Recommendation G.784

SYNCHRONOUS DIGITAL HIERARCHY (SDH) MANAGEMENT

The CCITT,

considering

(a) that Recommendations G.707, G.708 and G.709 form a coherent set of specifications for the synchronous digital hierarchy (SDH) and the network node interface (NNI);

(b) that Recommendation G.781 gives the structure of Recommendations on multiplexing equipment for the SDH;

(c) that Recommendation G.782 describes the types and general characteristics of SDH multiplexing equipment;

(d) that Recommendation G.783 specifies the characteristics of SDH multiplexing equipment functional blocks;

(e) that Recommendation G.958 specifies digital line systems based on SDH for use on optical fibre cables;

(f) that it is expected that further Recommendations will be produced concerned with other SDH equipment types, e.g. digital cross-connects and radio systems;

(g) that Recommendation M.30 defines the principles for a telecommunicationas management network (TMN);

(h) that Recommendation G.773 defines the protocol suites for Q-interfaces,

recommends

that the management of SDH equipment should be organized in accordance with the details contained within this Recommendation.

1 Introduction

This Recommendation addresses management aspects of the synchronous digital hierarchy (SDH), including the control and monitoring functions relevant to SDH network elements (NE). The SDH management sub-network (SMS) architecture, SDH embedded control channel (ECC) functions, and SDH ECC protocols are specified. Detailed message sets are for further study.

The management of SDH equipment should be seen as a subset of the telecommunications management network (TMN) described in Recommendation M.30, and reference is made to Recommendation G.773 for the specification of protocol suites to be used at external (Q) management interfaces.

2 Abbreviations and definitions

2.1 *Abbreviations*

ACSE Association control service element

AITS Acknowledged information transfer service

APDU Application protocol data unit

ASE Application service element

ASN.1 Abstract syntax notation one

CC Connect confirm

CLNP Connectionless network layer protocol

CLNS Connectionless network layer service

CMIP Common management information protocol

CMISE Common management information service element

CONP Connection oriented network-layer protocol

CR Connection request

CV Code violation

DCC Data communications channel

DCN Data communications network

ECC Embedded control channel

ES Errored second

FLS Frame loss second

FU Functional unit

GNE Gateway network element

IFU Interworking functional unit

IP Interworking protocol

IS Intermediate system

ISO International for standardization organization

LCN Local communications network

MAF Management applications function

MCF Message communications function

MD Mediation device

MF Mediation function

MO Managed object

MOC Managed object class

NE Network element

NEF Network element function

NLR Network layer relay

NNE Non-SDH network element

NPDU Network protocol data unit

NSAP Network service access point

OAM&P Operations, administration, maintenance and provisioning

OS Operations system

OSF Operations system function

OSI Open systems interconnection

PDU Protocol data unit

PJC Pointer justification count

PPDU Presentation protocol data unit

PSN Packet switched network

ROSE Remote operations service element

SAPI Service access point identifier

SDH Synchronous digital hierarchy

SMN SDH management network

SMS SDH management sub-network

SNDCF Sub-network dependent convergence function

SPDU Session protocol data unit

STM Synchronous transport module

SVC Switched virtual circuit

TEI Terminal end-point identifier

TMN Telecommunications management network

TPDU Transport protocol data unit

TSAP Transport service access point

UAS Unavailable second

UAT UnAvailable time

UI Unnumbered information

UITS Unacknowledged information transfer service

2.2 *Definitions*

2.2.1 **data communications channel (DCC)**

Within an STM-N signal there are two DCC channels, comprising bytes D1-D3, giving a 192 kbit/s channel, and bytes D4-D12, giving a 576 kbit/s channel. D1-D3 (DCC_R) are accessible by all SDH NEs whereas D4-D12 (DCC_M), not being part of the regenerator section overhead, are not accessible at regenerators. D1-D3 are allocated for SDH NE use. The D4-D12 channel can be used as a wide area, general purpose, communication channel to support TMN including non-SDH applications. This would include both communication between OSs and communication between an OS and a network element (including SDH network elements). The application of the D4-D12 channel requires study for general TMN applications and also for SDH network element management applications.

2.2.2 **embedded control channel (ECC)**

An ECC provides a logical operations channel between SDH NEs, utilizing a data communications channel (DCC) as its physical layer.

2.2.3 **SDH management network (SMN)**

An SDH management network is a subset of a TMN, responsible for managing SDH NEs. An SMN may be subdivided into a set of SDH management sub-networks.

2.2.4 **SDH management sub-network (SMS)**

An SDH management sub-network (SMS) consists of a set of separate SDH ECCs and associated intra-site data communication links which have been interconnected to form an operations data communications control network within any given SDH transport topology. An SMS represents an SDH specific local communication network (LCN) portion of a network operator's overall operations data network or TMN.

2.2.5 **management application function (MAF)**

An application process participating in system management. The management application function includes an agent (being managed) and/or manager. Each SDH network element (NE) and operations system or mediation device (OS/MD) must support a management application function that includes at least an agent. A management application function is the origin and termination for all TMN messages.

2.2.6 **manager**

Part of the MAF which is capable of issuing network management operations (i.e. retrieve alarm records, set thresholds) and receiving events (i.e. alarms, performance). SDH NEs may or may not include a manager while SDH OS/MDs will include at least one manager.

2.2.7 **agent**

Part of the MAF which is capable of responding to network management operations issued by a manager and may perform operations on managed objects, issuing events on behalf of managed objects. The managed objects can reside within the entity or in another open system. Managed objects from other open systems are controlled by a distant agent via a local manager. All SDH NEs will support at least an agent. Some SDH NEs will provide managers and agents (being managed). Some NEs (e.g. regenerators) will only support an agent.

2.2.8 **managed object (MO)**

The management view of a resource within the telecommunication environment that may be managed via the agent. Examples of SDH managed objects are: equipment, receive port, transmit port, power supply, plug-in card, virtual container, multiplex section, and regenerator section.

2.2.9 **managed object class (MOC)**

An identified family of managed objects that share the same characteristics, e.g. “equipment” may share the same characteristics as “plug-in card”.

2.2.10 **message communications function (MCF)**

The message communications function provides facilities for the transport of TMN messages to and from the MAF, as well as facilities for the transit of messages. The message communications function does not originate or terminate messages (in the sense of the upper protocol layers).

2.2.11 **operations system function or mediation function (OSF/MF)**

A telecommunications management network (TMN) entity that processes management information to monitor and control the SDH network. In the SDH sub-portion of the TMN, no distinction is made between the operations system function and the mediation function; this entity being a MAF containing at least a manager.

2.2.12 **network element function (NEF)**

A function within an SDH entity that supports the SDH based network transport services, e.g. multiplexing, cross-connection, regeneration. The network element function is modelled by managed objects.

2.2.13 **operations system or mediation device (OS/MD)**

A stand-alone physical entity that supports OSF/MFs but does not support NEFs. It contains a message communication function (MCF) and a MAF.

2.2.14 **network element (NE)**

A stand-alone physical entity that supports at least NEFs and may also support OSF/MFs. It contains managed objects, a MCF and a MAF.

3 SDH management network

3.1 *Management network organizational model*

The management of an SDH network uses a multi-tiered distributed management process. Each tier provides a pre-defined level of network management capabilities. The lower tier of this organizational model (see Figure 3-1/G.784) includes the SDH NEs providing transport services. The management applications function (MAF) within the NEs communicates with, and provides management support to, peer NEs and mediation device(s) (MDs)/operations system(s) (OSs).

The communication process is provided via the message communication function (MCF) within each entity.

The MAF at each entity can include agents only, managers only, or both agents and managers. Entities that include managers are capable of managing other entities.

Each tier in the multi-tiered organizational model can provide additional management functionality. However, the message structure should remain the same. A manager within an SDH NE may suppress alarms generated by one or more of its managed NEs due to a common failure, and replace them by a new alarm message, directed to the OS/MD, identifying the source of the problem. The new alarm message format will be consistent with other alarm messages.

FIGURE 3-1/G.784

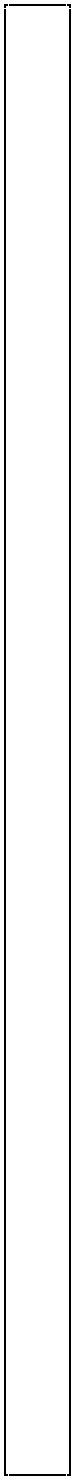
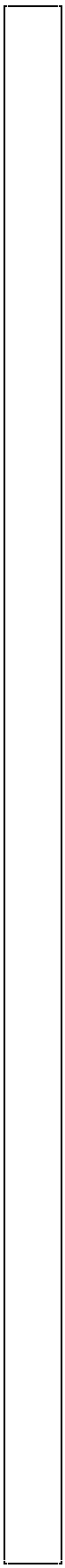


FIGURE 3-2/G.784



The message format will be maintained as messages are elevated up the hierarchy, i.e., SDH NE to SDH NE messages will have the same structure as SDH NE to MD messages and SDH MD to OS messages.

Figure 3-2a/G.784 illustrates examples of management communication using a Q-interface implemented in the MCF where logically independent communications are provided over a single physical interface:

– between a manager in the OS and two different agents; one in the MD and one in NE2 (interface a);

– between a manager in the MD and an agent in NE1; between a manager in the OS and an agent in NE2 (interface b).

Figure 3-2b/G.784 illustrates examples of management communication using Q-interface protocols implemented in the MCF:

– between a manager in the OS and an agent in the MD (interface c);

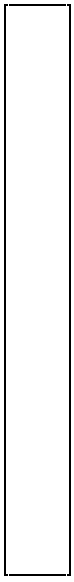
– between a manager in the MD and an agent in NE1 (interface d);

– between a manager in NE1 and an agent in NE2 (interface e).

3.2 *Relationship between SMN, SMS and TMN*

The inter-relationship between the SMN, SMS and TMN is shown in Figure 3-3/G.784. Figure 3-4/G.784 shows specific examples of SMN, SMSs and connectivities within the encompassing TMN.

FIGURE 3-3/G.784



The following sub-sections describe the SMS in more detail, addressing:

– access to the SMS; and

– SMS architecture.

3.2.1 *Access to the SMS*

Access to the SMS is always by means of an SDH NE functional block. The SDH NE may be connected to other parts of the TMN through the following sets of interfaces:

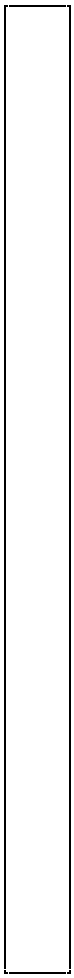
1) workstation (F);

2) mediation device (a Q-interface);

3) operations system (a Q-interface);

4) non-SDH NE or site related information (interface(s) for further study).

FIGURE 3-4/G.784



The functionality required to be supported by the SDH NE will determine the type of Q-interface to be provided. For instance, the two main varieties of SDH NEs expected are the SDH NEs with mediation functions (MF) and "regular" SDH NEs. An example of the SDH NE with MF is shown in Figure 3-5/G.784. An example of a "regular" SDH NE is shown in Figure 3-6/G.784.

3.2.2 *SDH management sub-network architecture*

In Figure 3-4/G.784 a number of points should be noted concerning the architecture of the SMS:

a) *Multiple NEs at a single site*

Multiple, addressable SDH NEs may appear at a given site. For example, in Figure 3-4/G.784 NEe and NEg may be collocated at a single equipment site.

b) *SDH NEs and their communications functions*

The message communications function of an SDH NE terminates (in the sense of the lower protocol layers), routes or otherwise processes messages on the ECC, or connected via an external Q-interface.

i) All NEs are required to terminate the ECC. In OSI terms, this means that each NE must be able to perform the functions of an end system.

ii) NEs may also be required to route ECC messages between ports according to routing control information held in the NE. In OSI terms, this means that some NEs may be required to perform the functions of an intermediate system.

iii) NEs may also be required to support Q- and F-interfaces.

c) *SDH inter-site communications*

The inter-site or inter-office communications link between SDH NEs will normally be formed from the SDH ECCs.

d) *SDH intra-site communications*

Within a particular site, SDH NEs may communicate via an intra-site ECC or via an LCN. Figure 3-4/G.784 illustrates both instances of this interface.

Note – A standardized LCN for communicating between collocated network elements has been proposed as an alternative to the use of an ECC. The LCN would potentially be used as a general site communications network serving both SDH and non-SDH NEs (NNEs). The LCN is part of the TMN and thus the specification of the LCN is beyond the scope of this Recommendation.

3.3 *SMS topology and reference models*

3.3.1 *ECC topology for the SDH management sub-network*

It is intended that this Recommendation should place no restriction on the physical transport topology to support the ECC. Thus it is expected that the supporting DCCs may be connected using string (bus), star, ring or mesh topologies.

Each SDH management sub-network (SMS) must have at least one element which is connected to an OS/MD. This is called a gateway network element (GNE) and is illustrated in Figures 3-5/G.784, 3-6/G.784 and 3-7/G.784. The GNE should be able to perform an intermediate system network layer routing function for ECC messages destined for any end system in the SMS.

Note – This is a specific instance of the general requirement that messages passing between communicating sub-networks shall use the network layer relay.

The communications function is illustrated in Figure 3-7/G.784. Messages passing between OS/MD and any of the end systems in the sub-network are routed through the GNE and, in general, other intermediate systems.

FIGURE 3-5/G/784

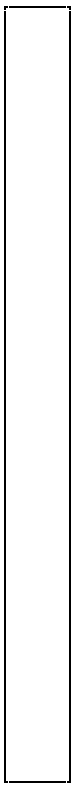


FIGURE 3-6/G.784

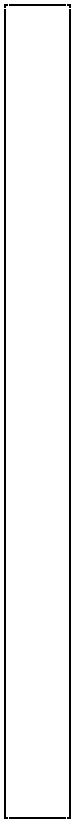
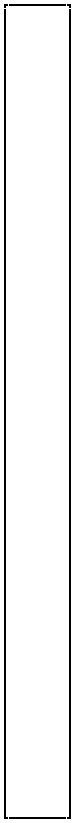


FIGURE 3-7/G.784



3.3.2 *Message routing at SDH NE sites*

The means of generation and administration of routing control information amongst communicating sub-networks and within sub-networks is detailed in § 6.2.3.

3.3.3 *SMS reference models*

Reference models are particularly suited for test cases and for design verification and acceptance testing. The reference configurations in Figure 3-8/G.784 and Figure 3-9/G.784 are examples of test cases for SMS management. Examples of SMS connectivity are given in Figure 3-10/G.784.

Other variations of Figure 3-9/G.784 are also of interest as reference configurations; for example, on routes where the operator chooses not to implement the multiplex section protection (MSP) function, the ECCs would be provided on at least two SDH lines, and optionally on any remaining SDH lines of a particular route.

FIGURE 3-8/G.784

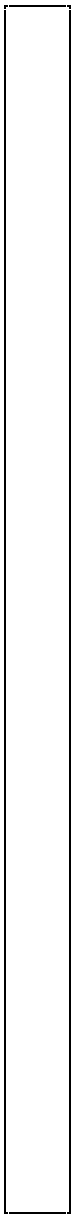


FIGURE 3-9/G.784

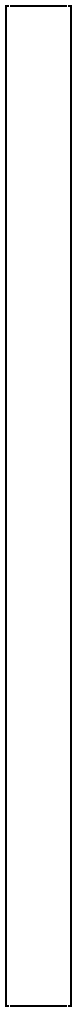
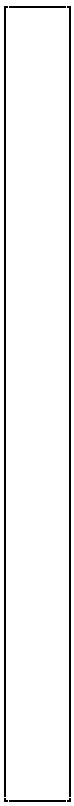


FIGURE 3-10/G.784



4 Information model

An overview of object modelling and the objectives for the SDH specific model are given in Annex D.

Detailed specifications are for further study.

Note – This section will contain the information required to specify the ASN.1 encoded manager-agent messages needed to support the management functions described in § 5.

5 Management functions

This section provides an overview of the minimum functions which are required to support inter-vendor/-network communications and single-ended maintenance of SDH NEs within an SMS, or between communicating peer NEs across a network interface (§§ 5.1.1, 5.2.1, 5.3.1, 5.4.2). Single-ended maintenance is the ability to access remotely located NEs to perform maintenance functions.

Other management functions have been identified (§§ 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.2.2, 5.2.3, 5.4.1, 5.4.3, 5.5) and will be specified in the latter stages of the 1988-1992 CCITT study period.

It should be noted that the management functions have been categorized according to the classifications given in Recommendation M.30.

Detailed specifications of the management functions, in terms of support objects, attributes and message specification, are given in Annex A.

5.1 *General functions*

5.1.1 *Embedded control channel (ECC) management*

In order for SDH NEs to communicate they must manage the ECC. The ECC management functions defined below are examples of functions required to be supported with ECC messages:

a) retrieval of network parameters to ensure compatible functioning, e.g., packet size, timeouts, quality of service, window size, etc.;

b) establishment of message routing between DCC nodes;

c) management of network addresses;

d) retrieval of operational status of the DCC at a given node; and

e) capability to enable/disable access to the DCC.

5.1.2 *Security*

For further study.

5.1.3 *Software*

For further study.

5.1.4 *Remote login*

For further study.

5.1.5 *Time-stamping*

The required accuracy and precise details of the time-stamping of events/reports is the subject of further study. (Maximum values in the range 1 to 30 seconds have been mentioned for the permissible inaccuracy compared to real time.)

5.2 *Fault (maintenance) management*

5.2.1 *Alarm surveillance*

Alarm surveillance is concerned with the detection and reporting of relevant events/conditions which occur in the network. In a network, events/conditions detected within the equipment and within the incoming signal, as well as those external to the equipment, should be reportable. Alarms are indications that are automatically generated by an NE as a result of certain events/conditions. The user shall have the ability to define which events/conditions generate autonomous alarm reports. The remaining events/conditions are reported on request.

The following alarm-related functions shall be supported:

– report autonomous alarms;

– request all alarms;

– report all alarms;

– allow/inhibit alarm reporting over the ECC;

– request status of allow/inhibit alarm reporting;

– report status of allow/inhibit alarm reporting.

A summary of alarm conditions is given in § 2 of Annex A. Detailed message sets are for further study.

5.2.2 *Testing*

For further study.

5.2.3 *External events*

For further study.

5.3 *Performance management*

5.3.1 *Performance monitoring*

Note – Fixed window processing of the primitive performance information (15 minutes and 1 day) is considered satisfactory for the purpose of network surveillance and of fault identification and sectionalization. This does not preclude the additional use of other window processing techniques for detailed performance or fault characterization where it is demonstrated that these provide significant additional information on the nature of errored events. If an alternative window processing technique is used, it should be capable of default to the fixed window method.

5.3.1.1 *Performance data collection*

Performance data collection refers to the event count associated with each of the performance parameters indicated in Recommendation G.783. The parameters are derived from performance primitives associated with SDH frame formats defined in Recommendations G.707, G.708 and G.709. Event counts are inhibited under certain failure or unavailable conditions as specified in § 5.3.1.7.

Parameter requirements specific to each digital signal are summarized in § 3 of Annex A. Detailed message sets are for further study.

5.3.1.2 *Performance monitoring history*

Performance history data is useful to assess the recent performance of transport systems and sectionalize the trouble or degradation. This history can also enable performance assessment against long-term performance objectives.

Limited historical data, in the form of event counts for each monitored parameter, shall be stored in NEs, or in mediation devices associated with NEs. Separate performance monitoring data shall be stored for individual directions of transmission.

A current 15-minute and current day register, a previous 15-minute and previous day register, and a certain number of recent 15-minute and day registers will be provided per monitored parameter, per direction (as detailed in § 3 of Annex A).

The 15-minute and day registers shall function as follows:

a) Current 15-minute register – contains the impairment count for the parameter during a 15-minute period. The current 15-minute register shall be reset to zero each 15 minutes after the data is transferred to the previous 15-minute register.

b) Current day register – contains the impairment count for the parameter during a 1-day period. The current day register shall be reset to zero each day (e.g. at midnight) after the data is transferred to the previous day register.

c) Previous 15-minute register – contains a 15-minute count for the parameter. At the end of each 15 minutes the impairment count from the current 15-minute register is stored in the previous 15-minute register and the old data from the previous 15-minute register is transferred to the first recent register (if recent 15-minute registers are provided; if not, the old data is discarded).

d) Previous day register – contains a 1-day count for the parameter. At the end of each day the impairment count from the current day register is stored in the previous day register and the old data from the previous day register is transferred to the most recent register (if recent day registers are provided; if not, the old data is discarded).

e) Recent 15-minute registers – a group of *n* registers, each of which contains a 15-minute count, so that performance data for the *n* most recent 15 minutes (plus the previous 15 minutes) is stored (values of "*n*" are specified in § 3 of Annex A). At the end of each 15 minutes the count from the previous 15-minute register is stored in the first recent register. The values in each successive recent register are pushed down one register in the stack. The oldest 15 minutes at the bottom of the stack is discarded.

f) Recent day registers – a group of *m* registers, each of which contains a 1-day count, so that performance data for the *m* most recent days (plus the previous day) is stored (values of "*m*" are specified in § 3 of Annex A). At the end of each day the count from the previous day register is stored in the first recent register. The values in each successive recent register are pushed down one register in the stack. The oldest day at the bottom of the stack is discarded.

The above registers shall be readable on demand, and routine (e.g. daily) retrieval of the previous plus recent data shall be possible without loss of data. The registers may be manually reset to zero at any time. The registers shall not be automatically reset when service is restored after failure.

Note – The need to provide a limited number of registers which could provide, on request, event history of a selectable parameter, time stamped on a 1-second basis is for further study.

5.3.1.3 *Threshold setting and threshold crossing notifications*

Threshold crossing alarm messages signify performance degradations reaching and/or exceeding (i.e. > = function) preset thresholds, and as such, are an integral part of the performance monitoring process. Thresholds may be set in the NE to notify the OS before service is affected. The value of the threshold shall be settable over the minimum range given in Table A-6/G.784.

When the NE recognizes a threshold crossing for a given parameter, a threshold crossing notification should be generated. When a threshold is crossed, the NE shall continue counting to the end of the accumulation period, when the current count is stored and reset. No more than one threshold notification (per parameter, per direction of transmission) shall be sent during any accumulation period.

Details of threshold setting functions are given in § 5.3.1.5.

5.3.1.4 *Performance data reporting*

Data reporting is useful for initiating appropriate maintenance actions and also when following up trouble reports. That is, performance data stored in the NE may be collected and analysed. If marginal troubles are detected, appropriate maintenance actions can then be carried out.

Also, routine data collection may be performed periodically to support trend analysis to predict future failure/degrade conditions.

To report performance data, the parameters (e.g. ES, SES), the direction of transmission (i.e. near end, far end) and the accumulation period (e.g. current 15 minutes, day) need to be specified. The reporting intervals are nominally 15 minutes and a day.

Performance data shall be reportable across the OS/NE interface in each of the following ways:

a) on demand per port when requested by the OS;

b) automatically upon the crossing of a performance monitoring threshold (e.g. 15-minute alert and current 15-minute register values for all parameters);

c) periodically for specific ports as required by the OS. The suppression of reporting of zero counts is for further study.

Note – The term "port" means a single section, line or path termination, or monitoring point, in the NE.

An OS can request an NE to report performance monitoring data on demand or periodically on selected ports.

If the NE is unable to begin periodic reporting of data in response to the OS command, the NE should respond with an unable to comply message.

For 24-hour data specifically, the OS may instruct the NE on when to begin measurement of the 24-hour period for the purpose of collecting data. The NE shall be able to begin the measurement at the start of any hour.

The specific functions which should be supported at the OS/NE interface to support data collection and thresholding are:

a) Request data – OS requests the NE to send data including parameters, direction of transmission and accumulation period; NE responds with a data report.

b) Schedule data report – OS directs the NE to establish a schedule for the reporting of data including parameters, direction of transmission, reporting interval, start of reports and number of reports; NE responds by sending the appropriate period data reports, or NE responds with an unable to comply message if not equipped to handle scheduling of data reports.

c) Request data report schedule – OS directs the NE to send the current data reporting schedule; NE reports with the schedule including parameters, direction of transmission, reporting interval (i.e. 15 minutes, daily), time of next report, and remaining number of reports.

d) Start/stop data – OS directs the NE to start or stop the reporting of data including reporting interval, parameters, direction of transmission; NE responds with verification that reporting will start/stop.

e) Data report – NE sends performance data to the OS including parameter, direction of transmission, type of threshold, threshold level and register value. It may be generated periodically by the NE (when periodic reporting is scheduled by OS), sent upon demand by the OS or by exception when a parameter threshold has been exceeded.

f) Set attributes – OS directs the NE to assign designated attributes including parameter to be monitored, type of threshold (i.e. 15 minutes, daily), threshold value, data reporting mode (e.g. scheduled, start/stop), and start time of 24-hour period; NE responds with new attribute designations.

g) Request attributes – OS requests the NE to send to the OS the current attributes; NE responds by sending the currently assigned attributes including parameter to be monitored, type of threshold, threshold value, whether data reports are enabled or inhibited, and start time of 24-hour period. It is permissible for the NE to code the set (or sets) of attributes so as to minimize message traffic, and also to use the code to signify operational status of the NE. How this latter function can be achieved in the context of standardized OS/NE messages is for further study.

5.3.1.5 *Register and threshold setting functions*

5.3.1.5.1 *Initialization*

The NE shall allow the OS to initialize current storage registers. The specific function related to data initialization which should be supported at the OS/NE interface is:

– Initialize data – OS directs the NE to reset storage registers for data, including type of registers (i.e. 15 minutes, daily).

5.3.1.5.2 *Capability for threshold setting*

The OS shall be able to retrieve and change the settings of the 15-minute and daily thresholds on a per port basis.

Threshold crossing notifications shall have default thresholds, as well as locally and remotely settable non-default thresholds.

When the OS requests that a threshold be changed, the NE shall respond with the new value to which the threshold has been set. If the OS requests a threshold value higher than allowed by a given NE implementation, the NE shall set the threshold to the nearest lower threshold value which the NE implementation allows and report this change to the OS.

The ability to inhibit threshold setting on a per port basis or on a per NE basis shall be supported. The OS shall be notified of such a condition when data is collected, and when attributes are requested. When threshold setting is re-enabled, threshold values shall be restored to the same ones in place just prior to the inhibit.

5.3.1.6 *Accuracy and resolution*

All parameter counts should be actual, except when there is register overflow, in which case the registers hold at the maximum value until they are read and reset at the end of the accumulation period.

15-minute and daily time intervals shall be accurate to within plus or minus (to be decided; values in the range 1 to 10 seconds have been proposed).

The start of 15-minute and daily counts shall be accurate to within plus or minus (to be decided; values in the range 1 to 30 seconds have been proposed).

5.3.1.7 *Performance monitoring during unavailable and trouble conditions*

Performance parameter counts shall be inhibited during UnAvailable time (UAT) as given in Table A-7/G.784. Monitoring shall be correlated with UAT and trouble conditions, e.g. LOS, LOF and LOP, as well as AIS which is indicative of upstream trouble.

5.4 *Configuration management*

5.4.1 *Provisioning*

For further study.

5.4.2 *Status and control (protection switching)*

The general facility of protection switching is defined as the substitution of a standby or back-up facility for a designated facility. The specific functions which allow the user to control the traffic on the protection line are:

- operate/release manual protection switching;
- operate/release force protection switching;
- operate/release lockout;
- request/set automatic protection switching (APS) parameters.

5.4.3 *Installation functions*

For further study.

5.5 *Security management*

For further study.

6 Protocol stack

6.1 *Description*

The protocol stack shown in this section has been selected to satisfy requirements for the transfer of operations, administration, maintenance and provisioning (OAM&P) messages across the SDH data communications channels (DCC). It is in accordance with the current object oriented approach to the management of open systems. That is, the application layer includes the common management information service element (CMISE), and the remote operations service element (ROSE) and association control service element (ACSE) to support CMISE.

The presentation, session and transport layers provide the connection oriented service required for support of ROSE and ACSE. The transport layer includes the additional protocol elements required to provide a Connection Mode service when operating over the connectionless network layer protocol (CLNP) (ISO 8473 [1]). Data link support is provided by LAPD as defined in Recommendations Q.920 [31] and Q.921 [32].

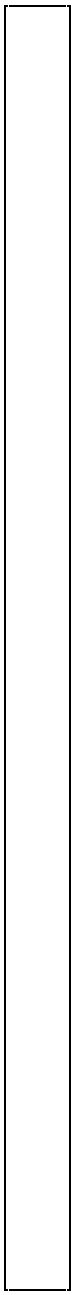
Layer 1, the physical layer of the stack, represents the SDH DCC.

6.1.1 *ECC protocol stack description*

The protocol stack given in Figure 6-1/G.784 is to be used for the communication of management messages over the SDH DCC. The specifications of options and parameters required in order to guarantee interoperation are described in § 6.2.

The protocols for each layer, as outlined in the following sub-sections, are to be used for management communications over the SDH ECC. The detailed specifications of these protocols are given in § 6.2.

FIGURE 6-1/G.784



6.1.1.1 *Physical layer (layer 1)*

The SDH data communication channel (DCC) constitutes the physical layer.

6.1.1.2 *Data link layer (layer 2)*

The data link protocol, LAPD (Recommendation Q.921) provides point-to-point connections between nodes of the underlying transmission network.

6.1.1.3 *Network layer (layer 3)*

The network protocol ISO 8473, provides a datagram service suitable for the high speed, high quality underlying network. Convergence protocols have been defined in ISO 8473/AD3 for the operation of ISO 8473 over both connection-oriented and connectionless data link sub-networks.

6.1.1.4 *Transport layer (layer 4)*

The transport protocol ensures the accurate end-to-end delivery of information across the network. The protocol creates a transport connection from the underlying connectionless network service (ISO 8073/AD2 [7]) and provides for flow-control and error recovery on this connection. Transport class 4 is selected to ensure reliable NPDU delivery over the connectionless mode network layer services.

6.1.1.5 *Session layer (layer 5)*

The session protocol ensures that the communication systems are synchronized with respect to the dialogue under way between them and manages, on behalf of the presentation and application layers, the transport connections required.

6.1.1.6 *Presentation layer (layer 6)*

The presentation protocol and the ASN.1 basic encoding rules act to ensure that application layer information can be understood by both of the communicating systems – the context of the information being transferred and the syntax of the encoding of information.

6.1.1.7 *Application layer (layer 7)*

The following options of the application layer shall be utilized:

i) CMISE

The common management information service element (CMISE) of the ISO common management information protocol (CMIP) provides services for the manipulation of management information across the ECC. It has been selected by ISO as the carriage protocol for network management protocols. CMISE is based on an object-oriented paradigm that represents network entities, and network management functions and information as objects with attributes and operations that can be performed on the objects. The CMISE services enable a network management system to:

– create and delete the objects (CREATE/DELETE);

– define and redefine values of object attributes, (SET and GET);

– invoke operations on the objects (ACTION), and

– to receive reports from the objects (EVENT REPORT).

ii) ROSE

The remote operations service element (ROSE) permits one system to invoke an operation on another system and to be informed of the results of that operation. In the context of the ECC protocol stack, the operations are defined to be CMISE services.

iii) ACSE

The association control service element (ACSE) provides services to initiate and terminate a connection (association), between two applications. This association is then used to convey the management messages corresponding to the CMISE services.

6.2 *Protocol specifications*

This section specifies protocols for the SDH ECC.

Protocol options, features, parameter values, etc., in addition to those specified in this Recommendation may be included in a conforming system provided they are not explicitly excluded by this Recommendation and they do not prevent interoperability with conforming systems that do not provide them.

A control network topology is outlined in § 3.2.2.

6.2.1 *Physical layer protocol specification*

The regenerator section DCC shall operate as a single 192 kbit/s message based channel using the section overhead bytes D1 to D3. The multiplex section DCC shall operate as a single 576 kbit/s message based channel using the section overhead bytes D4 to D12.

6.2.2 *Data link layer protocol specification*

The data link layer shall provide point-to-point transfer, over the SDH DCC, of Network Service Data Units (NSDU) through a single logical channel between each pair of adjacent network nodes.

The data link layer shall operate under the rules and procedures specified in Recommendation Q.921 [32] for the Unacknowledged Information Transfer service (UITS) specified in § 6.2.2.1, and for Acknowledged Information Transfer service (AITS) specified in § 6.2.2.2. Both services (UITS and AITS) shall be supported. AITS shall be the default mode of operation.

A mapping between the connection-mode Data Link service primitives defined in ISO 8886 (Recommendation X.212) and Recommendations Q.920/Q.921 primitives is defined in Table 6-1/G.784.

TABLE 6-1/G.784

Mapping of Data Link service and Q.920 primitives

Data Link Service Primitive	Q.920 Primitive
DL-CONNECT request DL-CONNECT indication DL-CONNECT response DL-CONNECT confirm	DL-ESTABLISH request DL-ESTABLISH indication (Note 1) (Note 2) DL-ESTABLISH confirm
DL-DATA request DL-DATA indication	DL-DATA request DL-DATA indication
DL-DISCONNECT request DL-DISCONNECT indication (Note 3)	DL-RELEASE request DL-RELEASE indication DL-RELEASE confirm

Note 1 – This primitive indicates that the data link connection is open.

Note 2 – Recommendation Q.921 will ignore this response.

Note 3 – Network layer will ignore this confirmation.

6.2.2.1 Unacknowledged information transfer service (UITS)

UITS shall follow the rules and procedures specified in Recommendation G.921 [32]. For the UITS, the sub-network dependent convergence function (SNDCF) provides a direct mapping onto the data link layer as specified in § 8.4.4.1 of ISO 8473/AD3 [2]. For this application, mandatory and optional service and Protocol parameters shall have the values specified in Table 6-2/G.784.

TABLE 6-2/G.784

UITS specification

a)	The unnumbered information (UI) frames shall be used for data transfer as specified in Recommendation Q.921 [32].
b)	As specified in Recommendation Q.921 [32], UI frames shall always be commands. The assignment of user-side/network-side roles (and hence the C/R bit value) shall be made prior to initialization.
c)	Service access point identifier (SAPI) Value: 62* * The need for additional SAPIs is for further study, e.g. to support SDH DCC maintenance.
d)	Terminal end-point identifier (TEI) Value: 0
e)	The frame size shall be capable of supporting an Information Field of 512 octets as specified in ISO 8473, § 8.4.2 [1].
f)	TEI management procedure, as specified in Recommendation Q.921 [32], shall NOT be supported.
g)	Poll/Final Bit shall always be set to 0, as specified in Recommendation Q.921 [32].

6.2.2.2 *Acknowledged information transfer services (AITS)*

AITS shall follow the rules and procedures specified in Recommendation Q.921 [32]. For AITS, the SNDCF provides a mapping onto the data link layer as specified in § 8.4.4.2 of ISO 8473/AD3 [2]. For this application, mandatory and optional service and protocol parameters shall have the values specified in Table 6-3/G.784. In addition, the requirements specified in c) to f) of Table 6-2/G.784 shall also be followed.

6.2.3 *Network layer protocol description*

The connectionless mode network layer service provided to the transport layer is defined in ISO 8348/AD1 [3] and the protocol to provide this service shall conform to ISO 8473 [1]. Network protocol data units (NPDUs) are routed through intermediate systems to end systems using routing control information at each intermediate system. All NEs must be designed to function as an intermediate system, as an end system or both. An intermediate system is defined as having one or more ports to which a received NPDU may be forwarded, while an end system has none.

TABLE 6-3/G.784

AITS specifications

a)	The assignment of user-side/network-side roles, and hence the C/R bit value, shall be made prior to initialization.
b)	The default value for (k) 7
c)	The default value for T200 ..... 200 ms
d)	The default value for T203 ..... 10 secondes *Note* – This parameter is used with the optional procedures listed as item f) below.
e)	The default value for N200 3
f)	Data link monitor functions as specified in Recommendation Q.921 [32] are optional.
g)	Parameter negotiation as described in Appendix IV of Q.921 may be used to select alternative parameter values.

The routing control information is used to select the underlying service needed to reach the next system in the route. It is recommended that the derivation and provisioning of this routing information should be supported in one of the following ways.

a) manual administration;

b) use of the end system to intermediate system routing exchange protocol as defined in ISO 9542 [4] (i.e. can be used between an intermediate system and all end systems connected to it to establish the routing control at the intermediate system);

c) intermediate system to intermediate system intra-domain routing exchange protocols are currently under study and may be used when available. They are expected to be backward compatible with the end system to intermediate system routing exchange protocol referred to in b) above.

Note – Until intermediate system to intermediate system intra-domain routing exchange protocols are available, and if the manual administration of routing tables is too burdensome, then one of the schemes described in Annexes B and C may be used. However, when selecting one of these schemes, network operators should take into account the possible backward compatibility implications of introducing intermediate system to intermediate system intra- domain routing exchange protocols, once finalized.

For this application, the full protocol subset of category 1 functions, as specified in ISO 8473 [1], shall be supported. Category 2 functions, as specified in ISO 8473 [1], may be supported. Category 3 functions, as specified in ISO 8473 [1], that are not required or prohibited in Table 6-4/G.784, may also be supported. The service/protocol parameters shall have the values specified in Table 6-4/G.784.

TABLE 6-4/G.784

Network layer service/protocol parameters

a)	Destination and source addresses used by this protocol shall be Network Service Access Points (NSAP) addresses, as specified in ISO 8348/AD2 [5]. The destination and source addresses are of variable length. The destination and source address fields shall be encoded as network protocol address information using the preferred binary encoding specified in ISO 8348/AD2 [5].
b)	Partial source routing shall NOT be supported. A defect exists with this option which can cause NPDUs to loop in the network until their lifetime expires.
c)	Inactive subset – Implementations shall not transmit NPDUs encoded using the ISO 8473 [1] inactive subset. Received NPDUs encoded with the inactive subset shall be discarded.
d)	Segmentation – The non-segmentation subset shall NOT be used. However, implementation shall be capable of receiving and correctly processing NPDUs which do not contain de segmentation part.
e)	Segmentation permitted flag – Implementation shall NOT generate data NPDUs without a segmentation part, i.e., the segmentation permitted flag (SPF) shall be set to 1 and segmentation part shall be included.
f)	Lifetime control – The lifetime parameter shall be used as specified in clause 6.4 of ISO 8473 [1]. This parameter shall have an initial value of at least three times the network spans (number of network entities) or three times the maximum transmission delay (in units of 500 milliseconds), whichever is greater.
g)	Quality of service maintenance – The quality of service (QOS) Maintenance function shall be supported. The QOS parameter shall be used as specified in §§ 6.16, 7.5.6 and 7.5.6.3 of ISO 8473. The coding of the QOS parameter for the selection of UITS/AITS is shown below: 1) The absence of a QOS parameter shall select AITS in the data link. 2) In the QOS parameter, bits 7 and 8 set to 1 (globally unique QOS) and bit 1 set to 1 shall select AITS. 3) In the QOS parameter, bits 7 and 8 set to 1 (globally unique QOS) and bit 1 set to 0 shall select UITS. 4) The use of QOS parameter bits 2, 3, 4, 5 and 6 are not the subject of, or specified in, this Recommendation. The criteria for selecting AITS or UITS is the network provider's responsibility.

6.2.4 *Transport layer protocol specification*

The required transport layer protocol shall be the connection-mode protocol as specified in ISO 8073 [6], together with ISO 8073/AD2 [7] for class 4 operation over CLNS. Transport protocol class 4 (TP4) shall be the only supported transport protocol class over the SDH DCC.

Transport layer attribute values are given in Table 6-5/G.784.

6.2.5 *Session layer*

The session layer conforms to the service definition and protocol specification in Recommendations X.215 [19] and X.225 [20] respectively. Support of version 2 of the session protocol is mandatory.

TABLE 6-5/G.784

Transport layer attributes specification

	Parameter	Range	Default
a)	Maximum TPDU (octets) (Note 1)	128, 256, 512, 1024 (2048, 4096 optional)	128
b)	TSAP-ID (Note 2) Class of service Alternative class Expedited Data	Up to 32 octets 4 None Non-use	
c)	Optional for class 4 Data TPDU numbering (Note 3) Checksum (Note 4)	Normal, extended Use, non-use	Normal Non-use
d)	Parameters for class 4 T1 retransmission time N retransmissions L Bound on reference I Inactivity time	0.25 – 64 seconds (Note 4) 2 (Other values for further study) 1 – 256 seconds 2 – 512 seconds	8 32 64

Note 1 – TPDU size negotiation shall be supported.

Note 2 – Some systems may not require TSAP-IDs. However, all systems shall be capable of generating called TSAP IDs in CR TPDUs and be capable of receiving calling TSAP IDs in received CR and CC TPDUs.

Note 3 – Extended format option shall be implemented. Non-use of this option shall be negotiable. The responder shall honour the initiator's request whenever possible. Negotiation to other than what has been requested shall only occur under abnormal conditions, for example, severe congestion, as determined by the implementor. Initiators shall be prepared to operate in the mode confirmed by the responder.

Note 4 – Use of checksum is required for CR TPDU. All implementations shall support “non-use” of the checksum. Both transport entities shall agree to “non-use” of the checksum. All implementations shall be able to operate with checksum if requested.

Note 5 – The transport timer T1 should always be greater than the link layer T1 timer.

Note 6 – If a responder receives an alternate class of none, it shall respond with the class of TP4.

Note 7 – User data on the connect request (CR) and connect confirm (CC) transport PDU (TPDU) may be ignored and shall not cause a disconnect.

Note 8 – Quality of service (QOS) negotiation is outside the scope of this Recommendation. QOS parameters, including throughput, residual error rate, priority and transit delay in the CC and CR TPDUs may be ignored.

Note 9 – Protection negotiation is outside the scope of this Recommendation. Protection parameters in the CC and CR TPDUs may be ignored.

Note 10 – Unknown TPDU parameters and the Additional Options parameters shall be ignored.

General note – The default values shall be part of a vendor's offering. That is, unless otherwise specified by the user, the default parameters shall be the initial values supplied. They can be subsequently changed by the user within the specified range.

Two session layer functional units (FU) are required in this Recommendation:

1) Kernel,

2) Duplex.

Restrictions applied to parameters and their values are specified in the following sections.

6.2.5.1 *Session protocol data units*

The following session protocol data units (SPDUs) associated with the Kernel and Duplex functional units shall be supported as detailed in Table 6-6/G.784.

TABLE 6-6/G.784

Session PDU

Connect	(CN SPDU)
Accept	(AC SPDU)
Refuse	(RF SPDU)
Finish	(FN SPDU)
Disconnect	(DN SPDU)
Abort	(AB SPDU)
Abort Accepted	(AA SPDU)
Data Transfer	(DT SPDU)

6.2.5.2 *Transport expedited service*

The use of the transport expedited service is as stated in Recommendation X.225 [20]; if available, it must be used. When the transport expedited service is available, the prepare (PR) SPDU shall be supported as in Recommendation X.225 [20]. The prepare type parameter value in the PR SPDU, to indicate the arrival of an abort (AB) SPDU, is ABORT.

6.2.5.3 *Parameters*

All mandatory parameters defined in Recommendation X.225 [20] for the SPDUs required by the Kernel and Duplex FUs are mandatory parameters for this Recommendation.

6.2.5.4 *User data*

The maximum length of the session user data shall be 10 240 octets. This restriction implies that the overflow accept (OA) and connect data overflow (CDO) SPDUs are not required to be supported. Session selector (S-selector) parameter values shall have a maximum length of 16 octets.

6.2.5.5 *Reuse*

Reuse of the transport connection is not required. The transport disconnect parameter value (PV) field may be absent or set to "transport connection is released" in appropriate SPDUs. Furthermore, on receipt of a transport disconnect PV field indicating "transport connection is kept", the transport connection can be released.

6.2.5.6 *Segmentation*

The segmentation feature in the session layer is not required. Support for extended concatenation of SPDUs is not required.

6.2.5.7 *Invalid SPDUs*

Upon receipt of an invalid SPDU, the session protocol machine shall take any action specified in § A.4.3.2 of Recommendation X.225 [20] with the exception of action "d" (take no action).

6.2.6 *Presentation layer*

It is mandatory that the presentation layer conform to the services and protocols specified in Recommendations X.216 [21] and X.226 [22] respectively. One presentation layer functional unit (FU) is required in this Recommendation: Kernel.

The presentation protocol shall be used in the normal mode. Restrictions applied to parameters and their values are specified in the following sections.

6.2.6.1 *Presentation protocol units*

The following presentation protocol units (PPDU) associated with the Kernel functional unit shall be supported, as detailed in Table 6-7/G.784.

TABLE 6-7/G.784

Presentation PDU

Connect presentation	(CP PPDU)
Connect presentation accept	(CPA PPDU)
Connect presentation reject	(CPR PPDU)
Abnormal release provider	(ARP PPDU)
Abnormal release user	(ARU PPDU)
Presentation data	(TD PPDU)

6.2.6.2 *Parameters*

All mandatory parameters defined in Recommendation X.226 [22] for the above PPDUs are mandatory for this Recommendation. The presentation context identifier value shall be encoded in no more than 2 octets. Also, the value(s) in the parameter presentation context definition list shall be consistent with the value(s) defined in the application-specific standards. Presentation-selector (P-selector) parameter values shall have a maximum length of 4 octets.

6.2.6.3 *Encoding rules for transfer syntax*

The encoding rules defined in Recommendation X.209 [23] shall be applied to derive the transfer syntax for the application protocol data units (APDUs). The ASN.1 OBJECT IDENTIFIER {joint-iso-ccitt asn.1(1) basic-encoding(1)} shall be used as the value for the transfer syntax name. The maximum value of an ASN.1 basic encoding tag that needs to be handled for conformance to this Recommendation is 16 383. This is the largest unsigned integer that can be represented in 14 bits. Hence the identifier octets shall consist of an initial octet and up to two more octets, thus occupying a maximum of three octets. Also, the largest number of octets in the contents octets component of an ASN.1 data value encoding that needs to be handled for conformance to this Recommendation is 4 294 967 295. This is the largest unsigned integer than can be represented in 32 bits. Hence in the long form encoding, the length octets shall consist of an initial octet and up to four more octets, thus occupying a maximum of five octets. (Note that this restriction does not apply to indefinite length encodings.)

6.2.7 *Application layer*

It is mandatory that the application layer conforms to the architecture for the application layer outlined in ISO 9545 [8]. Abstract syntax notation one (ASN.1) shall be used as the abstract syntax for specifying application protocols.

6.2.7.1 *Supporting ASE*

It is mandatory that the association control service elements (ACSE) conform to the services and protocols specified in Recommendations X.217 [24] and X.227 [25]. The ACSE shall establish, release and abort the associations required. The ACSE service shall operate in the normal mode.

Network management transaction oriented applications shall use the common management information service element (CMISE). Services defined by CMISE that are applicable include:

1) the reporting of an event to an OS/MD;

2) the transfer of information between OSs/MDs and NEs;

3) the transfer of action requests and results between OSs/MDs and NEs.

6.2.7.2 *Application protocol data units*

The following application protocol data units shall be supported, as detailed in Table 6-8/G.784.

TABLE 6-8/G.784

Application PDU

A-Associate-Request	(AARQ APDU)
A-Associate-Response	(AARE APDU)
A-Release-Request	(RLRQ APDU)
A-Release-Response	(RLRE APDU)
A-Abort	(ABRT APDU)

All mandatory parameters defined in Recommendation X.227 [25] for the above APDUs are mandatory for this Recommendation.

6.2.7.3 *Abstract syntax name*

The ACSE abstract syntax name has the ASN.1 type OBJECT IDENTIFIER. The following value shall be used to identify the ACSE abstract-syntax-definition:

{
joint-iso-ccitt association-control(2)
abstract-syntax(1) apdus(0) version(1)
}

6.2.7.4 *Common management information*

6.2.7.4.1 *Services*

The common management information service element (CMISE) shall be a mandatory service element. The CMISE service description is detailed in ISO 9595 [9], ISO 9595/DAD1 [10] and ISO 9595/DAD2 [11].

Multiple object selection, filter and multiple reply functional units as defined in ISO 9595 [9] are optional. Their use is application dependent. The negotiation during association establishment to use or not use the Functional Units shall be supported.

Support of the extended service functional unit defined in ISO 9595 [9] is not required for conformance to this Recommendation and negotiation shall be supported, at association establishment, for its non-use.

6.2.7.4.2 *Protocol*

Implementations shall support those operations defined in ISO 9596 [12], ISO 9596/DAD1 [13] and ISO 9596/DAD2 [14] that are required by specific applications. All mandatory parameters defined in ISO 9596 [12], ISO 9596/DAD1 [13] and ISO 9596/DAD2 [14] for the required operations are mandatory parameters for this Recommendation.

6.2.7.5 *Remote Operations Service Element (ROSE)*

Network management transaction-oriented applications shall use the following underlying service defined in Recommendation X.219 [26]:

– Remote Operations Service Element (ROSE). The protocol is specified in Recommendation X.229 [27].

The requirement specified above implies association class 3 in ROSE.

7 EEC Interworking

7.1 *Introduction*

Within the TMN architecture (see Recommendation M.30 [29]), the SMS is a type of local communication network (LCN). Communications between an SMS and OS will take place (optionally) over one or more intervening wide-area data communications networks (DCN) and LCNs. Therefore, interworking is necessary between the SMS and either a DCN or another LCN. Interworking may also be necessary between a DCN and an LCN. This section will only specify the interworking between a SMS and DCN.

The regenerator section and multiplex section DCCs will use the seven layer, OSI protocol stack specified in § 6 and includes the connectionless-mode network protocol (CLNP) that is specified in ISO 8473 [1]. For the purpose of this Recommendation, the communications on the DCN between the OS and entry point(s) to the SMS will use an OSI protocol stack that includes the X.25 [28] connection-mode network protocol (CONP) specified in ISO 8208 [15] with ISO IP (ISO 8473 [1]) as an option in the OS.

The OSI architecture describes the view that interworking between sub-networks, such as the SMS and DCN, should take place within the network layer, with the transport and higher layers operating strictly on a peer-to-peer basis between end systems (SNE and OS). ISO 7498 [16] specifies that the network layer will provide the transparent data transfer between transport-entities, i.e. end systems, that is independent of the characteristics, other than quality of service, of different sub-networks. This is identified as the routing and relaying function in the network layer. ISO 8648 [17] specifies the OSI principles of interworking within sublayers of the network layer.

7.2 *Interworking between the SMS and DCN*

Interworking between the SMS's CLNP and the DCN's CONP OSI protocol stacks shall be required. Interworking, at the lower layers, between the SMS's and the DCN's OSI protocol stacks shall be based upon ISO DTR 10172 [18]. The ISO interworking PDTR defines an interworking functional unit (IFU) that will perform relaying and/or conversion of PDUs between networks.

7.3 *Network layer relay overview*

The IFU, operating in the NLR mode, would function as a regular intermediate system and is the only OSI compliant method of interworking between end systems with different OSI network protocols. As specified in ISO 7498 [16] and ISO 8648 [17], interworking is a network layer function. ISO 8473 [1] specifies the CLNP and describes an SNDCF that specifies the rules for operating the CLNP over a X.25 [28] packet switched network (PSN).

The NLR could provide interworking between the SMN and the DCN if both the SMN and DCN operated the ISO 8473 [1] CLNP and utilized TP class 4 (TP4) connections. The top-level SMS SNE – DCN OS network service would then be connectionless, with the X.25 [28] PSN providing an underlying CONP from the IFU to the OS via the DCN. The IFU would examine the destination address of network PDUs (NPDU) received from the SMN and then transfer those CLNP NPDUs (from the SMS) to an appropriate X.25 [28] switched virtual circuit (SVC) on the DCN.

8 Operations interfaces

8.1 *Q- interface*

For interconnection with the TMN, the SMS will communicate through a Q-interface having a protocol suite, B1, B2 or B3 as defined in Recommendation G.773 [30]. The selection of which of the three protocol suites to adopt is a network provider's decision.

8.2 *F-interface*

For further study.

ANNEX A

(to Recommendation G.784)

Support object, attributes and messages[1)]

A.1 *ECC*

For further study.

A.2 *Alarms*

A.2.1 *SDH alarm indications*

Table A-1/G.784 contains a summary of alarm indications required to be available for reporting, if enabled. This information is derived from the anomalies and defects tables in Recommendation G.783.

A.3 *Performance monitoring*

A.3.1 *SDH data collection*

Required (R) primitives and parameters are given in Tables A-2/G.784 and A-3/G.784 respectively. Other parameters are indicated as optional (O).

A.3.2 *SDH performance monitoring history*

SDH history requirements are given in Table A-4/G.784.

A.3.3 *SDH thresholding*

SDH thresholding requirements are given in Table A-5/G.784.

The minimum range for SDH performance thresholds is specified in Table A-6/G.784. Except for bit error ratios (related to CV counts), these ranges are independent of the SDH signal, and for completeness are shown for both required and optional parameters.

Parameter counts shall be inhibited under unavailable and alarm conditions as detailed in Table A-7/G.784.

A.4 *Protection switching control*

For further study

A.5 *Configuration*

For further study.

A.6 *Security*

For further study.

A.7 *Testing*

For further study.

---

1) Detailed message sets are for further study.

A.8 *External events*

For further study.

A.9 *Software download*

For further study.

A.10 *Remote login*

For further study.

A.11 *Detailed network model*

For further study.

TABLE A-1/G.784

Required SDH alarm indications

Events/Conditions		SDH				
		RSect	MSect	Path		Other
				HVC	LVC	
Failures	TF	R				
	LOS	R				
	LOF	R			R+	
	E-BER		O			
	SD		R			
	LOP		R	R		
	FERF		R	R	R	
	MIS			O	O	
	LOM			R#		
	LOT					R
	TIF					O
	AIS		R	R		
Protection Switching	PS		R*			

R Required to be reportable
O Optional

Abbreviations

TF Transmit fail
SD Signal degrade
E-BER Excessive bit error ratio
LOM Loss-of-multiframe
LOT Loss-of-tributary
AIS Alarm indication signal
RSect Regenerator section
MIS Mismatch path trace Id/signal label
HVC High order virtual container (VC-3/4)
LVC Low order virtual containerr (VC-1/2/3)
LOS Loss-of-signal
LOF Loss-of-frame
LOP Loss-of-pointer
FERF Far-end receive failure
TIF Timing input fail
PS Protection switching
MSect Multiplex section
* Required if protection switch equipped
\+ For byte synchronous mappings only
\# Only required for payloads that require the multiframe indication

TABLE A-2/G.784

Required SDH performance primitives

Impairment events	Performance primitives	SDH			
				Path	
		RSect	MSect	HVC	LVC
Errors	BIP FEBE	A	R	R O*	R O*
Frame synch	OOF	R			
Clock synch	PJ#				

R Required
O Optional
A Application specific (i.e. not required in the case of no intermediate regenerators)

Abbreviations

BIP Bit interleaved parity (coding violation)
FEBE Far-end block error
OOF Out-of-frame
PJ Pointer justification
For further study
* Required for monitoring the far end when the far end is managed by a different network manager/operator than the near end.

TABLE A-3/G.784

Required SDH performance parameters

Impairment events	Performance parameters	SDH			
		RSect	MSect	Path HVC	Path LVC
Errors	CV	A	R	A	A
	ES	A	R	A	A
	SES	O	R	A	A
Frame synch	OFS	O			
Clock synch	PJC#				
Failure (as per Table A-1)	UAS+	O	O	O	O
Protection switching	PSC		R*		
	PSD		O		

R Required
O Optional
A Application specific

Abbreviations

CV Code violation (generic term for error count)
ES Errored second
SES Severely errored second
PJC Pointer justification count
UAS UnAvailable second
PSC Protection switching count
PSD Protection switching duration
OFS Out-of frame second
\# For further study
* Required if protection switch equipped
\+ The precise definition of UnAvailable second, in the context of lower and higher order paths, is under study in CCITT SG XVIII.

Note – Further study is necessary in order to determine the appropriate status for the performance parameters that are application specific.

TABLE A-4/G.784

History requirements for SDH signals

Parameter		Current 15 min	Current Day	Previous 15 min	Previous Day	Recent 15 min	Recent Day
RSect	CV	1	1	1	1		
	ES	1	1	1	1		
	OFS	1	1	1	1		
MSect	CV	1	1	1	1		
	ES	1	1	1	1		
	SES	1	1	1	1		
	PSC*	1	1	1	1	(Note 2)	(Note 3)
Path-HCV	CV	1	1	1	1		
	ES	1	1	1	1		
	SES	1	1	1	1		
Path-LCV	CV	1	1	1	1		
	ES	1	1	1	1		
	SES	1	1	1	1		

* Required if protection switch is equipped.

Note 1 – The numbers in the table represent individual 15-minute and daily counts.

Note 2 – It has been proposed that either 31 or 95 registers be provided.

Note 3 – It has been proposed that these registers are optional.

TABLE A-5/G.784

Thresholding requirements for SDH signals

Parameter		Threshold setting capability 15 min	Threshold setting capability Day
RSect	CV	R	R
	ES	R	R
	OFS	R	R
MSect	CV	R	R
	ES	R	R
	SES	R	R
Path-HVC	CV	R	R
	ES	R	R
	SES	R	R
Path-LVC	CV	R	R
	ES	R	R
	SES	R	R

R Required

TABLE A-6/G.784

Minimum threshold ranges (for all SDH signals – provisional values)

Parameter	per 15-min	per day
CV (STM-1)	1-13997	1-1343693
(VC-11)	1-150	1-14377
(VC-12)	1-202	1-19354
(VC-2)	1-617	1-59167
(VC-3)	1-4407	1-423015
(VC-4)	1-13531	1-1298903
ES	1-900	1-65535
SES, OFS, UAS	1-255 each	1-4095 each

Note 1 – The 15-min and day ranges for the ES parameter correspond to < 100% and < 76% of seconds respectively.

Note 2 – The 15-min and day ranges for all other 1 second based parameters correspond to < 28% and < 4.7% of seconds, respectively.

Note 3 – The ranges given for CV are consistent with resolving error ratios better than 10^{-7}, assuming a random error distribution. The upper values for the ranges given for CV of an STM-1 signal should be multiplied by N for an STM-N signal.

TABLE A-7/G.784

SDH monitoring during unavailable time and fault conditions

Monitored parameter		Unavailable time and fault conditions in											
		RSect			MSect			HVC path			LVC path		
		UAT*	LOS	LOF	UAT	SIA	LOP#	UAT	AIS	LOP+	UAT	IAS	
RSect	CV		I	I	M	M	M	M	M	M	M	M	
	ES		I	I	M	M	M	M	M	M	M	M	
	SES		I	I	M	M	M	M	M	M	M	M	
	OFS		I	I	M	M	M	M	M	M	M	M	
	UAS		M	M	M	M	M	M	M	M	M	M	
MSect	CV		I	I	I	I	M	M	M	M	M	M	
	ES		I	I	I	I	M	M	M	M	M	M	
	SES		I	I	I	I	M	M	M	M	M	M	
	PJC*												
	PSC		I	M	M	M	M	M	M	M	M	M	
	PSD		I	M	M	M	M	M	M	M	M	M	
	UAS		M	M	M	M	M	M	M	M	M	M	
HVC path	CV		I	I	I	I	M	I	I	M	M	M	
	ES		I	I	I	I	M	I	I	M	M	M	
	SES		I	I	I	I	M	I	I	M	M	M	
	PJC*												
	UAS		M	M	M	M	M	M	M	M	M	M	
LVC path	CV		I	I	I	I	I	I	I	I	I	I	
	ES		I	I	I	I	I	I	I	I	I	I	
	SES		I	I	I	I	I	I	I	I	I	I	
	UAS		M	M	M	M	M	M	M	M	M	M	

I Inhibit parameter count
M Monitor parameter count
* For further study
\# LOP affects HVC paths but the pointers are located in the MSection overhead
\+ LOP affects LVC path but the pointers are located in the HVC path.

General note – In interpreting the table, unavailable and fault conditions for lower rate signals do not affect the monitoring of higher rate signals, and the higher rate signals can therefore continue to be monitored in a normal manner. For example, MSect, HVC path unavailable and fault conditions do not affect RSect monitoring, so that RSect monitoring can continue as shown in the table.

ANNEX B

(to Recommendation G.784)

Network layer protocol procedures

If it is felt that the administrative procedures for manually inputting routing information is burdensome or no routing information is available, another procedure may be used. This procedure, called broadcast routing, consists of the forwarding of the network protocol data units to all underlying services except the service from which it may have been received.

The ISO IP protocol (ISO 8473) [1], requires an error message be created when an NPDU is received with an unknown address. The error reporting flag may be set to inhibit error messages. However, this procedure inhibits all error messages and not just routing error messages. It may be utilized, with the loss of some maintenance functionality, at the discretion of the user.

ANNEX C

(to Recommendation G.784)

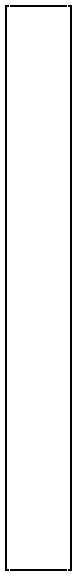
A mechanism to eliminate routing control administration in the SMS

A layer 2 multicast function and a media access (MA) sublayer are introduced to eliminate the need for intermediate system functionality at branch points in the SMS. Thus, any SMS, no matter how complex the topology, will consist of one intermediate system (the GNE) and a number of end systems.

C.1 *Data link layer protocol description*

The main purpose of the data link layer is to provide a broadcast service with address filtering, to the network layer. It must achieve this using the underlying SDH DCC network, which is made up from a series of physical point to point links. The data link layer is made up from two sublayers, one controlling logical links and one dealing with media access (see Figure C-1/G.784).

FIGURE C-1/G.784



C.1.1 *Logical link control (LLC) sublayer description*

Since the network layer assumes an underlying connectionless mode sub-network, ISO 8802 class 1 logical link control shall be used. This protocol needs 3 octets at the start of the LLC PDU:

Octet	Field
1	Destination service Access Point (DSAP)
2	Source Service Access Point (SSAP)
3	Control (CNTL) field
4-N	LLC information field

These octets are carried in the media access sublayer information field.

C.1.2 *Media access sublayer description*

The description of the media access (MA) sublayer covers three areas, the general operation, the format of various fields and the bit oriented frame structure. The sublayer is based on a combination of the IEEE 802.3 MAC services plus part of the frame structure and the Recommendation Q.921 HDLC frame structure.

The service this sublayer provides is to transfer LLC PDUs from one LLC sublayer entity to a peer LLC sublayer entity, by transporting the LLC PDUs across a physical sub-network, which is made up from SDH NEs connected by point to point SDH DCCs.

The sublayer uses HDLC framing and the octets shown below are carried in the HDLC frame information field:

Octet	Field
1-6	Destination address (DA)
7-12	Source address (SA)
13-14	Length (Len)
15-N	MA information field

DA MA address of the NE for which the PDU is intended.
SA MA address of the NE that originated the PDU
Len Length in octets of LLC PDU, which is carried in the MA information field.

The provision of the NE address is a local matter, but it shall be assigned to a NE prior to initialization.

The operation of the sublayer is a combination of address filtering and frame relay. When an MA frame is received at an SDH NE, the following basic algorithm is applied. If the MA destination address (DA) of the received frame matches the MA address of the NE or it is a group address, the HDLC information field is passed to the logical link sublayer. If the MA destination address (DA) of the received frame does not match the MA address of the NE or it is a group address, the frame is sent out on all DCC physical ports, except the one it was received on.

C.1.3 *HDLC description*

The purpose of the HDLC frame is to provide a bit structure that can be transmitted to and received from the SDH DCC physical line. It also provides for the removal of corrupted frames using the cyclic redundancy check. Since the frequency of errors on an optical line is so low, it is not efficient to perform retransmission of lost frames at this layer.

The HDLC frame described in Recommendation Q.921, § 2 shall be used. However, the address (Recommendation Q.921, § 2.3) and control (Recommendation Q.921, § 2.4) fields shall not be used, because they are redundant. Present hardware will be able to operate with this partial use of HDLC.

The fields shall be defined as follows:

Octet	Field
1	Flag
2-(N-3)	HDLC information field
(N-2)	CRC
(N-1)	CRC
N	Flag

The HDLC information field length must be at least 529 octets (512 + 3 + 14); 512 octets for the NPDU, 3 octets for LLC 1 and 14 octets for the MA address.

Two further options in the use of HDLC are outlined in the section entitled “HDLC options”.

C.2 *Physical layer description*

The physical layer consists of a point to point connection, between SDH network elements, where it is terminated. The data link PDUs are carried in the octets (D1 to D3 or D4 to D12) of the SDH DCC, which form two clear channels. There is no physical layer signalling protocol associated with this layer.

ANNEX D

(to Recommendation G.784)

Object model overview

An information model provides a structured means of describing a portion of the real world that is of interest. Information models use a formal notation and vocabulary for organizing, classifying, and abstracting items. Information is identified in terms of objects. Detailed characteristics of each object are described in terms of attributes and behaviour. Objects with similar properties may be grouped into object classes. Additionally, associations between object instances may be described by relationships.

A telecommunications information model provides a means of describing those items used to provide telecommunications services. Such an information model, applicable to all telecommunications networks, is essential for the consistent management of different types of telecommunications networks. The SDH information model is a subset of the telecommunications network information model.

The SDH information model will allow a manager to obtain the following from an agent regarding those entities for which it is responsible:

a) object classes and instances (what the entities are);

b) attributes and methods (what they know and how they behave);

c) relationships (what they are related to and how they relate).

Criteria for evaluating the SDH information model include:

1) Satisfactory management of the transport reference configurations, a subset of which is given in Figure D-1/G.784 below. Test cases are for further study. These test cases should minimally address the network-wide management of paths, as well as the management of equipment.

2) Unambiguous inter-vendor communications, when the reference configurations are provided by equipment from different vendors.

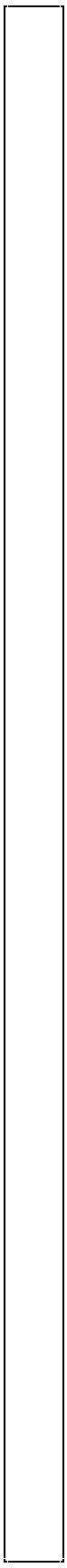
3) Unambiguous inter-operator communications when the reference configurations cross one or more inter-operator boundaries.

4) Ability to generate a unique mapping of the information model to the functional reference model described in Recommendations G.782 and G.783.

5) Ability to manage the reference configurations in the context of a large network which has many network elements and crosses multi-operator boundaries.

6) Controlled mechanism for extending the information model within the procedures of CCITT.

FIGURE D-1/G.784



References

[1] ISO 8473 – *Information processing systems – Data communications – Protocol for providing the connectionless-mode network service*, 1988.

[2] ISO 8473/AD3 – *Information processing systems – Data communications – Protocol for providing the connectionless-mode network service – Addendum 3: Provision of the underlying service assumed by ISO 8473 over point-to-point sub-networks which provide the OSI data link service*, 1988.

[3] ISO 8348/AD1 – *Information processing systems – Data communications – Network service definition – Addendum 1: Connectionless-mode transmission*, 1987.

[4] ISO 9542 – *Information processing systems – End system to intermediate system routing exchange protocol for use in conjunction with ISO 8473*, 1988.

[5] ISO 8348/AD2 – *Information processing systems* – Data *communications-Network – service definition – Addendum 2: Covering network layer addressing*, 1988.

[6] ISO/IEC 8073 – *Information processing systems – Open systems interconnection – Connection oriented transport protocol specification*, 1988.

[7] ISO/IEC 8073/AD2 – *Information processing systems – Open systems interconnection – Connection oriented transport protocol specification – Addendum 2: Operation of class 4 over connectionless network service, 1989.*

[8] ISO/IEC 9545 – *Information processing systems – Open systems interconnection – Application layer structure (ALS)*, 1989.

[9] ISO 9595 – *Information processing systems – open systems interconnection – Common management information service definition (CMIS)*, 1990.

[10] ISO 9595/DAD1 – *Information processing systems – Open systems interconnection – Common management information service element definition (CMIS), CANCEL-GET.*

[11] ISO 9595/DAD2 – *Information processing systems – Open systems interconnection – Common management information service definition, REMOVE.*

[12] ISO 9596 – *Information processing systems – Open systems interconnection – Common management information protocol specification (CMIP)*, 1990.

[13] ISO 9596/DAD1 – *Information processing systems – Open systems interconnection – Common management information protocol specification, CANCEL-GET.*

[14] ISO 9596/DAD2 – *Information processing systems – Open systems interconnection – Common management information protocol specification, REMOVE.*

[15] ISO 8208 – *Information processing systems – X.25 packet level protocol for data terminal equipment,* 1987.

[16] ISO 7498 – *Information processing systems – Open systems interconnection – Basic Reference model,* 1984.

[17] ISO 8648 – *Information processing systems – Open systems interconnection – Internal organization of the Network Layer*, 1988.

[18] ISO DTR 10172 – *Information processing systems – Data communication network transport protocol interworking specification.*

[19] CCITT Recommendation – *Session service definition for open systems interconnection (OSI) for CCITT applications*, Vol. VIII, Rec. X.215 (ISO 8326, 1987).

[20] CCITT Recommendation – *Session protocol specification for open systems interconnection (OSI) for CCITT applications ,* Vol. VIII, Rec. X.225 (ISO 8327 – 8327/AD1 – 8327/AD3, 1988).

[21] CCITT Recommendation – *Presentation service definition for open systems interconnection (OSI) for CCITT applications*, Vol. VIII, Rec. X.216 (ISO 8822, 1987).

[22] CCITT Recommendation – *Presentation protocol definition for open systems interconnection (OSI) for CCITT applications*, Vol. VIII, Rec. X.226 (ISO 8823, 1988).

[23] CCITT Recommendation – *Specification of basic encoding rules for abstract syntax notation one (ASN.1)*, Vol. VIII, Rec. X.209 (ISO 8825, 1987).

[24] CCITT Recommendation – *Association control service definition for open systems interconnection (OSI) for CCITT applications*, Vol. VIII, Rec. X.217.

[25] CCITT Recommendation – *Association control protocol definition for open systems interconnection (OSI) for CCITT applications*, Vol. VIII, Rec. X.227 (ISO IS 8650, 1988).

[26] CCITT Recommendation – *Remote operations: Model, notation and service definition*, Vol. VIII, Rec. X.219 (ISO 9072-1, 1988).

[27] CCITT Recommendation – *Remote operations: Protocol specification*, Vol. VIII, Rec. X.229.

[28] CCITT Recommendation – *Interface between data terminal equipment (DTE) and data circuit terminating equipment (DCE) for terminating operating in the packet mode and connected to public data networks by dedicated circuit*, Vol. VIII, Rec. X.25 (ISO 8208, 1984 and ISO 7776, 1986).

[29] CCITT Recommendation – *Principles for a telecommunications management network (TMN)*, Vol. IV, Rec. M.30.

[30] CCITT Recommendation – *Protocol suites for Q-interfaces for management of transmission equipment*, Vol. III, Rec. G.773.

[31] CCITT Recommendation – *ISDN User-network interface – Data link layer – General*, Vol. VI, Rec. Q.920.

[32] CCITT Recommendation – *ISDN User-network interface – Data link layer – Specification*, Vol. VI, Rec. Q.921.

INTERNATIONAL TELECOMMUNICATION UNION

CCITT G.784

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

GENERAL ASPECTS OF DIGITAL TRANSMISSION SYSTEMS; TERMINAL EQUIPMENTS

SYNCHRONOUS DIGITAL HIERARCHY (SDH) MANAGEMENT

Recommendation G.784

Geneva, 1990

FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation G.784 was prepared by Study Group XV and was approved under the Resolution No. 2 procedure on the 14 of December 1990.

CCITT NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

© ITU 1990

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.