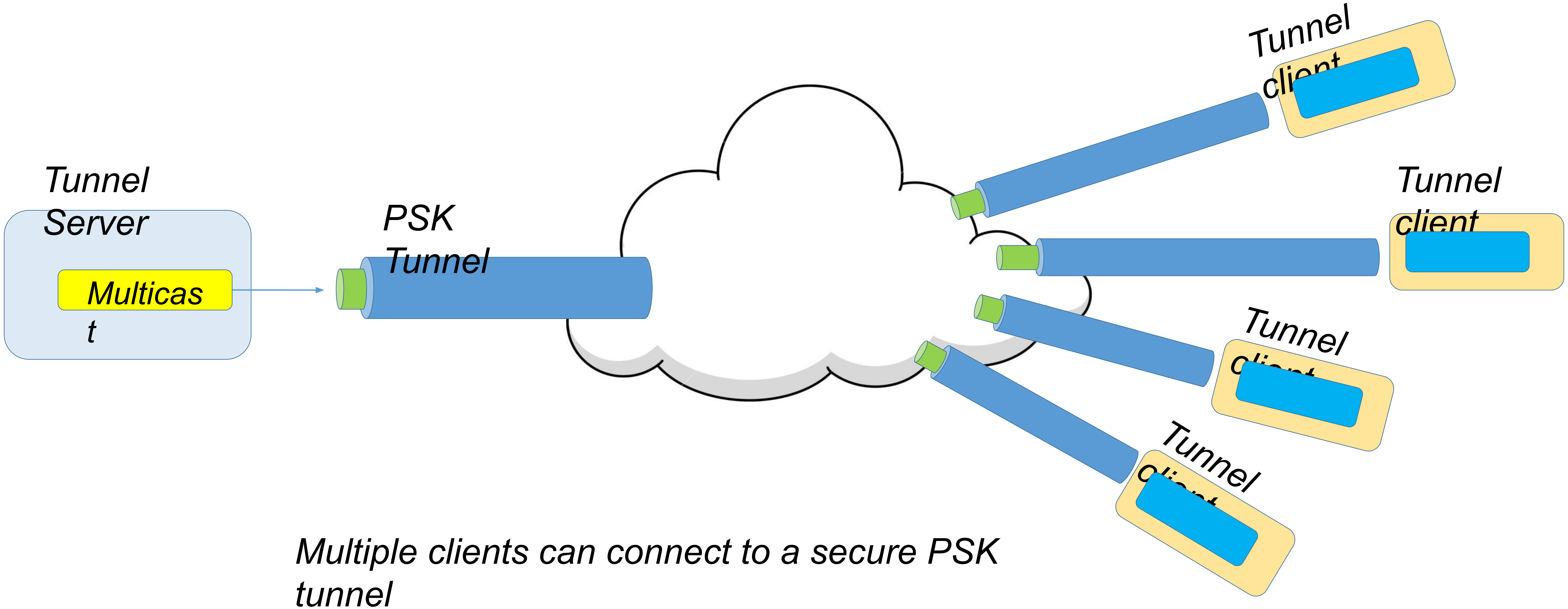
Tunnel Encryption



Pre-Shared Key (PSK) Operation

- RIST Main Profile supports Pre-Shared Key operation
- Details:
  - AES 128/256-CTR encryption
  - Key derived from pre-shared passphrase
  - Support for rotating keys
    - Very important for security
    - Minimum key rotation every GRE sequence 32-bit wrap
    - Key rotation period is configurable or user initiated for extra security
  - Support for on-the-fly change of passphrase
    - Used to de-authorize a subset of receivers, if needed
- Suitable for one-to-many and unidirectional environments

Point to Multipoint secure distribution



Multiple clients can connect to a secure PSK tunnel

RIST Main Profile stages

Stream

- Simple receiver
- Simple sender
- RTP extended header sender
- RTP extended header receiver

Packet mode

- Full Datagram
- Reduce mode

Tunnel

- Configuration
- Tunnel
- Keep A live

Authentication

- No Authentication
- Self Signed
- Known CA

Encryption

- DTLS AES256
- DTLS AES128
- DTLS No Encryption
- PSK AES256
- PSK AES128
- No Encryption

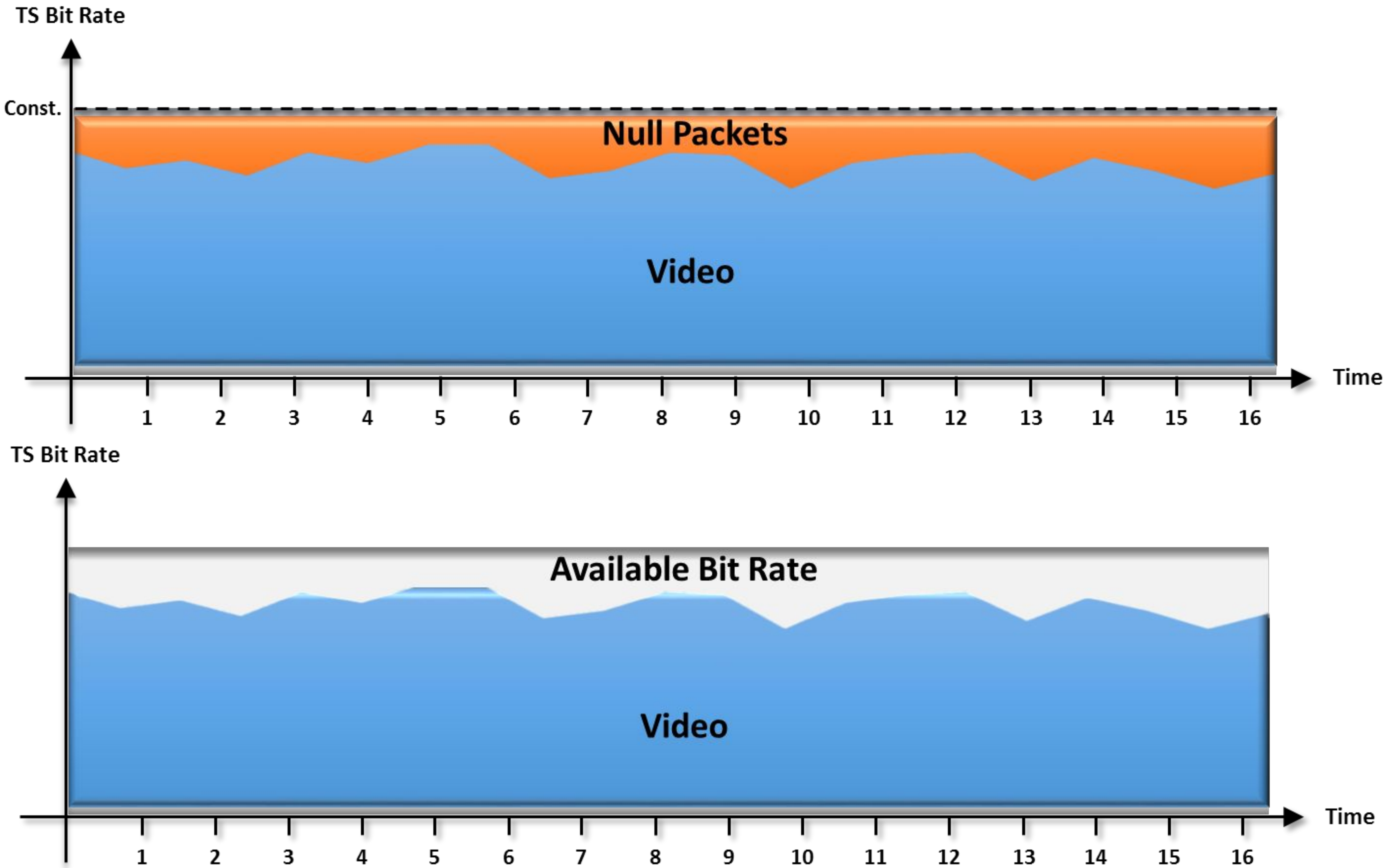
VideoFlow

VSF VIDEO SERVICES FORUM

Bandwidth Optimization

- MPEG Transport Streams typically have about 5% NULL packets
- NULL packets have no data (padding), but are necessary to keep stream timing
- NULL packet bandwidth can be reclaimed as follows
  - Remove NULL packets before transmitting, but keep track of their exact locations
  - Transmit a (possibly) smaller packet with flags to indicate the original location of the NULL packets
  - On reception, insert NULL packets in the indicated locations
- Allowed by ISO/IEC 13818-1 section 2.4.1

NULL Packet Deletion



VideoFlow

VSF
VIDEO SERVICES FORUM

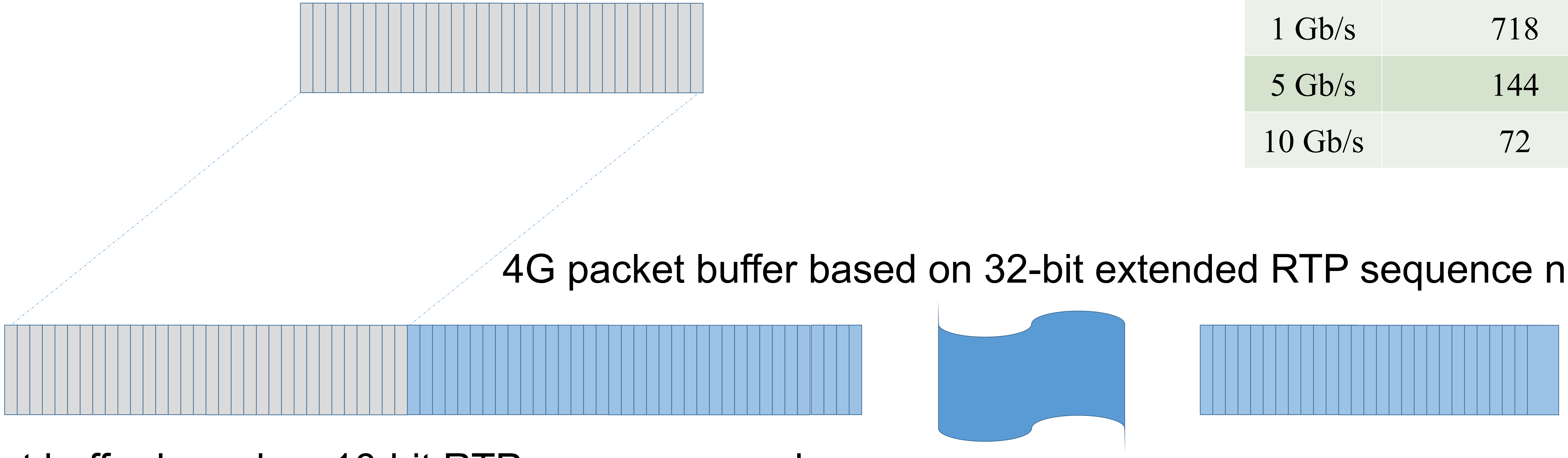
Extensions for High Bit Rate Operation

- RIST Simple Profile uses RTP, which has a 16-bit sequence number
- This limits the NACK window to 64K packets
- At high bit rates, this will be insufficient to accommodate typical network latencies
- RIST Main Profile includes header extensions to bring the sequence number to 32 bits (4G packets)

Header Extension Example

Bit Rate	Window at 64K Packets (ms)	Max RTT at 7 Retries (ms)
100 Mb/s	7183	1026
1 Gb/s	718	103
5 Gb/s	144	21
10 Gb/s	72	10

64K packet buffer based on 16-bit RTP sequence number



4G packet buffer based on 32-bit extended RTP sequence number

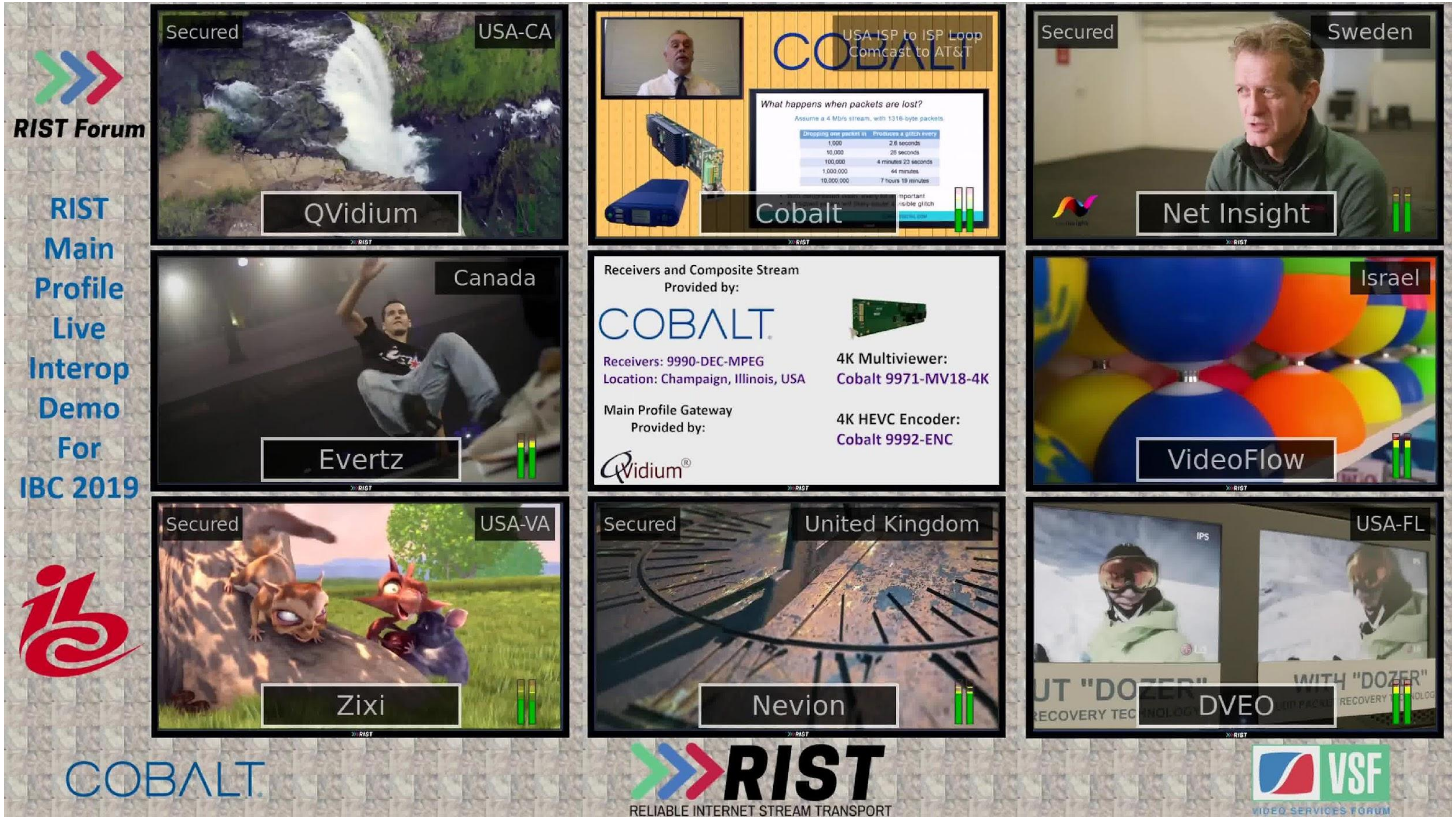
64K packet buffer based on 16-bit RTP sequence number

RIST Main Profile Status

- IBC Interop Demo available on YouTube
  - Implementations from Cobalt, DVEO, Evertz, Net Insight, Nevion, Qvidium, VideoFlow and Zixi
  - Streams running over the Internet from multiple locations in the world to the Cobalt HQ in Champaign, Illinois, USA
  - Technology demonstrations:
    - GRE tunneling
    - DTLS encryption
- VSF TR-06-2 Main Profile Specification approved at the Activity Group level
  - Next step is approval from the VSF board
  - Publication is expected in the next few months
  - Full functionality demo planned for VidTrans in Feb 2020

VideoFlow

VSF VIDEO SERVICES FORUM



RIST Forum

RIST Main Profile Live Interop Demo For IBC 2019

Receivers and Composite Stream Provided by:

COBALT

Receivers: 9990-DEC-MPEG
Location: Champaign, Illinois, USA

Main Profile Gateway Provided by:

QVidium

4K Multiviewer:
Cobalt 9971-MV18-4K

4K HEVC Encoder:
Cobalt 9992-ENC

VideoFlow

VSF
VIDEO SERVICES FORUM

Extensive interoperability test suite

- To ensure rapid market deployment, the RIST AG agreed on extensive and comprehensive test suite:
  - Tunnel only
  - Tunnel + DTLS modes
  - Tunnel + PSK
  - Inner IP negotiation
  - Null Packet Deletion
  - Disconnect and reconnect
  - Advance KeepAlive messaging
  - 32Bit extended header
- Suite includes over 150 tests to assure interoperability

Applications

- Stream securely and reliable from any location to main NOC/Cloud
- Stream securely from the cloud to anywhere
- Bidirectional remote PTZ camera interview
- Unified encrypted streaming to many receivers
- Using lower bandwidth overhead
- Checkout https://www.rist.tv/articles-and-deep-dives/2019/9/25/paper-rist-main-profile-overview for more information

How to join the activity

- Participation is Free
- Contact The VSF to join the RIST Activity Group
  - Contact Bob Ruhl
- Optional Join the RIST forum to promote the multi vendor and client collaboration
  - Register your company at https://www.rist.tv/join

THANK YOU!

Contact Info:
Adi.Rozenberg@video-flow.com