

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION

ISO/IEC JTC1/SC2/WG11

CODING OF MOVING PICTURES AND ASSOCIATED AUDIO

ISO/IEC JTC1/SC2/WG11
MPEG 92/ 754
November 1992

Title: Requirements and Method for High-level Multiplexing of MPEG and Other Digital Service Bitstreams With Universal Transport Layer

Source: Anthony J. Wasilewski, Scientific-Atlanta

Purpose: Contribution to MPEG Systems for MPEG-2 System Development

1 ABSTRACT

This note presents an overview of the requirements and processes for multiplexing and providing transport and conditional access in a Digital Compression Services Delivery System (DCSDS). It considers an array of application domains that address numerous business segments and recognizes a plurality of digital services that include full motion video, film, audio, teletext and character/binary data. Basic multiplexing requirements, techniques and a suggested method of transmitting a multiplicity of services, including MPEG bitstreams and entitlement information via a Transport Layer are discussed.

2 APPLICATION DOMAINS

Any practical approach for a DCSDS must take into account the nature of the transmission media and the decoding environments of the intended application domains. In particular, the design of the system must promote economical implementation of the decoders by shifting complexity into other parts of the hardware solution; this usually means the encode device(s) or other parts of the transmission network. The system

design must also be heavily influenced by the needs of the end users (consumers) of the payload signals.

Further, the transmission approach must support physical routing of multiplexes of services as seamlessly as possible over multiple transmission media, with the ability to straightforwardly decompose the constituent data streams and recombine them in new combinations, all with hardware of minimal cost at intermediary and endpoint nodes.

This transmission flexibility must be coupled with a fully transparent and uniform access method that allows adaptable and dynamic packaging of services in accordance with the (changing) business model of the network operator and the network itself.

Figure 1 shows a typical system architecture in the CATV/DBS environment. As indicated, a layered approach to multiplex construction, which includes compression, error-correction and conditional access is possible.

The DCSDS should embody a solution that functions favorably in the following application domains:

2.1 NTSC, PAL, SECAM

A primary requirement for a commercial DCSDS is the transport and subsequent decoding of conventional television signals which originate in the NTSC, PAL and SECAM formats. This must take into account the diverse display parameters found in these standards such as horizontal line rate, frame rate, number of scan lines per frame and color subcarrier frequencies. Ideally, the multiplexed data stream itself would run at rates which provide a common clock source that can be used by the decoders to reconstruct the specific rates and frequencies needed.

The multiplex should also permit multiple modes of compression to be utilized for each analog standard and for the simultaneous transport of videos sourced from and displayed for all the analog standards.

2.2 Digital Audio

Of equal importance is the transport and decoding of a multiplicity of digital audio signal standards. Standards exist which encode digitized audio at sampling rates of 32 KHz, 44.1 KHz and 48 KHz. The channel bit rates for these standards range from 64 Kbps to 320 Kbps and in most cases must be synchronized with associated video programs.

A number of applicable standards exist or are being developed, for example:

SEDAT I, II - Scientific-Atlanta

AC1 (ADM), AC2, AC3 - Dolby Labs

Musicam - Phillips

2.3 C-Band and Ku Band Satellite

The DCSDS must be designed to accommodate transport over existing and future C-band (36 Mhz) and Ku Band (24 Mhz) satellites. The preferred modulation method is QPSK. These transmission systems are characterized primarily by a Gaussian noise distribution, but protection for burst errors must also be considered.

Because of variations in signal strength over the satellite footprint and a large range of equipment

parameters in existing downlink receive sites, provision must be made for the DCSDS multiplex to be adaptable to varying receive margin requirements. These may cause the requirements for overall data rate and error correction to be divergent on a case-by-case basis.

2.4 CATV, SMATV

The existing installed base in international CATV plant presents a broadband transmission path that is very attractive for consumer delivery of compressed, multiplexed entertainment/informational signals. RF modulation methods such as 16-QAM, 4-VSB and others provide or will provide commercially-viable means for transport of a large number (150+) of 6, 7 or 8 Mhz channels. Each channel, has capacity to carry up to 10 compressed film/video sources with current compression techniques.

Programmers and operators are already considering many new applications for the coming expanded channel capacity. Near Video-On-Demand (NVOD) and Video-On-Demand (MOD), One-way interactive services, Video Game delivery, ad insertion and Text-based News delivery typify the anticipated directions.

Consumers want a large variety of services which are selectable in a simple and friendly manner with short signal acquisition times to accommodate "channel surfing". Electronic Program Guides (EPGs) will likely be needed to help the user in sorting through the greatly expanded service offerings. The user interface must be uniform and self-revealing even though a wide range of service types are available.

Specialized Satellite Master Antenna TV (SMATV) applications, such as movie service distribution to hotels and hospitals, will present demands similar to those of terrestrial cable.

2.5 Broadcast/HDTV

Because the broadcast HDTV standard selected by the U.S. FCC will likely be an all-digital one, a DCSDS must be able to carry such a standard for delivery over broadband media, like those listed above. The main requirement is that the payload bit rate supported must be in the 16 Mbps to 18 Mbps range. A provision for applying conditional access to the HDTV data stream should also be available.

2.6 Direct Broadcast Satellite (DBS)

Directly broadcasting to the home via C-band or Ku Band satellite channels is greatly augmented by compression technologies. The leveraging factor of many services per channel is perhaps of even greater importance than in the CATV case, since the cost of adding extra channels (transponders) is greater.

The consumer issues are all very similar to those found in cable distribution. Decoder cost is somewhat less critical than for home terminal converters, but is nonetheless an important driver in the DBS business model.

Uncomplicated and cost-effective integration of the receive and decode functions is of primary importance in this application. Switchable decompression solutions in the decoder may also be of interest.

2.7 Business Television and Videoconferencing

Distribution of strategic, informational and training-oriented business information in video, audio and data formats, amongst geographically separate locations, is currently served with systems that multiplex digital and analog services, such as Scientific-Atlanta's B-MAC products. The migration to an all-digital system with the feasibility of a totally encryption-based security approach and, of course, the greater information bandwidth offered by compression, will be a natural one.

Business Television (BTV) applications that call for live teleconferencing between potentially several geographically separate locations, bring specific access requirements in the area of point-to-point addressing, cross-networking and authorization churn that must be handled in a viable system design. In the large though, these BTV operations also share many of the characteristics of the traditional entertainment delivery systems.

2.8 North American Digital Hierarchy and SONET/ATM

It is often noted that a convergence of television, telephones and computers is underway. This will emphasize the need to transport compressed video, audio and data services in a common multiplex across not only the usual broadcast channels, but also over terrestrial channels conforming to the ANSI T1.107-1988 Digital Hierarchy (DS1, DS3, etc.) and the ANSI T1.105-1991 Digital Hierarchy -Optical Interface Rates (SONET). At the very least, scalability of the multiplex to at or near the specified overall channel rates is implied.

These standards feature specific framing and stuff-bit patterns which a DCSDS multiplex will be called upon to conform with. Timing or synchronization requirements within the DCSDS multiplex must survive any alterations in rate imposed by the telephony transmission standards. Asynchronous Transfer Mode (ATM) provides the concept of an Adaptation Layer (AAL) for this purpose and the CCITT is working to achieve a common segmentation and reassembly (SAR) layer for the 4 classes of services they have identified.

ATM, while not yet a finalized protocol, has nonetheless already garnered considerable support and may very likely appear in LAN solutions even before it emerges in a wider network arena. It is a frame relay approach which uses fixed-length packets as its delivery mechanism. Mapping into this standard may be important for a DCSDS.

2.9 Worldwide Telephony

Compatibility with standards such as the CCITT Rec. G.742 second-order multiplex and other related line rates is also required.

2.10 Traditional Data Networks

While current medium-speed data networks such as Ethernet are not fully suited for transmission of compressed real-time video because of their non-deterministic access methods, multimedia applications will drive the need for video and audio transmission over networks of computers. Inter-office teleconferencing between ordinary PCs or workstations over high-bandwidth Fiber Channel

(ANSI X3T9.3), FDDI and/or ATM-based LANs may become common.

The design of the DCSDS should anticipate its usage over such communication channels.

3 REQUIREMENTS

Considerations from the application domains mentioned in § 2 lead to an assortment of technical requirements for the multiplex format and transport strategy for the DCSDS. A practical implementation should take these requirements into account in providing a cost-effective solution.

This section highlights the requirements for the DCSDS. The concept of a "transport layer" is introduced.

3.1 Separation of the Transport Layer from Services/algorithms

The digital services and the compression algorithms that are used for their transmission will likely change and evolve with time. While DCT-based video compression algorithms represent the currently preferred approach, investigation of wavelets, fractals, vector quantization and presently unknown methods may bring about advances that make their use appropriate and cost-justified. Indeed, new, currently-unimagined application domains may be better served by such compression approaches.

The design of the DCSDS must anticipate this evolution and permit a seamless and transparent changeover in the network. The multiplex, in fact, should accommodate the concurrent transport of multiple compression standards, both audio and video.

In many cases, several services may be transmitted as an associated set; one video and many audio channels providing stereo pairs in several languages is an example. This associated set should be combined into a "channelized" bitstream which can be de-multiplexed and routed as an independent entity.

At the same time, many applications will require multiple channelized services, conditional access, security and system data to be carried in a single multiplex. This latter data is, in the large, independent

of the service types and compression algorithms used for the services. It is therefore desirable for the DCSDS bitstream to be constructed from:

- a) a high-level multiplexing strategy
- b) a transport layer
- c) channelized service packages

The transport layer is used as a universal vehicle for the conveyance of certain parameters of the multiplexing strategy, conditional access data streams and system information.

The transport layer describes the number and type of services that are carried in a multiplex and supplies the mechanism by which these services may be accessed, controlled and demultiplexed. The transport layer may also provide certain system services such as operational teletext messages that decoders may access and display for user interface or exception handling conditions.

3.2 Independence of multiplex from transmission medium

The DCSDS multiplex must be oriented towards the end-consumer of the transported services, not solely to the technology or to the physical channel over which it is carried. This channel may vary, even along one end-to-end transmission path; a program originated at a C-band uplink may be received at a CATV headend and then sent directly through a terrestrial distribution plant to be decoded by a home terminal in a subscriber premise. The distribution plant may have a fiber-optic trunking system and traditional coax cable thereafter.

In other applications, regionally-produced programming may be backhauled over fiber-optic networks and then uplinked over Ku Band satellite transponders.

The multiplex should be inexpensively and seamlessly routable over such network combinations and its subparts should be extractable at intermediate nodes without costly processing.

3.3 Error management optimized for the transmission channel

Another requirement driven by the need for

Independence of the bitstream from the transmission medium, is the optimization of error correction for the physical channel. The degree and type of error correction/detection must deliver appropriate operational characteristics without burdening the system with undue overhead.

Thus, error correction sufficient for the relatively low BERs found on optical networks will not be suitable for CATV applications where burst error rates and powerline-frequency-synchronized ingress may cause temporary signal loss due to the "cliff effect" of digital systems. In CATV systems, normal operating procedures, such as the use of frequency sweepers for plant diagnostics are an expected source of channel noise. Error correction suitable to channel BERs of 10^{-4} are required.

For C-band satellite, similar protection is called for, but in the Ku band the most powerful schemes are needed, because error rates are higher (to 2×10^{-3}) and less predictable.

3.4 Seamless, layered error correction from satellite to cable or other medium

The differing error requirements of the various physical media of interest, should be applied as layers or "sheaths" that may be readily removed at boundaries between the media. This enhances the possibility of producing cost-efficient hardware for commercial applications of the DCSDS in situations where the payload signals must traverse a large number of media on their way to the end-user.

3.5 Error management optimized to data type

Within the context of a fixed overall channel error protection, parts of the bitstream may be more critical than others. Also, some parts of the bitstream will comprise a much smaller share of the bandwidth than others, thus allowing the overhead due to error correction to be larger.

A hierarchy of error coding may be established which combines both of these principles. From highest to lowest protection, the hierarchy is:

- 1) Synchronization
- 2) System Data, Encryption seeds,
Multiplex control
- 3) Conditional Access
- 4) Utility Data
- 5) Video/audio/teletext

Conditional access data may require additional error-detection so that packets which can not be fully error-corrected may be rejected by the receive terminal to be obtained later on a re-transmission.

3.6 Fast Acquisition time/cryptographic cycles

The consumer demands fast signal acquisition times - at least for video. The practice of "channel surfing", that is, depressing either the increment or decrement key on the home terminal remote control while watching the pictures go by, in order to make (or perhaps to avoid making!) a selection, is commonplace. At least in the U.S., consumer studies have shown that periods between picture lock-up that are longer than about 200 ms become annoying, while 500 ms periods are unacceptable. This presents a significant challenge in digital systems.

The time required for acquisition, in the most general case, will be composed of:

- a) tuner slew
- b) de-multiplexing
- c) de-erroring
- d) Seed delivery and decryption
- e) rate buffering
- f) I-frame sequence (if predictive coding)

Assuming linear or non-linear PRBSs are used to encrypt the basic service streams and that asymmetric, private key cryptography is employed at other levels, such as seed encryption, the time needed to acquire and deliver the seeds for the PRBS generators and the frequency with which the seeds are changed (cryptographic cycle) will be a determining factor for signal acquisition speed.

If predictive video coding is used, it is most efficient to harmonize the cryptographic cycle and I-frame sequence.

3.7 HDTV compatibility

As noted in § 2, a digital HDTV standard is highly likely. The compressed bitstreams of the four all-digital proposals should be considered as potential services to be carried over the variety of network types previously discussed. In fact, it is probable that the selected High-Definition standard may be commercially transmitted over satellite and CATV pathways before widespread over-the-air broadcast becomes available. A viable DCSDS will include the capability for this type of transport.

The four digital Advanced Television (ATV) proposals: Zenith/AT&T, ATRC, ATA Digicipher, and ATA Channel Compatible Digicipher, share many common features such as DCT-based and entropy coded compression, 16:9 aspect ratio, motion estimation/compensation, frame rate (59.94 Hz) and Reed-Solomon error correction. They differ in other areas such as their scanning systems (1050 Interlace vs. 787.5 progressive), motion estimation techniques (block size, convergence method), DCT coefficient coding techniques (ADPCM, vector, adaptive vector), channel modulation specifics (32-QAM, 2/4-VSB, 32-QAM dual carrier) and audio systems (Dolby AC-2, Musicam, MIT).

The DCSDS should be able to treat the transport of these ATV signals with reasonable adaptations. Where mixed modulation modes are used, a single mode may be substituted. The data rates required (on the order of approximately 17 Mbps) should be accommodated.

3.8 Can be transmitted over standard circuit-switched TDM telephony multiplexes

The North American Digital Hierarchy as defined in ANSI T1.107-1988, the CCITT G.742 and its related standards and other international telephony multiplexes, specify discrete channel bit rates and relatively rigid framing and bit-stuffing rules to provide adjustability for rate-matching in time-division-multiplexed (TDM) digital channels. Some example North American rates are:

Standard	Overall Rate (Mbps)	Information Rate
DS1	1.544	1.536
DS1C	3.152	3.088
DS2	6.312	6.176
DS3	44.736	43.232

The deployment penetration of any particular rate varies; DS1 and DS3 are the most popular. The capability of these multiplexes to combine voice and data over cost-effective leased lines may lead to a broader use of multimedia services in mainstream business telecommunication networks, if video can also be accommodated.

Therefore, a DCSDS multiplex should be capable of running at rates comparable to these and should have a channel bit rate that is selectable with a suitable granularity so as to be efficiently less than or equal to the nominal information rates shown above.

In meeting such requirements the DCSDS would support transmission of service multiplexes (which may include video) over existing circuits utilizing industry-standard switching and crosspoint equipment.

3.9 SONET/ATM compatibility

Future digital telephony services will provide significant global data delivery mechanisms in the current and following decades. Some promising standards which are still in the process of becoming finalized and which have not yet received extensive service-carrier support are the Synchronous Optical Network transmission hierarchy (SONET) and Asynchronous Transfer Mode (ATM). These provide the physical, data and transport protocols for the Broadband Integrated Services Digital Network (B-ISDN).

SONET will make available very large bandwidth (gigabit and above) data pipelines over the world's telephone system. Deployment of such networks is progressing very slowly, and even Narrowband-ISDN (N-ISDN) line access is currently only between 15% and 50% in the seven regional Bell companies in the U.S.

Both SONET and ATM seem destined for widespread

popularity, however. The ability to use SONET and to map the DCSDS multiplex approach into the asynchronous cell-relay format offered by ATM will give it a more universal relevance in global digital switched delivery environments in the latter part of this decade.

ATM provides fixed-length 53 byte "cells" which occur in the transmission channel on an isochronous basis. Each cell is pre-pended with a 5-byte header that contains routing and channel-usage information. This yields a 48-byte payload. Thus, a connection-oriented service is possible in which a single point-to-point or point-to-multi-point transfer is accomplished via explicit cell routing. ATM cells provide a high-speed switching mechanism (millions of cells per second) with low delay, in which video, voice and data traffic can flow on a freely intermixed demand-packet basis. For data, ATM can supply non-blocking transmission and a guaranteed bit-rate. In fact, ATM may see deployment in private LAN environments before its general usage in wide-area networks.

It should be noted that without some additional conditional access mechanism, ATM data streams would be liable to illegal reception and distribution, although the intended physical transmission medium (if optical fiber) may make this more difficult than some other methods. The DCSDS should provide the additional security and signal protection.

3.10 Scalability in service data rates

A practical digital services transmission system must support a large range of service rates: From HDTV signals at 16 to 18 Mbps to computer-oriented services at 9600 bps or less. Within a single service category, bit rates may also vary widely. Thus, a single system may need capabilities to accommodate the transmission of relatively low bit-rate (approximately 1 Mbps) movie-sourced material or studio-quality video signals at around 8 Mbps. These may need to be carried simultaneously or the channel bandwidth may need to be re-allocated over time to a changing array of services at varied bit rates.

The control of such allocation and the flexibility of data rates provided must be scalable so that service allocations within a fixed channel rate may be simply and efficiently altered in a manner that may be handled by a uniform encode/decode hardware implementation.

3.11 Flexible re-allocation of bandwidth between services

Depending on specific network features, the fixed bandwidth available in a transmission channel may demand reallocation amongst a changing array of services on daily, hourly or even more frequent intervals. The control structures in the DCSDS should provide a mechanism for such reallocation.

Some examples would include one high-rate video being replaced by several videos of lower rate; audio channels being reassigned as data conduits; and an entire channel being designated to carry conditional access packets during certain hours.

3.12 Support for statistical multiplexing

An even more dynamic form of data reallocation is required in the form of statistical multiplexing. This is the active sharing of the total channel video data rate amongst several independent video bitstreams on a frame-by-frame basis. Thus, video bit rate not used to encode a video with a scene of relatively lower complexity (and/or high temporal correlation to a previous scene) can be assigned in real-time to video streams which have scenes of higher complexity (and/or low internal temporal correlation).

3.13 Scalable in overall channel data rates

The design of the DCSDS multiplex must be directly adjustable to handle total channel data rates over as wide a range as permitted by the physical transmission media over which the signal is sent. The basic framing, synchronization, interleaving, cryptographic and other parameters required for transmission should be adaptively variable as overall bit rate increases or decreases.

3.14 Uses simple and convenient clock/PLLs for service regeneration (NTSC, PAL, Secam, digital audio, etc.)

In the most general multiplex, a mix of service types may be anticipated. The regeneration of such services into the analog domain will require that clocks, phased-locked loops (PLLs) and frequency dividers with parameters specific to the individual

application domains be available in the decoder. Further, since it may be desired that several video (or other) services which are co-generated travel together in a gen-locked fashion, it would be favorable to use the data channel itself to derive the overall system clock.

This being the case, manufacturing economics are best served by selecting a fundamental multiplex rate which can be used to derive all frequencies demanded by the application areas of interest.

This basic clock should be simple to generate and provide for sufficient granularity in the establishment of overall channel and service data rates.

It is also advantageous if the clock is conveniently related to input sampling rates as well.

3.15 Robust and stable syncing in channels with high (10^{-3}) BER

CATV error characteristics tend to be bursty and BERs of 10^{-4} are quite common. Thus, sufficient error correction and a robust synchronization method is essential.

Satellite applications, especially, will bring about the need for highly robust transmission signals. It can be assumed that for Ku Band channels, operation at 10^{-3} error rates will be necessary. Since digital video signals degrade from excellent quality to total loss over a relatively narrow error regime (approximately 1 dB) compared to analog transmission and because channel bit-error rates may be very unpredictable, the need for a strong syncing strategy is increased.

Also, over any transmission channel, the reliable transport of system and conditional access data will be required even after some services have become unusable. This would support, for instance, the stable delivery of entitlement, tuning and other data required for the staging and initialization of home terminals before their deployment at subscriber premises. It would also permit vital encryption key management information to arrive with greater certainty.

To maintain continuity of these other data streams, a dependable synchronization method is fundamental.

3.16 Supports delivery of system and conditional access data in a predictable and suitably short period

Asymmetric cryptographic systems which rely on keys or seeds which are fixed over long periods of time, present attractive targets for signal piracy. To increase security and to ensure short signal acquisition times, these encryption parameters should be changed with frequencies of approximately 5 to 10 Hz. The DCSDS must accommodate these cycles by reliably providing for their transmission within the required tolerances.

3.17 Allows simple de-muxing and re-muxing in the digital domain to support flexible re-routing of service packages

Collections of services called "packages", are content-related bundles that are intended to be transported indivisibly until their arrival at the final decode-and-display point. However, it may be desired that these bundles be freely combined with other bundles for transmission over a high bit rate channel to be later extracted for separate transmission over a lower bit rate channel. Similarly, because of common origin, several bundles of services may have to be transferred over a common channel (e.g., satellite transponder) to be later unbundled and recombined with other bundles from different channels of like (or different kind) into a secondary hop channel in a distribution network (e.g., CATV channels).

The method of framing or packetizing in the DCSDS multiplex should support such de-routing and re-routing without requiring that complete de-muxing, de-erroring, decrypting or other processing-intensive activities (and their inverses) be applied to the bitstream.

3.18 Supports a hierarchical transport mechanism ("superframing")

It is desirable in a DCSDS to support a multiplexing strategy in which smaller content- or logically-related sub-frames ("bundles") may be easily combined into larger structures that are handled uniformly by the transport hardware (as mentioned in the previous section). This concept can be described as "superframing". It is intimately related to the re-routing strategies of the previous section.

Data structures in the DCSDS multiplex should furnish a wide range of superframing capability. This should include large or no limits on the number of subframes that may be combined, flexible and dynamic allocation of subframe sizes and a means of uniquely identifying subframes.

3.19 Provides for independent conditional access data streams within all levels of the multiplexing hierarchy

Flexible re-routing of services from diverse programming sources may lead to demanding cross-networking requirements. That is, the payload signals received and decoded at the final subscriber or end-user node, may have originated from dozens or more service providers. Each provider would like to have total end-to-end security and conditional access control of its service bitstreams which are being transmitted over a common physical network or networks. This is possible if the DCSDS supports service- and programmer-specific encryption and multiple non-interfering conditional access data streams.

While implanting a large number of encryption algorithms in consumer-oriented decoders may not be economically practical because of the cost of secure silicon devices, the use of programmer-specific keys and seeds is quite feasible, whether block or stream ciphers are employed. The amount of physically-secure non-volatile storage will, of course, present limits to the number of such keys that may be stored.

Also, separate, addressable conditional access data streams (CADs) to carry entitlements and key distributions should be supported by a full-featured DCSDS. This includes not only unique encryption of addressed packets on a decoder-specific basis but also the provision for transporting parallel entitlement data streams.

3.20 Connection-less or connection-oriented services

Traditional CATV, DBS and BTV applications tend to be connection-less services. A large number of receive sites are broadcast to, in a multi-drop fashion from some smaller number of transmit sites. The receive sites each have a unique address by which they may be given entitlement, tuning and other

information required for the reception of the broadcast signals. This approach leads to primarily one-way services, in which any reverse-channel, if present, is asymmetric and carries much smaller bandwidth.

Future applications of digitally-compressed video signals may require more symmetric communications paths in highly interactive two-way systems. Since continuously maintaining a multitude of point-to-point, wide bandwidth, two-way connections is likely to be impractical, a method of initiating, transmitting over and then closing such connections in the DCSDS is desirable.

Such connection-oriented services may be semi-permanent in some applications but may also be highly time-variant in others.

3.21 Synchronous or asynchronous multiplex operation and support for backhaul

Source material which is co-generated at a common location may be readily time-division multiplexed into a synchronous service stream. All payload signals may share a common clock and will not "drift" with respect to each other.

In certain circumstances, known as "backhaul", digital signals which are originated at different geographical locations with different clock sources may be transported to a common point where they are combined into a larger signal for further transmission. The DCSDS should provide a method to synchronize these backhauled services or otherwise allow for their asynchronous nature.

4 MULTIPLEX DESIGN

Consideration of the application domains characterized in § 2 and of the requirements described in § 3 suggest some approaches to the method of implementation of a DCSDS. As introduced earlier, a multi-layered approach may be constructed from three fundamental principles:

- a) a high-level multiplexing strategy
- b) a transport layer
- c) channelized service packages

A method is described in the following sections for

assembling a superframed, scalable, channelized multiplex that can meet the application domain requirements of interest.

An overview of this process is shown in Figure 2. The multiplex is built using a simple block construct into subframes and superframes. First, individual program components are compressed and (optionally) encrypted. These are combined by a channelization element into a self-synchronized bitstream. The output of several channelization elements are combined by a subframe multiplexer. Subframe control and sync information is also incorporated at this point. These subframes each have transport layers specific to their system requirements. Multiple subframes are then merged by a superframe constructor which adds the superframe transport layer information.

4.1 Channelizing of basic services (video, audio, data)

Channelizing means the combining of content-related service bitstreams into a self-contained construct for the purpose of independent, synchronized delivery. The MPEG (ISO 11172) bitstream is an example of such a construct. Through Presentation Time Stamps (PTS) in the MPEG System Layer, several video, audio and data services may be encoded and decoded and displayed with proper temporal relationships.

Channelized services are interpreted and decoded as autonomous bitstreams and may be kept in static storage for later playback and can be routed in hardware via a "single wire".

Other methods of channelizing data may be devised which employ variable-length frame formats with headers that describe the length and contents of each frame.

4.2 Clock Generation

A decoding system of encoders and decoders must be synchronized to a single time base. It is convenient to use the multiplex bitstream itself as the source of the clock signal, since it is available at all network nodes.

For the encoder, clock rates that are related to the digital sampling rate are beneficial. For the decoders, clock rates that support convenient generation of

output and display frequencies are desirable.

Also, because audio sampling rates, digital audio transmission and all telephony rates tend to be related to a fundamental of 8 KHz, it would be advantageous to have a clock which is related to this frequency as well.

The CCIR-601 base sampling frequency of 13.5 MHz offers a suitable digitizing standard for both NTSC and PAL/SECAM video, because it has an integer relationship to the horizontal line frequencies of both television standards:

$$858 f_H (\text{NTSC}) = 864 f_H (\text{PAL}) = 13.5 \text{ MHz}$$

It may also be observed that a 27 MHz clock will possess a similar relationship to these line rates and that such a clock can be used to produce 8 KHz-related frequencies with simple dividers/PLLs:

$$27 \text{ MHz} / 8 \text{ KHz} = 3375 \text{ (exactly)}$$

This frequency can also be used in the decoder to generate the NTSC and PAL color subcarriers (along with their horizontal line rates) with a single PLL, since:

$$2 f_{sc} (\text{NTSC}) = 455 f_H$$

and

$$f_{sc} (\text{PAL}) = ((1135/4) + (1/625)) f_H$$

The MPEG system layer local system time clock (STC), which is initialized by the system clock reference (SCR) codes and incremented nominally at 90 KHz between updates or corrections, also enjoys a simple relationship to 27 MHz.

Thus, a family of multiplexes with a wide range of bit rates related to 27 MHz may be generated which allow a simple clock strategy in the DCSDS.

4.3 Multiplex construction and framing

A DCSDS multiplex may be constructed as a sequence of simple, fundamental **blocks** of fixed length (for example) 1600 bits. Each block has a standard format, protected by a Reed-Solomon code, which begins with an 8-bit block sync (BSYNC) and ends with 0-to-N Reed-Solomon parity bytes. Figure 3 shows an example with a $t=10$ correcting code and has 20 parity bytes. The Reed-Solomon code does not protect the BSYNC byte.

The blocks carry information bytes which are of four general types:

- a) Superframe Sync (FSYNC)
- b) Superframe Transport
- c) Subframe Transport
- d) Subframe Data

The data comprising these four basic types may be in the form of a bitstream or, in the preferred embodiment for the transport types, as a sequence of packets. In general though, the blocks may be considered as pure transport mechanisms and place no restrictions on bitstream or packet boundaries, which may span two or more blocks.

The variable Reed-Solomon code provides an adjustable intra-channel error correction mechanism that may be tailored to the channel error characteristics by adjusting the number of parity bits and error-correcting strength. It is especially effective on burst error patterns. Other extra-channel techniques, such as Viterbi soft-decision decoding of convolution FEC codes, may also be added as an additional error correction layer.

Consecutive blocks are arranged into three larger, hierarchical constructs:

- a) superframe transport layer
- b) subframe transport layer
- c) subframe data region

These constructs then form a superframe through their combination into a larger transport framework that may be uniformly and inexpensively handled by practical hardware implementations. Figure 4 shows a typical configuration for the superframed multiplex.

A superframe so constructed may then be transmitted at some fixed frame rate, say 30 Hz, to dispatch a continuous stream of multiple services. The presence

of superframe and subframe transport layers in every frame is used to guarantee the timely delivery of conditional access data by configuring the contents and size of the layers to accommodate the required bandwidth.

The length of each block is not required to be precisely 1600 bits as in the example, but must be some fixed length. Once determined, the overall data rate is given by:

$$R = BL \times N_b \times SFR$$

where: BL = block length (bits)

SFR = superframe transmission rate (Hz)

N_b = number of blocks per superframe

It should be emphasized that the DCSDS multiplex is a fixed, but adjustable frame approach. That is, the design is parameterized so that frame characteristics can be tailored to the application; once the parameters are selected, the benefits of a fixed frame are obtained. Having a fixed frame length is advantageous for:

- synchronization purposes - high bit rate, error-prone channels
- guaranteed cryptographic cycles
- predictable, fast acquisition times

Having an adjustable frame is advantageous for:

- customization of transmission to channel characteristics
- scalable overall channel rates
- extensibility for future requirements

It is possible to alter the frame characteristics by information download in the system data packets.

4.4 Interleaving of the superframe

A superframe is sent in a byte-interleaved fashion to even out the arrival time of subframe data and to further reduce the effects of burst errors in the channel. All bytes of the superframe except those of the FSYNC and BSYNC are sent in "column-major" order, that is, orthogonal to the Reed-Solomon blocks. Thus, burst errors will tend to be spread out over many blocks instead of being concentrated into one or a few. This greatly increases the effectiveness of the Reed-Solomon code.

Another consequence of this approach is that the decoder will require memory for a de-interleave buffer that is equivalent to the size of a superframe. The size of this buffer may be decreased while maintaining a constant data rate in the channel by transmitting superframes at a higher rate.

4.5 Robust sync words and BSYNC/FSYNC strategy

The frame synchronizing strategy employed is two-tiered and is related to that of the Zenith/AT&T DSC HDTV proposal. The decoder synchronization element searches first for the BSYNC byte. Since the BSYNC value may occur at intervals in the data portions of the multiplex, the BSYNC framer must find several BSYNC bytes at repetitive intervals which are exactly the block length. The framer may thus keep several "shadow" counters, if other BSYNC patterns are found out-of-sequence while waiting for the block-aligned repeats.

Once BSYNC is located, the decoder synchronization element searches for the FSYNC pattern immediately after each BSYNC. The FSYNC pattern is (in the example) 179 bytes in length and comprises two components:

- a) FSYNC word 1336 bits
- b) Superframe ID 96 bits

The FSYNC word is a value generated by a pseudo-random sequence, the parameters of which are:

PN Length = 255
Starting Seed = 10000000

Characteristic Polynomial =

$$X^8 + X^6 + X^5 + X + 1$$

The 255-bit sequence is repeated roughly two-and-two-thirds times which yields 337 1's-characters and 331 0's-characters. For QPSK modulation, each bit is doubled, yielding 1336 bits. This sync word can be loaded from a lookup table in the decoder for comparison with the incoming bitstream.

For further reference on this PRBS please see,

F. MacWilliams and N. Sloane
Proc. of the IEEE, vol. 64, no. 12, December 1976

The superframe ID contains information that describes the highest-level structure of the superframe and the identity of the transmitting entity. The transmitter may be in the format of a SMPTE header/descriptor. Some of the superframe structure parameters are:

- a) superframe transport block count
- b) Reed-Solomon t-strength number
- c) superframe encryption flag

4.6 Superframe transport design

The superframe transport structure is a header that describes the overall superframe, the number and type of subframes and the location in the data stream of the components of the superframe. It also carries the Subframe Virtual Channel maps and has a provision to specify routing information for connection-oriented services (the Virtual Path Identifier) similar to that found in the B-ISDN Asynchronous Transfer Mode (ATM). The superframe transport is shown in Figure 5.

The Superframe Encryption Packets carry the global seed and other information pertinent to an overall layer of encryption applied to the entire superframe. This layer of encryption is optional.

The method of construction of the superframe is shown in Figure 6.

As mentioned previously, several subframes may be globally encrypted at the superframe level (in addition to any service and/or subframe global encryption they have received). Seeds for the optional superframe encryption are packetized as are the other superframe transport data. These components are then combined into the superframe along using the fundamental block structure and sync words.

4.7 Sub-frame and sub-frame transport

A sub-frame is a content-related collection of channelized services that is to be commonly transported indivisibly over all branches of the network until the final point of decode-and-display. It has two major components: the subframe transport layer and the subframe data region. Its structure is shown in Figure 7. The components of the subframe transport layer are the following packets:

- Subframe multiplex map
- System Data
- Video Mux Control
- Virtual Channel Maps
- Addressable Data Packets (ADPs)
- System Teletext Packets

The subframe transport layer packets are discussed further in § 5.

A functional view of the construction of the complete subframe is shown in figure 8. Individual bitstreams in channelized format are combined with the subframe transport packets. Error correction is applied as required by packet type. Encrypted service seeds are built into the system data packets. Synchronization and the subframe multiplex map are then assembled into the subframe construct by adding BSYNC and Reed-Solomon parity and correctly sequencing the fundamental blocks.

One of the benefits of the block-oriented nature of the multiplex is the ability to readily de-multiplex and re-multiplex entire subframes with simple cost-effective hardware. Thus, as shown in Figure 9, subframes from two different programmer superframes may be extracted, re-combined and re-routed, at a regional CATV hub, for example.

4.8 Scalability of channel data rate

Channel data rates can be specified to within a granularity given by:

$$\Delta R = BL \times SFR$$

where: BL = the block length

SFR = superframe transmission rate

For the example superframe discussed herein, the block length is 1600 bits and the superframe rate is 30 Hz. Thus, the overall channel data rate may be altered in increments of 48,000 bps. Other increments, such as 64 Kbps can be obtained with slightly different parameters.

4.9 Subframe transport layer and relationship to services

The subframe transport layer carries data structures for encryption, system data and for specification of the subframe data region. It occurs at a regular and predictable interval and thus is central in establishing the cryptographic cycles and seed changes. Other than providing the necessary ancillary data and describing the structure of the subframe data region, this transport layer places no restrictions on the types or amount of service data that may be carried.

The general functionality provided by the transport layer is shown in Figure 10. Error correction, synchronization and conditional access provide the delivery mechanism for the services, but do not constrain their implementation or rates. Entitlement data streams are also handled in the transport layer.

4.10 Channel error management (Viterbi, Reed-Solomon)

Adaptable channel error correction is made available through the adjustable-strength Reed-Solomon block code and, for satellite channels, a soft-decision Viterbi decoding algorithm. The Viterbi is a maximum-likelihood algorithm that is very useful in bandlimited channels with intersymbol interference.

The Reed-Solomon is a member of a class of codes known as non-binary BCH codes. It is a powerful random error-correcting cyclic code and is capable of correcting multi-bit errors. The Reed-Solomon "t-number" indicates its error-correcting strength. A

$t=10$ code can correct errors in any 10 bytes of the block. The number of parity bytes is given by $2t$. This code by itself can withstand burst lengths up to 74 bits or 3μ sec long.

5 TRANSPORT LAYER

This section deals with the characteristics and strategy of the subframe (universal) transport layer. Each subframe has its own transport layer which carries system, encryption and frame control information unique to that subframe. Each subframe consists of a subframe transport layer and a subframe data (or program) region. All ancillary information needed for the routing, demultiplexing, service selection/tuning, decryption, packet error correction and conditional access of an individual subframe is handled by the transport layer. This allows the subframe to be handled as a "single wire" conduit for network routing purposes.

5.1 Subframe sync word

Each subframe begins with an optional sync word (SFSYNC). This may be the same as the superframe FSYNC word (§ 4.4) or can be different. It may be entirely omitted or may be included to support subframe re-routing without local sync regeneration. It is not required for detection of the beginning of the subframe boundaries.

5.2 Dynamic Multiplex Maps

The subframe transport layer, like the superframe transport layer, starts with a multiplex map, the "subframe multiplex map". The number and arrangement of other packets in the transport layer as well as a description of the format of the subframe data region are specified within this map.

These descriptive parameters may be changed as often as on a per-frame basis, and thus provide a highly dynamic allocation of bandwidth to the various components of the subframe. In particular, with suitable concealment, such as a freeze-frame, one or several transport frames may carry ADPs, text or other packets in a burst mode, by replacing the program (video) service(s) with packets of the desired type. Alternately, an entire subframe may be configured semi-permanently as a text or addressability channel.

5.3 System Data Packets

The system data packets handle information that is required by all decoders that are to receive a particular multiplex. The packets sent in the System Data family are:

- System Information
- System Tuning
- Global Seed
- Service Seed

The system information and system tuning parameters are generally delivered on a cycled basis which is not constrained to occur entirely within the cryptographic cycle of the system. Data regarding global configuration of the decoders and system are handled in this manner.

The global and service seed packets transport the encryption seeds and are constrained to be completely conveyed within the cryptographic cycle boundaries. The seeds are used as initializing values to the PRBSs that protect the services and for a global (over the subframe) level of encryption. This is discussed further in § 5.9.

5.4 Virtual/Composite Channel Maps

A Virtual Channel is the logical association of one or more services (video, audio, text, data) within a single multiplex. A sequence of virtual channel maps are transmitted in the multiplex, correlated with the cryptographic cycle. The decoder interprets these maps to select services from the multiplex.

A composite channel is a related set of virtual channels that are remotely tuned on a sequential time-varying basis, transparently to the subscriber. Virtual channel numbers and composite channels may be selected directly by the subscriber or at the headend; or they may be selected by some other decoder user interface. Ultimately however, the decoder must receive a virtual channel number in order to tune.

Some of the parameters in the virtual channel map

are:

- Program assignment
- PPV event number
- Force Tune Channel
- Blackout code
- Blackout Alternate Channel
- Fingerprint trigger

5.5 Mux Control/Statistical Multiplexing

Mux control packets are used to characterize the structure of the subframe data area. Since the subframe may carry more than one channelized service, the demultiplexing hardware must be instructed on the method to extract each service.

This can be accomplished in several ways. One is to divide the subframe data region into packets of equal length, say 60 bits. The mux control packet then contains program weighting counters that specify what proportion of each packet each channelized program can occupy. Since the mux control packet is carried in every subframe's transport layer, this proportion can be dynamically varied on a frame-by-frame basis, thus preparing the way to statistical multiplexing.

5.5 Addressable Data Packets

Addressable Data Packets (ADPs) carry information bound for specific decoders. Each packet contains a length field, a clear address field, a secret serial number (SSN) select field, a command field, the addressable data and a CRC check.

ADPs are discussed further in § 6.

5.6 Utility Data/closed captioning

Utility data is oriented toward low-speed serial communications in the range of 300 bps to 38.4 Kbps. It may be encrypted and accessed via the virtual channel interface as with any other program material.

5.7 Teletext/subtitling

System teletext packets carry informational and instructional messages to be displayed by the decoder in certain error or operational states. Some of the messages of this type may be stored in ROM in the decoder, but providing a large internal storage for such messages may be cost-prohibitive.

Teletext as a companion service (for example, subtitling) is carried in the channelization layer.

5.8 Packet Error correction/detection

To optimize the error management scheme to the transmitted data, different error correcting and detecting codes are applied at the packet level. These codes in combination with the channel error correction and Reed-Solomon code, increase the ruggedness of the data which they protect while causing acceptable overhead.

As mentioned in § 3.5, a hierarchy of error protection is called for. This leads to the following combinations of majority logic and convolution FECs to be used for the packet families:

System Data, Mux Control, Virtual Channel Maps

The data for these packets are first encoded using a (3,2,40) convolution FEC. This code is double-error correcting over its constraint length $((40+1)*3 = 123$ bits). Each one of the bits of this code are then protected using a 5:1 majority logic encoding. The entire stream is further protected by the Reed-Solomon block. The RS/Interleave provides the same burst error protection afforded to the rest of the multiplex. At high random error rates, the Reed-Solomon shuts off without altering the data, which is then decoded as-is by the convolution code. The (3,2,40) with the 5:1 provides protection up to about 3×10^{-2} error rates.

Conditional Access

The ADPs, like the system and mux control packets, are given some additional random error protection. A (2,1,6) convolution FEC is preferred. Although this code will be experiencing errors at 1×10^{-2} error rate, a large portion of the ADPs will be decoded correctly.

The probability that the Reed-Solomon would decode at the 1×10^{-2} rate is almost nil. ADPs are also covered with a 24-bit CRC to allow rejection of failed packets.

Utility Data

The Utility data packets are covered by a (3,2,13) convolution code.

5.9 Security Architecture

In the DCSDS, a layered security approach is used in which several random number keys are employed in a hierarchy to protect all aspects of the transmitted signal. The keys serve either as initial (seed) values to Pseudo-Random Binary Sequence generators (PRBSs) or as encryption keys in a DES-level algorithm.

The system encryption structure is shown in figure 11.

The overall system security architecture, shown in Figure 12, provides for sturdy signal protection on an end-to-end basis whether the receive site is a CATV headend, DBS backyard Integrated Receiver Decoder (IRD), digital home terminal at a subscriber premise or other network node.

This architecture calls for hardware in the encoder multiplexing unit or in auxiliary equipment to perform several different levels of encryption. A decoder database is kept by a control computer element.

5.9.1 Cryptocycle concept

A collection of random seeds is generated and used to encrypt the video, audio, text, data and OSPs in a series of transmitted frames. This range of frames is called a session or cryptocycle. Although the length of the cryptocycle is dependent on the hardware, it is convenient for it to occur in even multiples of frames. The length (in frames) should be as short as possible, as it affects the decoder signal acquisition time. The random session seeds serve as the initial values for the PRBS generator algorithms in the encoder multiplexer subsystem. The PRBS logic is reloaded on a frame boundary and uses the same value until the end of the cryptocycle.

The decoder must receive the session seeds in advance of the next cryptocycle or session. Thus, the

seeds for the upcoming session are transmitted in the System Data Packets of the current session. A unique and independent seed is used to encrypt each video, audio, data, or teletext service.

5.9.2 Secret Serial Numbers

Each decoder is assigned a unique SSN at manufacture time. This SSN is stored in a protected NVM within the die of a secure microprocessor. An SSN database is maintained by a control computer (Encoder Management Computer - EMC), and all ADPs bound for a specific decoder are encrypted with its unique number by the encoder multiplexing unit.

As an example, the Multi-session keys (MSKs) that are used to encrypt the session (service) seeds are delivered in this fashion as are the entitlements.

5.9.3 Hierarchy of Keys

As shown in Figure 11, the MSKs are used to encrypt the session (service) seeds and global seeds. The session and global seeds are used to encrypt the program services. At each level in this hierarchy, the seeds are renewable. This renewability can also be accomplished through smart card distribution which can include algorithm change as well.

5.9.4 Global and service encryption

The service encryptions are accomplished by generating a PRBS and convolving it via modulo 2 addition with the individual service bitstreams. If desired, a global layer of encryption can be applied in the same manner over all the packets in the subframe data region.

5.9.5 PRBS algorithm

The generating algorithm for the PRBSs is a fundamental component of interoperability. Any systems of encoders and decoders that have commonality on this level, can with other provisions, be made to transmit, receive and decode the same signals and reliably control access to them. The use of a common transport and multiplexing approach is also required.

5.9.6 Broadcast Key per programmer

Figure 11 shows a broadcast key associated with the generation and encryption of the MSKs. The use of

this key is one method to achieve a differentiated encryption on a network shared by many programmers. The larger MSK is common to the entire network. The shorter broadcast key is unique to and selectable by each programmer. The programmers convolve the broadcast key with the universal MSK to obtain a secondary key which is then used to encrypt the service seeds belonging to that programmer. To receive the services of a specific programmer, the decoder must first have a) the network-wide MSK, b) the programmer's broadcast key and c) the correct entitlement message.

The broadcast key is, of course, delivered encrypted with the unique SSN of each decoder. It may be shorter than the MSK to conserve both secure non-volatile storage and ADP bandwidth.

5.10 Service rate scalability

Service rates may be temporally varied by altering the subframe structure. This may be accomplished by increasing or decreasing the number of blocks per subframe or by reallocating bandwidth between channelized services within a subframe through the Mux Control packets as discussed in § 5.5.

Both the number of channelized services carried and their data rate allocation can be controlled in this manner.

5.11 Channelized Packet Structure/MPEG Transport

As mentioned previously, the ISO 11172 Systems Layer syntax is an exemplary channelized program structure. Thus, it is suggested herein that it may be used as an input to the subframe multiplexer as depicted in Figure 2. It may be noted that MPEG bitstreams may be carried in the same subframe concurrently with other channelized program structures.

5.11.1 PanScan

PanScan refers to the displaying of a 4:3 aspect ratio subset of a 16:9 aspect ratio signal. The "window" displayed can be moved or scanned horizontally through the larger display area to accommodate artistic content in all zones of the picture. PanScan

values which specify which part of a 16:9 aspect ratio video signal is to be mapped into the 4:3 aspect ratio output signal should be incorporated into the MPEG syntax.

5.11.2 Copy Protection

The Eidak method of copy prevention exploits differences in the sensitivity of television receivers and VCRs to small changes in vertical frame rate. In particular, the electromechanical nature of the VCR causes it to be more sensitive to such disturbance.

The Eidak copy-protection technique varies the field rate in such a way that proper synchronization is upset, the VCR servo loses lock, and the video signal is improperly applied to the recording tape. The effect is to create gaps in the program material. The variation in the field rate is achieved by adding or deleting horizontal lines.

For maximum effect, the technique is applied with periodic variations, adding or deleting horizontal lines in pairs. Additionally, adjustment is made to the timing of the first vertical sync pulse to assure proper display interface when the line count is changing.

Profile information which can be used to negate the effects of Eidak is generated at the encode site and may be transmitted with the program material. Audio delay/advance must also be performed by encode equipment.

In a digital system, the decoder must generate the analog Eidak effects based on the profile information in the program bitstream. Of course, this copy protection mode may be addressably disabled; in this case, the decoder does not enforce the profiles.

It would be appropriate for the channelized program bitstream to convey the synchronized Eidak profiles.

6 CONDITIONAL ACCESS

A schematic overview of the conditional access and security architecture of the DCSDS is shown in figure 12. This discussion will focus on the:

- Encryption structure
- Addressability design

- System Control

and is presented to communicate the relationships between the multiplexing strategy and the control of service access.

It should be emphasized that the physical security of the decoder devices and the overall security plan for initialization and distribution of hardware, encryption key delivery and decoder repair must also be sound. These topics are beyond the scope of this document.

6.1 Standard Decoder Model

A functional diagram of a "standard" superframe decoder is shown in figure 13.

The decoder obtains programming by receiving a user channel selection and, if it is authorized for that channel, reads the corresponding frequency from a pre-stored tuning table. This frequency is tuned and after data sync is obtained, the superframe multiplex map is interpreted. This allows the decoder to select the correct subframe for demultiplexing. If the optional superframe layer of encryption has been used, the superframe global seed is obtained and decrypted and is used to initialize the superframe PRBS.

Once the subframe is acquired, the subframe multiplex map is interpreted and the appropriate channelized program bitstream is extracted by interpreting the subframe virtual channel map. The encrypted service seeds are likewise obtained from the transport layer and are decrypted in the secure microprocessor using the proper pre-stored Broadcast key and/or MSK. The service decryptors (D) are initialized with their seeds and produce the clear bitstreams to the decoding elements.

6.2 Addressable Data Packet Design

Addressable Data packets carry the decoder-specific conditional access data stream.

Each packet contains the clear (public) address of an individual decoder. This address is normally programmed into the decoder (along with the SSN) during factory testing. Group addressing is also desirable and can be accomplished by downloading

one or more group addresses to the decoder through an individually addressed data packet.

The addressable data consists of the information that pertains to a single decoder or group of decoders. Some examples are: the encryption key(s), virtual channel authorization maps and pre-reserved PPV orders.

A CRC check character is used to check the integrity of the data packet. If the CRC indicates a packet error, the entire packet is rejected by the decoder. The ADP data stream must therefore be repeated at some interval to make the lost information available again at a later time.

Multiple, independent conditional access data streams may be supported, if the addressable data packets are sent with a universal header, identifying the stream to which they belong.

6.3 Virtual Channels/Composite Channels

The length of the specifier for the virtual channel number is nominally 12 bits, allowing for a network-wide total of 4096 different virtual channels. There is no restriction on the number of virtual channels (out of the 4096) that can be defined within a given multiplex, although the available data bandwidth and signal acquisition time must be taken into account.

A Composite Channel is a service that is composed of different virtual channels on a time-varying basis. The fact that the decoder is changing tuning on a scheduled basis is controlled from the point of signal origination and is transparent to the subscriber. An example is a "football channel" that is comprised of ESPN's service when football is shown, then changes to a regional sports channel when a local college game is showing and later picks up a scores and highlights teletext channel.

This example is shown in Figure 14.

The key to handling Composite Channels is the use of a "vectoring" approach. The decoder stores a map which associates a Composite Channel number with a "Home Virtual Channel". When a Composite Channel is selected at the decoder, the Home Virtual Channel is tuned. Within the multiplex where the Home Virtual Channel is found, Composite Channel Map Definitions (CCMs) are transmitted in the

transport layer. These maps contain a Virtual Channel vector that indicates what the current "active" virtual channel is for a given Composite Channel. The decoder re-tunes to the current "active" virtual channel if it is different from Home Virtual Channel.

6.4 Decoder Tuning Maps (Logical and Physical)

The decoder is loaded with (unencrypted) tuning frequency information which it stores in a non-volatile memory element. This information may be sent in the system data in the programming multiplex. It is used to select the proper frequency when a user channel selection is made. This is the physical tuning map.

To provide a uniform channel-to-service correspondence over a large network encompassing many distribution nodes (CATV headends, for example), a logical tuning map may also be utilized. This may be used to provide, for example, a consistent channel line-up for a nationwide network, to simplify the generating of a program guide (electronic or printed). The logical tuning map may also be loaded into the decoder NVM and provides the link between the global channel line-up and any variations in the virtual channel mappings of the individual distribution nodes.

6.5 Teletext Design/Implementation

Text packets carry characters that may represent ASCII alphanumeric, primitive graphics or other International Language character sets.

Collections of text pages (or a single page) are considered to be services and thus are assigned a service number. This service number may be selected via a Virtual Channel. Each text page is encrypted with a seed that changes on the usual crypticycle boundary. The encryption may however, be inhibited (turned off) on a per-page basis. One text service may have up to 65,536 pages. System teletext pages are transmitted in the transport layer and are usually sent unencrypted.

Text packets are of two types: Text Header and Text Row. The Text Header packets contain information which describes how to interpret the actual Text Row packets that follow. All Text Row Packets occurring between headers are considered to belong to the

same text page. The Text Headers are protected by additional Majority Logic encoding using one byte to represent a bit (7:1). In Text Row packets, only the header flag is majority logic encoded.

Each displayed text row consists of forty characters, and there are twenty displayed rows to a page. The characters include upper-case and lower-case ASCII alphanumeric and simple graphics in eight colors.

6.6 PPV/IPPV/MOD structure

Pay-per-View and Impulse Pay-per-View represent significant and growing revenue streams for many CATV operators. They may also be used in the DBS environment.

PPV refers to the reserving in advance of a one-time program for viewing at a specific pre-scheduled time. IPPV is similar but implies an authorization mechanism local to the subscriber device which then transmits the "buy" information back to a billing center in real-time or in a store-and-forward mode.

MOD or Movie-On-Demand is a more interactive version of PPV/IPPV in which many showings of a single title are presented with small time offsets from each other (15-30 minutes) to provide a nearly continuous availability.

All of these modes of program purchase require identifying information to be embedded within the channelized bitstream. Other system-wide information, such as the phone number of the billing center for Telco-return systems, may be transmitted to the decoders within the system data.

6.7 Decoder Blackout handling

In conjunction with certain programming (especially sports events) selected decoder sub-populations must be restricted from viewing a service even though they are normally authorized for that service. This is called a service blackout.

A blackout population is usually comprised of a group of decoders that are in a common geographical area. One method of blackout control assigns group codes to decoders. The assignment to a specific group is done by the control computer element. The channelized bitstream associated with the blacked-out

program carries the blackout code. The decoders compare that code with their own and will not authorize the service if they are a member.

An additional, geographic-coordinate-based method of blackout control may also be implemented. The control computer still makes the blackout assignments, but assigns both a group blackout code and a geographic (x,y) coordinate blackout code to each decoder. The system data packet then carries the group code and/or a geographic centroid (x,y) and radius (r) for the blackout zone. Each decoder uses an internally-stored location coordinate to calculate whether it is within the blackout zone and will not authorize if it is. An alternate channel (also specified in the system data packet) may be tuned by a blacked-out decoder.

The control computer assigns blackout codes and coordinates to decoders via ADPs. The decoder must store the coordinates in secure non-volatile memory.

6.8 Addressable Copy Protection

Control of the Eidak process described in § 5.11.2 can be addressably controlled per decoder. This permits the marketing of copy-enabled programming to subscribers, while perhaps promoting an earlier release of "high-interest" material by satisfying the program owner's desire to prevent widespread reproduction.

6.9 Force Tune

Under certain circumstances, it may be desirable to remotely cause the decoder to tune to a specified channel overriding any subscriber selection. This is called force tuning. The channelized bitstream should be able to carry an indicator and a force tune channel number to facilitate this feature.

6.10 Decoder fingerprinting

Decoder fingerprinting is another anti-copy technique. When enabled, fingerprinting causes a special code (unique to the decoder) to be inserted into the analog video data stream output of the decoder. This code may be used to identify the originating source decoder in the event the program is copied and distributed.

The channelized program bitstream should be capable of carrying a fingerprint trigger indicator which activates this mechanism.

7 CONCLUSION

A discussion has been presented that considers a method for system multiplexing of a plurality of services in a Digital Compression Services Delivery System (DCSDS). A survey of a broad assortment of application domains and the specific technical requirements for producing equipment for implementation in such applications have been reported.

A multiplex design which is constructed from three essential principles:

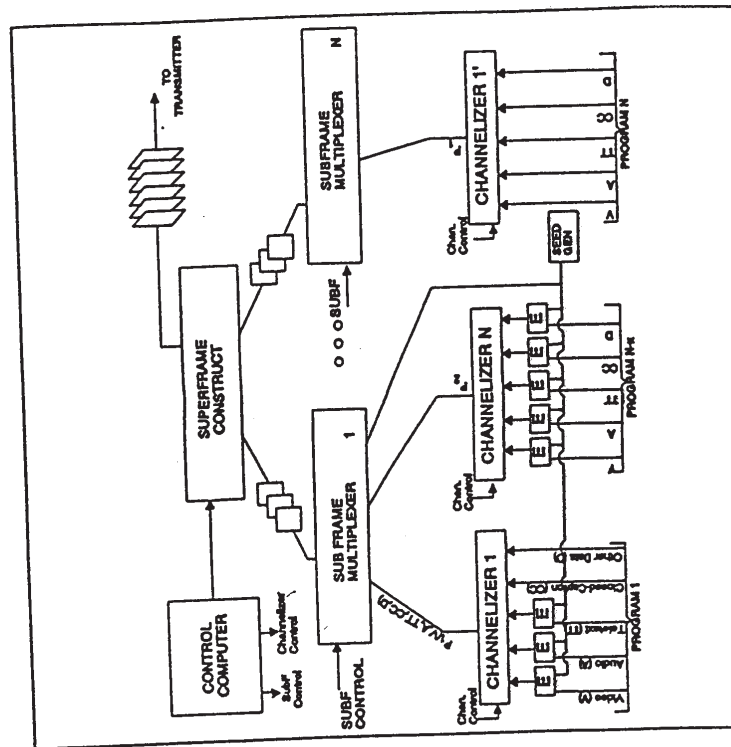
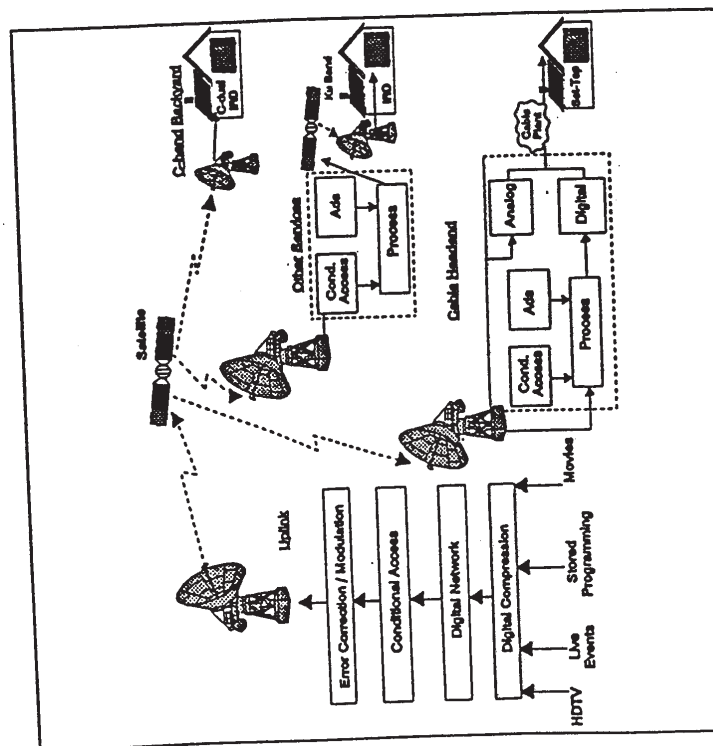
- high-level multiplexing strategy
- transport layer approach
- channelized service packages

is described. This method uses a fundamental blocking strategy to provide channel-optimized error-protection and to support a hierarchical approach to building multiplexes which are scalable over a wide range of channel bit rates.

The multiplexes are constructed as a sequence of fixed (but adjustable) frames, each possessing a subframe structure.

A transport layer at the superframe and subframe layers provides for data synchronization, conditional access, an encryption subsystem, system-wide information and dynamic multiplex control. This layer supports the conveyance of a wide range of digital service bitstreams and includes extensibility to future services.

A virtual and composite channel mechanism allows uniform and transparent subscriber selection of a service or services from a multiplicity of compressed or non-compressed signals, which may include MPEG (ISO 11172) bitstreams, in channelized packages.



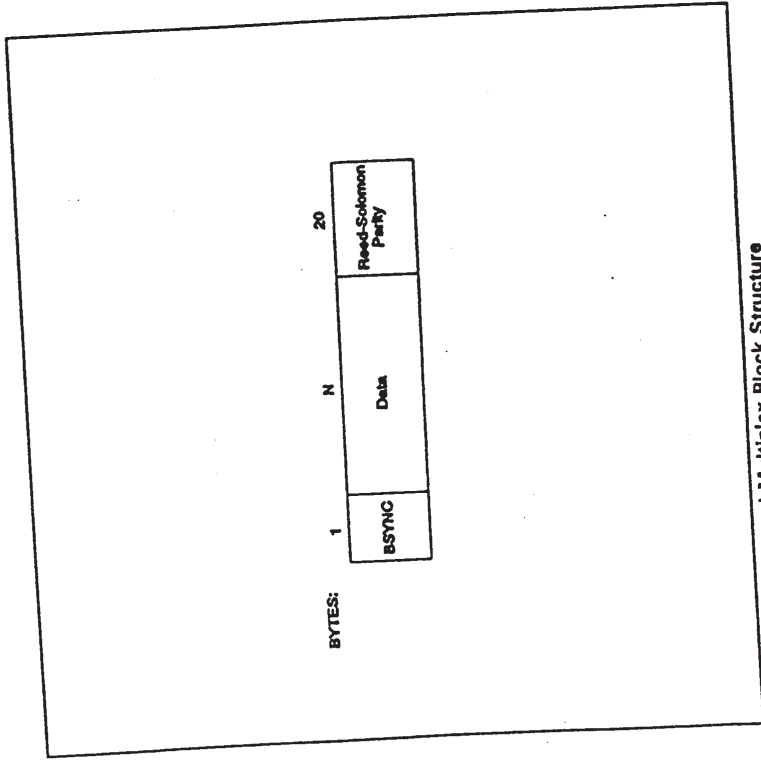


Figure 3 - Fundamental Multiplex Block Structure

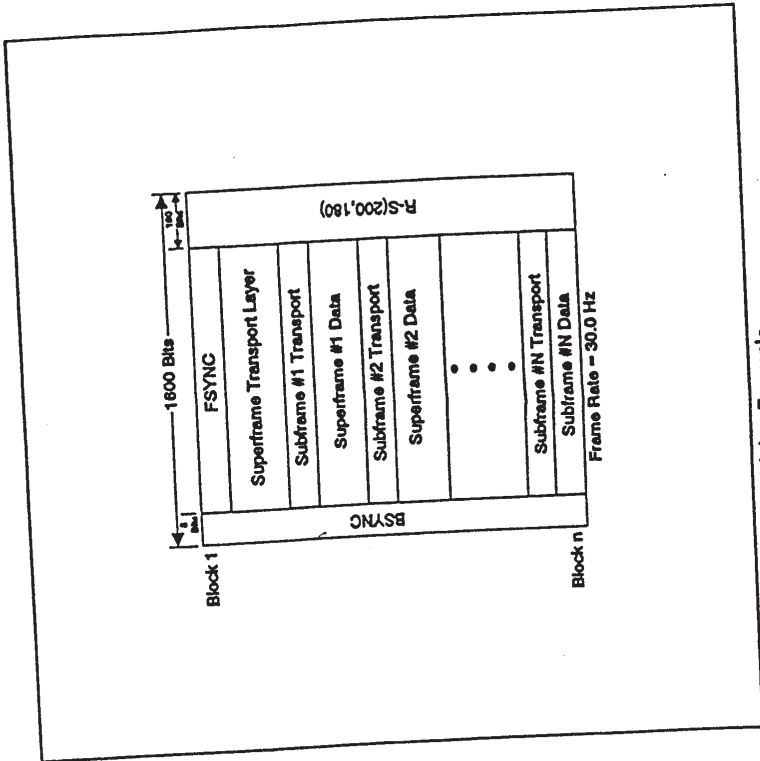


Figure 4 - Superframe Multiplex Example

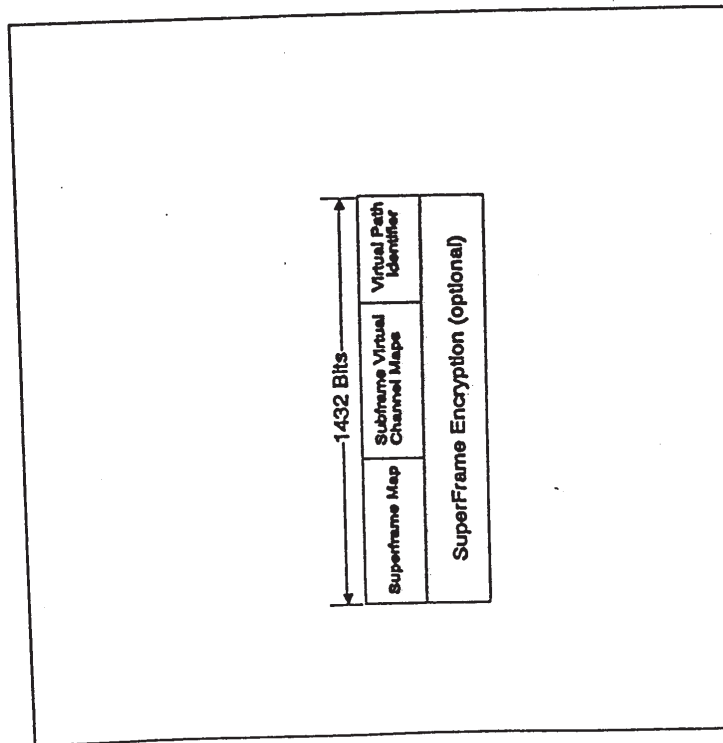


Figure 5 - Superframe Transport Layer

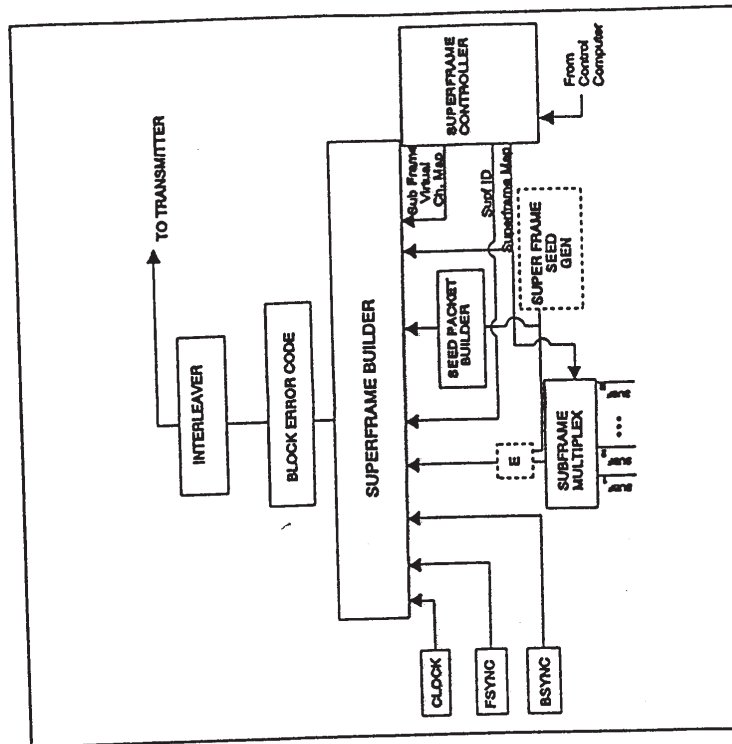


Figure 6 - Superframe Transport Layer Construction

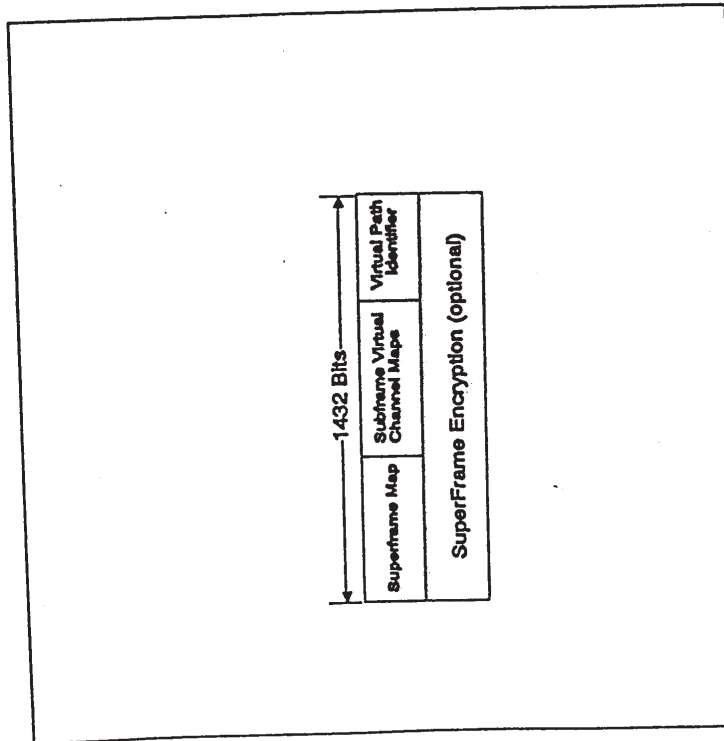


Figure 5 - Superframe Transport Layer

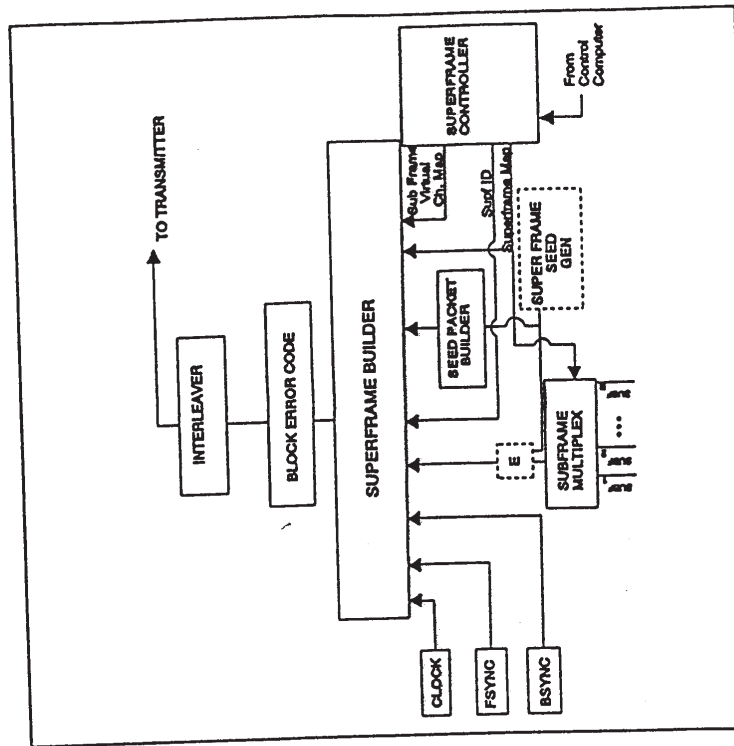


Figure 6 - Superframe Transport Layer Construction

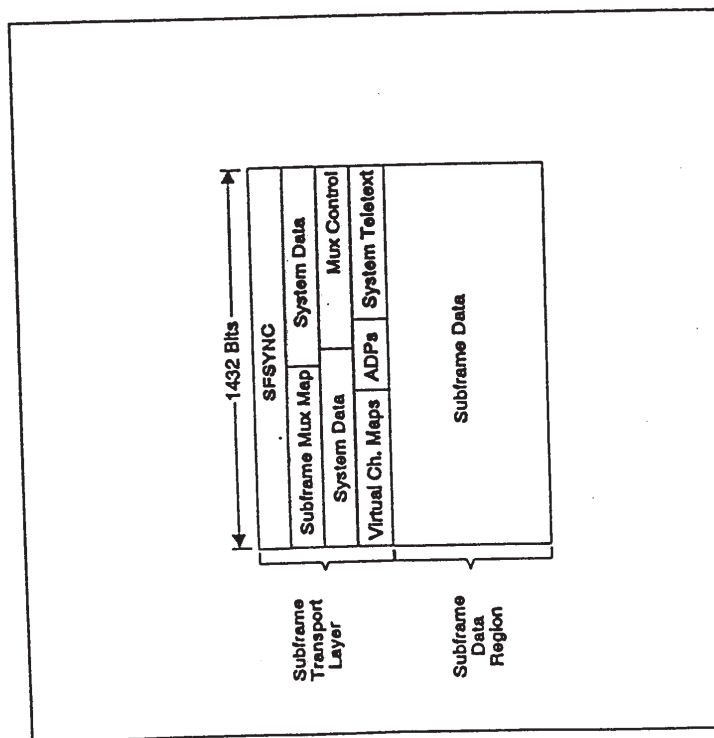


Figure 7 - Subframe Structure

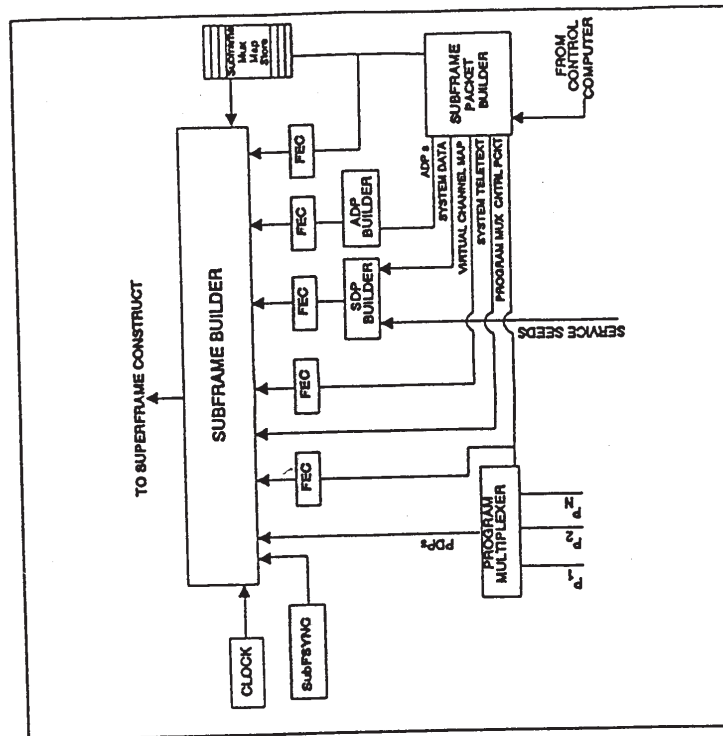


Figure 8 - Construction of the Subframe

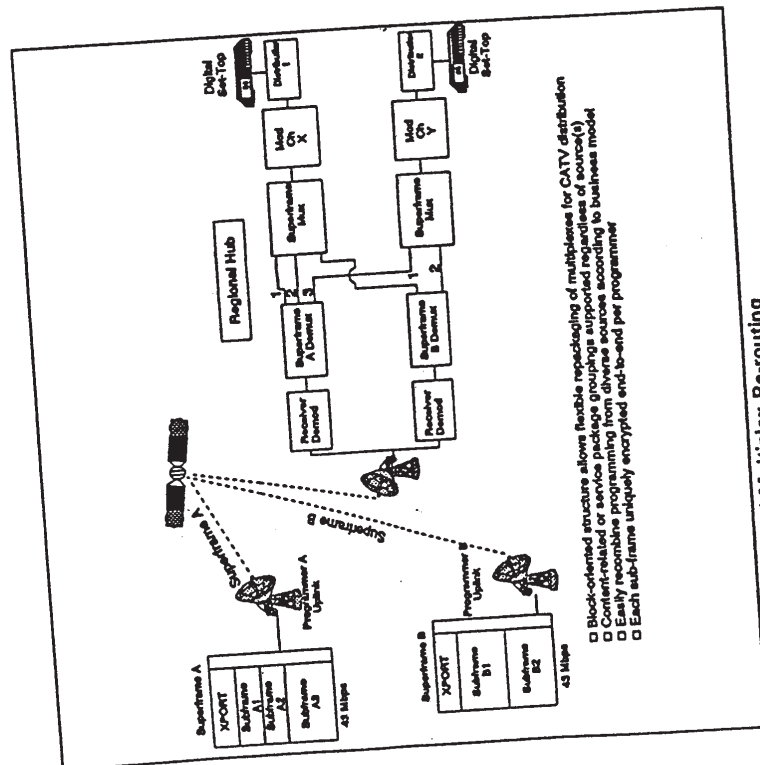


Figure 9 - Superframed Multiplex Re-routing

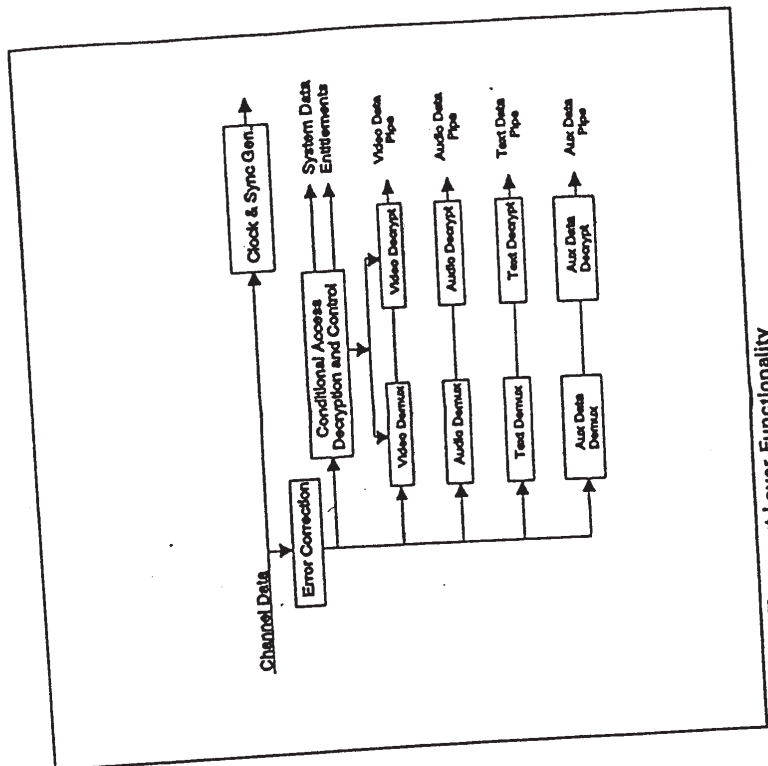


Figure 10 - Transport Layer Functionality

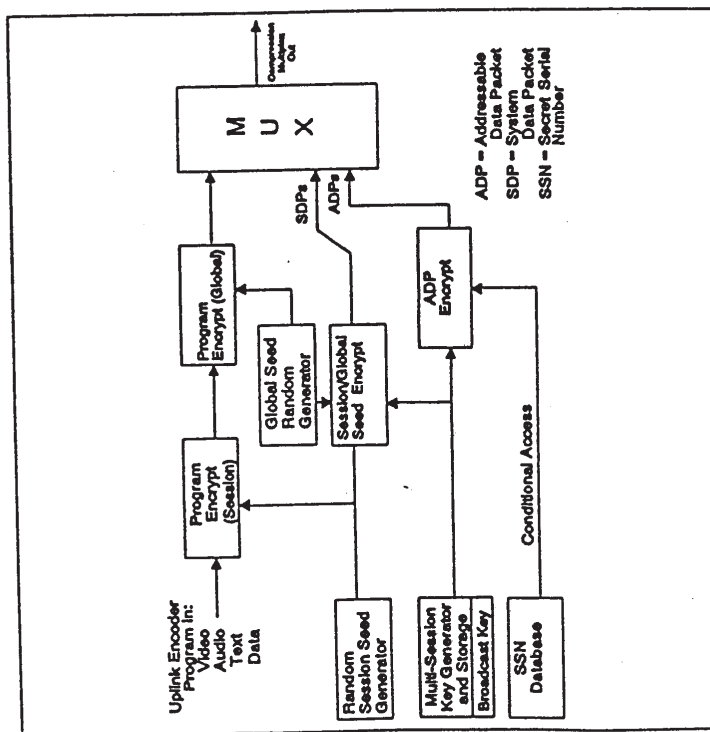


Figure 11 - System Encryption Architecture

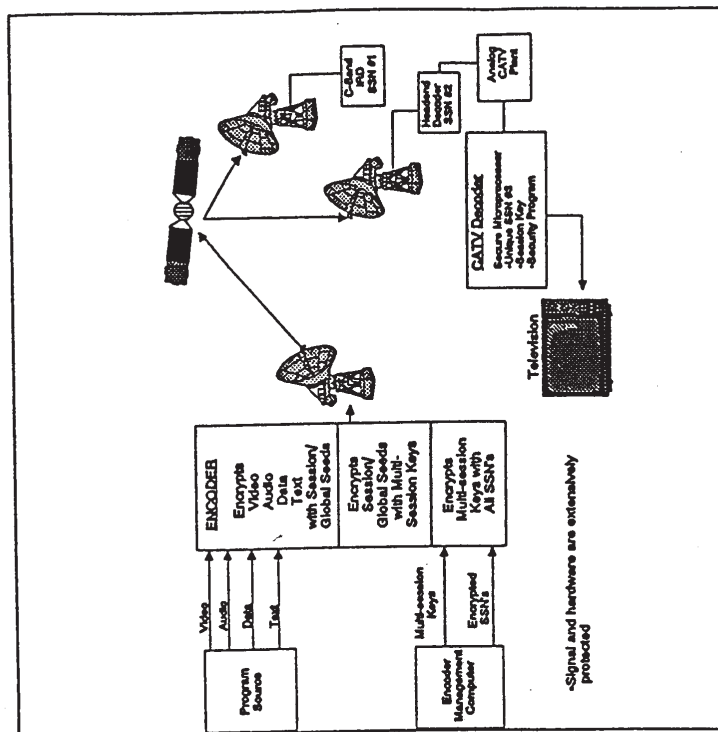


Figure 12 - System Security Architecture

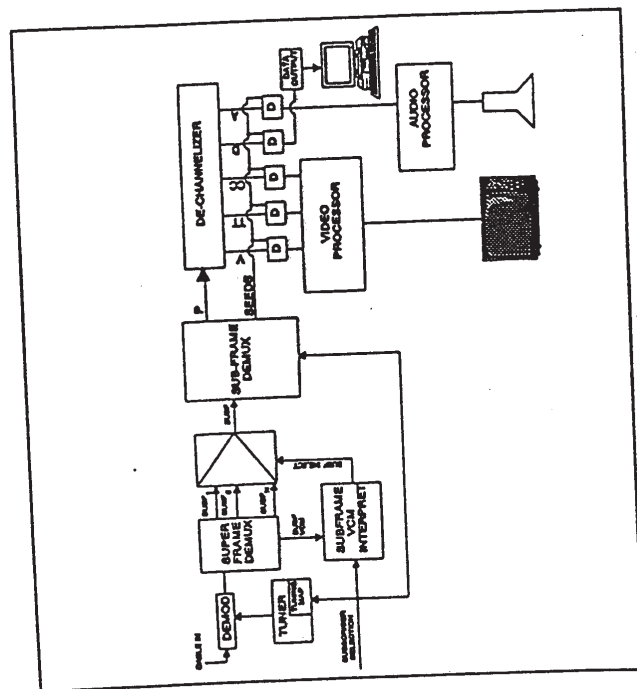


Figure 13 - Standard Decoder Model

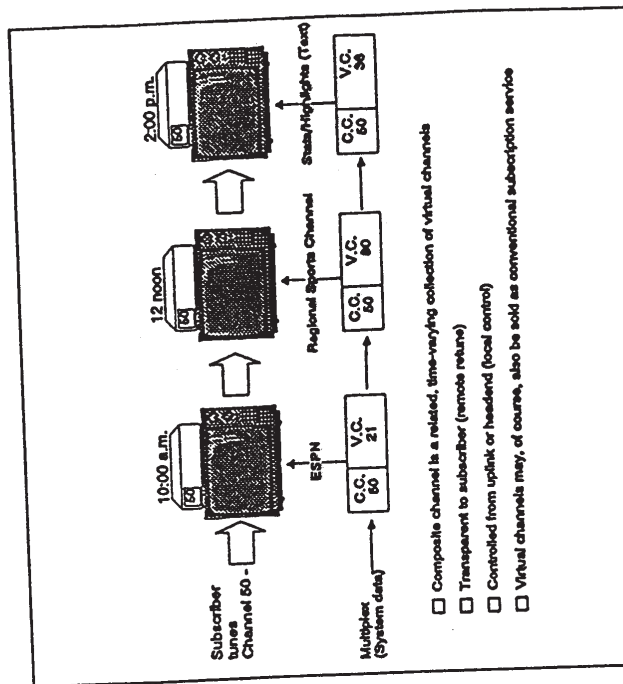


Figure 14 - Operation of Composite Channels

Sources for Obtaining Wasilewski '92:

1. International Organization for Standardization, ISO/IEC JTC1/SC2/WG11, MPEG 92/754 (November 1992)
2. File History of U.S. Patent No. 5,359,601, issued October 25, 1994.