Introduction to RIST Advanced Profile

Ciro Noronha, Ph.D.

Cobalt Digital

IP SHOWCASE

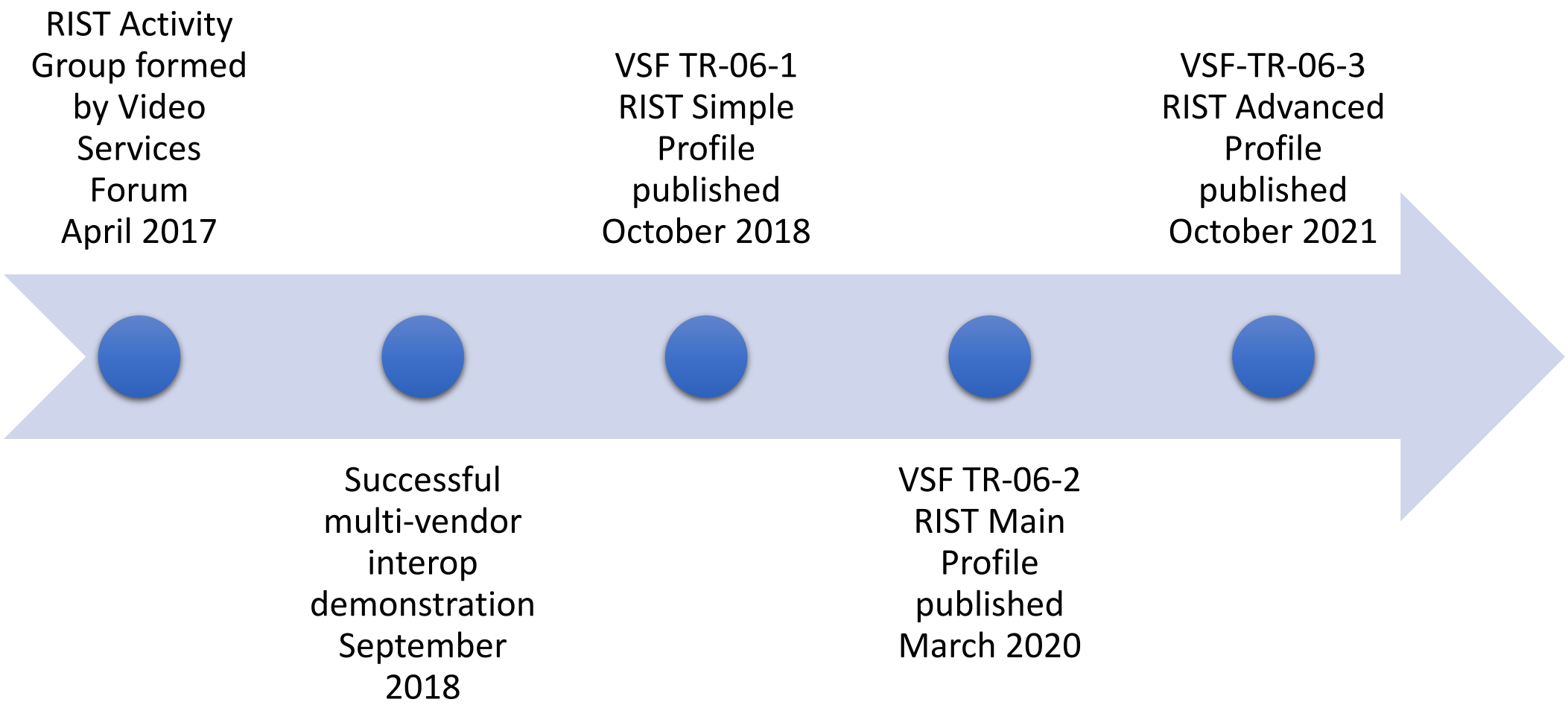
Audio Engineering Society · AIMS Alliance for IP Media Solutions · AMWA Networked Media. Working. · EBU · SMPTE · VSF Video Services Forum

Agenda

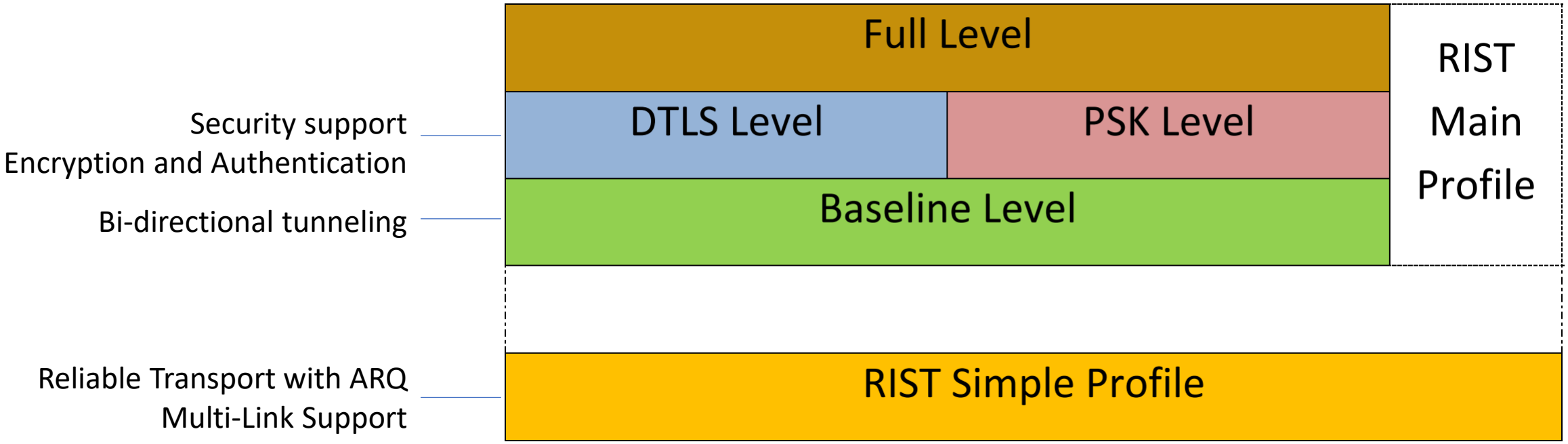
- Quick Review of RIST Simple and Main Profiles
- Benefits of the Advanced Profile
- Overview of RIST Advanced Profile Features
- Future Directions

RIST Simple and Main Profiles

RIST Milestones



RIST Profiles and Levels

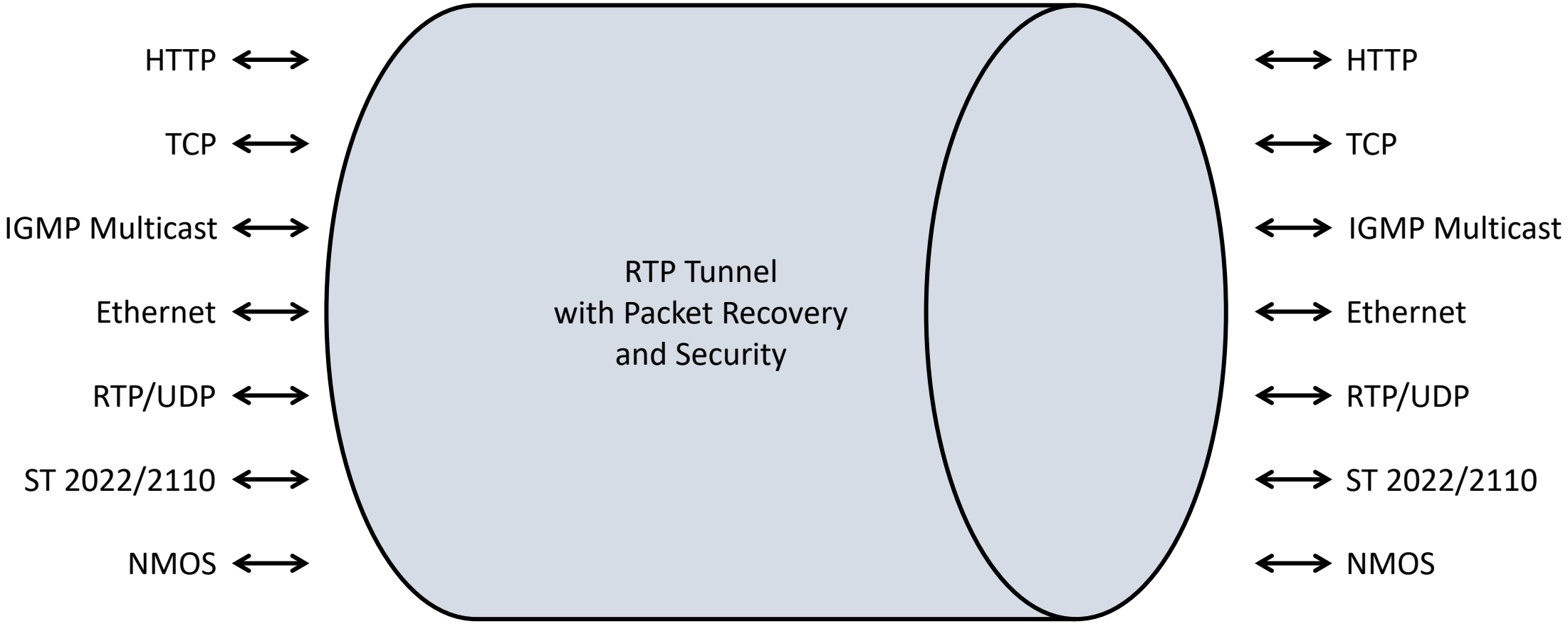


Benefits of the Advanced Profile

The new RIST Profile: Advanced

- Greatly enhanced tunneling capabilities
  - Any protocol delivered securely and reliably
  - Transparent Fragmentation
  - Mathematically Lossless Compression
- Enhanced PSK Security
  - New ciphers, payload hashing for data integrity
- Direct payload transport and Protocol Registry
  - Reduce size of packet headers
- Flow Attributes

Advanced, Bi-Directional Tunneling



Advanced Tunnel Benefits

- Bi-directional data flow
- Reliable transport, with ARQ and FEC
  - Extends RIST support to any existing protocol
- Secure transport using PSK or DTLS
  - Can support authentication, authorization and data integrity
- Single UDP port capability for simpler firewall configuration

Overview of RIST Advanced Profile Features

Top-Level Technical Details

- The base packet format is RTP
  - Format is aligned with the work being done by the VSF ST 2110 over WAN AG
  - Header includes a sequence number extension to 32 bits
  - 1 MHz timestamp for more precise timing
  - Additional optional fields to support enhanced functionality
- RTP packet payload is an encapsulated tunnel packet or a control packet

Supported Encapsulated Types

- IPv4 Packet
- IPv6 Packet
- TR-06-2 Reduced-Header UDP Packet
- Control Packet (defined by Advanced Profile)
- Direct Payload Packet (defined by Advanced Profile)
- Layer-2 Ethernet Frame
- Generic GRE Packet
- TR-06-2 GRE Packet

Transparent Fragmentation

- It is relatively common today to have MTU mismatches between local networks and the Internet
  - Local networks may support jumbo packets, unlike the Internet
  - Tunnel overhead may take a packet over the MTU
- IP fragmentation is messy, and permanent
- RIST Advanced Profile fragmentation is reversible
  - Packets restored to their original state at tunnel receiver
- BONUS: ARQ operates on fragments
  - Fully reliable transport with smaller retransmissions
  - Fragments are recovered and re-ordered prior to reassembly – much simpler implementation than IP fragmentation

Lossless Compression

- Optional LZ4 Compression can be used on any packet
  - Mathematically lossless – no change to data in any way
  - Very good compression performance
- Can significantly reduce signal bandwidths
  - Particularly for uncompressed and compressed video signals
- Specification can be updated in the future with other lossless compression algorithms
  - Similar format as used in IPComp

New PSK Ciphers

- RIST Main Profile only supported the AES-CTR cipher, with no hashing
- RIST Advanced Profile support:

Cipher Suite	Notes
AES-CTR	Same as Main Profile, no hashing
HMAC-SHA256	No encryption, hashing only
AES-CTR-HMAC-SHA256	Main Profile encryption with hashing
AES-GCM	Encryption and hashing, native in many CPUs
CHACHA20-POLY1305	Encryption and hashing

Hashing for Data Integrity

- PSK systems based on AES-CTR can be vulnerable to malicious packet replacement or corruption
  - If fake packets with flipped bits are injected in the stream, they may be accepted by the receiver
  - Can cause erroneous data to be decoded and corrupt the stream
- Relies on shared secret hash key at sender and receiver
  - Secure hash added to each packet at sender using secret key
  - Receiver calculates same hash using shared key
  - If receiver result does not match hash from sender, then packet is dropped

Direct Payload Transport

- Eliminate need for IP/Ethernet headers for many popular protocols
  - Can reduce overheads significantly
  - Can act as NAT function for bridging between address spaces
  - Allows the use of low-latency audio/video multiplex alternatives
- Uses unique, registered Payload ID for each protocol/packet type

Protocol Registry

- Direct payload identifiers are registered in open database
  - Based on standards organization and standard numbers
  - Innovative way to ensure interoperability
- Registry currently maintained by VSF
  - Simple, open approval process for adding new entries
  - Hosted on GitHub
  - Registry is not public yet – will be launched when TR-06-3 is approved

The Registry Today

main ▾ 1 branch 0 tags Go to file Add file

cjr052402 Include instructions to sort the spreadsheet. f85d2ef on May 6

Admin-Guide.html	Include instructions to sort the spreadsheet.
LICENSE	Initial commit
README.md	Add the Admin Guide.
Registered_Payload_Format_Des...	Transferred the data from the test repository.
Registered_Payload_Format_Des...	Transferred the data from the test repository.
Registered_Payload_Format_Des...	Transferred the data from the test repository.

README.md

VSF TR-06-03 Payload Format Descriptor Registration

This is a registration repository for the Payload Format Descriptor field in the upcoming VSF TR Specification.

How to add new entries to the table

Important: The table is a Microsoft Excel file with formulas. It must only be edited with Excel. Other tools may break it.

The steps are:

1. Carefully review section 5.2.7 of VSF TR-06-3 for the rules on how to assign values.
2. Open the Excel spreadsheet.
3. Use the drop-down in the **Organization** column to select the organization from which the document

Organization	ID Type	Document	Part/Sub-Part	ID Flavor	Descriptor (Dec)	Descriptor (Hex)	Description
VSF	0	1	0	0	4096	00001000	TR-01: JPEG2000 using 7 TS packets as per ST-2022-2
VSF	0	1	0	1	4097	00001001	TR-01: JPEG2000 using 7 TS packets as per ST-2022-2 Column FEC
VSF	0	1	0	2	4098	00001002	TR-01: JPEG2000 using 7 TS packets as per ST-2022-2 Row FEC
RFC	1	2250		0	269011456	1008CA00	MPEG2 Transport Stream over RTP
RFC	1	6184		0	270018560	10182800	AVC elementary stream over RTP. Includes the RFC 6184 RTP header.
RFC	1	6416		0	270077952	10191000	MPEG4 audio (AAC) over RTP
RFC	1	7231		0	270286592	101C3F00	HTTP traffic on Advanced Profile Tunnel
RFC	1	7540		0	270365696	101D7400	HTTP2 Traffic on Advanced Profile Tunnel
RFC	1	7587		0	270377728	101DA300	Opus audio over RTP
RFC	1	7741		0	270417152	101E3D00	VP8 over RTP
RFC	1	7742		0	270417408	101E3E00	WebRTC ?
RFC	1	7798		0	270431744	101E7600	HEVC elementary stream over RTP. Includes the RFC 7798 RTP header.
SMPTE	2	2022	1	0	603128064	23F30100	FEC Packets
SMPTE	2	2022	2	0	603128320	23F30200	TS over RTP as per ST 2022-2
SMPTE	2	2022	3	0	603128576	23F30300	Piewise linear VBR video
SMPTE	2	2022	5	0	603129088	23F30500	FEC Packets
SMPTE	2	2022	6	0	603129344	23F30600	Uncompressed Transport of Full SDI Raster over RTP (including audio and ancillary data)
SMPTE	2	2022	8	0	603129856	23F30800	Uncompressed Transport of Full SDI Raster over RTP (including audio and ancillary data) with PTP
SMPTE	2	2049	0	0	604012544	24008000	MXF OP1a streaming transport with RFC 6597 defining MXF KLV over RTP
SMPTE	2	2110	20	0	606016512	241F1400	Uncompressed Video Essence over RTP
SMPTE	2	2110	30	0	606019072	241F1E00	Uncompressed Audio Essence over RTP
SMPTE	2	2110	31	0	606019328	241F1F00	Uncompressed Transparent AES3 over RTP
SMPTE	2	2110	40	0	606021632	241F2800	ST291 Ancillary Data over RTP
ISO/IEC	4	13818	1	0	1102041152	41AFD040	Payload is a transport stream without RTP or other wrapper
ISO/IEC	4	13818	1	1	1102041153	41AFD041	Payload is a program stream without RTP or other wrapper
ISO/IEC	4	23008	1	0	1120862272	42CF0040	MMT
AES	5	67		0	1342194432	50004300	AES 67 Audio
ATSC	6	324		0	1631846400	61440000	STLTP and DSTP

Flow Attributes

- Mechanism to provide useful info for receivers
  - Flow ID, flow bandwidth, priority, SDP file
- Standardized JSON schema
  - Each flow can be labeled uniquely
  - Includes timestamps for version control
  - Supports sub-flows within other flows
- Similar to PAT/PMT/SDT in Transport Streams

Advanced Profile Levels Annex

- Advanced Profile has a large number of options suitable for different applications, using a common packet format.
- There is a minimum “Baseline” level that all devices need to meet.
- The Levels Annex document specify interoperability levels to allow vendors to precisely state which options they are offering.
- This is similar to Main Profile Levels.

Advanced Profile Levels

Encryption Level ● Encapsulation Level ● Protection Level

- Baseline
- DTLS
- PSK
- Wireguard

- IPv4-Tunnel
- IPv6-Tunnel
- Layer2-Tunnel
- Main-Profile-Tunnel
- Media:
  - Media-TS
  - Media-ST2022-6
  - Media-ST2110

- None
- ARQ
- ST2022-1
- ST2022-5
- ST2022-7

Example: DTLS:PSK ● IPv4-Tunnel:Media-TS ● ARQ:ST2022-1

Future Directions

TR-04 Parts (subject to change)

- TR-06-4 Part 1: Receiver Synchronization **(work complete)**
- TR-06-4 Part 2: Use of Wireguard VPN in RIST Systems **(work complete)**
- TR-06-4 Part 3: Firewall Traversal – RIST Relay **(work complete)**
- TR-06-4 Part 4: Control and Management for RIST Systems **(work started)**
- TR-06-4 Part 5: RIST Congestion Control
- TR-06-4 Part 6: Source Adaptation in RIST Systems **(work complete)**
- TR-06-4 Part 7: Automatic Configuration for RIST Systems
- TR-06-4 Part 8: Internet/Satellite Hybrid Model
- TR-06-4 Part 9: RIST IGMP Listener

Who is behind RIST?

The Players

VIDEO SERVICES FORUM

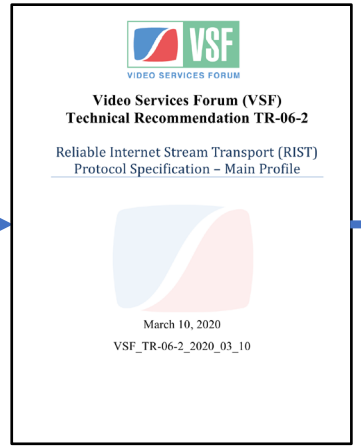
All the companies in the RIST AG also participate in the RIST Forum

RIST Forum

RIST Activity Group

The tech people

RIST Specification



The marketing people

Sampling of RIST Forum Members

IP SHOWCASE

Over 180 member companies

Thank You ….. Or ….. Any Questions?

Ciro Noronha

IP SHOWCASE

Audio Engineering Society · AIMS Alliance for IP Media Solutions · AMWA Networked Media. Working. · EBU · SMPTE · VSF Video Services Forum