An Overview of the Reliable Internet Stream Transport (RIST)

Ciro A. Noronha, Ph.D.
Cobalt Digital Inc.

Presenter

Dr. Ciro Noronha

Ph.D. in Electrical Engineering from Stanford University

Worked in Compression Since 1995

Engineering Director/Vice President At:
Optivision, SkyStream, Tandberg Television and Ericsson

Founder of ImmediaTV
Maker of Encoders, Decoders, and other compression devices

Current EVP of Engineering at Cobalt Digital
Member of the RIST AG, editor of the RIST Specifications
President of the RIST Forum for 2020-2022

The Players

VIDEO SERVICES FORUM

All the companies in the RIST AG also participate in the RIST Forum

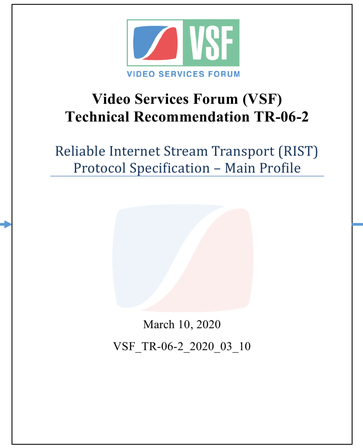
RIST Forum

180+ Companies

RIST Activity Group

The tech people

RIST Specification



The marketing people

What is the Problem?

- I want to use the Internet as a **cost-effective** means of transporting high-quality, **broadcast-grade video**
- But:
  - The delivery through the Internet is not guaranteed, video may glitch
  - I need to be able to use any link or combination of links anywhere to move my content
  - Many solutions add a lot latency (not useful for live cases)
  - I need my content to be protected so it doesn’t get stolen
  - Bad people must not be able to hijack my feed (send their content instead of mine)
  - My IT people are very busy, this must be easy and straightforward for them to set up

Other People Have Solutions Like This …

- A number of solutions that meet many of these requirements have been available for a while from different vendors
  - Why is RIST different?
- RIST was designed as a **joint effort** between many of the leading companies that provide video delivery over the Internet:
  - Experts with hundreds of man-years of experience freely contributed to the effort
  - Best-of-class technologies in every aspect of the protocol, while following established standards wherever possible
  - Final result: you have a **CHOICE** to pick the **BEST EQUIPMENT** for your specific application – you are not locked to a single vendor, and you do not need to compromise quality!

RIST Roadmap

Advanced Profile – Available (Released 2021)

- Tunnel-Level ARQ (use RIST to carry any protocol, including data transfers)
- Lossless Compression
- Payload identification
- Low-overhead media transport
- Additional security and data integrity options
- Common channel session management

Main Profile – Available (Released 2020)

- Multi-Stream Tunneling
- Stream encryption
- Authentication
- High Bit Rate Support
- Null packet suppression

Simple Profile – Available (Released 2018)

- Interoperable ARQ
- Retransmission Throttling for Stability
- Link aggregation/bonding
- Redundant transmission paths

What's in RIST Simple Profile?

- Basic compatibility with non-RIST systems using standard RTP as the base protocol
- Packet loss recovery using NACK-based ARQ
  - No acknowledgement for packets received correctly
  - Lost packets are requested by the receiver and re-sent
    - Retransmission bandwidth throttling available
- Features
  - Bandwidth efficient
  - Tunable tradeoff between latency and protection
- Multi-link support
- IP Multicast Support

The Tech Details

- Stream is sent using standard RTP
  - Baseline compatibility with non-RIST devices
  - Requires two UDP ports (RTP and RTCP)
- Sender transmits periodic RTCP messages to establish states in firewalls
- Receiver transmits periodic RTCP messages to keep return channel operating
  - Custom “RTT Echo” message to measure latency
- If packets are lost, RTCP NACK messages are sent
  - RFC 4585 Bitmask NACK (“salt and pepper” losses)
  - Custom RIST Range NACK (block losses)

Multi-Link Operation

- RIST supports usage of multiple links in parallel for a given stream
- Modes of operation:
  - **Bonding**
    - The stream is split between links, in order to combine their capacities
  - **Seamless Switching**
    - The stream is replicated over the links
    - Receiver merges the packets
    - If one link fails there is no glitch
    - Follows SMPTE-2022-7

RIST Main Profile Features

- Encryption
  - Protect high-value streams in flight on the Internet
- Authentication
  - Make sure that the other endpoint is who you think they are
- Tunneling
  - Simple Profile requires two UDP ports per stream
  - If you have lots of streams, you will not be popular with IT
  - Support for non-RIST traffic (e.g., for 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 Main Profile

- 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 Content Protection

- 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

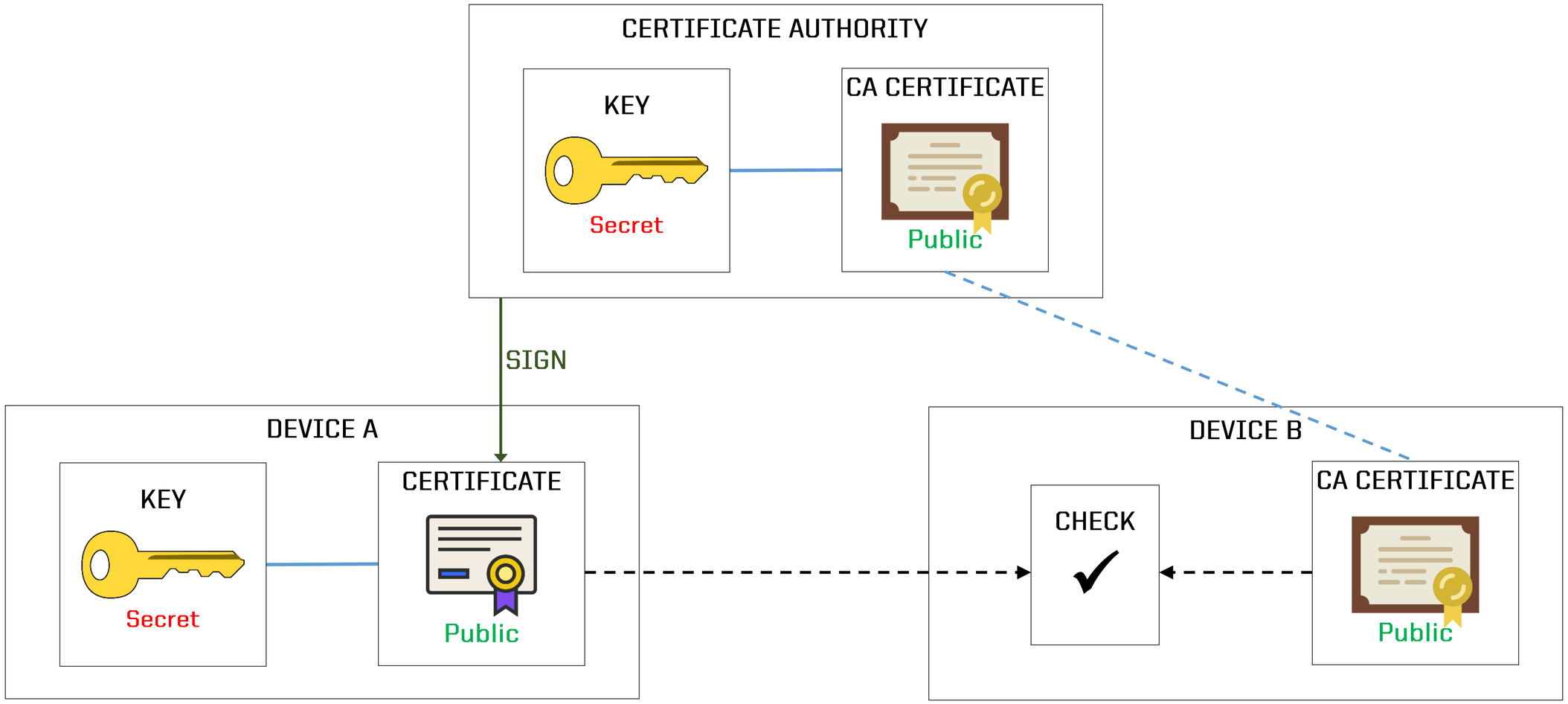
Required Cypher Suites

- A subset of cypher suites has been selected, and all vendors must support them
- These include:
  - AES 128 (with RSA and ECDSA authentication)
  - AES 256 (with RSA and ECDSA authentication)
  - 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

RIST Authentication

- RIST Main Profile includes certificate-based authentication
  - Same technology used to authenticate bank web sites
  - Both server and client can authenticate each other
  - User is in full control:
    - Use a “whitelist” of allowed certificates
    - Use a private CA to sign certificates
- Password-based authentication (TLS-SRP) is also supported

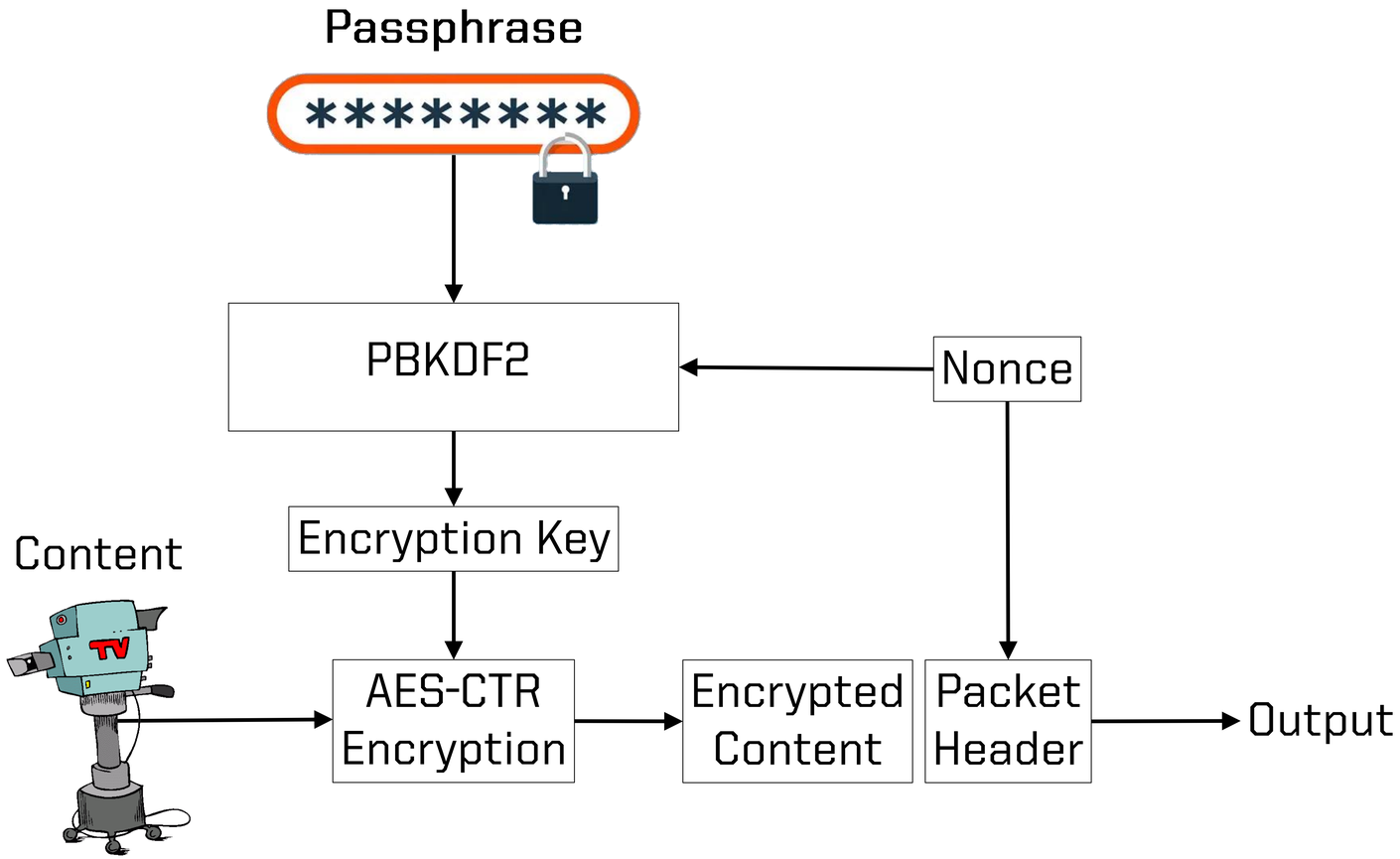
Authentication Example



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
  - Variable IV
  - Support for rotating keys
    - Very important for security
    - Minimum key rotation every GRE sequence 32-bit wrap
    - Key rotation period is configurable
  - 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

PSK Illustration



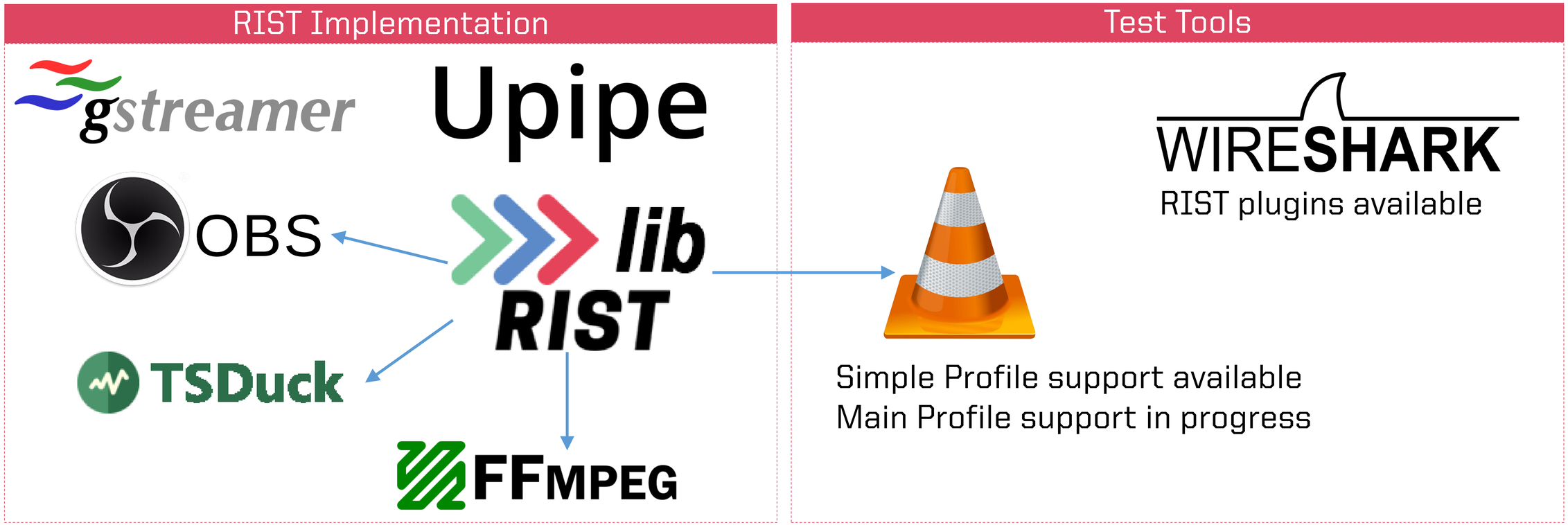
RIST Advanced Profile

- RIST Advanced Profile was released in late 2021
  - No products in the market currently support Advanced Profile
- The primary feature of Advanced Profile is the ability to use RIST as a transport mechanism for any generic protocol, even data
  - Ideal for gateways
- Other features include lossless compression, additional encryption, and payload identification

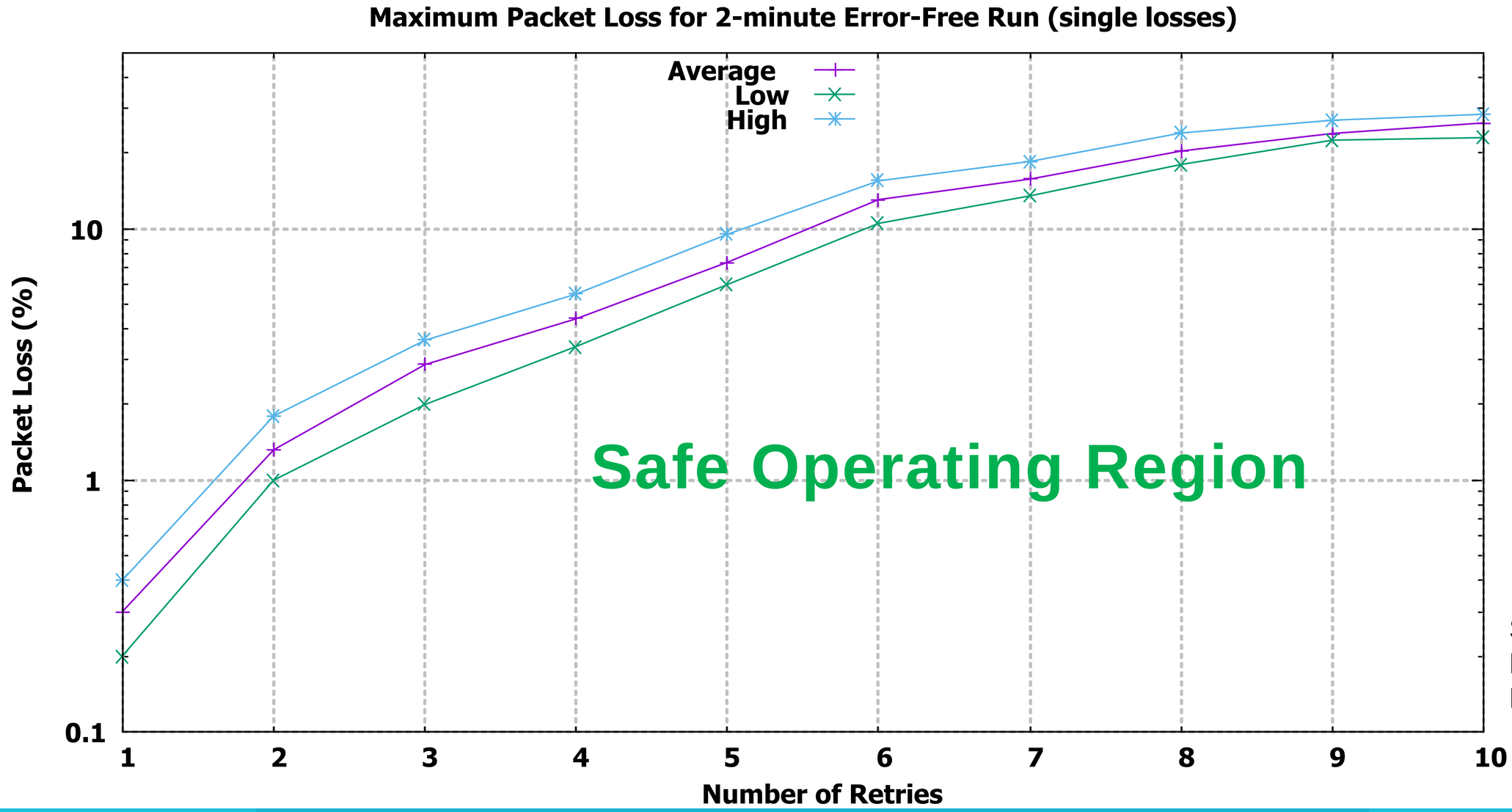
Standards/RFCs used in RIST

NAME	STATUS	USED IN	NOTES
SMPTE ST-2022-1, -2	Standard	Simple Profile	TS over RTP baseline
SMPTE ST-2022-7	Standard	Simple Profile	Seamless switching
IETF RFC 3550	Internet Standard (STD 64)	Simple Profile	RTP, RTCP baseline
IETF RFC 4585	Proposed Standard	Simple Profile	ARQ NACK messages
IETF RFC 2784	Proposed Standard	Main Profile	Tunneling
IETF RFC 8086	Proposed Standard	Main Profile	Tunneling
IETF RFC 8259	Internet Standard (STD 90)	Main Profile	JSON for Tunnel Management
IETF RFC 3686	Proposed Standard	Main Profile	PSK encryption
IETF RFC 6347	Proposed Standard	Main Profile	DTLS encryption and authentication
IETF RFC 7468	Proposed Standard	Main Profile	Encoding of certificates
IETF RFC 5054	Informational	Main Profile	Password Authentication
IETF RFC 8018	Informational	Main Profile	PSK key generation

Open Source RIST

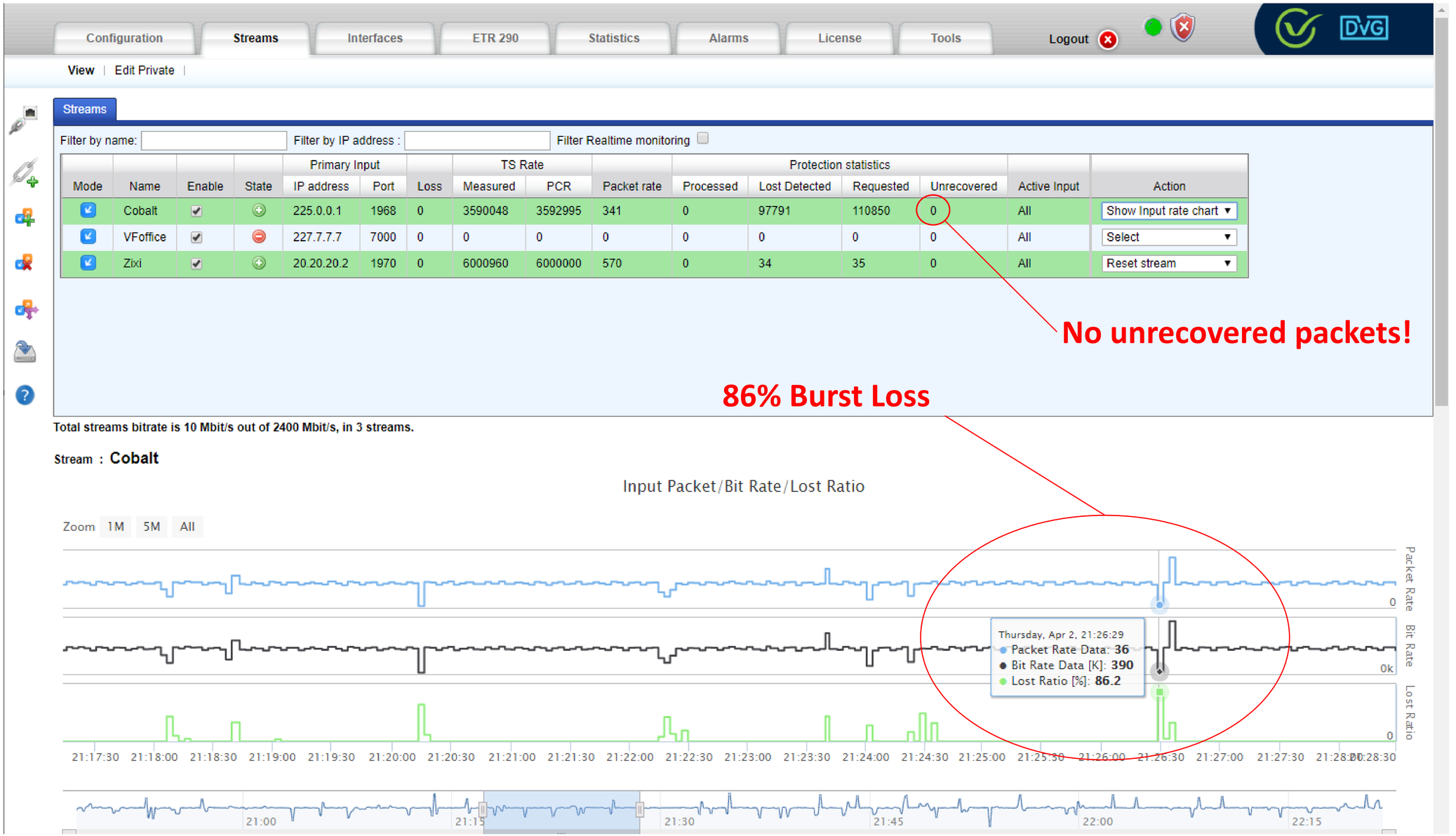


How well does it work?



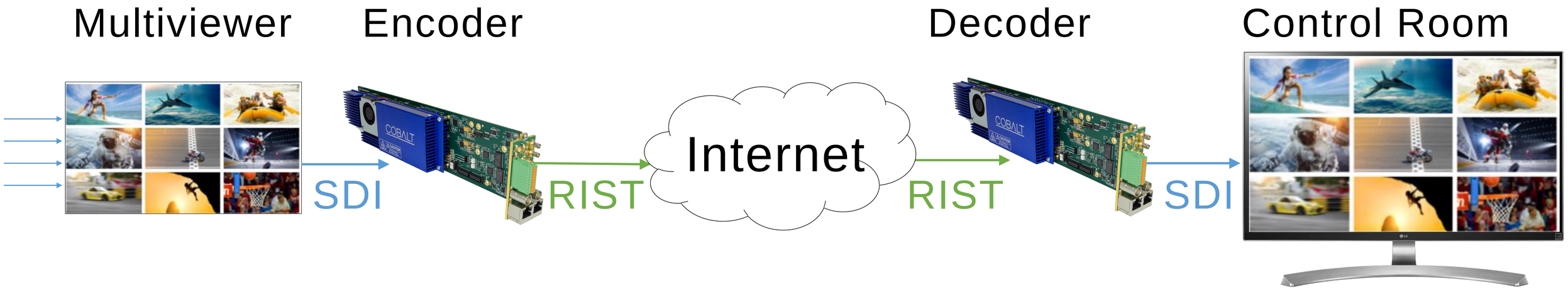
Source:
RIST Evaluation
BEITC 2019

Performance Snapshot on Internet Link



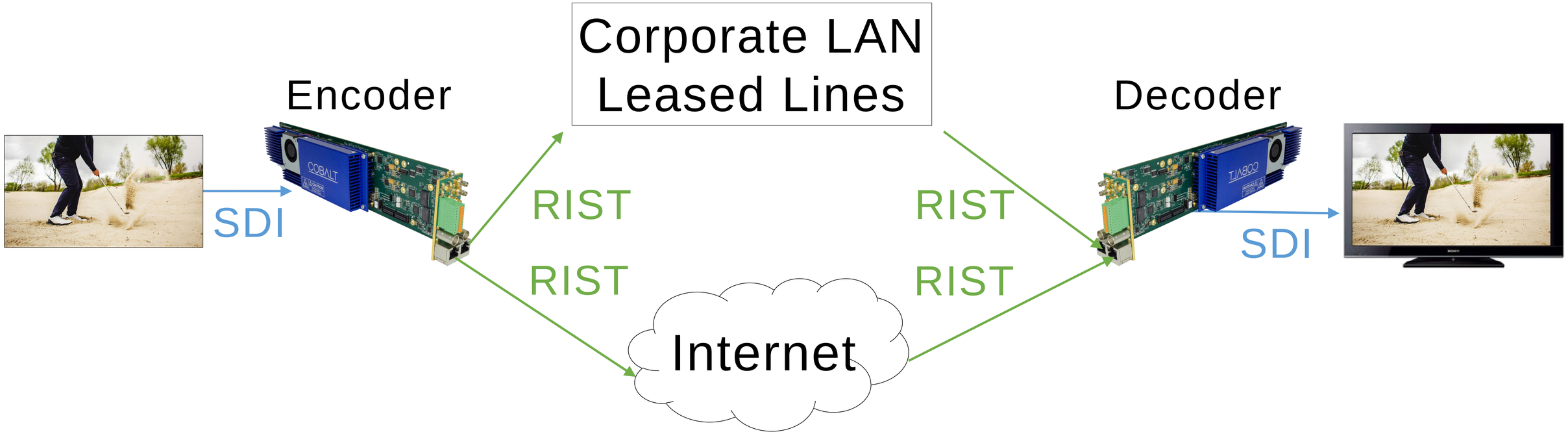
Source: Virtual NAB 2020 Demo

Remote Monitoring Application



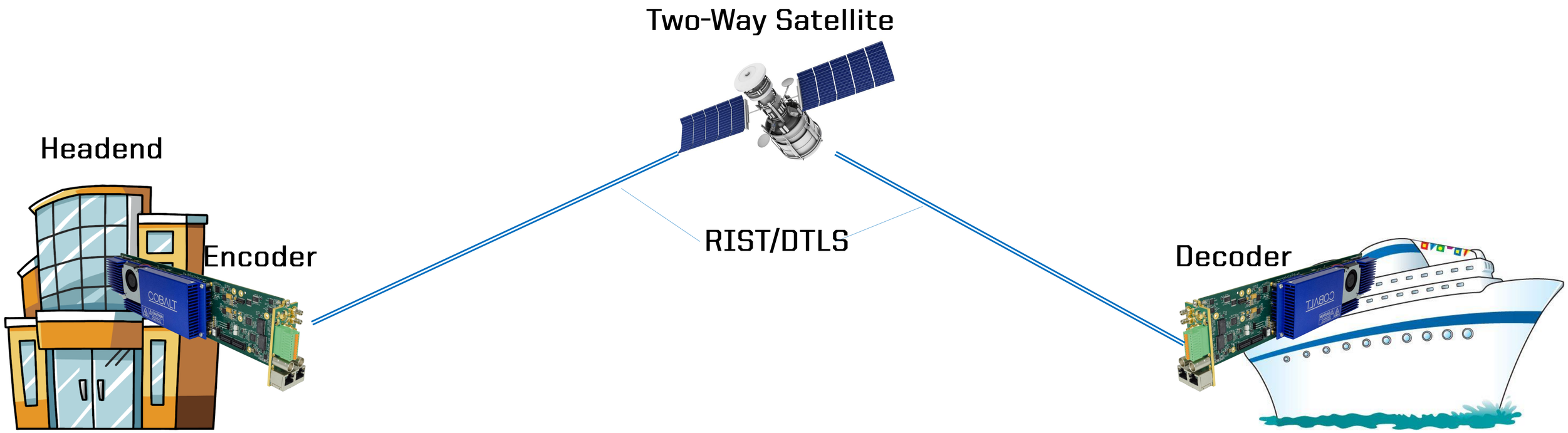
- Objective: send multiple signals from a station to a central monitoring location
- Signals are combined in a Multiviewer at the source
- Multiviewer output is compressed and transmitted using RIST to a central location
- Since these are not signals to be put on air, a single Internet connection is used without any backups

Seamless Redundancy



- Objective: have high signal reliability
- Customer has a Corporate LAN connected using dedicated private lines between locations
- Each location is also connected to the Internet
- Two full copies of each stream are sent, one through the Corporate LAN and another through the Internet
- SMPTE ST-2022-7 Seamless Redundancy (part of RIST) is used

Shore-to-Ship Content over Satellite



- Objective: send multiple channels of video content for shipboard entertainment
- Content protection (encryption and authentication) is an absolute requirement
- System uses RIST Main Profile tunnels with DTLS

Further Reading

- VSF TR-06-1
  https://vsf.tv/download/technical_recommendations/VSF_TR-06-1_2020_06_25.pdf
- VSF TR-06-2
  https://www.vsf.tv/download/technical_recommendations/VSF_TR-06-2_2021-04-26.pdf
- VSF TR-06-3
  https://www.vsf.tv/download/technical_recommendations/VSF_TR-06-3_2021-10-19.pdf
- RIST Activity Group web page
  http://vsf.tv/RIST.shtml
- RIST Forum (events, case studies)
  http://rist.tv
- RIST Performance Evaluation (NAB BEITC 2019)
  https://rb.gy/h8ztrl

Further Watching

- RIST Promo Video
  https://www.youtube.com/watch?v=_x-f0_QV4XU
- ARQ Primer
  https://www.youtube.com/watch?v=ulTTDgSdmXU
- Playlist with RIST Tradeshow Demos
  https://www.youtube.com/playlist?list=PLx8UACLVcUBHpshU15Rf8Ea-wQa2nisaj
- RIST Forum YouTube Channel
  https://www.youtube.com/channel/UC2mb6-S-Nh5L4zAzcdAppzA/videos

THANK YOU!

Contact Info:
ciro.noronha@cobaltdigital.com