Integrated Real-time Protocol

The Integrated Real-time Protocol (IRP) is a next-generation, open-source, fully-secure live internet streaming protocol designed to support the severe demands of Glass-to-Glass streaming.

First, what is Glass-to-Glass streaming? This is how Streamonix defines it:

1. Lens-to-Screen: As its name suggests, Glass-to-Glass streaming transmits high-resolution digital media, including camera metadata, in real-time from the lens of a camera to the glass of users' screens. To achieve this, Glass-to-Glass software is embedded directly in the camera itself (or in the encoder connected to the camera). And to exploit the many advantages of camera metadata (described below), Glass-to-Glass software runs on the user's device (SmartPhone, PC, SmartTV, Metaverse head-set, etc).

2. Real-time, Ultra Low-latency: Glass-to-Glass streaming operates in real-time. From the user's perspective, live audio, video and other digital media from the camera are received and displayed instantaneously. In more precise terms, Glass-to-Glass streaming has ultra low-latency delivery, with less than one second of latency from the camera to the screen, for all streams, for all content, to all users, at all times.

3. Metadata Included: Glass-to-Glass streaming transmits not only the audio and video produced by the camera, but also the metadata – such as color lookup table, aperture, geospatial coordinates, acceleration readings – generated by the camera during streaming. The inclusion of metadata in the stream opens up new opportunities for enhanced playback in Glass-to-Glass-enabled screens and head-sets. Using the incoming metadata, screens and head-sets can dynamically tune and adjust playback to display the video with the highest possible fidelity and the most accurate colors. What the camera's lens sees, the user sees. Or, in the case of mixed reality (MR) streams, screens and head-sets can heighten realism by using the metadata to correctly position real-world 3D objects in virtual worlds.

4. Comprehensive Security & Deep-Fake Detection: Streamonix believes that all internet communications, Glass-to-Glass streaming included, is confidential and private and must be fully protected. This protection takes two forms. First, the transmission of the stream must be secured through the use of state-of-the-art encryption. Every packet must be encrypted, with no exceptions. The encryption algorithms must be selected not only to maximize security but also to minimize processing requirements, especially in the case of cameras and sensors with modestly performing embedded CPUs. Second, the provenance and veracity of the stream's payload must be verified and protected in real-time. This protection assures the user that the stream they requested is in fact the stream they are receiving. This is a deeper level of protection than simply encrypting the stream's packets: it is a mechanism for detecting and rejecting deep-fakes.

5. Current and Future Payloads: Distance education, telehealth, interactive design, remote work, the Internet-of-Things, ISTAR[1] and the Metaverse are ushering in a Cambrian explosion of media types. A modern streaming protocol must carry not only traditional audio and 2D video payloads, but a wide array of 3D objects and augmented, virtual and mixed reality experiences – plus a variety of new digital media types that will emerge in the future. These media types will have a wide range of bit-rates that range from a few kilobits per second for IoT sensor data, to 90 Mbps for 8K video, to multi-gigabits for large-scale mixed reality worlds. A Glass-to-Glass protocol must have an extensible and flexible container that enables it to carry all conceivable digital media types.

In short, Glass-to-Glass streaming is the secure, real-time transmission directly from cameras (and other sources) of ultra high bit-rate media streams carrying a wide array of metadata and payloads, whether 8K video, immersive studio-quality audio, high-resolution medical imagery, 3D scenes or mixed reality worlds. Many of these payloads will be the digital raw material of the Metaverse. Whatever form the Metaverse ultimately takes, its emergence will be hastened and its utility enhanced by Glass-to-Glass streaming.

No current internet streaming protocol, whether TCP- or UDP-based, meets the requirements of Glass-to-Glass streaming. Nonetheless, the live streaming industry is attempting, with limited success, to use current-generation protocols to transport next-generation payloads. But using these protocols to carry the real-time, high-resolution, rich media of the Metaverse and other advanced applications is the digital equivalent of hammering a square peg into a round hole. None of these protocols is optimal:

- QUIC, conceived as a light-weight UDP-based transport for HTTP payloads, has morphed into a complex beast catering to the needs of Google and the ad tech industry, not the real-time, multi-dimensional requirements of the Metaverse.
- RTP (Real-time Transport Protocol), while showing its age, still works well in applications like WebRTC, but is ill-suited for secure, high bit-rate streaming, especially for complex media types such as the Metaverse's mixed reality streams.
- SRT (Secure Reliable Transport) is designed for secure audio and video streaming, but is not intended to carry the rich media types of the Metaverse nor the ultra high bit-rate streams of the 8K market.

IRP Overview

A new protocol is needed to unlock the full potential of Glass-to-Glass streaming and enable the emergence of the Metaverse. Streamonix is developing IRP to meet that need.

IRP is based on UDP and its transport and security features are derived from MinimaLT[2] (Minimal Latency Tunneling), a very innovative and extremely secure network transport protocol designed by a team including Daniel J Bernstein, one of the world's preeminent cryptographers. MinimaLT's advanced security features and state-of-the-art encryption

1 ISTAR: Intelligence, surveillance, target acquisition, and reconnaissance
2 MinimaLT: https://cr.yp.to/tcpip.html

endow IRP with the capacity to fully protect network communications against eavesdropping, modification, and to a large extent, Distributed Denial of Service attacks. Additionally, IRP protects privacy by providing decentralized cryptographic authentication of servers, clients, and users – an absolute necessity for medical imagery streaming and other sensitive applications.

Integrated Media Container: IRP is more than a transport protocol. It includes an integrated universal media container to carry a full range of digital payloads, whether existing media types or newly invented media for the Metaverse. The media container is based on a simplified version of MMT (MPEG Media Transport). Streamonix has cherry picked the best features of MMT and combined them with new features optimized for the requirements of the Glass-to-Glass streaming market.

Any and All Bit-rates: IRP, with its integrated media container, supports a wide spectrum of bit-rates, from sub-kilobit IoT data streams, to massive 100 Gbps MR object streams and everything in between – whether 1 Mbps high resolution audio, 10 Mbps HD TV shows, 100 Mbps 8K movies, 200 Mbps medical motion imagery, or multi-gigabit 8K ProRes Raw streams.

Protection Against deep-fakes: The emergence of deep-fake technology obsoletes conventional approaches to media delivery. Simply delivering digital media on a "no questions asked" basis is now insufficient when that media may have been altered somewhere along the Glass-to-Glass pathway, with the original content swapped for deep-fakes. To reliably and securely deliver digital media over the Internet from camera lens to user screen, and to verify the media's authenticity and the provenance of its origin, these questions must be correctly answered:

- Who requested the media, and did they receive it?
- What media was requested, and was it delivered?
- When was the media requested, and when was it delivered?
- Where was the media generated, and where was it consumed?

IRP's encryption properties and its integrated universal media container are designed to generate and carry the answers to these crucial questions, while establishing and preserving privacy. Hashgraph[3], a soon-to-be open source[4] distributed ledger which provides a much more efficient type of blockchain, provides the ideal immutable store of truth to hold these answers. IRP closely couples with Hashgraph to write into the ledger the cryptographically correct (and privacy protecting) answers to all questions regarding the veracity, authenticity and delivery of digital media. With IRP, there is simply no way to inject deep-fake data into a Glass-to-Glass stream.

IRP's extensive security measures, real-time capabilities, universal media container and integration with Hashgraph ledger technology will make it the preeminent protocol for a wide range of 8K streaming and Metaverse use cases and applications.

3 Hashgraph: https://en.wikipedia.org/wiki/Hashgraph
4 Hashgraph IP becoming open source: https://hedera.com/blog/hedera-governing-council-votes-to-purchase-hashgraph-ip-commits-to-open-source-worlds-most-advanced-distributed-ledger-technology

IRP Key Benefits:

- Encrypts every packet of every stream
- Reduces latency of delivered packets
- Protects privacy
- Detects deep-fakes
- Boosts bit-rates
- Flattens layers & cuts complexity
- Supports essentially unlimited range of digital payloads
- Embeds camera metadata for enhanced playback
- Increases quality of experience
- Runs on a full range of devices: Cameras, IoT sensors, Smartphones, SmartTVs, PCs, game consoles, servers

IRP Features:

- **High Performance**
  - Low latency handshakes and processing
  - UDP based, reliable packet transmission
  - Optimized for long running multi-Gbps live streams
  - High-resolution clock and packet counters for jitter measurement and mitigation
  - Light-weight, runs well on embedded CPUs in cameras and sensors
- **Extreme Security & Content Integrity**
  - Every packet is encrypted, no exceptions
  - Decentralized cryptographic authentication
  - Anti-Denial of Service (DOS) mechanism
  - Real-time detection and rejection of deep-fakes
- **Integrated Universal Media Container**
  - Carries compressed and uncompressed video and audio streams of any bit-rate
  - Extensible packet structure holds all types of digital media payloads
  - Multiplexed design supports variety of media payloads in one stream
  - High resolution universal clock embedded in every packet, used by all containers
  - Time alignment of all elements of complex multi-media programs for perfectly synchronized playback with no lip-sync or other clock skew problems
  - High-capacity packet counter supports precise stream navigation
  - Harmonized content state information for intelligent lost packet mitigation for all payloads
  - Supports Hashgraph ledger-based media signatures to verify content provenance
- **Maximized Privacy**
  - Disassociated IP addresses to protect identities
  - Cryptographic authorization of peers (both real and pseudonymous identities)
  - Anonymized metrics for submission to the Hashgraph ledger

- **Metadata Driven Enhanced Playback**
    - Camera and sensor metadata delivered to screen enables optimized and improved playback
    - Real-time, automatic, dynamic updating of screen's color lookup table to match camera's color lookup table
    - Geospatial metadata enables accurate positioning of 3D objects in virtual worlds
- **Open-source Design and Implementations**
    - Enables porting to wide range of hardware platforms
    - Encourages scrutiny of all algorithms and logic
    - Attracts content creators and encourages development of custom media containers

IRP Enables Innovative Use Cases

Performance and Privacy on 5G Networks: IRP has explicit support for 5G mobile networks. First, IRP is optimized for the high bit-rate, low-latency transmissions that 5G networks provide. Second, IRP's streaming sessions are portable across IP addresses and persist even as IP addresses change. This is a crucial benefit when traversing 5G (and 4G) networks, where a dropped connection often results in a new IP address and a disruption of the stream. With IRP the user picks up the stream right where it left off, without the time-wasting renegotiation of a new session. And when the user moves from the mobile network to a local Wi-Fi network, the streaming session continues without a break. This produces a third important benefit: IRP strengthens privacy on mobile and other networks. When an IRP session spans multiple IP addresses, third parties are denied the ability to match a specific IP address to a specific user and a specific server. At best, only a very incomplete view of a user's streaming session can be obtained by snooping third parties.

Ultra High Resolution Streaming: Streaming bit-rates are steadily climbing, driven by the emergence of 4K and 8K videos and the coming wave of bandwidth-intensive mixed reality objects and 3D avatars streamed to and from the Metaverse. Unlike current protocols, IRP is specifically designed for operating at extreme bit-rates with very low latency. And its integrated universal media container is designed to carry virtually any type of digital media. This combination of high performance and future-proofing ensures that IRP will be able to accommodate the Metaverse's evolving mix of digital content.

Large-Size File Transfers: The same features that enable IRP to support media streaming at multi-gigabit bit-rates, enable IRP to support the transfer of large files peer-to-peer and point-to-point, whether gigabytes or terabytes. IRP operates at wire-speed. The speed of the transfer is limited only by CPU power and the network's available bandwidth – which are typically never maxed out. IRP ensures the complete integrity of all its payloads. The delivery of every byte of the file is guaranteed and, thanks to IRP's Hashgraph ledger-based verification, the file that is received is guaranteed to be a bit-perfect copy of the file that was sent. This capability is essential for transmitting medical imagery, design assets and a wide range of video production files.

Digital Dailies: The TV and movie production industry has a serious problem that demands a comprehensive solution: how to securely and quickly transmit digital dailies – the unedited prints, rough cuts, effects shots and other footage – that are sent once per day or more from shooting locations back to studio facilities. With its large-size file transfer capabilities, IRP is the ideal protocol for transmitting digital dailies and is the optimal foundation of a digital dailies delivery platform.

IRP Open Source Development Approach

Streamonix is developing IRP as an open source project. We are open sourcing the design and architecture of the protocol, under a permissive open source license, and will provide the source code for reference implementations, in C and C++, from our GitHub account.

To ensure the versatility of IRP's integrated universal media container, we will partner with digital creators and media producers to design the container's features, not only for today's payloads but for future payloads as well.

To demo some of IRP's Glass-to-Glass capabilities, we will develop an open source IRP-based media player.

We will utilize the open source community's array of static code analyzers, fuzzers and other tools to identify and remove all weaknesses and vulnerabilities in the IRP software. We will leverage advanced verification tools such as Tamarin and Prover to ensure correctness.

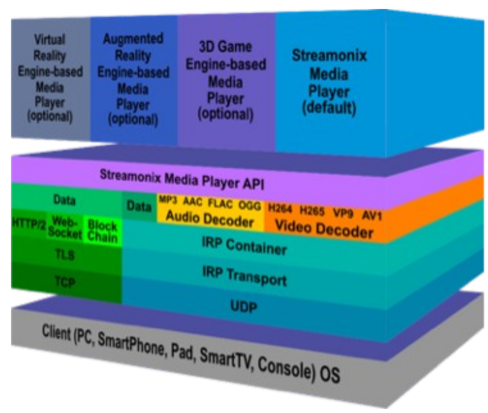

Figure 1: Streamonix IRP Media Player