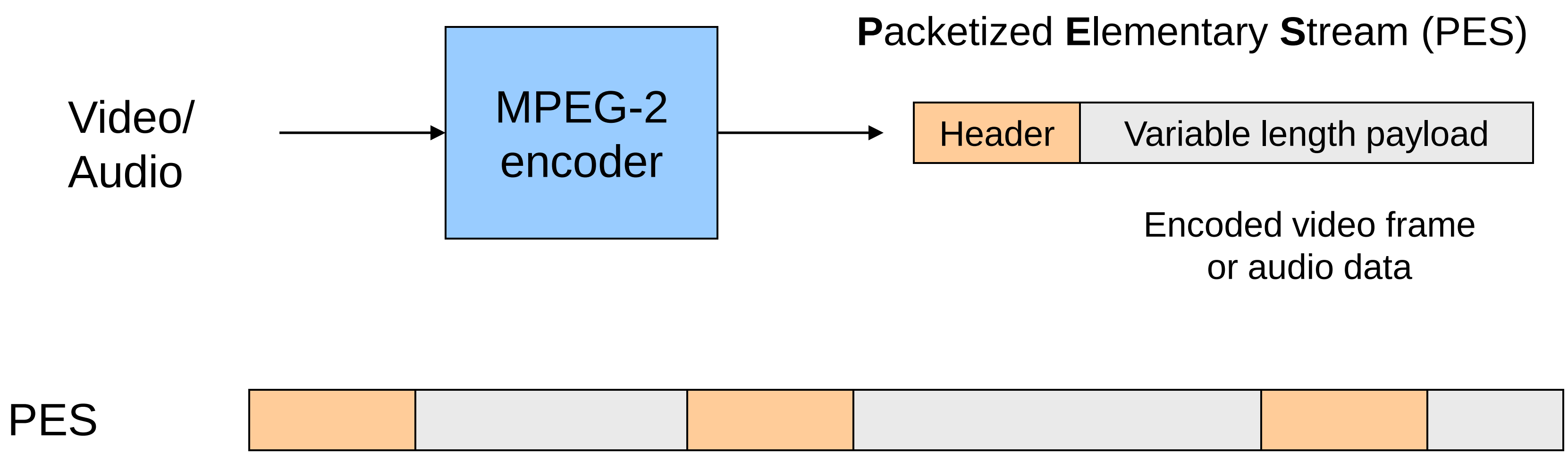
ECE160
Multimedia

Lecture 14: Spring 2011
Multimedia Streaming over IP

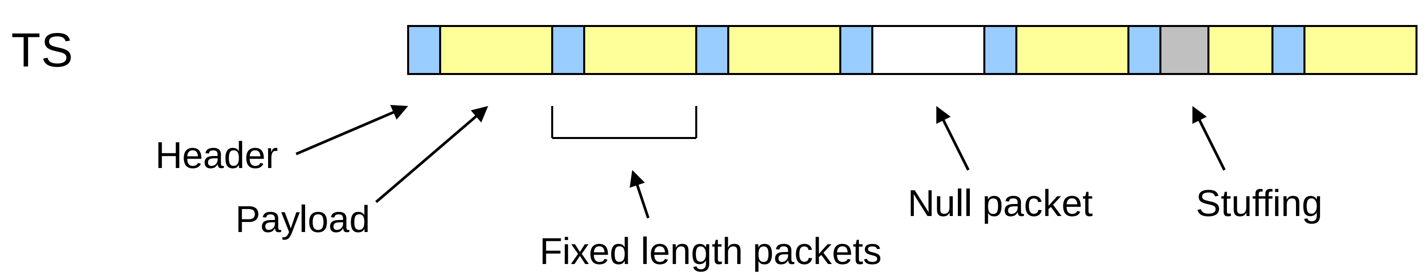
Why “Video over IP”?

- Video
  - Actually MPEG-2 Transport Stream
  - DVB (Digital Video Broadcasting) defined format for packet based transmission of encoded video, audio and data
  - As used for cable (DVB-C, J.83), satellite (DVB-S) and terrestrial (DVB-T) transmission
  - Adopted standard for compressed video transport, such as Netflix
  - ASI (Asynchronous Serial Interface) is a transport layer for TS
- IP
  - Internet Protocol
  - Network Access Layer for this design is 100M or Gigabit Ethernet
- So, could be called “Transport Stream over Ethernet”
  - But “Video over IP” has association with “Voice over IP” (VoIP) and valuable “triple play” voice/video/data applications

Raw Video to Transport Stream

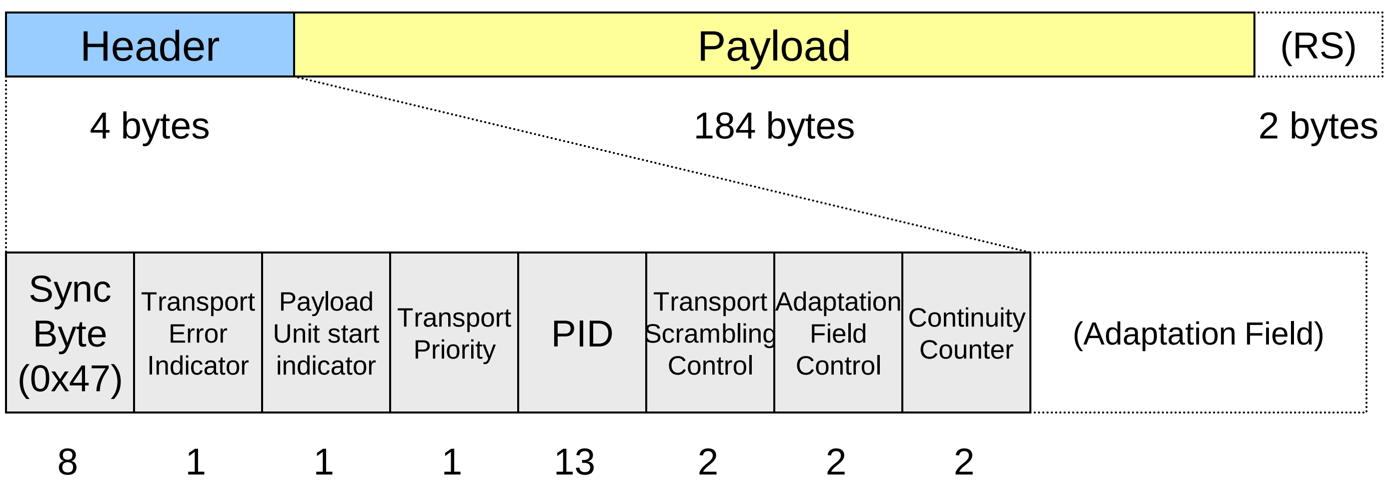


PES is divided into fixed length transport packets. Packets from a number of sources are then combined to make a Transport Stream



Transport Stream Packet

- Continuous stream of 188 byte packets
- Optional 16-bit RS extension is defined
- Can contain single program (SPTS) or multiple programs (MPTS)
- Constant Bit Rate (CBR) or Variable Bit Rate (VBR)
  - Padded to match bit rate of transport layer



Transport Stream Tables

- Header "PID" field is used to identify packet type or "source"
- Transport Stream includes a description of the content
  - Referred to as Program Specific Information (PSI) tables
- The "root directory" for the transport stream is called the Program Association Table (PAT)
  - Always uses PID 0x0000
- Each individual program has a Program Map Table (PMT) which lists all the contents of that program (video, audio and data components) and their allocated PID's
- Network Information (NIT) and Conditional Access (CAT) tables are also defined
- PID 0x1FFF is reserved for null packets

Transport Stream PAT & PMT

PAT

Prog. 1	PMT PID 0x0065
Prog. 2	PMT PID 0x0032
Prog. 3	PMT PID 0x0120
CAT	PID 0x0016

Program 1 PMT

Video	PMT PID 0x0131
Audio English	PMT PID 0x0132
Audio German	PMT PID 0x0133
ECM	PMT PID 0x0150

Program 2 PMT

Video	PMT PID 0x0021
Audio English	PMT PID 0x0022
Audio German	PMT PID 0x0023
ECM	PMT PID 0x0151

Null	PID 0x1FFF

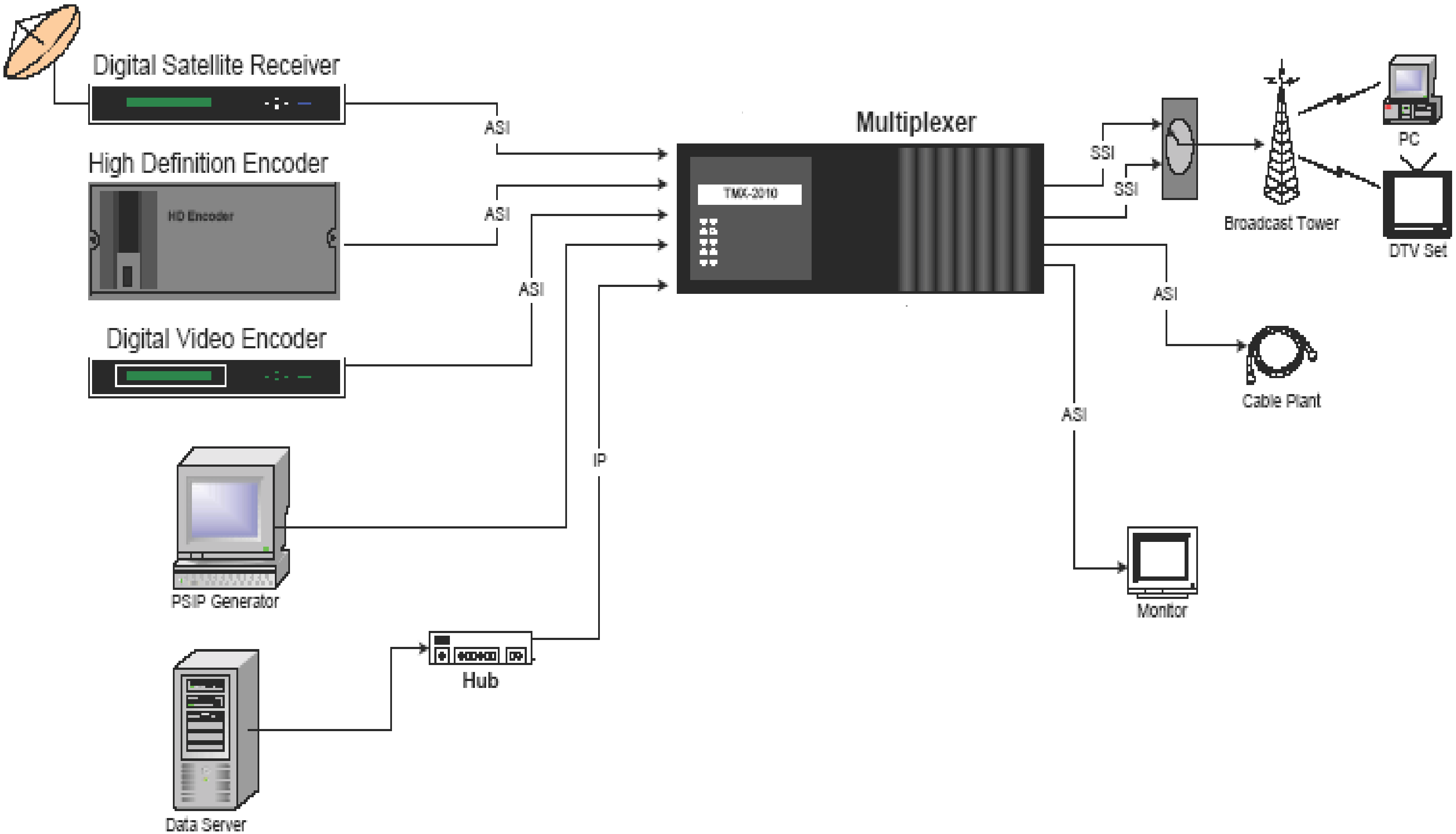
Parse PAT to find PMT for program of interest.

Then parse PMT to identify program content
ECM is entitlement control message

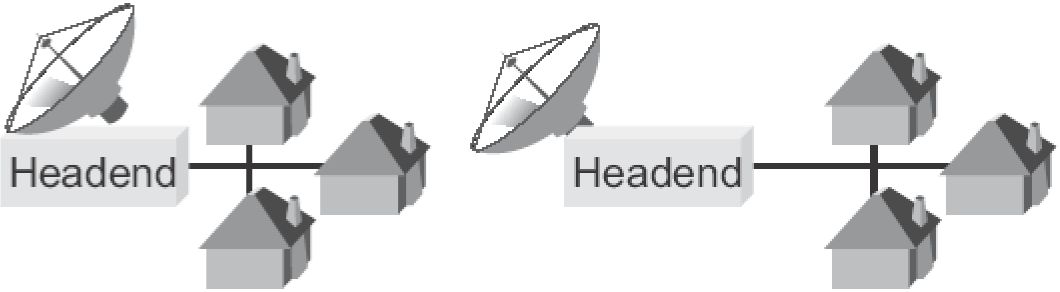
Transport Stream Timing

- The decoder must be frequency locked to the encoder for “real-time” presentation
  - To ensure correct synchronization of video and audio
  - To avoid overflow/underflow of buffers
- A PLL is used to lock the receiver to the encoder’s 27MHz System Time Clock (STC)
- Timing information is included in the Transport Stream to facilitate this
  - Program Clock Reference (PCR) timestamps are sent at least every 100ms
  - Encoder compares local elapsed time between timestamps with actual difference between the timestamp data and adjusts PLL accordingly
  - PCR “jitter” must be controlled to ensure quality of regenerated clock

First - What is a Headend?



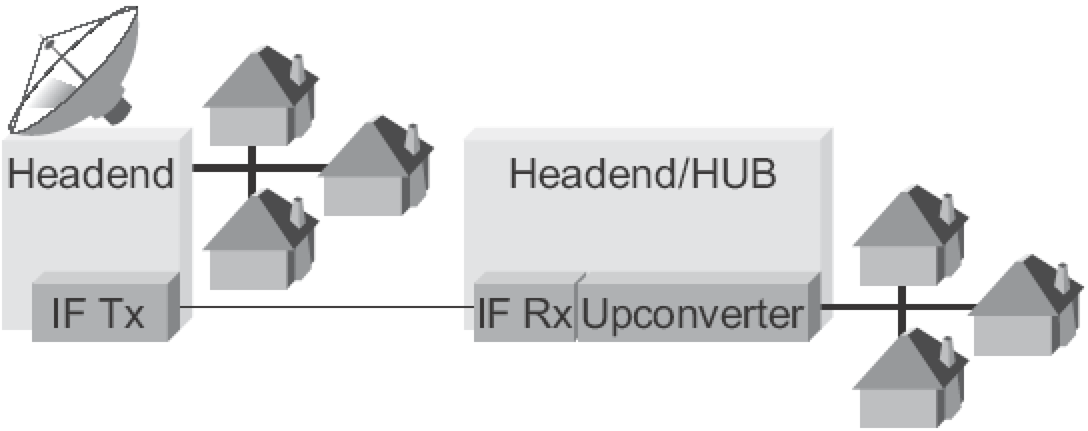
Evolving Cable Architecture



"Centralized Architecture"

Each home connected directly to Headend by cable

Evolving Cable Architecture

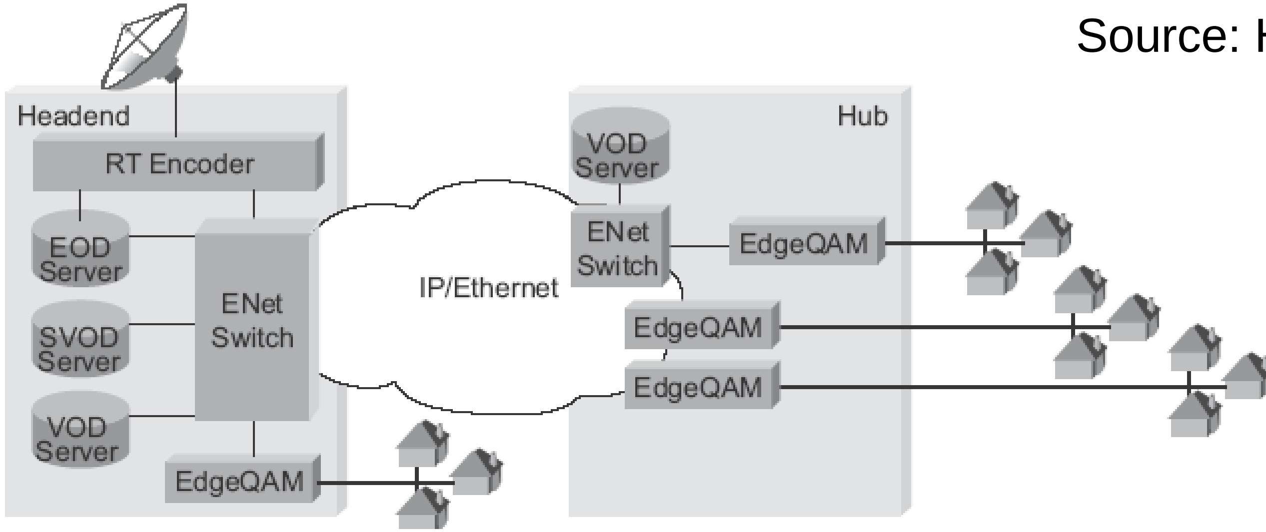


"Trunked-IF Architecture"

IF distribution (via fiber) allows Headend to serve wider area, spreading investment costs between more subscribers

Evolving Cable Architecture

Source: Harmonic



Data and telephony services are now being deployed using IP/Ethernet. Cable companies can benefit from using a single transport technology for their “Triple play” voice/video/data offering. The cost of adding video capacity to existing IP/Ethernet backbone is low.

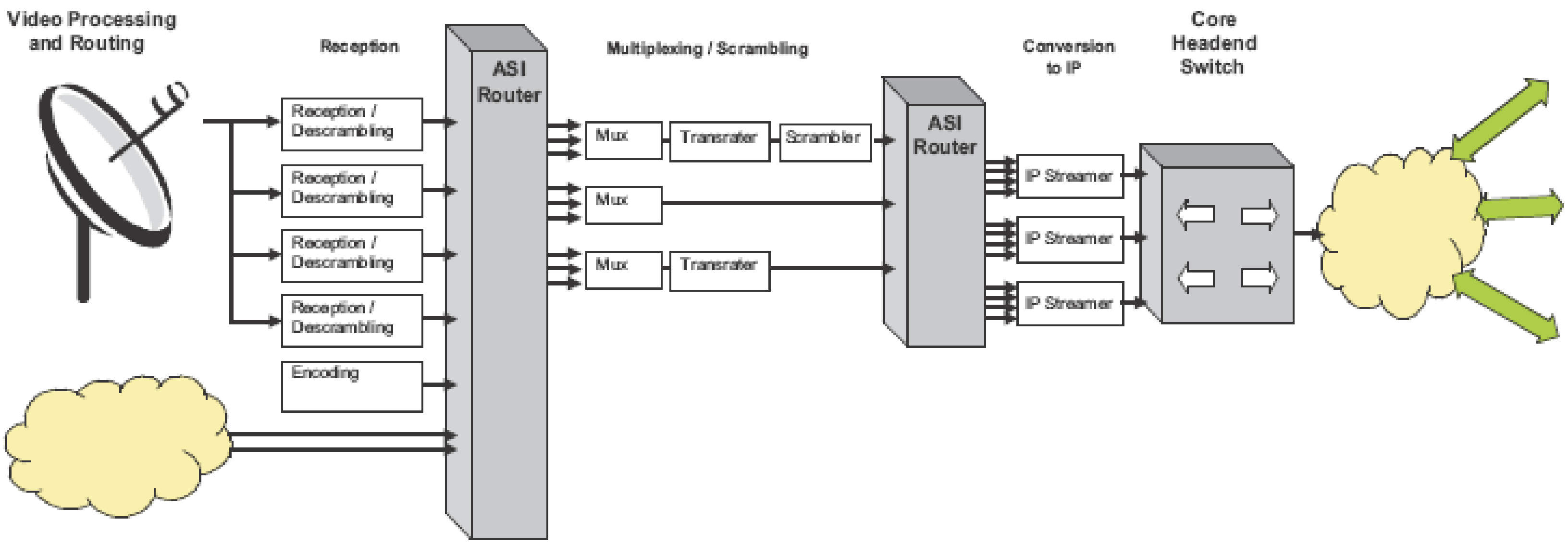
The cost (equipment and support) of an IP/Ethernet backbone is cheaper than ATM, it has better scalability, and link efficiency is higher. The bi-directional nature of IP is also better suited to applications such as Video on Demand and gaming.
QAM is Quadrature Amplitude Modulator.

Video over IP Advantages

- Lower transport network cost
  - Ethernet switches are cheaper than dedicated ASI routing equipment
- Network resources are easily shared
  - Physical location of device less important if connectivity is IP based
  - Processing devices can be centralized
- Simple headend and hub wiring
  - Cat5 or fiber based, like data networks
  - Several connections can be carried over a single cable

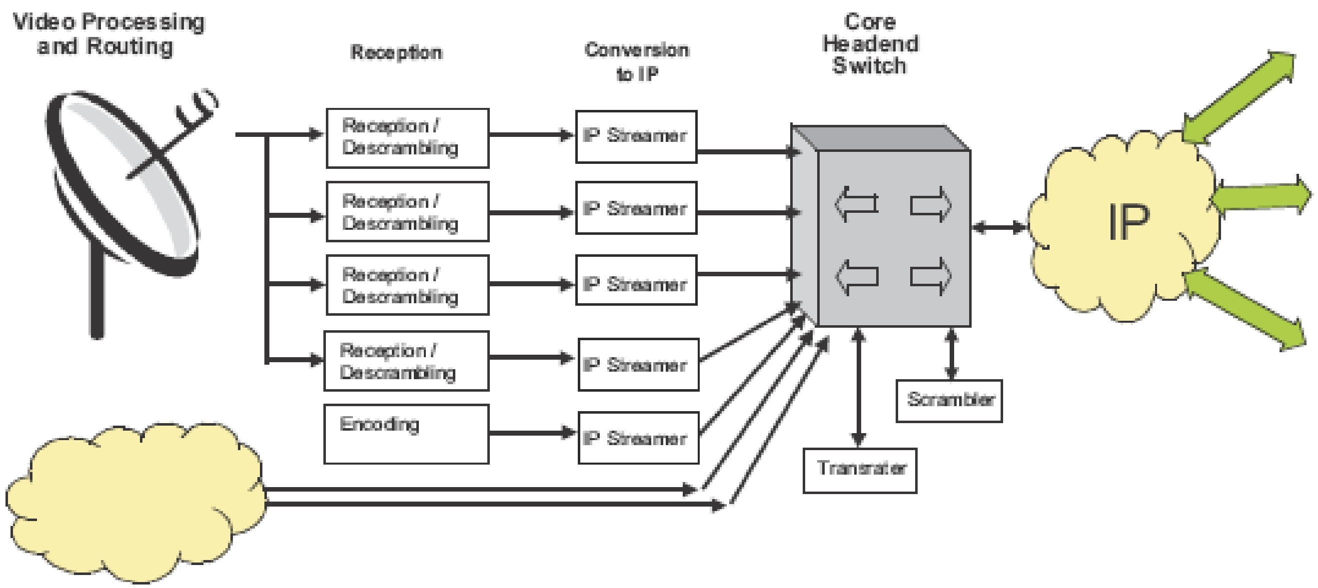
- IP supports broadcast and multicast
- Easier to distribute SPTS and therefore avoid unnecessary remultiplexing

Classical Headend With IP Output



Classical Headend with IP Streaming Output

Future IP-based Headend



Future Headend with Early Conversion to IP

Typical Applications

- ASI (Asynchronous Serial Interface) replacement within Headend
  - For connectivity reasons
  - For early encapsulation to IP
- Distribution – CHE (Central Head End) to RHE (Regional Head End)
  - Utilize IP/Ethernet backbone
  - Exploit benefits of IP Multicast
- Monitoring
  - Remote monitoring easier with IP
- “Modulation” alternative
  - Ultimately IP broadcast (Video over DSL (Digital Subscriber Loop) or IPTV) is enabled
- Home Networks
- Security
- SDI (Serial Digital Interface) over Ethernet applications: WAN distribution, Monitoring, Medical

Keep in mind

- “The R&D spend of Cisco and the rest of the IP networking community is greater than the R&D budget for the entire global broadcast industry”
- “IP will become ubiquitous as a connection medium, eventually reaching the set-top box”
- “Proprietary interfaces that currently dominate the broadcast market will become extinct”

Network Encapsulation Layers

OSI Reference Model

Application	7
Presentation	6
Session	5
Transport	4
Network	3
Data Link	2
Physical	1

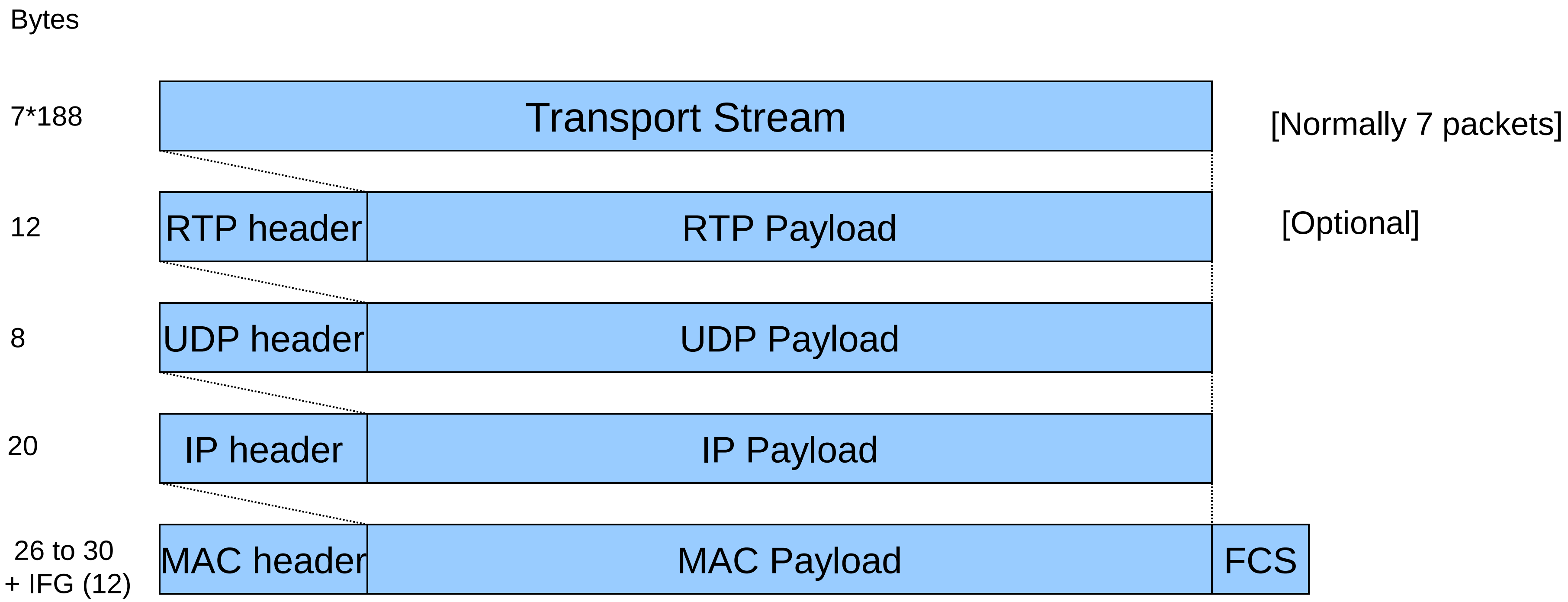
TCP/IP Reference Model

Process/ Application	e.g. FTP, HTTP
Host-to-Host	e.g. TCP, UDP, ICMP
Internet	e.g. IP, ARP
Network Access	e.g. Ethernet

Transport Stream Encapsulation

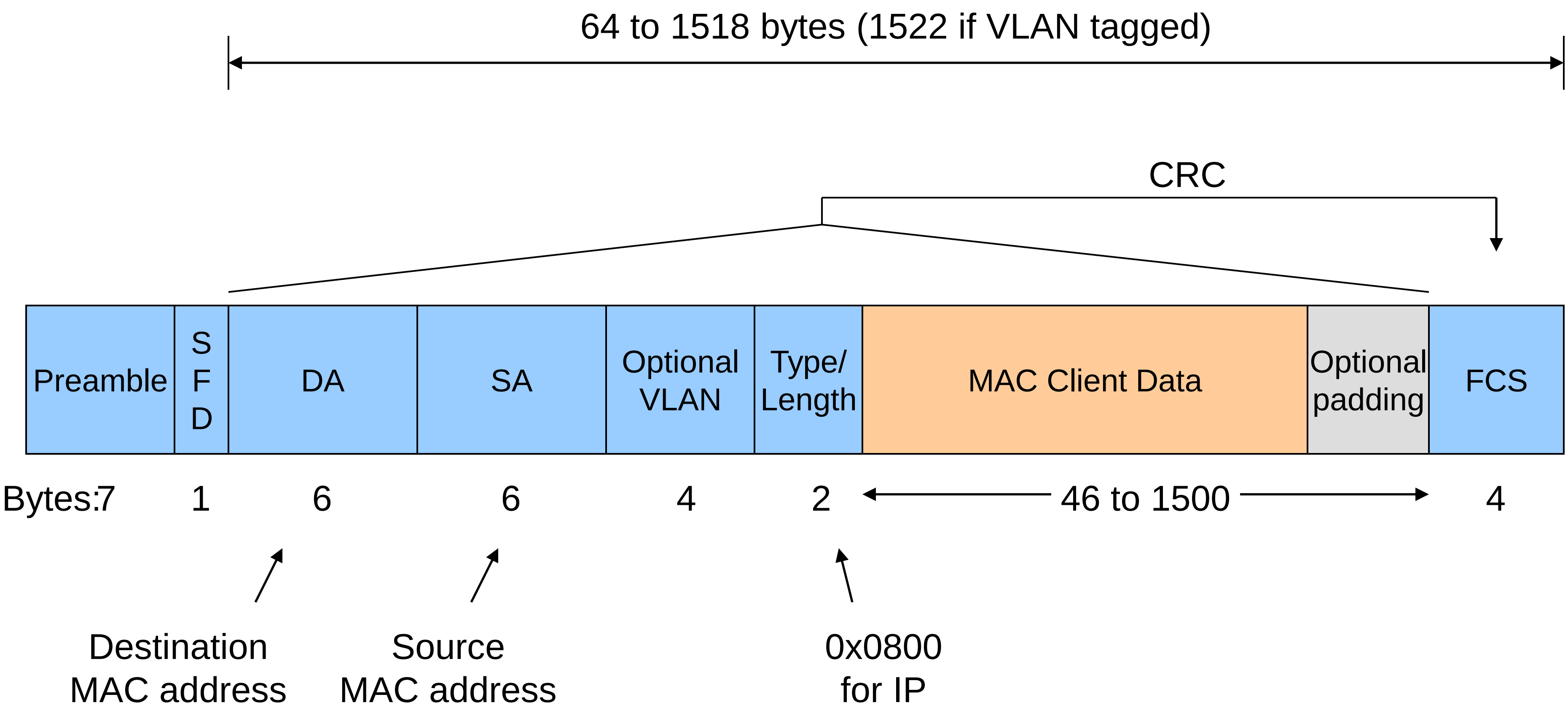
- Transport Stream data is most commonly encapsulated using the User Datagram Protocol (UDP)
  - Simple encapsulation with low overhead
  - Suited to high bandwidth data, especially for broadcast or multicast applications
  - But no guarantee of delivery (unlike TCP)
- UDP payload can just be TS packets
- But the Realtime Transport Protocol (RTP) is often used as an additional layer of encapsulation
  - Provides sequencing information that is missing from UDP
  - Includes timestamp which may be useful for reducing network induced jitter
- Ethernet is the most common network medium for LAN applications
- WAN distribution of IP is enabled by technologies such as DWDM (Dense Wavelength Division Multiplexing)

Transport Stream Encapsulation



Up to ~94% of frame can be TS payload

MAC Layer



96-bit minimum interframe gap

IP Layer (IPv4)

20 byte header (shown as used, without options)

<table>
<tr><td>Version</td><td>IHL</td><td colspan="2">Type Of Service</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>0</td><td>DF</td><td>MF</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>

UDP Layer

8 byte header

UDP Source Port Number	UDP Destination Port Number
Message Length	Checksum
Data	

The port number represents a "connection". Different applications running on the same machine will uses different port numbers so that individual packets can be associated with their application. The combination of IP address and port number is often referred to as a "socket".

The UDP checksum is typically not calculated for Transport Stream applications

RTP Layer

12 byte header (shown as used, without options)

<table>
<tr><td>V
(2)</td><td>P
(0)</td><td>X
(0)</td><td>CC
(0)</td><td>M
(0)</td><td>PT
(33)</td><td>Sequence number</td></tr>
<tr><td colspan="7">Timestamp</td></tr>
<tr><td colspan="7">Synchronization Source (SSRC) Identifier</td></tr>
<tr><td colspan="7">Data
(1 to 7 TS packets)</td></tr>
</table>

A Payload Type (PT) of 33 is used for MPEG-2 Transport Stream
The Sequence Number increments for each RTP frame sent
The Timestamp is the value of a local 90kHz counter at the time of transmission

Specifications

- IP, UDP and RTP were all defined by the Internet community under the control of the Internet Engineering Task Force (IETF)
- Relevant “Request For Comment” (RFC) documents are:

Protocol	**RFC**
IP	RFC791
UDP	RFC768
RTP	RFC3350
RTP Payload Format for MPEG1/MPEG2 video	RFC2250

Concerns Relating to IP Networking

- Packet loss
- Packet reordering and duplication
- IP Fragmentation
- Latency
- Jitter
- Network failure
- Security

Packet loss

- Loss of 1 Ethernet frame results in loss of up to 7 TS packets
  - Highly likely this will have a visible effect
- UDP does not provide delivery guarantee
- Bit errors
  - Little different to any other connection medium
  - Will result in CRC error and dropped frame
- Network congestion
  - If switch buffer capacity is exceeded, frames will be dropped
  - Likely to lose a burst of frames
  - Can prioritize traffic so that “data” is dropped first (DiffServ model)
  - Can design network to handle traffic bandwidth and therefore avoid congestion in the first place
- Recovery mechanisms can be implemented based on retransmission or forward error correction
  - Both schemes affect latency so not suitable for every application

Packet reordering and duplication

- Individual routing of IP packet from source to destination can result in packets being received out of order, or being received more than once
- Typical network switching and routing protocols will establish a single path from the source to destination, once initial learning process is complete
  - Reordering event only likely if network configuration changes or if routing information is “aged”
- UDP does not provide a means to detect packet order
- RTP adds a sequence number

IP Fragmentation

- IP packets can be up to 65535 bytes in length
- If underlying network cannot handle the packet size, the IP packet is “fragmented” resulting in multiple layer 2 frames
  - Maximum Ethernet frame size is 1500 bytes
- IP fragmentation and reassembly is undesirable for a high bandwidth connection due to processing overhead and latency penalty
- If the DF bit is set in the IP header then the packet will not be fragmented. Instead a message is sent back to the source indicating the maximum packet size that can be supported. The source can then reduce the size of the packets it generates
  - This is the recommended mechanism for Video over IP

Latency

- Not important for TV broadcast applications
- Much more important for
  - Video Conferencing
  - Remote Control, e.g. Remote Surgery

Jitter

- Variable network latency will result in packet arrival jitter
- A buffer at the receiver is required to accommodate the maximum anticipated delay and thus avoid overflow
- A minimum depth must be maintained in the receiver buffer to avoid underflow
  - This adds latency to the connection
- Jitter also affects the PCR (Program Clock Reference) based clock recovery scheme
  - The time that the PCR packet is received is compared with the time that it was expected (using difference from previous value and local elapsed time)
  - Any difference is used to adjust the local clock frequency
  - PCR jitter will look like a frequency error
  - Network jitter can therefore propagate to local clock and may affect the quality of the output video
  - There is a ±500ns constraint on PCR accuracy (PCR_AC, the accuracy of the value stored in the original stream) but no defined constraint for overall PCR jitter (PCR_OJ)

Network Failure

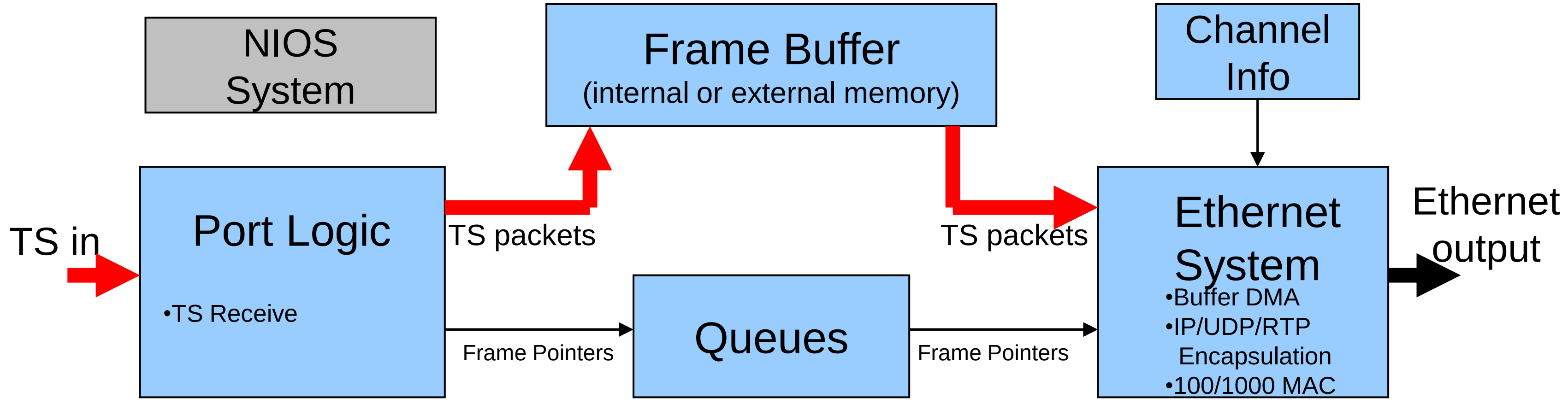
- Packet loss
  - Quite frequent
  - Can use forward error correction
- Network path loss
  - Alternative network paths

Security

- Not well developed
- Encryption is quickly broken

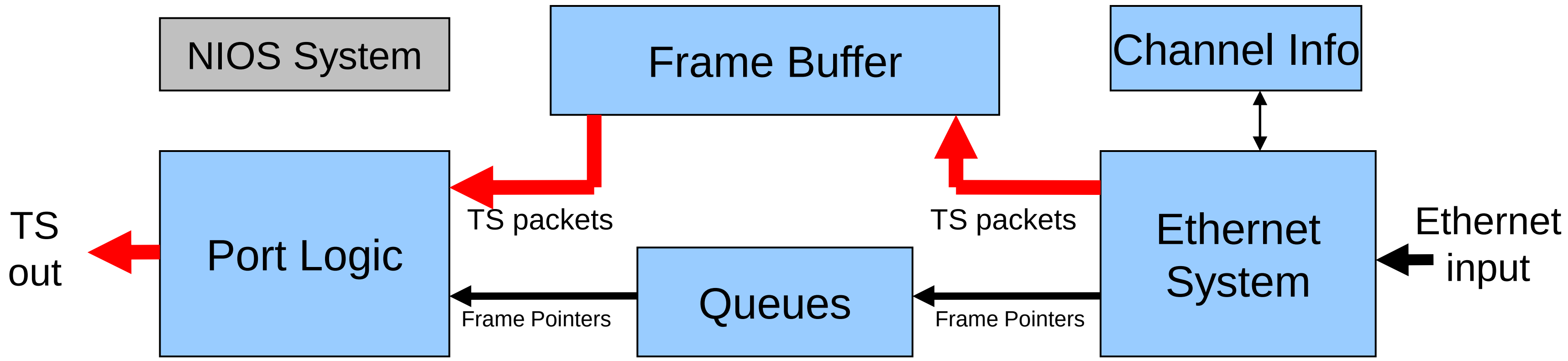
TS to Ethernet

- 1-7 TS packets (188/204 bytes each) are aggregated to make one Ethernet frame (1500 bytes max) which is stored in the Frame Buffer
- Once frame construction is complete, an entry is loaded to the transmit queue
- The transmit queue is read and the related frame fetched from the Frame Buffer and encapsulated by the hardware for Ethernet transmit
- Encapsulation parameters (e.g. MAC destination, IP addresses, UDP ports) are read from the software configurable Channel Info block



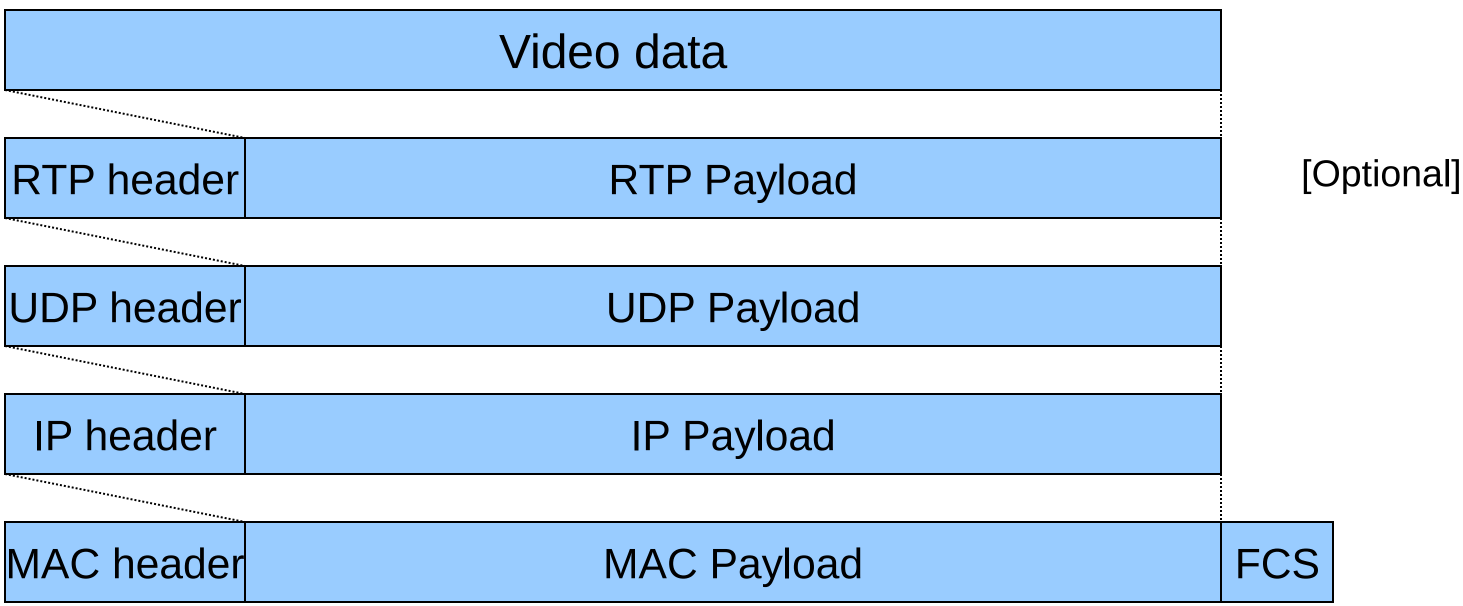
Ethernet to TS

- Frames are received from the Ethernet input, address matched and written to the Frame Buffer
- The frame destination (e.g. TS output or host) is determined by the Channel Info block by matching encapsulation type, IP address, UDP ports etc
- An entry is loaded to the appropriate receive queue
- The receive queue is read and the related frame fetched from the Frame Buffer
- For video traffic, the frame is split in to TS packets and output on the appropriate port



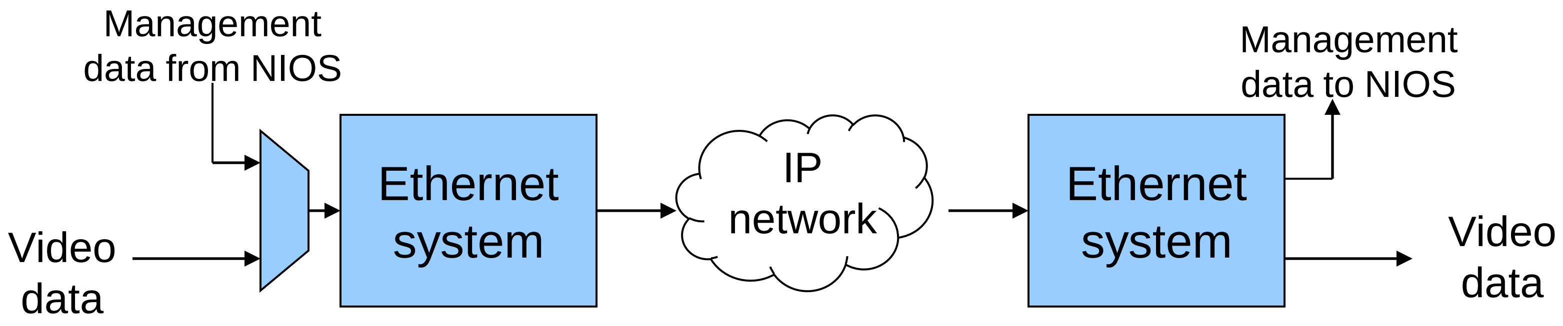
Hardware IP/UDP/RTP Encapsulation

- Video data is encapsulated using IP, UDP and (optionally) RTP headers
- Encapsulation and de-encapsulation is performed in hardware to maximize bandwidth and minimize latency
  - No software involvement for transfer of video traffic
  - Line rate performance is achievable
- Encapsulation parameters are configurable per transport stream

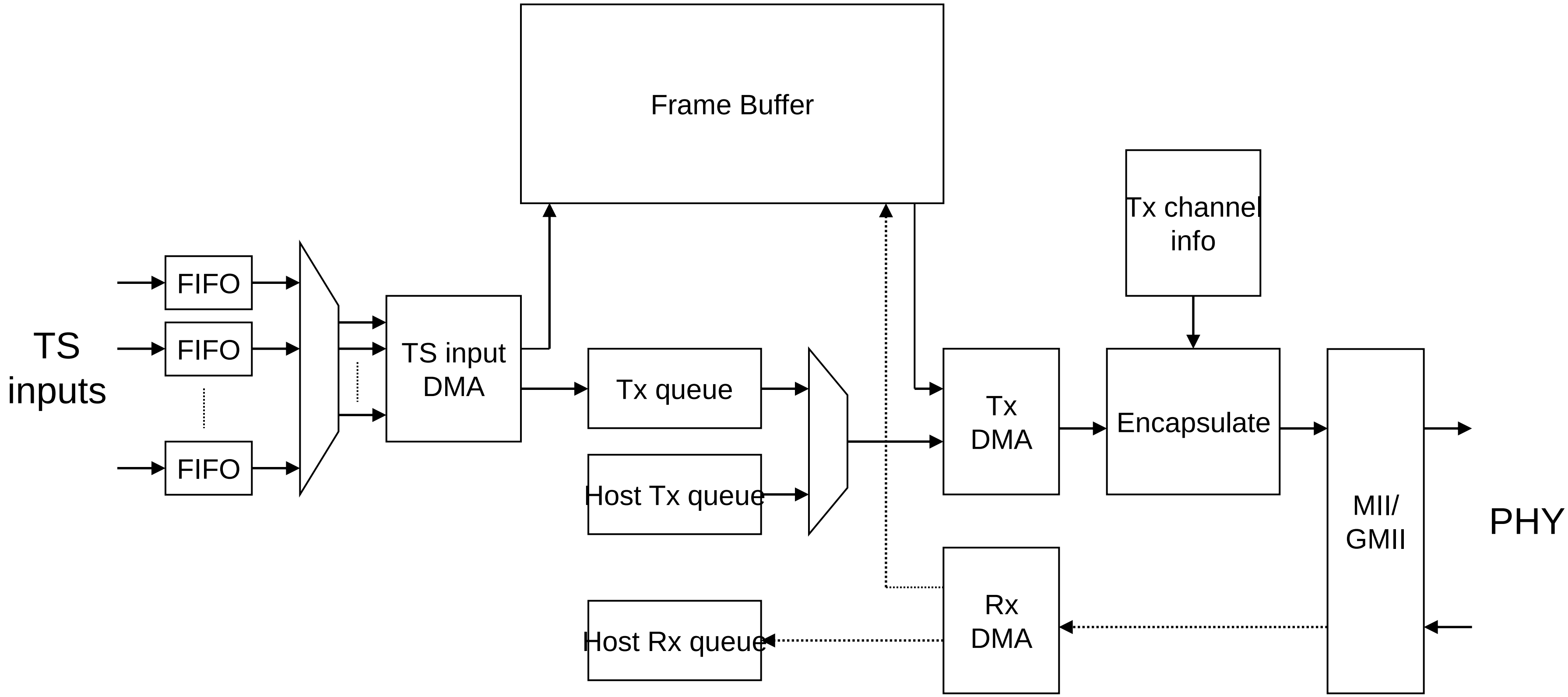


Nios Management Port

- Management packets are processed in software running on a Nios-II processor
  - MAC/IP layer management, e.g. ARP, ICMP
  - Resource reservation, e.g. DiffServ
  - Session management, e.g. RTSP, IGMP
- The reference design includes basic software to:
  - Configure operation
  - Manage the Ethernet link
  - Collect statistics
- A web server is implemented to support remote monitoring and control over the IP network

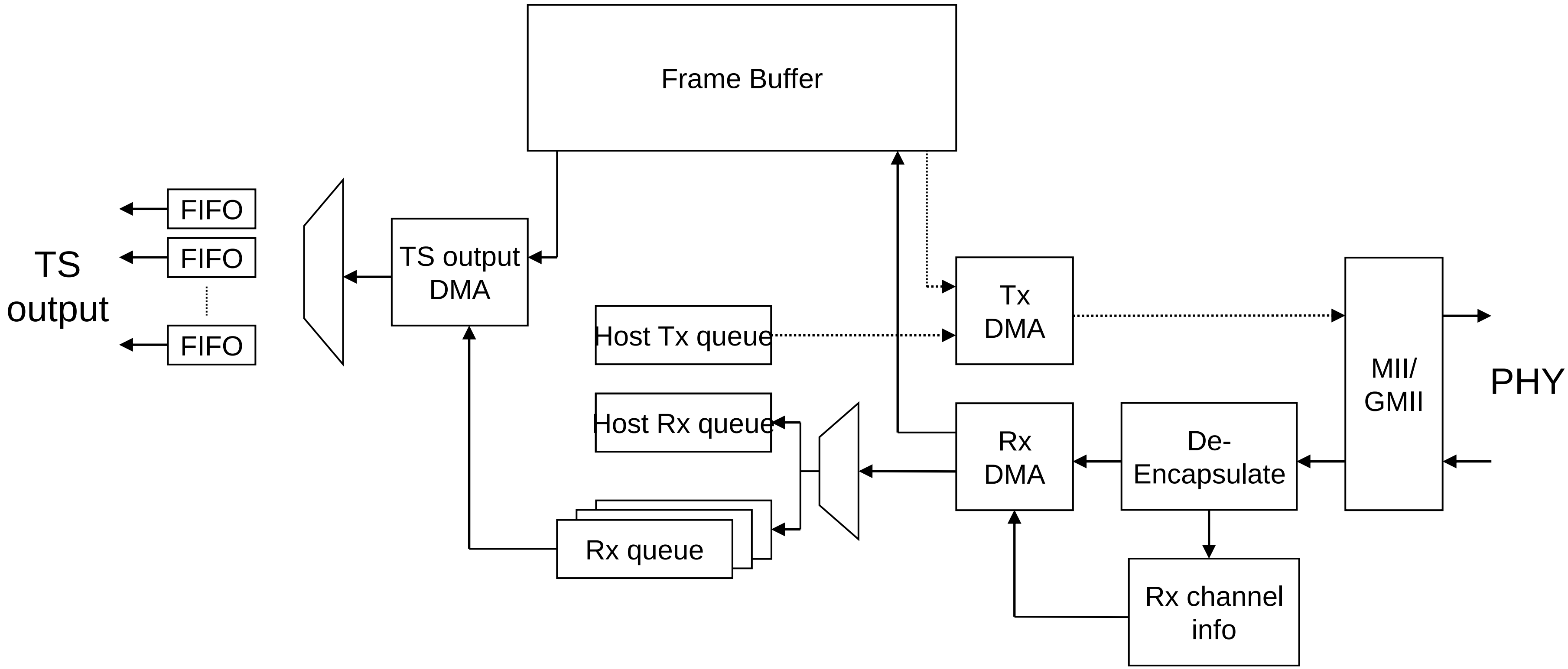


TS to Ethernet Bridge



Note: The design can handle traffic in both directions simultaneously

Ethernet to TS Bridge



Note: The design can handle traffic in both directions simultaneously

BitTorrent

- Distribute a large video file to many destinations
  - A node with the complete file is called a seed
  - A node that needs the file is called a client
  - A node that has part of the file is called a peer
  - A coordination node is called the tracker
- The file is distributed in pieces, between 32kB and 16Mb, typically 512kB

BitTorrent

- A client who needs a file contacts the tracker
- The tracker instructs the client to contact a peer that has a part of the file
- The client contacts that peer and downloads that part of the file
- The client now becomes a peer and can distribute that part of the file to others
- The client contacts the tracker again for another part of the file
- Continue until everybody has all they want

BitTorrent

- Files are not downloaded in sequence This is not a streaming protocol
  - (A BitTorrent streaming protocol is under development)
- Use BitTorrent to download and store an entire movie and then watch the movie

BitTorrent

- The advantage of BitTorrent is that the message transmission load is distributed more evenly across the network
  - If hundreds of clients all want the same movie and if the source must send a copy to each client then the source node might be overwhelmed
- It is possible to arrange for clients to contact peers that are close to them in the network
  - This might reduce the load on the network

BitTorrent

- A disadvantage of BitTorrent is that you are transmitting as well as receiving data
  - If your ISP starts to charge you per byte, which most of them will probably soon do, you will have to pay extra for transmissions
- Another disadvantage of BitTorrent is that, if the movie is pirated which is quite usual, then you are distributing pirated information

Further Reading

- "RTP – Audio and Video for the Internet", Colin Perkins

  Includes a good overview of relevant networking issues, as well as the basics of RTP
- DVB-IPI and Pro-MPEG WAN specs
- Whitepapers from Scientific Atlanta and Harmonic

  Overview of the potential markets from the headend equipment suppliers' perspective
- Whitepapers from Path1

  Path1 make equipment dedicated to video transport over IP and therefore have a strong understanding and good experience of this application
- Whitepapers from Tektronix, Ineoquest and Pixelmetrix

  The test equipment providers