TELESTREAM

WHITE PAPER

Improved Digital Media Delivery with Telestream HyperLaunch™

THE CHALLENGE

Increasingly, Internet Protocol (IP) based networks are being used to deliver digital media. Applications include delivery of news to a broadcast station or approvals from a content creator to a client. The delivery of digital media over IP data networks has presented an ongoing challenge due the extremely large amounts of data involved and the strain that puts on the network.

This paper examines the challenges of delivery over IP networks, and it discusses a technical solution from Telestream called HyperLaunch™. Like all Internet communication schemes, HyperLaunch builds upon Internet Protocol.

IP is a *routing* protocol. It defines the addressing scheme used within the Internet and routes data packets between network end points.

IP is also a *connectionless* protocol. This means that it does not exchange control information between the end points before packets are transmitted. Because IP provides no error detection or recovery mechanisms, it is often referred to as an *unreliable* protocol.

IP relies on a transport layer protocol, such as Transmission Control Protocol (TCP), to establish a connection between the end points and provide a reliable data stream.

Once a reliable connection has been established, *application* layer protocols such as File Transfer Protocol (FTP) and HyperText Transfer Protocol (HTTP) allow the end points to participate in a *session*.

TELESTREAM SOLUTION FOR OPTIMIZED DELIVERY

Telestream HyperLaunch (patent pending) performs several important functions to optimize delivery of digital media files via the Internet:

- Automatically resumes transfers interrupted by network interrupts or failures
- Automatically resumes interrupted transfers even if the sender changes locations – critical for delivery in portable applications
- Minimizes the effects of packet loss to enhance throughput over lossy connections such as wireless
- Handles complex content such as the media essence file and one or more related metadata files

HyperLaunch also includes encryption capability for users who require secure delivery of their content. In addition, for facilities which may be receiving multiple deliveries simultaneously, HyperLaunch comes with a management console which allows an administrator to prioritize one or more transfers over others.

Reliability

Telestream HyperLaunch combines both transport and application layers within a single protocol. HyperLaunch creates a reliable connection between the end points and establishes a session which is shared by the communicating applications.

Throughput Optimization

A reliable protocol must detect and recover from the loss, duplication or incorrect sequencing of data packets.

Packet loss is typically caused by congestion in the devices that route data packets through the network. Packet loss may be *ambient*, meaning that it is caused by other traffic present in the routers, or it may be *induced* by the traffic being exchanged between the communicating end points. In either case, packet loss degrades the rate at which information is exchanged between the end points.

An efficient protocol must implement a mechanism for avoiding congestion while maximizing the data transfer rate. While TCP is a reliable transport protocol, it is not necessarily an efficient one. As packet loss increases, the congestion avoidance mechanism causes the transfer rate to decrease geometrically. While this is generally not an issue for small amounts of data, it can have a significant impact on the time required to transport large media content.

In contrast, Telestream HyperLaunch implements a *flow control* mechanism that avoids congestion and degrades linearly in the presence of ambient packet loss. This ensures that content is transferred at the maximum rate possible for a given network connection. For example, with traditional TCP/IP a 3% packet loss might result in a 20% drop in throughput, whereas with HyperLaunch the throughput would be close to 97% of the potential data rate.

Connection Tolerance

Connection oriented protocols such as TCP are designed to tolerate a relatively small percentage of packet loss. They are not tolerant of a complete loss of network connectivity. If the physical network is disrupted, the connection between the end points is irrevocably severed, and any application protocol using that data stream will eventually fail.

Network disruptions can be caused by simply disconnecting an end point from the network or by a failure in some portion of the network infrastructure. Wireless networks are particularly prone to disruption due to RF interference and line of sight obstructions.

Telestream HyperLaunch technology is tolerant of network disruptions. Once a session is established, it is independent of the connection currently used to transport data between the end points. Therefore, if a media delivery session is interrupted by a loss of connection, HyperLaunch will attempt to resume the delivery. And, if the connection stays down for some time, an operator can resume the delivery manually when the network connection is re-established.

Network Portability

Following a network disruption it is possible that an end point will reconnect to the network at an entirely different IP address. This might be caused by a DHCP server assigning a new address to the end point or because the end point physically moved to a different network. For instance, a mobile journalist may run out of time to complete delivery of a large file and want to resume transmission from a hotel room or bureau.

After a session has been established, Telestream HyperLaunch allows either end point to move to a different network address. A *beacon* mechanism allows the end points to find each other following a network disruption, re-establish a reliable connection and continue the existing session. For the user, this means that HyperLaunch will automatically resume the disrupted transfer session from the point where it disconnected, and/or that the user can choose to stop the transfer, move to a new location, and HyperLaunch will automatically resume the existing transfer session from the point it left off.

Content Complexity

The primary purpose of Telestream HyperLaunch technology is to reliably and efficiently transport large, *complex* content between two network end points.

In this context, complex means that the content is comprised of more than one *aspect*. For example, a file transported using FTP has two aspects: the file *name* and the file *data*.

Telestream HyperLaunch extends this concept by allowing the content to be transported as multiple and separable aspects. An aspect might be used to transport the content *essence* or the *metadata* that describes the essence. Aspects may also be used to transport multiple related items, for example, the files contained within a folder.

Secure HyperLaunch

Data is normally transported *in the clear* across the network, meaning that no security measures take place. Because content security is an issue for some users, Telestream HyperLaunch provides an encryption capability which users can choose to turn *on* or *off*. If users choose to use encryption, some secure administrative set-up tasks need to be performed at both the send and receive end points prior to transmission. Once turned *on* content encryption occurs automatically at both ends.

Data security is only as good as the encryption key that is used. Telestream HyperLaunch uses *triple DES*, the government data encryption standard, to ensure maximum content security.

Transfer Management

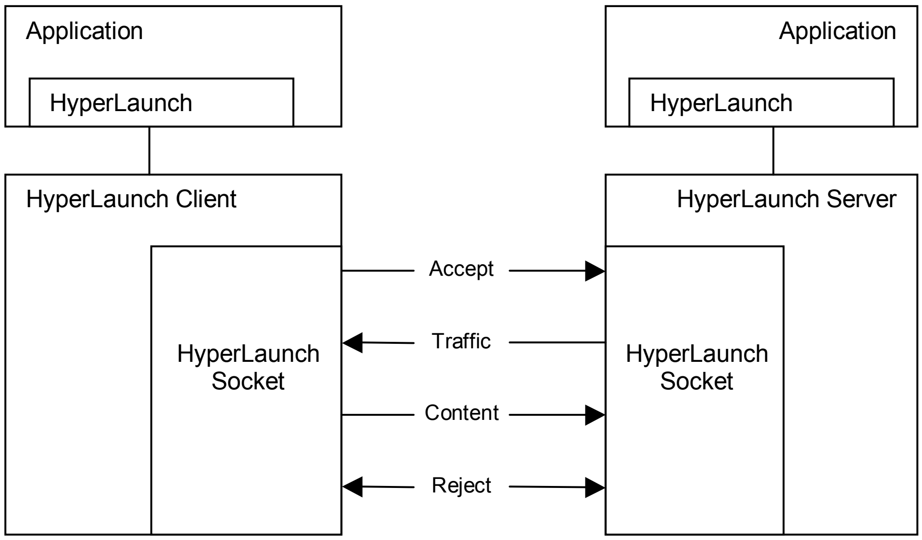
For facilities with limited Internet connection bandwidth, the speed of delivery from remote senders can be compromised, particularly if multiple senders are submitting large files simultaneously. For instance, news organizations may have multiple journalists sending content at the same time as the deadline for the evening news approaches. HyperLaunch comes with a transfer management utility which enables an administrator to pause one or more transfers, so that a higher priority story may be delivered more quickly.

IMPLEMENTING HYPERLAUNCH™

Telestream HyperLaunch employs the User Datagram Protocol (UDP) as its basic transport service. UDP is a connectionless, unreliable protocol; the only services it provides above IP are checksum protection of the datagram and multiplexing by port number (similar to TCP).

Each HyperLaunch packet is transported within a UDP datagram which is in turn transported within an IP packet. A HyperLaunch packet consists of a 16-byte header followed by a variable length array of data bytes.

The diagram below illustrates a HyperLaunch (PMP) session, conducted between a *client* and *server* application.



Packet Exchange

Packets are exchanged between the client and server as follows:

1. The client application initially creates the new session. The client assigns a unique identifier to the session which is used for all packets exchanged between the end points.

2. The client sends an **accept** message containing the credentials, if any, required by the server. The accept message is sent periodically until a response is received from the server or the client application closes the session.

3. If, for any reason (unsupported authentication scheme, invalid credentials, etc.), the server application is unwilling to accept the session, the server responds with a **reject** message describing the reason. The client terminates the session and informs the application accordingly.

4. If the session is accepted the server responds with **traffic** packet requesting the first content sequence (0). The server informs the application that it may begin reading the content stream. The traffic packet is sent periodically until a response is received from the client.

5. The client receives the initial traffic request and informs the application that it may begin writing to the content stream. When sufficient data is available from the application, the client sends the initial content sequence.

6. The client and server continue to exchange traffic and content sequence packets subject to the flow control mechanism.

7. If the network is disrupted the server continues to request the incomplete content sequences. The client, now unable to respond with content sequences, begins sending **beacon** messages to the server.

8. When the network is restored, the server examines the received beacon message. If the client location (IP address or port number) has changed, the server begins sending the traffic requests to the new location. Similarly, the client can examine the traffic packets to determine if the location of the server has changed.

9. When the client application has finished writing a particular aspect to the content stream, the client sends the **end-of-aspect** content sequence to the server.

10. When the client application has finished writing all data to the content stream it closes the session. The client sends the **end-of-content** sequence to the server and then waits for that sequence to be acknowledged.

11. The server continues to send traffic packets until all content sequences (including the end-of-content sequence) have been received and consumed by the application.

12. When the client has confirmation that all content sequences have been received, it sends a reject message in response to any further traffic for the session indicating that the session has been closed.

SESSION LIFETIME

Once a session has been established, it exists until one of the following conditions occurs:

- The content has been transferred successfully and the client closes the session.
- An unrecoverable error occurs within the client or server and that end point closes the session.
- The session expires due to inactivity (the inactivity timer is a user-defined parameter that defaults to 24 hours).

SUMMARY

HyperLaunch encompasses a number of technologies and techniques to enhance the speed, reliability and security of delivering inherently complex media files over IP networks. The benefits extend to not only mobile laptop users, but any content creator looking for simple tools to improve media delivery.

March 2005

TELESTREAM

848 Gold Flat Road
Nevada City, CA 95959
USA
www.telestream.net

877 257 6245 toll free (US only)
1 530 470 1300 tel
1 530 470 1301 fax
info@telestream.net