62

REQUIREMENTS AND PERFORMANCE OF PACKET SWITCHING NETWORKS WITH SPECIAL REFERENCE TO TELECONTROL

Working Group 03

of

Study Committee 35

(Communication and Telecontrol)

August 1991

REQUIREMENTS AND PERFORMANCE OF PACKET SWITCHING NETWORKS WITH SPECIAL REFERENCE TO TELECONTROL

Working Group 03
of
Study Committee 35 (Communication and Telecontrol)

August 1991

REQUIREMENTS AND PERFORMANCE OF PACKET SWITCHING NETWORKS WITH SPECIAL REFERENCE TO TELECONTROL

by
Study Committee 35
Working Group 03

INDEX

LIST OF TABLES

LIST OF FIGURES

1.FOREWORD AND SCOPE

Power Utilities are already using Packet Switching Networks (PSN) as data networks for carrying Telecontrol and Energy Management System (EMS) traffic and there is clearly a general interest in this kind of network [1,2,3].

Since there are no requirements yet set for the use of Packet Switching Networks in Telecontrol, this Report is a study that attempts to give a broad view of Packet Switching alternatives, aimed to gain insight into the characteristics of this type of technology which are relevant to Telecontrol.

In this direction an effort has been made to collect data about the target requirements used by different types of Packet Switching Networks and about the performance really obtained by them. The figures given are aimed to help the engineer to write specifications for PSNs and improve his knowledge on this technology. It is also to guide the possible action of standardization bodies on the subject.

The report concentrates only on Packet Switching, its performance and its requirements, to be used in data applications for Telecontrol with low to mean transmission requirements.

These requirements are those that can be handled with, let's say, the classical approach to Packet Switching, which is based on computers as switching elements.

This means that the Report is not dealing with Broadband-Integrated Services Digital Network (ISDN) or future advanced Packet Switching technologies.

Also outside the scope of the Report is the comparison with ISDN or any other networking alternative as well as the study of costs and transmission techniques.

2.INTRODUCTION TO PACKET SWITCHING NETWORKS (PSN)

A Packet Switching Network is a data transmission network with computerized nodes where messages entering the network are split in data packets (small messages with a maximum length limitation) which later are reassembled when leaving the network. These packets are adequately routed through the network by hopping between pairs of neighbour nodes, where they are stored.

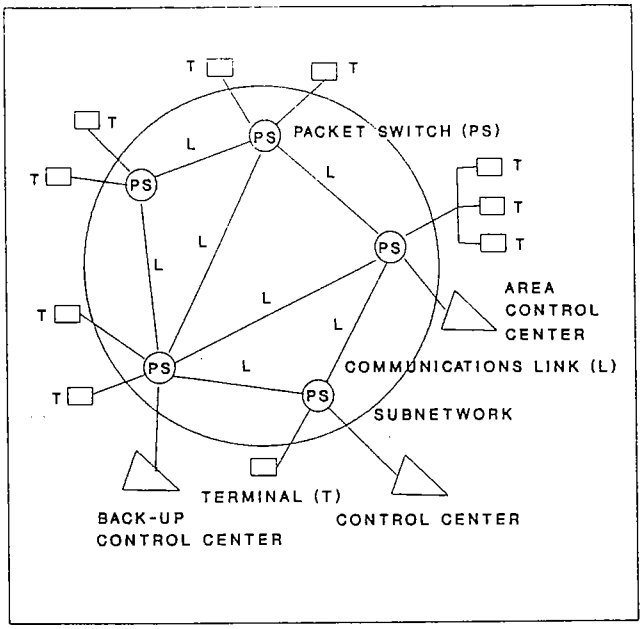
Basically this technique permits dynamic sharing of transmission resources among users since one packet occupies one link only for a short duration in the range of milli-seconds.

Packets meant for different destinations follow one another on links. The receiving computers or Packet Switches (PS) store them in their local memory, examine their addresses and send them on to other PSs when possible, until they reach the destination where they are sent to the appropiate computer, Control Center or RTU (Remote Terminal Unit).

This mode of communication keeps all network circuits in the common domain and, as a result, ensures that they have a high utilization and are available to any user (RTU or Control Center) requesting them. Each RTU uses a set of circuits only for a fraction of the time.

A typical PSN is represented in figure I. It is formed by communication links, packet switching nodes and terminals or computers connected to it.

It is clear that the main difference with respect to other more classical approaches to Telecontrol is the appearance of computer based Packet Switches in each of the network



TYPICAL STRUCTURE OF A PACKET SWITCHING NETWORK
Figure I

nodes specialized in performing a series of communications algorithms which give the PSNs their flexibility and avoid or limit the use of classical multiplexing systems.

The technique of Packet -switching achieves the aforementioned advantages at the expense of a higher complexity in the processing, for this reason the technique is specially indicated when the transmission resources are relatively expensive when compared with packet switching equipment.

Although in figure I the network being represented is a meshed one, Packet Switching does not impose any restrictions on topology and so it can be of any structure.

The basic characteristics of this type of network are :

- Sharing of transmission resources. Each Packet Switch acts as a concentrator/deconcentrator. Lines are shared in a kind of statistical TDM system that makes efficient use of transmission resources.

-Capability to manage any topology. PSNs are not restricted to use specific topologies such as ring, star or tree-like networks although the greatest benefit in the use of PSNs is achieved when operating meshed networks.

-Automatic adaptability to changing network conditions such as changes in topology (link or node failures or additions) or changes in traffic patterns and intensities, relieving maintenance personnel from changing the network configuration when work on communication lines has to be done.

-Possible improved network management by the use of a Network Control Center where all the alarms, status and statistics accumulated by the packet switches are received and displayed. It is possible to keep track automatically of the evolution of the network with great detail.

-Full networking capability. Communication between any pair of terminals or computers connected to the network is possible. This feature, already existing in telephone networks, does not usually exist in Telecontrol data networks and, as it will be seen later, it allows new possibilities in the way Electric Systems are operated.

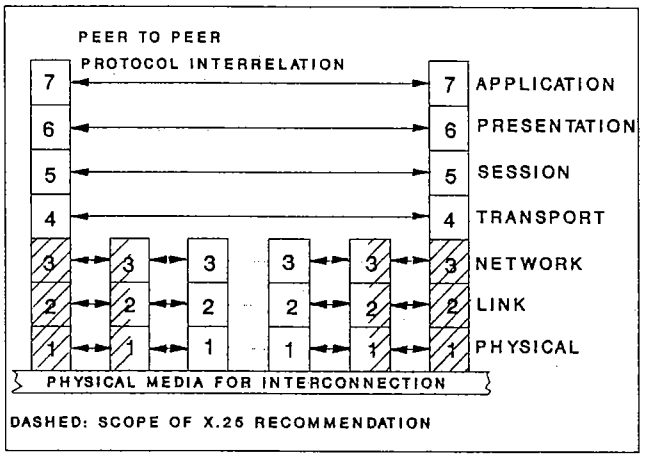
Since in PSNs packets may cross several links and nodes where they are stored before arriving at their destination, the delays will be longer than having a direct link with the same speed and they will be somewhat random. This apparent difficulty is mitigated due to the following two reasons.

Firstly, there is the so called "pipelining effect" by which packets are transmitted at the same time over successive links, thus reducing the Network end-to-end delay that tends to be that over a direct end-to-end link of the same speed for a long file. Secondly, a PSN is shared by many RTUs and thus the internal link speeds are typically much higher than the ones connecting RTUs directly to Control Centers. Similarly if the speed is higher, the problems with the random nature of delays are less important.

3.ARCHITECTURE OF PACKET SWITCHING NETWORKS

3.1.LAYERING AND THE ISO REFERENCE MODEL

In 1979 the ISO produced the first version of its "model of architecture for Open Systems Interconnection", which has been adopted as a reference model for public data network services in several countries and which is also very convenient for any data network [5]. The basic principle of the ISO model is that a communication architecture may be divided into seven layers. These seven layers are named : Physical layer, Link layer, Network layer, Transport layer, Session layer, Presentation layer and Application layer and have been represented in figure II [4].



ISO REFERENCE MODEL (ISO 7498)
Figure II

The ISO layers provide a terminology which is invaluable in allowing discussions about complex protocols, by dividing these protocols into well defined layers with a set of conceptual interfaces. There now follows a brief description of the four lower ISO layers :

The Physical Layer : The physical layer provides mechanical, electrical, functional and procedural characteristics to activate, maintain and de-activate physical connections for bit transmission between data-link-entities. A physical connection may involve intermediate open systems, each relaying bit transmission within the Physical layer. [5]

A typical example of this layer is the V.24 CCITT Recommendation.

The Link layer :
It provides the functional and procedural means to establish maintain and release data-link connections among network entities and to transfer data-link-service-data-units [5]. It also provides the functional and procedural means for connectionless-mode transmission among network entities [44].

The main objective of this layer is to detect, and possibly correct, errors which may occur in the Physical layer.

Line protocols such is ISO HDLC (High-level Data Link Control) belong to the link layer.

The Network Layer :

ISO first defined the network layer for connection oriented systems in [5]. Later it defined the connectionless service for the same layer in an addendum [44]. Because of this there is no unified ISO description on the network layer service. The definitions which are given below are taken directly from [5] and [44] and reflect the aforementioned situation.

The Network Layer provides the means to establish, maintain and terminate network-connections between open systems containing communicating application-entities and the functional and procedural means to exchange network-service-data units between two transport entities over network-connections. [5]

It provides to the transport-entities independence from routing and relay considerations associated with the establishment and operation of a given network-connection. [5]

In the case of connectionless transmission [44] the purpose of the network layer is to provide the functional and procedural means for connectionless mode transmission among transport-entities and therefore provides the transport entities with independence of routing and relay considerations associated with connectionless-mode transmission.

The Network layer includes the Routing and Reachability algorithms that will be introduced in section 3.2. as well as some Flow-Control procedures. It includes also the third layer of X.25 CCITT protocol where procedures to establish, maintain and terminate connections with a public PSN are defined.

This layer is more used in PSNs than in classical Telecontrol systems using dedicated links where it may be embedded in their physical structure and/or in the polling protocol used.

The Transport layer :

The transport layer provides transparent transfer of data between session (fifth layer) entities and relieves them from any concern with the detailed way in which reliable and cost effective transfer of data is achieved. [5]

The Transport Layer optimizes the use of the available network-service to provide the performance required by each session-entity at minimum cost. This optimization is achieved within the constraints imposed by the overall demands of all concurrent session-entities and the overall quality and capacity of the network-service available to the Transport Layer. [5]

All protocols defined in the Transport Layer have end-to-end significance.

The Transport Layer is relieved of any concern with routing and relaying since the network-service provides network-connections from any transport-entity to any other. [5]

In the case of Telecontrol networks, this layer has to provide the overall end-to-end data transmission data integrity required by the Telecontrol application.

3.2. BASIC ALGORITHMS IN PACKET SWITCHING NETWORKS

The basic algorithms performed by the Packet Switches are the following :

-Network Internal Line Protocol which allows recovery from communications line impairments by the use of coding and framing techniques that permit detection of line errors and recovery from them, detection of duplicated and lost packets and synchronization between sender and receiver.

This algorithm belongs to the second ISO layer (Link layer).

-Routing algorithm : Allowing the routing of packets through the network from origin to destination. These algorithms may be completely automatic and self-adaptive in case of changing network conditions, such as line or node failures or changes in traffic pattern.

Routing algorithms identify one or several minimum paths across the network between any pair of nodes and use them to forward packets. Typically, these algorithms work by exchanging routing information between neighbour nodes, although there are many types of routing algorithms.

This algorithm belongs to the third ISO layer (Network layer).

-Reachability or connectivity algorithm permitting identification of failed nodes or partitions in the network. Typically this algorithm is combined with the routing algorithm. The need for this algorithm is clear if it is realized that the network must discard packets going to non existent destinations or prevent their entrance into the network ; This means that the network should know which nodes are connected to it and which are not. This algorithm is also completely automatic. It belongs to the network layer of the OSI Basic Reference model [5].

-Flow Control It is apparent that even with the best possible routing procedure, messages will sometimes encounter congestion and will suffer long delays. This will occur if the network is offered traffic over the limit it can handle and may be due to normal statistical fluctuation in traffic or to unexpected surges at some points in the network. The resulting congestion may cause loss of data or control information, degradation in performance in the form of increased delay, or data arriving out of sequence. The congestion may be taken care of by the use of a hierarchical set of Flow Control techniques that apply to different parts of the network. The aim of these techniques is to stop excess traffic before entering the network by keeping the network operating point at its optimum.

Among the different Flow Control Techniques a widely known one is the windowing technique used often in Line Protocols, End-to-End protocols, Access protocols and Transport protocols. In this technique a window is defined so that the number of packets sent and not yet acknowledged by the receiver cannot exceed the window size.

In the context of telecontrol an important inherent feature of the data is that it can be ranked into priorities. This is very useful in dealing with congestion situations.

3.3.BASIC TYPES OF PACKET SWITCHING NETWORKS.

As will be seen later in this paper there are only standards for Line Protocols and for Access Protocols to Public Data Networks, but there are no standards for routing, connectivity and congestion control, that is to say, networks are not standardized in any way. The standardization effort has been made to normalize the access of terminals to networks, not the networks themselves.

Looking to the existing PSN's today it is possible to distinguish clearly two types of networks based on different phylosophies :

-Connectionless oriented networks : Where each packet is transmitted by a packet-mode data terminal equipment directly to the receiving data terminal equipment on the basis of the address contained in the address field of packet header. In this case the network transports discrete packets only. Different packets belonging to the same message or connection may arrive out of order at their destination as a result of possible alternative routing. If it is necessary to recover from this effect, packets must be reordered when going out of the network.

In network overload conditions or in case of failure, packets may be lost although, of course, they may be recovered on an End-to-End basis.

The advantages of connectionless oriented subnetworks, also called datagram subnetworks, are simplicitiy, flexibility, easiness of implementation, survivability and the natural encryption of messages they provide.

The disadvantages are the mandatory reordering of packets at the destination node if the order of packets must be ensured at the network layer, and the need for an End-to-End network protocol if no loss of packets is allowed. There is also a loss in efficiency due to the need to include the destination address in each packet.

-Connection-oriented networks: where, before exchanging any data, two terminals wishing to communicate must establish a network call and set up a fixed path (Virtual Circuit) through the network. In that case, packets arrive on sequence and should be delivered to the user without loss. This may imply in some networks the use of an End-to-End network protocol to recover from possible loss of data within the network.

The advantages of connection oriented networks are that reordering is simpler and that it is easier to control and to bill the users. Also, there are more chances to control the building of congestion inside the network.

The disadvantages are the increase in complexity, the need to maintain several fixed paths from origin to destination to enhance availability, (otherwise the delay in creating new Virtual Circuits after a failure could be too long), the access and disengagement delays, the waste in network resources that may be assigned to non used connections, the increase in standard deviation of delays, etc.

4.INTRODUCTION TO X.25 [40]

X.25 is a CCITT Recommendation which specifies the access of terminals and computers to Packet Switching Networks. It was first approved by the CCITT in 1976 with many subsequent modifications [40] and additions in each study period (4 years).

Recently the ISO has produced International Standards 7776 and 8208 which are the ISO versions of X.25 link and packet levels respectively. The differences from X.25 are minor [39, 41, 42].

X.25 follows the ISO Open Systems Interconnection Reference model and specifies the three lower layers within the terminal or computer (the DTE (Data Terminal Equipment) in CCITT teminology) connected to the network, as well as the reactions of the latter, though it does not specify the procedures within the network itself.

In figure II is represented the typical OSI layering scheme where the area of scope of X.25 is indicated (dashed area).

The X.25 Recommendation provides access to the following services available to the transport layer:

Service 1: Switched Virtual Circuit (SVC)

Service 2: Permanent Virtual Circuit (PVC)

Service 3: Fast Select

A Virtual Circuit (VC) is a bidirectional, transparent, flow controlled path between a pair of logical or physical ports.

A Switched Virtual Circuit is a temporary association between two processes within two DTEs and is initiated by a DTE Call Request packet.

A Permanent Virtual Circuit is a permanent association between two processes within two DTEs.

A Fast Select is a very short Switched Virtual Circuit consisting of one packet or Call Request packet and one return or acknowledge packet, both of which may contain user data.

In the 1980 version of X.25 there was another service later removed in 1984. This was a network connectionless service called "datagram" (See Appendix I) that could have been relevant for Telecontrol. This service was removed to protect the network from the users since, from the point of view of carriers, packet networks cannot control the rate at which packets could be pumped into the network by users. In a proprietary network both the network and the users belong to the same organization and thus there is no reason for rejecting the high degree of flexibility, simplicity, efficiency and availability provided by datagrams. This service, though removed by the CCITT, is now beig considered by ISO [44].

The physical level of X.25 specifies the use of a duplex, point-to-point synchronous circuits providing a physical transmission path between the DTE and the network. It also specifies the use of the physical interfaces X.21 and X.21bis (equivalent to V.24).

The link level of X.25 specifies the use of a data link control protocol which is compatible with ISO's HDLC (High-level Data Link Control). It is called LAPB (Link Access Procedure-Balanced) and it coincides with the balanced, asynchronous, point-to-point version of HDLC with the reject feature plus a restriction on the use of Information frames as commands only.

The basic phases of a virtual call are: establishment, data transfer and clearing. Permanent virtual circuits are a kind of switched virtual circuit without the establishment and clearing phases. The Fast Select service is a kind of SVC where data transfer is achieved in a establishment/clearing handshake. So, these two services can be considered degenerate cases of the SVC service, that is the one on which we are going to concentrate briefly.

The establishment phase starts when the calling DTE issues a CALL REQUEST packet. This packet when arriving at the called DTE is named INCOMING CALL packet. It ends when the called DTE accepts the call by issuing a CALL ACCEPTED packet, which is named CALL CONNECTED packet when it reaches the calling DTE.

The establishment phase also provides mechanisms for facility negotiations during call set up, for conveying system passwords to the higher layers, for reverse charging, etc.

The called DTE can refuse the INCOMING CALL packet by issuing a CLEAR REQUEST packet which may contain a diagnostic code for signalling the reason for call clearing. When arriving at the calling DTE this packet is called CLEAR INDICATION.

Call clearing, once the call enters the data transfer phase, may be initiated by either DTE or by the network in case of failure, by sending a CLEAR INDICATION packet.

During the data transfer phase user data can be conveyed through the network in two forms. DATA and INTERRUPT

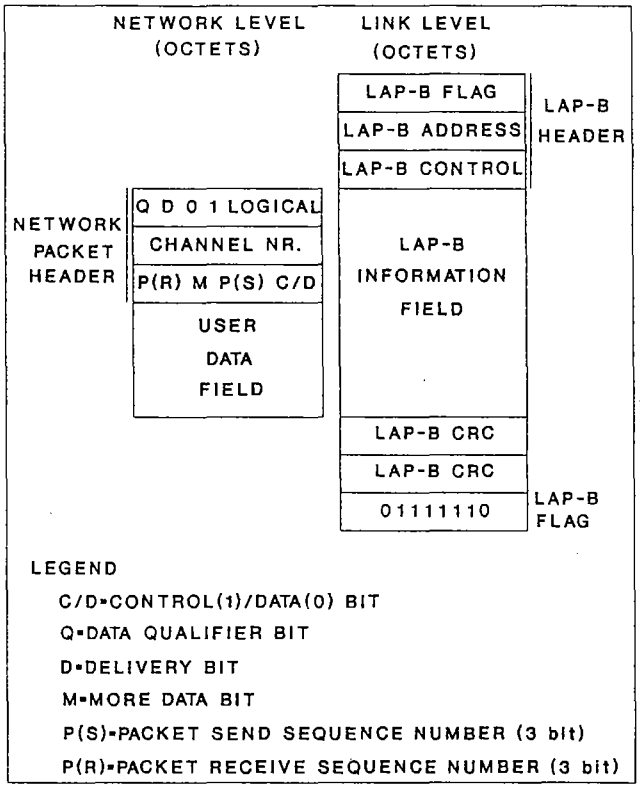


Figure III.- X.25 DATA PACKET FORMAT
(Common to CCITT's 1984 X.25 and ISO 8208)

packets. The DATA packets are a sequence of packets that are sequentially numbered for flow control purposes. They are the normal kind of packets and their general format is indicated in figure III. The sequence numbering is performed in modulo 8 using the Packet Send Sequence Number (P(S)) indicated in figure III. There is a maximum window size, $W \leq 7$, corresponding to the maximum number of sequentially numbered DATA packets that a DTE may be authorized to transmit to the network without a further authorization from it. The default value for window sizes, when no other value is agreed between the DTE and the network, is two.

The DATA packets are acknowledged by a Packet Receive Sequence (P(R)) in a kind of procedure parallel to the one used at level two by the LAPB protocol.

The significance of this numbering/acknowledgment scheme in X.25 has only local meaning across the DTE-network interface.

Nevertheless there is a relevant facility in X.25 which is a bit, the D-bit, in the header of packets that forces the acknowledegments to have DTE to DTE significance. In that case the network confirms the reception of packets by the other end.

The data field of DATA packets may be of any length up to a certain maximum value. Every network will support a maximum value of 128 octets.

INTERRUPT packets are non-numbered packets that may contain one octet of user data and are always delivered at or before the point in the stream of DATA packets at which they were generated. Only one unconfirmed INTERRUPT may be outstanding at a given time. The INTERRUPT packets may be used to convey urgent user data and provide an out-of-band signalling channel on virtual circuits.

A DTE can, in general, establish several virtual circuits with a number of DTEs over a single physical access circuit. Each packet contains a logical channel number which identifies the packet with a virtual circuit. Thus X.25 packet or network level employs a kind of packet-interleaved statistical multiplexing.

After this short description of X.25 it is relevant to focus on error recovery procedures in X.25.

The basic X.25 procedures for error recovery are the following:

Reset Procedure. It reinitializes one Virtual Circuit numbering in case of errors. All DATA and INTERRUPT packets in transit are discarded. A diagnostic field in the reset packet provides information to the DTE about the reason for resetting.

Restart procedure. It is a mechanism provided to recover from major failures. This procedure clears all Switched Virtual Circuits and resets the numbering of all Pemanent Virtual Circuits of a given user/network interface, all packets in transit regarding this interface are discarded.

Error handling in DATA packets. As indicated in figure III, DATA packets across the DTE/network interface are protected by the 16-bit CRC of LAPB link protocol. The protection inside the network may be of a different nature.

Error handling on Establishing/Clearing phases. Procedural errors during call establishment and clearing are reported to the DTE by diagnostic codes in packets.

To recover from errors, X.25 in general uses error tables to help produce several types of diagnostic codes/packets by either the network or the DTE. Also, different time-out procedures are necessary to recover from specific faulty situations.

Another noteworthy aspect of X.25 and, in general, of packet networks is the fact that in these networks the user is responsible for forming packets. The network only handles packets of a certain maximum size. If the user data at the Transport layer is longer than the maximum allowable packet size, the user (the Transport layer) is responsible for the packetization/depacketization process.

5.REQUIREMENTS FOR PACKET SWITCHING NETWORKS

5.1 STANDARDS

The ANSI X3.102 1983 Standard defines user-oriented performance parameters for data communications services and the ANSI X335/135 defines the corresponding measurement methods.

The aim of these two standards is to provide an objective base for comparing performance of alternative services from the users point of view.

The CCITT has issued Recommendation X.140 which specifies user-oriented, network independent Quality of Service parameters somewhat similar to those defined in ANSI X3.102 and with the same scope, but placing special emphasis on user requirements, how to specify them and how to relate them to the performance obtained.

The list of performance parameters defined in CCITT's Recommendation X.140 is as follows:

1.- Delay.
2.- Disengagement delay.
3.- User information transfer delay.
4.- Access denial probability.
5.- Incorrect access probability.
6.- Disengagement denial probability.
7.- User information loss probability.
8.- User information transfer denial probability.
9.- User information misdelivery probability.
10.-Extra user information delivery probability.
11.-Service outage duration.
12.-Service Availability.
13.-User information error probability .
14.-User information transfer rate.

Short definitions based on CCITT's Recommendation X.140 can be found in alphabetical order in Appendix I (Glossary of terms).

			WORKING DAY		BUSY HOUR OF WORKING DAY		BUSY HOUR OF THE YEAR	
			AVG.	90%	AVG.	95%	AVG.	90%
NETWORK TRANSIT DELAY	ACCESS DELAY*				600+500	900+800		
	DISENGAGEMENT DELAY				500	800		
	NETWORK ETE DELAY**				400	600		
ACCESS LINE DELAY (A.L.D.)	SOURCE A.L.D.							
	DESTINATION A.L.D.							
USER INFORMATION TRANSFER DELAY								
NODE TRANSIT DELAY								

* CALL REQUEST + CALL CONFIRMATION DELAY

** NETWORK END-TO-END DATA TRANSFER DELAY

TABLE I.- CCITT's X.135 DELAY OBJECTIVES FOR THE NATIONAL PART (in ms)

Some of the limit values for these parameters are already specified for international connections in CCITT's Recommendations X.135 (delay parameters) (See Table I) and X.136 (blocking parameters). In these Recommendations the contribution of the national parts of origin and destination to the total delay or blocking characteristics is also specified and these are the parts taken into consideration in Table I. An effort has been made to represent all the collected data about delay objectives and measurements of different networks in a unified way. The final outcome of this work has been the structure of Table I that is also used in other tables of this study to represent collected data. The Glossary of terms (Appendix I) and figure X define the concepts in Table I.

X.136 defines the following blocking parameters in connection with the use of X.25. The figures given here also refer to the national parts.

-Call request rejection probability (Access denial probability) due to network congestion: $\leq 3.10^{-3}$.

-Probability of Clear Indication packet reception during any period of 1 s due to network congestion: $\leq 3.10^{-6}$.

-Probability of Reset Indication packet reception during any period of 1 s due to network congestion for both permanent or switched virtual circuits: $\leq 10^{-5}$.

5.2.PUBLIC NETWORKS

The requirements of public Packet Switching Networks are of interest for power utilities from two points of view. Firstly, from the point of view of users of public PSNs and secondly, from the point of view of designers, builders and operators of private general and special purpose PSNs.

As a reference, we have taken two important public networks into consideration, TRANSPAC, the French public PSN, and DATAPAC, the Canadian PSN, both with extensive existing bibliography [15,16,31].
Table II shows TRANSPAC delay objectives and Table III shows the DATAPAC ones.

			WORKING DAY		BUSY HOUR OF WORKING DAY		BUSY HOUR OF THE YEAR	
			AVG.	90%	AVG.	95%	AVG.	90%
NETWORK TRANSIT DELAY	ACCESS DELAY•					1000 + 500		
	DISENGAGEMENT DELAY					700		
	NETWORK ETE DELAY••				150	200		
ACCESS LINE DELAY (A.L.D.)	SOURCE A.L.D.							
	DESTINATION A.L.D.							
USER INFORMATION TRANSFER DELAY								
NODE TRANSIT DELAY								

• CALL REQUEST • CALL CONFIRMATION DELAY

•• NETWORK END-TO-END DATA TRANSFER DELAY

TABLE II.- TRANSPAC DELAY OBJECTIVES (in ms)

In these tables we can see that requirements for access delay in public networks is in the range 650-1500 ms, and that Network End-to-End data transfer delay depends on the loading of the network, being for the busy hour of a working day an average of 150 to 300 ms. The data on delay in 90 or 95% of cases is also interesting.

DATAPAC considers two types of traffic, Priority and Normal. This feature is not common in public networks, although it is clearly very important for Telecontrol. Without these feature, Telecontrol critical functions may not have enough protection against network congestion during busy hours and during faulty network situations.

To exemplify availability design objectives we take the case of the German public PSN DATEX-P [24,25]. It is the requirement of availability of PSN nodes and it is as follows:

			WORKING DAY		BUSY HOUR OF WORKING DAY		BUSY HOUR OF THE YEAR	
			AVG.	90%	AVG.	90%	AVG.	90%
NETWORK TRANSIT DELAY	ACCESS DELAY•	PR.			650			
		N.			800			
	DISENGAGEMENT DELAY	PR.			350			
		N.			500			
	NETWORK ETE DELAY••	PR.	125	160	150	200	175	250
		N.	255	275	300	425	500	825
ACCESS LINE DELAY (A.L.D.)	SOURCE A.L.D.	PR.			97			
		N.			312			
	DESTINATION A.L.D.	PR.			97			
		N.			312			
USER INFORMATION TRANSFER DELAY		PR.			344			
		N.			924			
NODE TRANSIT DELAY		PR. N.						

• CALL REQUEST • CALL CONFIRMATION DELAY

•• NETWORK END-TO-END DATA TRANSFER DELAY

PR• PRIORITY N• NORMAL

TABLE III.- DATAPAC DELAY OBJECTIVES (in ms)

First phase of DATEX-P (until 1986) : 99.95%

Second phase of DATEX-P (after 1986) : 99.997%

In chapter 6.2., measurement data of these networks and others are given.

5.3.MILITARY NETWORKS.

Military networks, due to their need of stringent requirements on data integrity, service availability, as well as other features, are of special interest for Telecontrol. Early Packet switching development was significantly stimulated by the U.S. military sponsored academic research carried out in the ARPA network.

This network served as a test bed of ideas which later were to be applied in other military networks as well as in civil networks.

Among the breed of military networks based on ARPA network technology there is the AUTODIN network, which has two versions, the old, or AUTODIN I, and the new (after 1980), or AUTODIN II:

Some of the targeted features in the design of the latter network are as follow [22,27]:

-End-to-End undetected bit error rate of under 1×10^{-12} (Calculated worst case: 12.10^{-14}).
-User information (containing a maximum of 584 eight -bit characters) misdelivery probability of under 1×10^{-11}.
-Maximum Network end-to-end data transfer delay (99%) of 300 ms for highest precedence, 600- bit packets and 630 ms for low priority packets.
-Traffic priorities.
-Maximum packet size of approximately 5300 bits.
-Average delay of low priority packets : 200 ms.
-Access speeds : 110 bps to 56 Kbps.
-Trunk speeds : 9.6 Kps to 56 Kbps.
-Effective user information transfer rate : 76% of the slower access line in each connection pair (measurement).
-Service availability:
-Of single homed pairs of users: 99%
-Of dual-homed users: 99.95%

5.4.TELECONTROL NETWORKS

Although Packet Switched Networks have been used for telecontrol for more than a decade [1,2,3], there are no internationally agreed specific requirements yet set for Packet Switching Networks used for Telecontrol.

Nevertheless, the existing End-to-End requirements for Telecontrol services using other ways to communicate, should be maintained when using PSNs.

Existing requirements for Telecontrol services are as follows:

Integrity requirements.

IEC TC57 [10] defines three Integrity classes.

Class I1 is for cyclic updating systems and specifies a Residual Error Probability of 10E-6 for a Bit Error Rate of 10E-4 together with a slope of two.

Class I2 is for event initiated transmission procedures and specifies a Residual Error Probability of 10E-10 for a Bit Error Rate of 10E-4 together with a slope of four.

Class I3 is for critical information transmission functions such are telecommands and specifies a Residual Error Probability of 10E-14 for a Bit Error Rate of 10E-4 together with a slope of four.

In figure IV there is a representation of IEC integrity requirements.

ANSI-C37.1 [9] defines the following U.S. standard for data integrity in Telecontrol Systems: "Error control in concert with the communication protocol and line discipline should ensure that the probability of undetected bit errors is no greater than 10E-10 when the channel is operating within the limits of $\leq$ 1 bit error in 10E+4 bits".

This coincides with IEC Class I2 except for the slope, which is not specified in ANSI-C37.1.

Dependability (missing command probability) and Security (unwanted command probability) are measures of data integrity for the Teleprotection service. The requirements for this service can be found in [38] and other related IEC publications.

Availability requirements.

The CIGRE's "Guide for planning of Power Systems Telecommunication Networks" [37] defines the following three availability classes for telecommunication links linking RTUs to Control Centers.

Class A. Availability figure: 99.9%. It includes power stations interconnecting countries, critical nodes in the 200 kV, 400 kV and above grid and LFC stations.

Class B. Availability figure: 99%. It applies to non critical nodes in the 200 kV and 400 kV grid and to nodes of lower voltages.

Critical communication class. Availability figure: 99.99%. It applies to critical communication nodes affecting many RTUs.

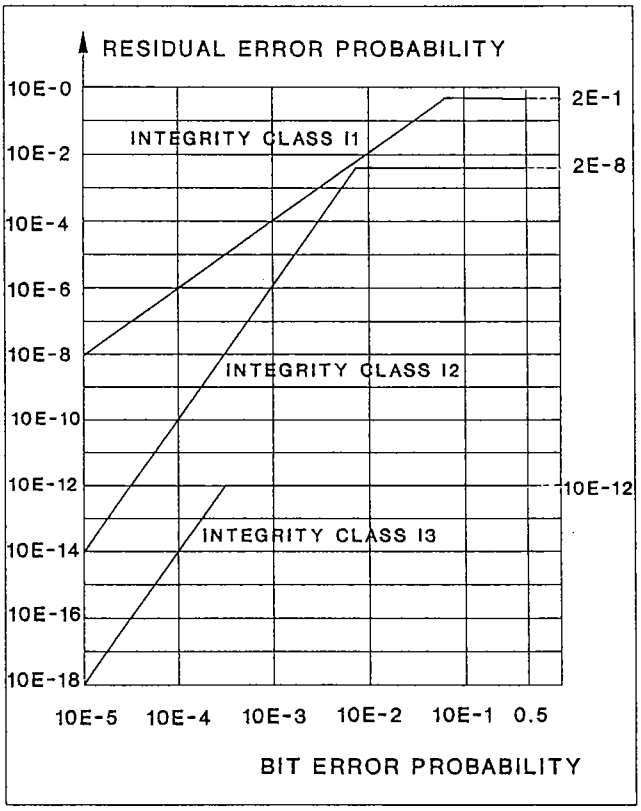
Delay requirements.

In the performance requirements defined by IEC in [21], overall transfer times are not mentioned. Nevertheless there are proposals to include figures relating to transfer times in the document.

There are several mentions of the range of transfer times in some CIGRE works [36].

All the mentions and proposals for transfer delays agree in that the range should be from "a few seconds to less than one second", probably depending on the type of service.

With respect to Teleprotection, transfer times are well established by IEC [38] and are in the range 15 to 60 ms. Unfortunately, it is difficult for current PSNs to support this service.



IEC DATA INTEGRITY CLASSES
Figure IV

6.PERFORMANCE MEASUREMENTS OF PSNs

6.1.RESEARCH NETWORKS

Based on the ANSI X3.102 standard an experiment was conducted to assess the data communications performance provided to a pair of Arpanet end users (host computer application programs).

The results of these measurements on the Arpanet Packet Switching Network may be found in table IV [33] and may be relevant to Telecontrol PSNs. The terminology in the

table has been adapted to that in CCITT's X.140, as in the rest of the paper.
The measurements showed that transmission errors were extremely rare in Arpanet and that the loss of user data in transit through the network was relatively common. The latter, which is the major Arpanet measured imperfection, appears to be caused mainly by hardware and software failures and by the delays in the network.

This behaviour measured in the ARPANET may be considered common to many PSNs.

Access delay (1.8 s) may be also considered typical of many PSNs.

PRIMARY PARAMETERS	
1. ACCESS DELAY	1.8 s
2. ACCESS DENIAL PROBABILITY	6•10E-3
3. ACCESS OUTAGE PROBABILITY	2.6•10E-3
4. USER INFORMATION LOSS PROBABILITY	6•10E-3
5. USER INFORMATION TRANSFER DELAY	
512-bit BLOCKS	262 ms
4096-bit BLOCKS	709 ms
6. USER INFORMATION TRANSFER RATE	4872 bit/s
7. DISENGAGEMENT DELAY	
ORIGINATOR	12 ms
NONORIGINATOR	2.5 s
8 DISENGAGEMENT DENIAL PROBABILITY	
ORIGINATOR	1.3•10E-2
NONORIGINATOR	0
9. USER INFORMATION TRANSFER DENIAL PROBABILITY	4.7•10E-2
ANCILLARY PARAMETERS	
10. USER FRACTION OF ACCESS DELAY	0.15
11. USER FRACTION OF BLOCK TRANSFER TIME	0.13
12. USER FRACTION OF SAMPLE I/O TIME	0.13
13. USER FRACTION OF DISENGAGEMENT DELAY	
ORIGINATOR	0
NONORIGINATOR	0.13

TABLE IV. SUMMARY OF ANSI X3.102 PERFORMANCE PARAMETER MEASUREMENTS FOR SELECTED ARPANET USERS.

6.2.PUBLIC NETWORKS

In chapter 5.2. the design objectives for public PSNs were introduced. Here measurement data of some public networks are presented . These data tell what can be reasonably achieved by the use of public networks and, in general, by the use of PSNs.

The work concentrates basically on two public networks. TRANSPAC, the French public PSN and DATEX-P, the German public PSN. Other networks will also be considered at a lesser extent.

In table V there have been summarized several measurements made in 1983 on TRANSPAC network [31]. Access delays are around 200 ms and network end-to-end delays (measured using 128-byte packets) under 100 ms. The node transit delay lasts an average of 6.6 ms.

In papers [24,25] there are extremely interesting measurement data on delay and user information transfer rate (throughput) in DATEX-P. Delay measurements can be found in table VI and throughput measurements in table VII. Access delays are around 0.5 seconds and network end-to-end delays around 150 ms on average. The throughput measurements in table VII [24,25] show the dependence of throughput on several parameters such are number of hops, number of virtual circuits sharing the access link, window sizes, setting of the X.25 D-bit to 1, etc.

		NR. OF HOPS	WORKING DAY		BUSY HOUR OF WORKING DAY		BUSY HOUR OF THE YEAR	
			AVG.	90%	AVG.	95%	AVG.	90%
NETWORK	ACCESS DELAY•	1,2			128	174'7		
		3			220	284		
TRANSIT DELAY	DISENGAGEMENT DELAY	1,2			15	20		
		3			15	20		
	NETWORK ETE DELAY••	1,2			50	60		
		3			87	100		
ACCESS LINE DELAY (A.L.D.)	SOURCE A.L.D.							
	DESTINATION A.L.D.							
USER INFORMATION TRANSFER DELAY								
NODE TRANSIT DELAY					6'6	8		

• CALL REQUEST • CALL CONFIRMATION DELAY

•• NETWORK END-TO-END DATA TRANSFER DELAY

TABLE V.- TRANSPAC MEASUREMENTS

		NR. OF HOPS	WORKING DAY		BUSY HOUR OF WORKING DAY		BUSY HOUR OF THE YEAR	
			AVG.	95%	AVG.	95%	AVG.	90%
NETWORK	ACCESS DELAY•	1	385	406				
		2	426	495				
		3	457	506				
		4	524	578				
TRANSIT DELAY	DISENGAGEMENT DELAY		108	<141				
	NETWORK ETE DELAY••							
ACCESS LINE DELAY (A.L.D.)	SOURCE A.L.D.							
	DESTINATION A.L.D.							
USER INFORMATION TRANSFER DELAY		1	122	140				
		2	139	170				
		3	179	214				
		4	191	225				
NODE TRANSIT DELAY								

• CALL REQUEST • CALL CONFIRMATION DELAY

•• NETWORK END-TO-END DATA TRANSFER DELAY

TABLE VI.- DATEX-P DELAY MEASUREMENTS (in ms) 24,25

NUMBER OF HOPS	NUMBER OF ACTIVE VCs	THROUGHPUT PER VC (pps)
1	1	4.12
	2	3.92
	3	2.80
2	1	3.79
	2	3.62
	3	2.78
3	1	3.42
	2	3.36
	3	2.78
4	1	3.30
	2	3.23
	3	2.81
5	1	3.12
	2	3.07
	3	2.76

1. INFLUENCE OF NUMBER OF HOPS AND OF NUMBER OF ACTIVE VIRTUAL CIRCUITS (SEND,RECEIVE AND SUBNET WINDOWS EQUAL TO 2)

WINDOW SIZES	THROUGHPUT (pps)
2	3.14
4	6.08
6	6.93
7	7.02

2. INFLUENCE OF WINDOW SIZES (IDENTICAL SEND, RECEIVE AND SUBNET WINDOW SIZES)

D-bit	THROUGHPUT (pps)		
	Ws = 3	Ws = 5	Ws = 7
0	7.60	8.60	8.59
1	6.03	6.27	6.28

3. INFLUENCE OF THE D-bit (Ws = SUBNET WINDOW SIZE)

USER DATA FIELD LENGTH IN OCTETS	THROUGHPUT (pps)
32	3.25
64	4.99
128	6.52

4. INFLUENCE OF THE PACKET SIZE

- ACCESS LINE: 9600 bit/s (8.8 DATA PACKETS OF 128 OCTETS PER SECOND)
- FRAME LEVEL WINDOW: 7
- 128 OCTET DATA PACKETS
- D-bit = 0
- NO ACKNOWLEDGEMENTS ON HIGHER LAYERS
- NUMBER OF ACTIVE VIRTUAL CIRCUITS: 1

5. DEFAULT VALUES

TABLE VII.- THROUGHPUT (USER INFORMATION TRANSFER RATE) MEASUREMENTS ON DATEX-P.

Access delays for a number of public PSNs such are Canada's DATAPAC [16], U.S. Telenet [17], EURONET [32] and the Italian Packet Switched Data Network [18,19] are always around or slightly below 1 second.

An experiment carried out on a U.S. public data network [33] where a computer accessed the PSN through the public switched telephone network, gave an average access delay of 45 s., from which 17 s. were due to the local telephone connection, 4 s. were due to the PSN connection and 24 s. to the host computer log-in time.

These delays clearly exclude accessing PSNs through telephone connections in Telecontrol systems unless they remain permanently connected.

However the gradual introduction of ISDN in public networks may change the situation since in this kind of network access delays are in the hundreds of milliseconds.

Another interesting delay component is the average node transit delay. In the U.S. Telenet in 1983 this delay was 60 ms [26] of which 23% (13.8 ms) was attributable to route processing.

6.3. TELECONTROL NETWORKS

6.3.1. THE TRAME NETWORK [3,11]

Measurements performed on the Spanish TRAME network in 1983 showed that a typical RTU generated a steady-state traffic of 92 bps when measured over a period of 5 minutes. This steady-state traffic included measurements for LFC (sent each 3 s), measurements for SE evaluation (sent each 30 s) and other measurements sent with periods of 120 s and 300 s.

Over this steady-state traffic there may appear sudden peaks of traffic due to emergency situations in the power network or demands of information coming from the Control Center or from supervisory terminals operated by personnel in the electrical maintenance sections. The maximum peaks measured over a period of 5 minutes for a typical RTU were three times larger than its steady state value.

In 1988, the evolution of the TRAME network gave the measured results shown in table VIII.

The average user information transfer rate or throughput generated by RTUs in ENHER's Telecontrol system was in 1988 only 0'25 packets per second (pps) (approximately 77 bps), compared to 0'29 pps (approximately 92 bps) in 1983. This is due to the incorporation to Telecontrol of distribution stations. The average flow for the RTUs of the power transport network is still around 90 bps.

The Input traffic/Output traffic ratio is the ratio between the number of packets per second entering the RTU and the user information transfer rate in pps in a given period of time sufficiently long to estimate an average.

The increase of user information transfer rate due to non periodic traffic (Commands, alarms, spontaneous changes of status, retrieval of data from CC and maintenance terminals, etc), measured in increase of the number of pps, gives a figure of only 4% for the whole system.

User information loss probability in the TRAME network, based on elimination counts in nodes and on the number of node initializations, gives a figure of around 5×10^{-4}.

The packet lengths handled by the TRAME network have a minimum length of 96 bits and a maximum length of 576 bits. The average packet length, averaged over all periodic traffic, gives a calculated figure of 308 bits. The overhead, including Line and Network header, is 96 bits per packet.

	AVERAGE OF ALL RTUs	LARGEST 400 kV STATION (RUBI)	SMALLEST 400 kV STATION (BEGUES)	SMALL DISTRI-BUTION STATION (FRAGA)
USER INFORMATION TRANSFER RATE (GENERATED BY RTU)	0.25 pps (77 bit/s)	0.56 pps (210 bit/s)	0.38 pps (93 bit/s)	0.053pps (15 bit/s)
INPUT TRAFFIC/ OUTPUT TRAFFIC	10 %	3.9 %	3.6 %	17 %
INCREASE OF USER INFORMATION TRANSFER RATE DUE TO NON PERIODIC TRAFFIC	4 %	4 %	3 %	27 %

AVERAGE NETWORK INTERNAL PACKET LENGTH : 308 bit
MINIMUM PACKET LENGTH : 96 bit
MAXIMUM PACKET LENGTH : 576 bit
MINIMUM NODE TRANSIT DELAY : 4 ms
USER INFORMATION LOSS PROBABILITY : 5*10E-4 (AT THE NETWORK LAYER)
RANGE OF NETWORK ROUND TRIP DELAYS : 30ms-900ms (96-bit PACKET)

TABLE VIII.- RESULTS OF MEASUREMENTS MADE ON THE TRAME NETWORK IN JUNE 1988

These lengths are internal to the subnetwork, which uses a synchronous line protocol with a format similar to IEC FT 3 [10] over the communications links. At the RTU-Subnetwork interface (Access link) the protocol used is asynchronous with the IEC format FT 1.2 [10]. To translate the internal length to the access one, it must be multiplied by (11/8) after having substracted 16 bits.

The range of round trip delays for 96-bit long packets range from 30 ms to 900 ms depending on the destination node, link speeds, network congestion, number of hops, etc. For a longer packet the delay will be longer but not proportionally longer since the delay has a fixed part (transit delays in nodes, modulation /demodulation delays, propagation delays, etc), a random part (queuing delays) and a proportional part (transmission delays). Also the parameter of interest is really the user information transfer delay while the measured delays are return delays for echo packets that go and return after bouncing on the destination node.

Unfortunately it is therefore difficult to calculate practical delays from the measured ones.

Improvements carried out on the TRAME network will permit continuous measurements to be made of the average one- way delay for the whole network or for parts of it as desired.

6.3.2.THE EDAPAK NETWORK

The EDAPAK network is an X.25 based PSN that links the Norwegian Control Centers. From this network there are the following average measurements available referring to the user information transfer delay between Control Centers.

These values of user information transfer delay were measured in 1987 during the ELCOM [43] test project. They are the elapsed time between the transmission of the first bit by the sending Control Center and the reception of the same bit by the receiving Control Center.

The large difference between the values "with" and "without" retransmissions was due to some low-quality links that caused too many retransmissions.

After network improvements that reduced retransmissions, the user information transfer delay including retransmissions was greatly decreased, being in 1989 close to the case without retransmissions in table IX.

ELECTRICAL MEASUREMENTS		CIRCUIT BREAKER INDICATIONS	
CYCLICAL DATA TRANSFER PACKET SIZE : 1024 bit		SPONTANEOUS DATA TRANSFER AVG. PACKET SIZE : 352 bit	
WITHOUT RETRANSM.	WITH RETRANSM.	WITHOUT RETRANSM.	WITH RETRANSM.
336 ms	790 ms	150 ms	308 ms

TABLE IX. MEASUREMENTS OF USER INFORMATION TRANSFER DELAY FROM THE NORWEGIAN EDAPAK NETWORK.

6.4.OTHER NETWORKS

6.4.1.THE ENEL PACKET SWITCHING NETWORK

6.4.1.1.INTRODUCTION

The ENEL network is a general purpose PSN not used for Telecontrol that is being operated by ENEL in Italy.

The scope of the report is to show the typical performances of this Packet Switching network with reference to the response times of messages in the normal transactions of ENEL's applications.

For the measurements, the Rome-Milan three-node link of the X.25 network has been considered.

6.4.1.2.METHODS OF MEASUREMENT

With reference to the test configuration shown in figure V, the measurement of the transmission time has been carried out through Comstate protocol analyzers inserted at the terminal points of the transmission chain (points A and B).

The transmission considered for the measurements consists of the following phases:

.Entering of the inquiry which consists of a SDLC 18-byte frame from the IBM 3276 terminal.
.Reception of the reply message from the computer, which consists of 14 SDLC frames of 1840 bytes as a whole.

The protocol analyzer detects the time intervals which elapse between the following events:

t1: entry of the input frame
t2: reception of the first character of the reply message
t3: reception of the last character of the 1840-byte message

t2-t1: is defined as the Tr response time
t3-t1: is defined as the Ts service time

6.4.1.3.MEASUREMENTS RESULTS

Tr and Ts time detection was carried out during normal office hours, by varying the speed of the connection between the terminal (IBM 3276) and Node 1 within the range of interest (1200-9600 bps.)

The speed of the other trunk lines was set at 9600 b/s. For internodal connections, X.75 protocol - SLP version (single link procedures) was used.

The main results of the measurements are shown in table X.

Table XI shows the amount of the response and service time due to processing in the host computer.

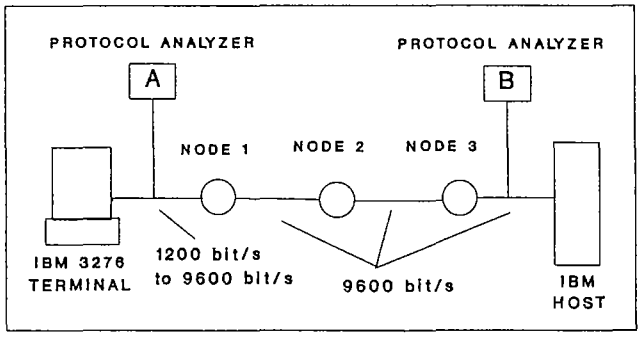
With reference to the terminal rate of 4800 bit/s figure VI shows in detail how the response time, Tr, and the service time Ts, are shared among the components of the transmission chain (nodes, host and lines).

At the top of figure VI the test configuration is represented.

Figure VI represents all time components of an enquiry from the terminal to the host computer and the corresponding reply, formed by 14 SDLC frames.

6.4.1.4.NETWORK EVOLUTION

The previous measurements refer to the model based on single-link (SLP) X.75 protocol in which the packets of a virtual circuit are serialized on a single physical line. In the near future the CCITT X.75 multi-link recommendation will be adopted.



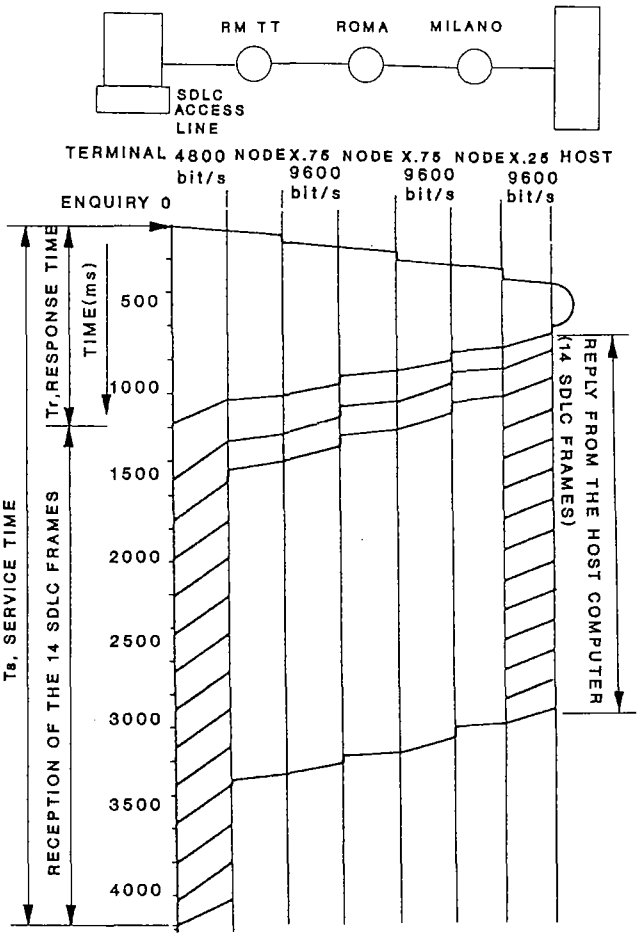
ENEL NETWORK TEST CONFIGURATION
Figure V

TERMINAL ACCESS LINE SPEED (bit/s)	RESPONSE TIME(ms)			SERVICE TIME(ms)		
	MIN	AVG.	MAX	MIN	AVG.	MAX
1200	837	1274	2101	13724	14278	15489
2400	907	1026	1355	7422	7743	8204
4800	730	1035	1541	4075	4824	5955
9600	719	1030	1758	3595	4149	5347

TABLE X : MEASUREMENT RESULTS FROM THE ENEL NETWORK

HOST COMPUTER RESPONSE TIME(ms)			HOST COMPUTER SERVICE TIME(ms)		
MIN	AVG.	MAX	MIN	AVG.	MAX
212	236	256	2308	2740	3575

TABLE XI. AMOUNT OF RESPONSE AND SERVICE TIME DUE TO THE HOST COMPUTER ON THE ENEL PSN.



COMPONENTS OF THE RESPONSE AND SERVICE TIME FOR A TERMINAL SPEED OF 4800 bit/s ON THE ENEL PSN.
Figure VI

This protocol is based on parallel packet transmission over the various physical lines connecting two nodes.

The utilization of X.75 ML protocol will permit reduction of service time to a value equal to the network response time plus the transmission time on the user link, on the assumption that the network to host connection does not introduce significant delays.

Other elements which still require study for performance improvements are higher line speed, packet length, packet level window, host connection speed.

In optimal conditions we expect to obtain a network

response time equal to 560ms. Therefore, under such conditions, the service time will be 560ms higher than the point-to-point SDLC connection service time.

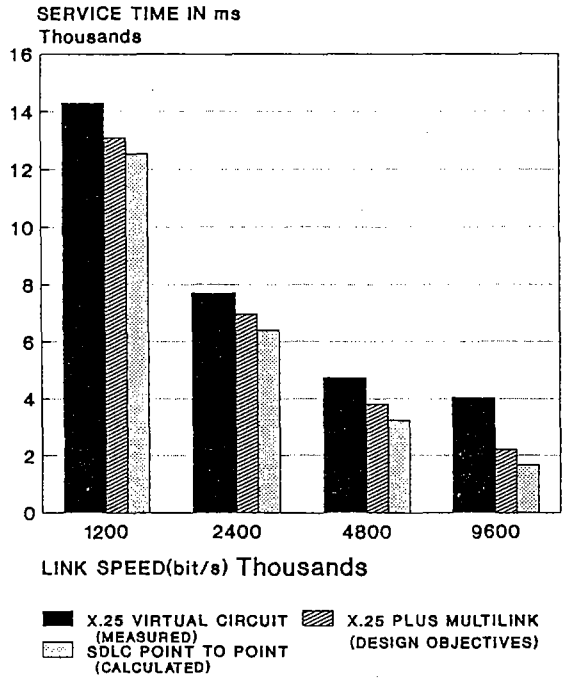
Figure VII shows the diagram of service time as a function of line speeds, in the following conditions:

- X.25 virtual circuit (measured values)
- Point-to-point SDLC connection (calculated values)
- X.25 virtual circuit under the multilink improvement (Service time equal to the previous case plus 560ms).

The point-to-point SDLC delays are in packet network necessarily lower than the measured X.25 virtual circuit delays for equal line speeds.

Figure VII shows how "worse" is a packet network in terms of delay with respect to direct point-to-point connections of speed equal to the network access speed.

It shows today's delay values measured in the ENEL network and planned values obtainable by improving protocols.



SERVICE TIME COMPARISON BETWEEN POINT-TO-OINT SDLC LINKS AND X.25 VIRTUAL CIRCUITS ON THE ENEL PSN.

Figure VII

7.SIMPLE MODEL FOR THE AVAILABILITY IN PACKET SWITCHING NETWORKS

The unavailability in PSNs may be caused by two different types of mechanisms, one functional and the other physical.

Functional unavailability, such is the one caused by network deadlocks, was reported in the early ARPA-net and it may be avoided by the use of proper techniques when designing the network.

Another kind of functional unavailability is the one due to software bugs.

None of these functional unavailability reasons are taken into account in this chapter.

The mechanism of physical disruption of paths is the one for which a very simple availability model is given here with the aim of giving a picture of what can be achieved and of helping the first stages in planning networks.

The conclusion of this simple model is expresed in figure IX in terms of the network availability figures necessary for Telecontrol as defined by CIGRE, as well as in terms of the link and node availability figures encountered in power utilities networks.

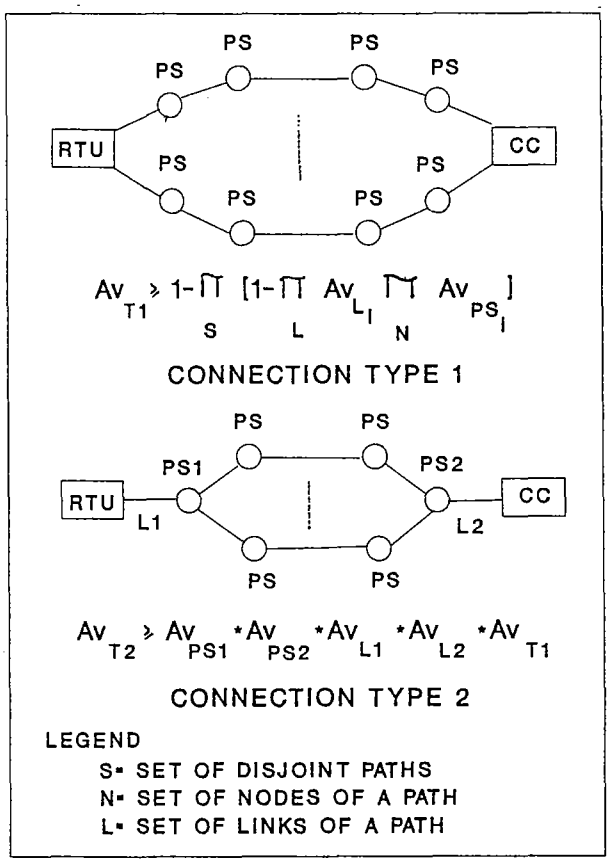
In figure VIII there is the representation of two types of connection of RTUs and Control Centers (CC) to a PSN. In type 1 they are connected to two nodes (the secondary connection may be simultaneous or switched after a failure of the primary route). In the type 2 connection they are connected to only one node.

In PSNs packets cross several links and nodes before arriving at their destination.

A possible model for the total availability (A_{VT}) is obtained by taking into consideration only the set (S) of disjoint paths between origin and destination. Each of the paths consists of a disjoint series of links and nodes.

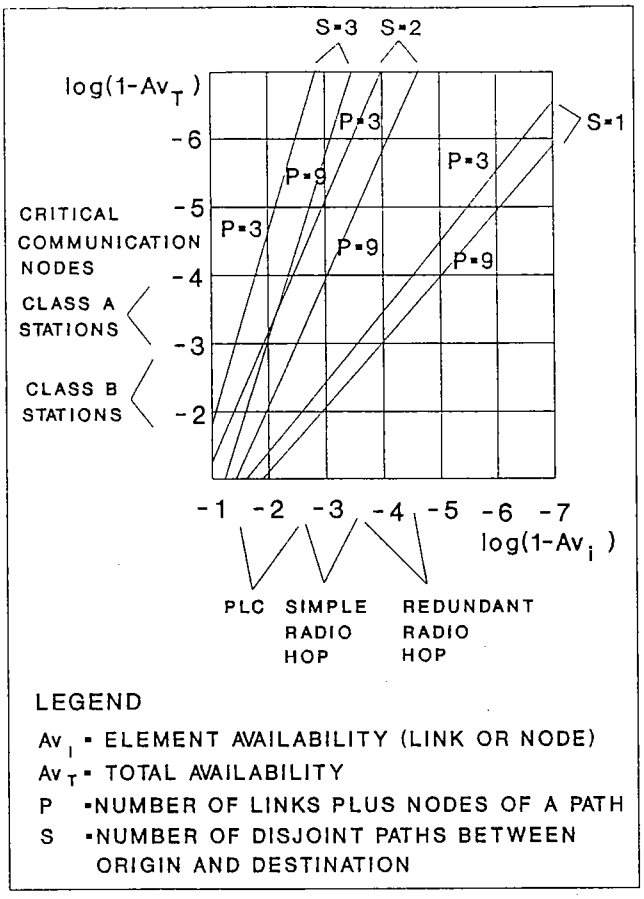
The end-to-end availability will be given by combinations of the classical availability equations:

$$A_{Vseries} := \prod_{1}^{N} A_i \qquad (1)$$



AVAILABILITY OF TWO TYPES OF CONNECTION TO A PSN

Figure VIII



TOTAL AVAILABILITY VERSUS ELEMENT (NODE OR LINK) AVAILABILITY
(EQ.3)

Figure IX

$$A_{Vparallel} := 1 - \prod_{i=1}^{N} \left[1 - A_i\right] \qquad (2)$$

In figure VIII there are the exact formulas that result.

A simplified but significant situation is to consider that the availability of links and nodes is the same for all of them, in which case the total availability for type 1 connection is given by:

$$A_{VT} := 1 - \left[1 - \left[A_{Vi}\right]^{p}\right]^{s} \qquad (3)$$

where s is the number of completely disjoint paths (typically 1, 2, 3 or 4) and p the number of links plus nodes of a path (typically 3, 5, 7 or 9). Equation (3) has been represented in figure IX from where it is easy to derive approximavely the type and the number of links to be installed due to availability reasons in class A and class B Power stations and in critical communication nodes on which several electrical installations depend. [37]

In the above approximation the not completely disjoint paths have been discarded so it is a pessimistic approach, being more pessimistic for larger p.

When RTU and CC are connected to only one node (See figure VIII, type 2 Connection) the availability of that node and of the corresponding link may very easily become dominant. This means that in this case the availability figures of nodes should be very high,higher than the availability figures of links, probably in the range of 99.99%, a figure that probably can only be achieved by redundant architectures.

8.TECHNIQUES TO IMPROVE PSN PERFORMANCE

Several techniques are available for improving the performance of systems which use PSNs. These techniques are interesting for an application such as Telecontrol that has more stringent requirements than general purpose applications. Some of them are the following.

8.1. TECHNIQUES TO IMPROVE DATA INTEGRITY

-USE OF AN END-TO-END ERROR DETECTING CODE

This technique consists of the implementation of a End-to-End protocol with an error detecting code, a time-out mechanism and an automatic repeat request procedure.

The error detecting code accompanies packets on their journey through the network, even within nodes.

It permits improvement of the Probability of Undetected Error in the network. The technique may overcome some deficiencies in the procedures and codes used at the link and node levels.

It may be used at a Network level between entry and exit points of the network and/or at a Transport level. In that case there is a standard ISO protocol, the Class-4 Transport Protocol, defined in ISO 8073.1986.

There is also the possibility to exercise end-to-end protection at the Application layer.

-TECHNIQUES TO IMPROVE HDLC

Several models have shown the low data integrity of standard HDLC. Also, several techniques have been proposed to solve the problem [8, 34, 35]. By the use of these techniques it may be possible to supplement or to avoid the use of a Network End-to-End error detecting code. They may also allow the use of a more simple Transport protocol.

Some of the techniques to solve the problem of HDLC data integrity can be applied at the Application layer by adding more redundancy to Application data when necessary.

In the case of using HDLC and considering the data integrity of this protocol for Telecontrol to be insufficient the technique may fill the gap.

It is interesting to mention that many public networks use internal network protocols with more protection than the one provided by HDLC. As an example, the French public TRANSPAC network uses a 24-bit CRC.

Also military networks [27,28] use LAPB protocol with a 32-bit long CRC. This technique improves HDLC reliability in five orders of magnitude [35].

-USE OF ERROR DETECTING CODES TO PROTECT FROM ERRORS IN NODES

Errors may occur both in links and in nodes. Link errors are prevented by the use of Line Protocols, typically using error detecting codes. Nodes may similarly be protected. Error detecting codes used to give protection from errors in nodes may have several forms and natures among which there are the following.

-A CRC or checksum which is appended to packets when entering the node and checked when being transmitted. Eventually the error detecting code may be the same as the one used on links.

-Protection of vital or even all databases and programs, especially those referring to the Routing System, by the use of error detecting codes. The protection may be checked periodically or when the appropriate part is going to be used.

-The technique of using an End-to-End error detecting code also protects packets within nodes. This technique overcomes the problem of errors at the moment of changing line for node error detecting codes.

8.2.TECHNIQUES TO IMPROVE AVAILABILITY

-USE OF REDUNDANT SWITCHES

The use of fault tolerant or redundant switches where critical components are duplicated and possibly operated in an executive/standby configuration is a good way of improving each node availability and, thus, the network availability.

-MULTICONNECTION OF TERMINALS

One alternative method to improve overall availability is for the terminals to be able to receive and send data from and to the network through two or more access lines, preferably connected to different nodes. This permits the selection of the level of availability required by each user.

8.3.TECHNIQUES THAT OPERATE ON DELAY

-USE OF PERMANENT VIRTUAL CIRCUITS

Permanent virtual circuits are a service that X.25 offers to the Transport layer. By the use of PVCs the delays associated with establishment and clearing phases are avoided in normal operation, although the service may permanently consume some network resources, such as buffers or table entries.

This does not reduce the flexibility of the system since modern PSNs dynamically share virtual circuits and recover from failures by switching to back-up paths in a form which is transparent to the user.

PVCs may be useful for the connection of RTUs directly to PSNs.

-USE OF NETWORK CONNECTIONLESS SERVICE

Connectionless service avoids the access and disengagement delays associated with connection oriented services, thus allowing instantaneous access to the network.

The difference with PVCs is that using the connectionless service, packets may arrive out of order and also be lost. The Transport layer may compensate for these problems.

In Telecontrol systems most of the messages are short self-standing packet messages, thus requiring short overhead, and many functions do not require to receive packets in sequence and are robust against data loss. So it is possible, and may even be convenient, to have both, connectionless and connection-oriented services, available.

-USE OF PRIORITIES

Priorities specify the relative importance of connections and data units.

Since in the application of Telecontrol priorities arise naturally, it is very useful in Telecontrol networks to be able to process them in some specific management entity or structure (e.g., Head-Of-the-Line priority queues).

There may be different priority parameters referring to different performance parameters.

As an example, some of them may be the following:

-Priority to gain a connection (affecting access delay and service availability).

-Priority to keep a connection (affecting service availability).

-Priority for quality of service degradation of data, when necessary (affecting user information transfer delay and user information transfer rate).

-Priority to discard data units to recover resources, if necessary (affecting user information loss probability).

This technique permits handling of the different performance requirements of Telecontrol functions.

8.4.OTHER TECHNIQUES

-MULTIDESTINATION CAPABILITY

The multidestination capability is the possibility for the network to send the data to a specified group of users involving a network function known as broadcasting.

This feature may permit a rough synchronization mechanism that may be useful in the implementation of polling, freezing or snap-shot commands.

It may also permit data to be sent to several Control Centers or Remote Terminal Units at the same time without involving so many network resources as in the case of sending messages sequentially from origin to each of the destinations.

Network broadcasting is not contemplated by ISO standards so far. The study of the need/convenience of this service for Telecontrol is an interesting one.

-SIMPLIFYING INTERNAL NETWORK PROTOCOLS

This paragraph refers to the possibility of simplifying internal line and network protocols but not the access protocols such as X.25. The aim of this simplification is to achieve higher network performance especially in terms of speed.

This is a trend in Packet Switching. The challenge to handle higher trunk and access speeds is met by the technique of simplifying internal protocols that capitalizes on the fact that digital high speed links and specially Fiber Optic Links have an extremely low Bit Error Rate. This permits great simplification of line protocols. The switching is also simplified and there is a trend to do it all by special purpose switching hardware fabrics. The technique is called Fast Packet Switching and is being developed for use in the future Broadband Integrated Services Digital Network.

The increase of speeds may permit the integration of new services in the network.

One simple way to do so without reducing the Undetected Error Probability is to use a Line Protocol with an Error Detecting Code but without any kind of Control message such as Acknowledgements, Negative Acknowledgements, Receive Ready and so on, and without any retransmission procedure at the link level. The packets are simply discarded when they are detected to be in error.

Since the code detection is typically made by hardware, this permits the achievement of very high throughputs. Occasional retransmission is left to a Network End-to-End protocol. The higher speeds and the lower bit error rates compensate for the occasional delays incurred in the case of retransmission.

Note that one network can employ simplified protocols only over links with the appropriate conditions.

9.PACKET SWITCHING NETWORKS IN ELECTRIC UTILITIES.

9.1.TELECOMMUNICATION SERVICES USED BY POWER UTILITIES

Power utilities make use of many telecommunication services which nowadays are in many cases handled by specialized networks.

Among these networks are:

-Data Transmission network for Telecontrol.
-Telephone network.
-Load-Frequency Control network.
-Facsimile network.
-Private telex network.
-Slow scan television network.
-Teleprotection network.
-Synchronization network.
-Mobile radio network.
-Teleprinting network.
-Data network for Distribution Automation.
-Administrative data network.
-Word-processing network.
-Network connecting Mainframe Telecontrol computer with other computers and Man-Machine Devices.
-Inter-Utility communications network.
-Data network between Control Centres.

9.2.INTER - UTILITY COMMUNICATIONS

Packet Switching Networks and specifically the X.25 protocol have proved to be very convenient in Inter-Utility communications, in Energy Management Systems and in data transmission between Control Centers. An important number of countries are using or plan to use the CCITT X.25 protocol Recommendation and an architecture based on the International Standards Organization (ISO) Basic Reference Model for their Energy Management System and Inter-Utility Communications [6,23,43,45].

Inter-Utility Communications involve powerful host computers of several vendors ; To harmonize these different hosts X.25 is the ideal method. Also because hosts are large mainframe computers, they can easily incorporate X.25 and even higher level protocol ISO layers, without suffering in their performance.

9.3.PACKET SWITCHING NETWORKS IN TELECONTROL

Packet Switching Networks have been used for over a decade to support the communications needs of Telecontrol systems, by linking RTUs and Control Centers together.

The first PSN used for Telecontrol was the Swedish TIDAS network (1), later followed by other networks [2,3].

It is interesting to note that networks in references [1,2,3] are either specifically developed or adapted to Telecontrol by including features normally not available in public networks, such are prioritized traffic, special interfaces for Telecontrol, use of procedures to improve HDLC reliability, multidestination transmission, etc.

Recently [45] general purpose PSNs based on X.25 have been considered for use in Telecontrol Systems by directly linking RTUs and Control Centers.

9.4.DATA TRANSFER METHODS FOR SCADA SYSTEMS USING PACKET SWITCHING NETWORKS

The lack of internationally agreed protocols for telecontrol produced in the past a pleyade of vendor oriented protocols with a wide spectrum of characteristics. So the situation today for existing systems is quite diverse.

Basically there are two types of systems, the one using polling and the event driven one which does not need polling. The older systems typically use the polling approach.

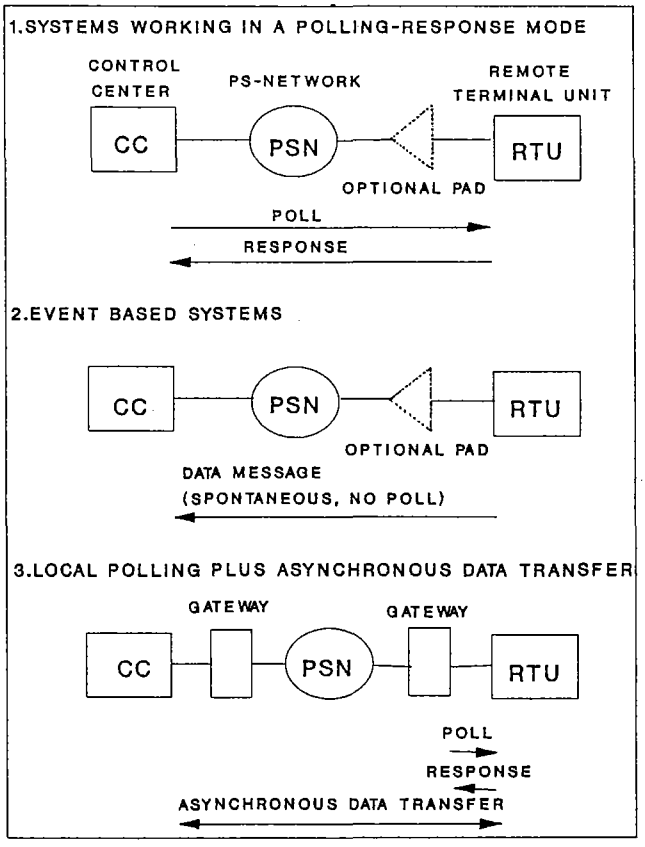
Within the polled systems we may distinguish two types of polling. The medium access control polling and the application polling. In the first case the Control Centre polls stations connected to the same transmission medium, for instance a multidrop line. This local level of polling is not addressed in the report.

Is the second case, the application polling, which is going to be treated here.

There are the three following possible types of configurations for connection of RTUs to PSNs (See figure X).

1. Systems working in a polling-response mode.

In these systems RTUs are polled by the Control Center which issues a command requesting data from the RTUs. It is common for the CC to initiate a timer to ensure that the response from the RTU is delivered in a specified time. If



CONFIGURATION FOR CONECTION OF RTUs TO PSNs

Figure X

the time expires before the response is received then recovery procedures, ranging from retries to suspending communication and error reporting, are used.

An initial solution for PSNs to support polled terminals is to convey all data generated, including polls, between the CC and the terminal and across the PSN.

The disadvantages of these systems when using PSNs are increased network load and random turnaround delays that may trigger time-out mechanisms in the CC.

2. Event based systems

These systems work in an asynchronous mode, sending data spontaneously only upon changes or request, but not periodically.

These systems do not have the disadvantages mentioned in systems working in a polling-response mode and are better suited for integration into PSNs.

In both cases (polling-response systems and event-based systems) if the RTUs are of the start-stop type they can be connected to packet networks by Packet Assembly/Disassembly (PAD) facilities following the CCITT standards X.3/X.25/X.29. This permits many current RTUs to be connected to PSNs.

The PAD performs the translation to and from the X.25 and serves as a concentrator.

3. Local polling mode plus asynchronous data transfer.

In this case the RTUs and the CC are connected to the network through specially developed Gateways incorporating the queue or Data Base, so making the translation up to the Application layer from the polling-response mode of the RTU and CC to the asynchronous environment of the network.

There will be a CC-Gateway between the CC and the PSN and a RTU-Gateway between the network and the RTU. The CC-Gateway should behave to the CC as the terminal system by having "virtual" terminals, which emulate the RTU responses. The RTU-Gateway should behave to the RTUs as the CC. Each Gateway presents an X.25 interface to the network and uses this interface to communicate with the other Gateways. Data received by the CC-Gateway from the CC is sent across the network to the RTU-Gateway. Data received by the RTU-Gateway in response to its polling the terminal is sent across the network to the CC-Gateway where it is held until solicited by the CC.

This Gateway supporting polled terminals should be specifically designed for each system.

With this use of Gateways no changes in CC or RTUs are necessary but the question of the suitability of X.25 is still raised. There is also a limitation in that it relies on the CC-Gateway being able to return an immediate response to a CC poll, that may not happen in some systems or situations. Related with this there is the possible inability to support freezing and snapshot commands.

The objective of a system snapshot or freezing command is to sample all data inputs at all RTUs as nearly simultaneously as possible. This permits a valid consistency of measurement and status data from all remote sites by the application programs. The ability of PSNs to handle these commands is an interesting point to study since it seems that a time skew in sampling of 50-100 ms seems acceptable for data consistency purposes. It is also interesting to assess the level of necessity for these type of commands.

A Gateway may be a separate interface computer or it may be as well a program in the network or within the RTU and CC.

In the case of using the idea of Gateways the X.25 interface provides a means for establishing a logical connection between the CC-Gateway and the RTU-Gateway. Further higher layer protocols including a Transport protocol are necessary to describe how the logical connection is used for carrying data and status and control information between the two Gateways.

This Transport protocol between Gateways, on top of the X.25, may be more or less complex . The idea is to use the Transport layer to overcome the possible inabilities of X.25 for Telecontrol and to match the Telecontrol requirements on top of the Transport layer.

This coincides with ISO : 8073 [46] and CCITT X.224 Recommendation which make provision for five classes of transport protocol providing different functions and levels of Quality of Service.

9.5.PACKET SWITCHING NETWORKS IN FUTURE TELECONTROL SYSTEMS

Todays RTUs are all based on microcomputers and often in multi-microcomputer structures for reliability and computation power reasons. The computation power of RTUs is likely to increase in the future due to the need to integrate more control funcions and to the availability of ever more powerful microcomputer structures. This means that in the future it will be possible for the RTUs to support complex communications protocols such as X.25 and the protocols standardized by ISO for the higher layers and specially for the Transport layer.

The use of PSNs in Telecontrol and the problem of the possible inability of X.25 to handle Telecontrol traffic because of its inherent low data integrity level [7,8,34,35] may be solved in different ways which can be summarized as follows :

Approach A. To use a completely special purpose packet switching network with protocols designed to achieve the data integrity level required by IEC/CIGRE for Telecontrol systems [10]. This is the approach used by the TIDAS [1] and TRAME [3] networks. This approach involves the definition of a Telecontrol Access Method to PSNs and the use of special line protocols. It also involves the protection of packets when crossing the nodes so as to achieve a high enough end-to-end data integrity level.

In this way, the network is protected adequately and the Transport layer can be simplified, even removing the need for Transport data integrity protection.

Approach B. To use a general purpose PSN together with a Transport protocol, specifically matched to the requirements of Telecontrol. It could be ISO/CCITT Class 4 protocol (46) using an error detecting code with end-to-end significance. Some military networks [27,28] use a similar technique, employing an end-to-end CRC for error detection.

The capabilities of Class 4 Transport protocol in Telecontrol have not been studied in depth so far. This is clearly an interesting field of study. This Transport protocol may be used either on top of a connectionless network service (Protocol under definition by ISO) or on top of a connection oriented (X.25) network service.

The subnetwork itself may have different characteristics and levels of data integrity, it may even match Telecontrol requirements between entry to exit node (in fact several general purpose networks employ non LAPB internal line protocols with added protection). In this latter case the Transport protocol needs only to correct the deficiencies

of standard network access methods, be it connectionless or connection oriented (X.25), a much easier thing than having to overcome other internal deficiencies.

In that situation probably ISO/CCITT Class 4 Transport protocol may be enough protection. In any case, it is of great interest to know to what extent Class 4 Transport protocol can overcome network deficiencies.

If Class 4 Transport protocol is not enough protection, it would be necessary to produce a Telecontrol protocol with higher protection for the Transport layer.

Several methods have been proposed [8, 34, 35] to correct the problem of LAPB data integrity. Some of these methods or simplifications/variations of them may be applied not only at the link layer but also at the Transport and even at the Application layer by adding redundancy to the data when necessary. These methods may be the basis for a Telecontrol Transport protocol.

Another similar possibility is to apply these methods at the Application layer, where selective techniques may be used for specific applications. The viability of this approach is also an interesting field of study.

Approach C. To use a modified general purpose PSN with a modified LAPB protocol using a 32-bit CRC (instead of a 16-bit one) and a 16-bit flag (instead of an 8-bit one). This approach is specified by some military networks [27,28] and by Ethernet. According to [35] it improves HDLC reliability in seven orders of magnitude (five due to the 32-bit CRC and two due to the 16-bit flag), although the slope of the probability of Undetected Error versus Bit Error Probability is still one. This means that the slope of four defined by IEC is not preserved by this method. Nevertheless IEEE C37.1 data integrity requirement may be achieved in this way. Other possible approaches to improve LAPB data integrity at the link layer are also possible [8,34].

9.6 NEW TELECONTROL SERVICES PERMITTED BY THE USE OF PSNs

The full nerworking capability of PSNs and especially the function of multiplexing virtual circuits on a single access link give Telecontrol systems several new and important capabilities. Four of them are the following:

Electric maintenance-personnel may have access to the data captured by RTUs from their offices. This means that there is the possibility of having access from any point of the network to any information that has been fed to RTUs. It is obvious that the Control Center is only concerned with information relevant to the operation of the electric network. More detailed information is not necessary at the Dispatching Center and it may be even disturbing, but the PSN permits use of this more detailed information at other places rather than the Dispatching Center and by other people. For instance it may be used by Protection personnel to track some disturbance. In order to do that, these protection personnel may have a terminal connected to any PSN node.

An RTU may depend on various Control Centers [45] and this dependence may be changed dynamically. For instance, an RTU controlling a substation with two levels of voltage : 25 KV and 220 KV may be operated simultaneously from the Dispatching Center for the part of 220 KV and from the Distribution Control Center for the part of 25 KV, and these two Centers may be located in completely different places. Or there is the possibility of having an emergency Dispatching center to which the RTUs are automatically hooked in case of failure in the Main Dispatching Center or when the communications network is split into two parts.

It is also possible to operate an RTU from a Master station located elsewhere during the day and to switch it to be operated by night from the Dispatching Center.

Maintenance personnel may access the data within RTUs from their homes.

The PSN can be accessed through the public switched telephone network by using portable, low cost terminals from which maintenance personnel can access detailed data from their home. This rapid access to detailed data may reduce repairing times by avoiding taking early inappropriate decisions due to lack of knowledge.

The data in any RTU may be accessed from any other RTU

This characteristic may be useful for maintenance people working in one substation and needing access to the data in neighbouring substations. It may also be useful in case of emergency since it may permit a rapid organization of operational zones around main substations.

These four features give an indication about the broad field of Electric Operation possibilities that are open by the use of PSNs.

9.7.INTEGRATION OF NON-TELECONTROL SERVICES

It is clear that the trend is to integrate all the services listed in 9.1. as fully as possible and to make all of them digital. This means that focusing only on Telecontrol networks may not be enough. Telecontrol data networks should be viewed in a wider environment where other services will be more economically and reliably provided by integrating heterogeneous networks.

The integration of Telecontrol networks with other services has benefits as well as drawbacks.

The benefits in integrating the services in 9.1. are:

The integrated network will be more reliable since the set of all links being used by all services will be more meshed and redundant than using separate networks for each service, and so by operating it properly, it may be more reliable.

The speed will be much higher since all the channels will be multiplexed in a TDM fashion instead of using low speed separate FDM. This higher speed should enable new services.

The cost will be reduced since, by operating the resulting integrated network properly and by the use of ever-decreasing-cost microprocessors, it will certainly need less links than several separate networks [2].

Integrating all the services listed in 9.1. is extremely difficult or even impossible nowadays but the integration of many or several is already possible by the use of Packet Switching technology.

Nevertheless, the integration of Telecontrol with other services, although convenient in general, should be carefully designed, since it may involve the use of larger and more complex packet switches that may be less reliable than smaller ones, thus hindering the increase of reliability due to meshing of the network. It is also necessary to be careful with the integration of Telecontrol with other services with traffic flow characteristics that could block or slow down Telecontrol traffic under some situations of congestion. In this respect priorities naturally come into play.

10.APPENDIX I: GLOSSARY OF TERMS

-ACCESS DELAY

Access delay is the value of elapsed time between an access request and successful access.

An access request is any interface signal that notifies the network of a user's desire to initiate a data communication session.

Elapsed time values are calculated only on access attempts that result in successful access. The successful access outcome is indicated in one of two ways:

1)By network issuance of a ready for data or equivalent signal to the calling user before access timeout, in networks that provide such a signal; or

2)By the fact that at least one bit of user information is input to the system before access timeout, in networks that do not provide a ready for data of equivalent signal. In connection-oriented services, there is the additional requirement that the intended called user must have been contacted and committed to the data communication session during the access attempt.

In the case of using X.25, it is the time interval that starts with the placing of the CALL REQUEST packet in the output queue of the calling DTE, and ends with the DTE receipt of the corresponding CALL CONNECTED (X.25) packet. This delay may include any retransmissions for error correction.

Access delay is divided into user-dependent and network-dependent components.

In the case of using X.25, the delay between the reception of an Incoming Call and the issuing of Call Accepted packet is only attributable to the destination DTE, not to the network.

-ACCESS DENIAL PROBABILITY

Access denial probability is the ratio of total access attempts that result in access denial to total access attempts in a specified sample. (It is actually an estimate of the probability).

Access denial (also termed network blocking) may occur in two ways:

1)The network issues a blocking signal to the originating user during the access period (preventing the start of user information transfer); or

2)The network excessively delays in responding to user actions during the access period, with the result that user information transfer is not initiated before access timeout. Access denial is distinguished from service outage by the fact that some active response (i.e. interface signal) is issued by the network during the access attempt.

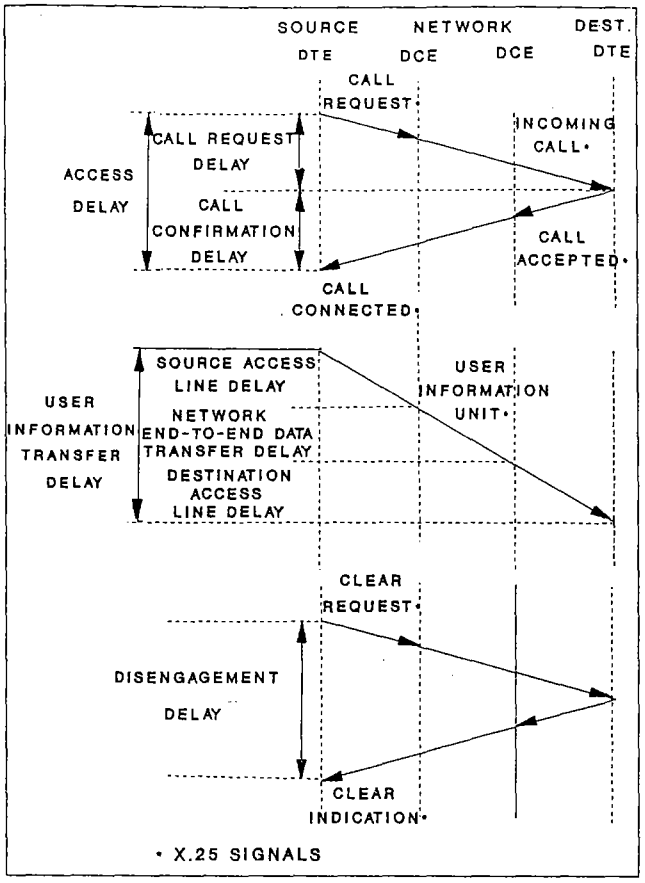
-CONGESTION CONTROL

See "Flow Control". Although some authors differentiate Congestion Control from Flow Control, here both terms are used synonymously.

-DCE

Data Circuit-terminating Equipment in CCITT terminology.

The PSN part of an access protocol to a PSN. It dialogues with a DTE.



DELAYS IN PACKET SWITCHING NETWORKS

Figure XI

-DISENGAGEMENT DELAY

Disengagement delay is the value of elapsed time between the start of a disengagement attempt for a particular user and successful disengagement of that user.

The successful disengagement outcome is indicated in one of two ways:

1)By network issuance of a clear confirmation or equivalent signal to the requesting user before disengagement timeout, in networks that provide such a signal; or

2)By the fact that the user is able to initiate a new access before disengagement timeout, in networks that do not provide a clear confirmation or equivalent signal.

-DISENGAGEMENT DENIAL PROBABILITY

Disengagement denial probability is the ratio of total disengagement attempts that result in disengagement denial to total disengagement attempts in a specified sample.

The disengagement denial outcome is indicated in one of two ways:

1)By the absence of a clear confirmation or equivalent signal within the disengagement timeout period (in networks that provide such a signal); or

2)By the inability of the user to initiate a new access within the specified disengagement timeout period (in networks that do not provide a clear confirmation or equivalent signal).

-DTE

Data Terminal Equipment in CCITT terminology.

A terminal or computer accessing a PSN. It dialogues with a DCE.

-EXTRA USER INFORMATION DELIVERY PROBABILITY

Extra user information delivery probability is the ratio of total (unrequested) extra information units to total information units received by a destination user in a specified sample.

An information unit received by a particular destination user is declared to be an extra information unit when none of the bits in the unit were input to the system by the source user for delivery to that destination.

-FLOW CONTROL

A function which controls the flow of data within a layer or between adjacent layers (5), to avoid the building of congestion. Means to balance the offered data load to the available network resources.

-HDLC

High-Level Data Link Control. Several International Standard (ISO 1111, 4335 and 3309) define HDLC. It is a Link Layer Protocol in the ISO layered architecture.

-INCORRECT ACCESS PROBABILITY

Incorrect access probability is the ratio of total access attempts that result in incorrect access to total access attempts in a specified sample.

Incorrect access occurs when the network establishes a physical or virtual circuit connection to a user other than the one intended by the call originator, and then does not correct the error before the start of user information transfer.

-LAYER

A Basic module in the architecture of data communication systems. International Standard : ISO 7498 [5,44] subdivides data communications systems in seven layers with well defined functions and interfaces between them.

-NETWORK CONNECTIONLESS MODE TRANSMISSION (Datagram Transmission)

The transmission of a data in a single self-contained entity containing sufficient information to be routed to the destination DTE whithout the need for call establishment and without requiring any kind of network acknowledgement or return packet [44].

-NETWORK CONTROL CENTER (NCC)

A Control Center that performs tasks of supervision and/or operational control of a Packet Switching Network.

-NODE TRANSIT DELAY

The interval of time between the reception of the last bit of a message and the successful sending of this last bit.

-PACKET SWITCH

A Switch of a Packet Switching Network. A PSN is formed by links and nodes or Packet Switches. Packet Switches store packets and forward them to the links.

-PACKET SWITCHING NETWORK (PSN)

A data network where information is transmitted by the use of short standardized messages with a limitation in their maximum length. These messages are called packets.

-PAD

Packet Assembly/Disassembly facility in CCITT's terminology. A device that permits the connection of asynchronous terminals to packet networks by performing the packetization/depacketization tasks. It is defined in CCITT's Recommendation X.3/X.28/X.29.

-ROUTING

A function within a layer which translates the title of an entity or the service-access-point-address to which the entity is attached into a path by which the entity can be reached [5].

-SERVICE AVAILABILITY

Service availability is the ratio of the aggregate time during which satisfactory or tolerable service is or could be provided, to the total observation period.

The time during which satisfactory or tolerable service is available includes all time that is not within the service outage duration as defined below.

-SERVICE OUTAGE DURATION

Service outage duration is the duration of any continuous period of time for which satisfactory or tolerable service is not available. It is recognized that the determination of an outage condition requires a finite observation period.

A service outage includes any period during which the user is unable or would be unable to elicit any response from the network; i.e. the network is "dead". It also includes any period during which the service provided by the network is unacceptable because of, for example, poor error performance or throughput.

-SUBNETWORK

A set of one or more intermediate open systems which provide relaying and through which end open systems may establish network-connections [5].

-USER INFORMATION ERROR PROBABILITY

User information error probability is the ratio of total incorrect user information units to total successfully transferred user information units plus incorrect user information units in a specified sample.

A transferred user information unit is defined to be an incorrect user information unit when the value of one or more digits in the unit is in error, or when some, but not all, digits in the unit are lost digits or extra digits (i.e. digits that were not present in the original signal).

Bit error ratio is a limiting case of user information error probability in which the user information unit length, on which the error performance is based, is a single binary digit.

The proportion of errored seconds is a particular case of user information error probability in which the user

information unit length is defined as one second.

-USER INFORMATION LOSS PROBABILITY

User information loss probability is the ratio of total lost user information units to total transmitted user information units in a specified sample.

A transmitted user information unit is declared to be a lost user information unit when none of the bits in the unit are delivered to the intended destination user within the specified timeout period, for which the network is responsible.

-USER INFORMATION MISDELIVERY PROBABILITY

User information misdelivery probability is the ratio of total misdelivered user information units transferred between a specified source and destination user in a specified sample.

A misdelivered user information unit is a user information unit transferred from a source user to a particular destination user that was actually intended for delivery to a different destination user.

-USER INFORMATION TRANSFER DELAY

User information transfer delay is the value of elapsed time between the start of transfer and successful transfer of a specified user information unit (e.g. block).

The successful transfer outcome is declared (on end of transfer) when an information unit is transferred from the source user to the intended destination user within the specified transfer timeout period, and the delivered unit has exactly the form and content intended by the source.

More specifically, it is the time interval between the data packet placement into the output queue by the DTE and the data packet reception by the remote DTE. This delay may include any retransmission for error correction.

It is the summation of three delays. Network End-to-End Data Transfer Delay, Source Access Line Delay and Destination Access Line Delay (See figure X).

-USER INFORMATION TRANSFER DENIAL PROBABILITY

User information transfer denial probability is the ratio of total transfer denials to total transfer samples during a specified observation period.

A transfer sample is a discrete observation of network performance in transferring user information between a specified source and destination user. A transfer sample begins on input of a selected user information digit at the source user interface, and continues until the outcomes of a given number of transfer attempts have been determined.

A transfer denial is a transfer sample in which the observed performance is worse than a specified minimum acceptable level. Transfer denials are identified by comparing the measured values for four supported quality of service parameters with specified transfer denial thresholds. The four supported parameters are user information error probability,user information loss probability, extra user information delivery probability and user information transfer rate.

-USER INFORMATION TRANSFER RATE (Throughput)

User information transfer rate is the total number of successfully transferred user information units in an individual transfer sample divided by the input/output time for that sample.

The input/output time for a transfer sample is the larger of the input time or the output time for that sample.

It is normally measured in packets per second (pps).

-VIRTUAL CIRCUIT

A logical, not necessarily physical, connection between two network entities. Normally they have an establishment phase, a data transfer phase and a disconnection phase. They deliver packets to the user in sequence and with no duplication or loss of packets.

-WINDOW

A Flow Control parameter used to control connections between two entities. The set of consecutive sequence numbers which an entity has been authorised by its peer entity to send at a given time on a given connection [46]

11. BIBLIOGRAPHY

[1] T. Jerlhagen and B. Leander
"A message switching network designed for data communications and remote control".
Proceedings of CIGRE - 21,29 August 1974.

[2] T. Yamazaki, M. Tsukiyama, T. Taguchi, T. Kai and T. Yamauchi
"Applications of the packet exchange method to the communication networks for electric power systems"
Proceedings of CIGRE, 1984

[3] J.M. Selga
"TRAME: a packet switching computer network for power systems"
Proceedings of CIGRE
September 1978

[4] Proceedings of IEEE
Special issue on "Open Systems Interconnection (OSI). Standard architecture and protocols.
December 1983.

[5] ISO 7498:1984
Information Processing Systems-Open Systems Interconnection-Basic Reference Model.

[6] I. Thurein
"Utility Data Exchange and System Operating Training Simulator"
Part 1. Status Report on Inter-Utility Data Exchange
Proceedings of CIGRE, 1988

[7] G. Funk
"Comparison of data reliability and efficiency in various standard protocols for information exchange in computer network"
Proceedings of EUROCON
May 1976, Venice (Italy)

[8] J.M. Selga and J. Rivera
"HDLC reliability and the FRBS method to improve it"
Proceedings of seventh data communications symposium
Mexico City, October 1.981.

[9] ANSI / IEEE C.37.1
"Definition, Specification and Analysis of Systems Used for Supervisory Control, Data Acquisition and Automatic Control".
1.985

[10] IEC TC57
"Telecontrol Equipment and Systems"
Characteristics of telecontrol equipment
Dec. 1985, part 5.1: Transmission Frame Formats

[11] J.M. Selga y J. Xampeny
"Flow adaptive updating procedure for dynamic routing.
Comparative simulation results".
Proceedings of international conference on communications
ICC - 80, Seattle, WA, June 8 - 12, 1980

[12] ISO 8208 : 1987
Information processing systems - Data communications - X.25 Packet Level Protocol for Data Terminal Equipment

[13] ISO 7776 : 1986
Information processing systems - Data communications - High-level data link control procedures - Description of the X.25 LAP-B - compatible DTE data link procedures.

[14] J.S. Turner
"Design of an Integrated Services Packet Network"
IEEE Journal on Selected Areas in Communications
Vol. SAC-4, No.8, Nov. 1986

[15] Durteste, B.
"Characteristics of the Transpac network"
INTELCOM'77

[16] Clipsham,W.W, Glave, F.E. and Narraway, M.L.
"Datapac Network overview"
Proc. of ICCC'76, Toronto.

[17] Roberts, L.G.
"Packet Switched network service"
International Seminar on Digital Communications
Zurich - 1976

[18] Ministerio delle Poste e Telecomunicazioni
"Specifiche della Rete Pubblica per Dati"
Roma 1980

[19] C.Boreggi and M.Burgassi
"Traffic characteristics and applications requirements for data transmission".
CSELT Rapporti Tecnici - Vol. IX - N.1 Febraio 1981

[20] Proceedings of the IEEE
Special Issue on Open Systems Interconnection (OSI) - Standard Architecture and Protocols
December 1983.

[21] IEC TC57
"Telecontrol Equipment and Systems"
Part 4: Performance Requirements
July 1985

[22] I.Lieberman
"AUTODIN II - Advanced Telecommunication System"
Telecommunication - May, 1981 - pp 43 to 48.

[23] Electrical World
"Establishing the Electronic Grid"
Electrical World, November, 1986, pp. 57 to 64.

[24] K.P. Steinruck and G. Gutzmerow
"Delay and Throughput Analysis for the German Packet Switched Public Data Network DATEX-P"
Proc. of Globecom'84. IEEE.

[25] D.Runkel
"Datex-P, The Public Packet Switching Network of the Deutsche Bundespost after five years of Experience".
Proceedings of the Eigth International Conference on Computer Communications (ICCC) Munich, September, 1986, pp. 441 to 445.

[26] E.E.Mier
"Packet Switching and X.25 - Where to from here?"
Data Communications, October 1983, pp. 121 to 138.

[27] H.B.Heiden, and H.C. Duffield
"Defense Data Network"
Proceedings of IEEE EASCON'82, 20-22 Sept. 1982, pp. 61 to 75.

[28] M.Corrigan
"DDN Interfacing Strategy"
Proc. of IEEE EASCON'82, 20-22 Sept. 1982, pp. 81 to 87.

[29] M.M. Matsubara, J.S. Luk, C.A. Campbell
"End-to-End Performance Objectives of the Datapac Network"
Proc. of the ICCC'84 (North-Holland)

[30] M. Gien, J.L. Grangé
"Performance Evaluations in CY CLADES"
Proc. of the ICCC'80

[31] P. Angosto and D. Bouesnard
"Performance measurement of the TRANSPAC Network"
In: Performance of Computer-Communications Systems. H. Rudin and W. Bux (Editors), Elsevier Science Publishers B.V. (North Holland) -IFIP - 1984.

[32] B. Alton; A. Potel, M. Purser and J. Sheehan
"The performance of a packet switched network - A Study of EURONET"
In: Performance of Computer-Communications Systems. H. Rudin and W. Bux (Editors), Elsevier Science Publishers B.V. (North Holland) -IFIP - 1984.

[33] N.B. Seitz
"User-Orientated Data Communication Performance Standards"
Comm. International, March, 1984

[34] G. Funk
"Message Error Detecting Properties of HDLC Protocols"
IEEE Transactions on Communications, Vol. COM-30, No.1, January, 1982

[35] J. Ma
"On the Impact of HDLC Zero Insertion and Deletion on Link Utilization and Reliability".
IEEE Transactions on Communications, Vol. COM-30, No. 2, February, 1982

[36] CIGRE - SC35 - WG01
"Operational and Functional Requirements for Telecontrol Systems"
June, 1980. Rev. 1981.

[37] CIGRE - SC35
"Guide for planning of Power Systems Telecommunication networks"
CIGRE - 1986

[38] IEC - TC57
"Design principles for telecommunication services for electricity supply systems"
March, 1986

[39] G.C. Kessler
"A Comparison Between CCITT Recommendation X.25 and International Standards 8208 and 7776"
IEEE Transactions on Communications, Vol.36, No.4, April, 1988.

[40] CCITT Recommendation X.25 "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuits", Fascicle VIII. 3, 1984

[41] ISO 7776 "Information processing systems - Data Communication-High-level data link control procedures - Description of the X.25 LAP-B - Compatible DTE data link procedures". ISO, 1985.

[42] ISO 8208 "Information processing systems - Data Communication X.25 packet level protocol for data terminal equipment", ISO, 1987.

[43] A. Indrehus and J. Hegge
"A Communication system for high-level data exchange between and within Norwegian control centers"
Proceedings of CIGRE - Paris, 1988

[44] ISO 7498 : 1985 / ADD.1, 1987
Information processing systems - Open Systems Interconnection -Basic Reference Model - Addendum 1: Connectionless mode transmission.

[45] J. Komulainen
"Application of the Packet-Switching Techniques for the Power Systems"
Proceedings of CIGRE Bournemouth Symposium - June - 1989

[46] ISO : 8073 : 1986
Information Procesing Systems - Open Systems Interconnection -Connection oriented transport protocol specification.

21 rue d'Artois - F-75008 PARIS