JPRS L/10139

25 November 1981

Worldwide Report

TELECOMMUNICATIONS POLICY, RESEARCH AND DEVELOPMENT

(FOUO 16/81)

FBIS FOREIGN BROADCAST INFORMATION SERVICE

NOTE

JPRS publications contain information primarily from foreign newspapers, periodicals and books, but also from news agency transmissions and broadcasts. Materials from foreign-language sources are translated; those from English-language sources are transcribed or reprinted, with the original phrasing and other characteristics retained.

Headlines, editorial reports, and material enclosed in brackets [] are supplied by JPRS. Processing indicators such as [Text] or [Excerpt] in the first line of each item, or following the last line of a brief, indicate how the original information was processed. Where no processing indicator is given, the information was summarized or extracted.

Unfamiliar names rendered phonetically or transliterated are enclosed in parentheses. Words or names preceded by a question mark and enclosed in parentheses were not clear in the original but have been supplied as appropriate in context. Other unattributed parenthetical notes within the body of an item originate with the source. Times within items are as given by source.

The contents of this publication in no way represent the policies, views or attitudes of the U.S. Government.

APPROVED FOR RELEASE: 2007/02/09: CIA-RDP82-00850R000400070054-1

JPRS L/10139

25 November 1981

WORLDWIDE REPORT

TELECOMMUNICATIONS POLICY, RESEARCH AND DEVELOPMENT

(FOUO 16/81)

CONTENTS

JAPAN

CONCEALED IMAGE TRANSMISSION METHOD DEVELOPED

Tokyo NIKKAN KOGYO SHIMBUN in Japanese 21 Sep 81 p 3

[Text] New Secure Communication Method Developed by Professor Tominaga et al of Waseda University; Industrial Espionage Throws Up Hands

In the field of facsimile, which is one of the three "divine objects" of OA (office automation), a new method of communication developed for the purpose of "keeping things secret" has been the topic of conversation recently. As the amount of information in society increases, many problems are expected to crop up. That is, there is urgent need for transmission of confidential documents by means of facsimile transmission, for measures to counter the theft of documents and "eavesdropping" on microwave millimeter wave transmission, and for protection of images (documents) transmitted which are of value to a third party. A new concealed image transmission method has been developed by a research group headed by Professor Hideyoshi Tominaga, Department of Electronic Communication, Faculty of Science and Technology, Waseda University. The "concealed image transmission method" developed by this group uses a format that may be called a "hidden image" conversion method. Secrets can be kept and certification (confirmation of document exchange) can be accomplished conveniently by this new method. It has caught the attention of many, because development of such software enables the confidential management of various "documents" according to their importance even after the OA document management has entered the paperless age.

Documents and Images Protected, Jumbled Transmission, Sharp Reception

Facsimile transmission is a method of transmitting images such as documents by electronic means over a distance to a receiver. The original document that is to be transmitted is scanned with a light, and the black and white density of the image is converted into electric signals. At the receiving end, the electric signals are converted back into the corresponding image. However, facsimile equipment used in an office is shared by many for economic reasons and is used for transmitting various types of documents including both confidential documents and open letters. Under such circumstances, if a document that must be kept secret can be transmitted with jumbled signals which can only be decoded by the rightful receiver with a certain key into a clear image (document), then the confidentiality of the document can be maintained.

There are many applications of this method. For example, it can be programmed to detect whether the seal of electronic mail has been broken by a third party or not, or only a portion of the document such as the signature may be concealed by the jumbled signals so that only the rightful receiver is able to reproduce the signature. Thus, the transmission of documents which could be of value to a third party, such as tickets, entrance tickets, and checks, can also be carried out, and "many other new uses may crop up," says Professor Tominaga.

The basic principle of the method is as follows: the arrangement of the image (letter) point and the arrangement of black and white are mixed up so that the rearranged signals have the appearance of a jamming signal. The change in arrangement can be accomplished by changing the order of scan lines according to a random number generator and repeating this pattern periodically. In an actual machine, this becomes part of the logic inside the shift register before codification.

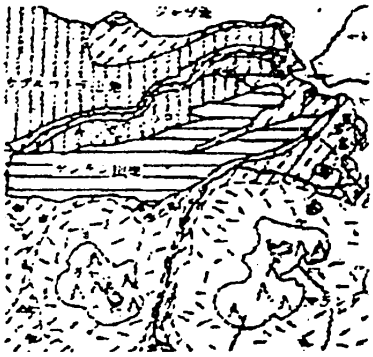
The decoding key used by the receiver for reproduction of the image consists of the same random number generator. With this key, a register logic which is the reverse of the transmitter is created so that the scan lines are restored to their original arrangement.

There are infinite variations of this rearrangement scheme, and if the period of random number generation is increased, the process required to decode it also increases proportionately. However, the standard proposed by the CCITT (Consultative Committee for International Telephone and Telegraph) is centered around a technology which is aimed at shortening the fascimile codification of the image information in order to imrpove the circuit efficiency. A technology in which the random number generation is made more complex runs counter to the effort to make codification more efficient. Therefore, the problem is how to reconcile these two. That is, the algorism for arrangement change must be decided by the codification efficiency and the content of the document.

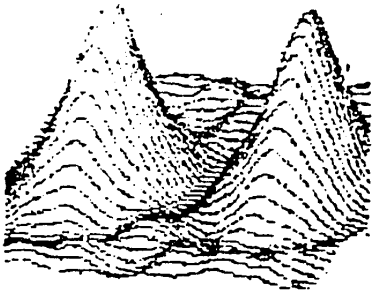
The method for arrangement change may be varied according to the degree of secrecy desired. One of the methods is called shuffling. The original manuscript (Figure A) is shuffled into random order by a single scan line as in shuffling a deck of cards (Figure B); or points may be rearranged on the same scan line (Figure C); or points may be rearranged between different scan lines (Figure D); or blocks may be rearranged as a unit. [Figures not reproduced] This process of randomly changing the arrangement is called scrambling. The scrambled signals appear to a third party as nothing but noise.

Concealed image transmission is a method of transmission of a more advanced degree than the scrambled signals. The signals transmitted by this method consist of the scrambled signals of a confidential document superimposed on the normal signals of an ordinary document. Unless one knows the decoding key, the signals appear to him as an ordinary transmission with garbles. "As the algorith for removal of garbled information in order to improve the image becomes more commonplace in the future, the unsuspecting third party will throw away a large quantity of concealed images disguished as garbles," says Professor Tominaga.

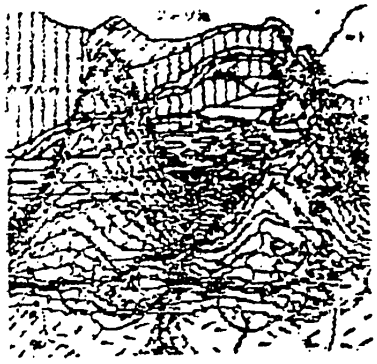
Reproduction of this concealed image is achieved by turning it over so to speak, that is, by interchanging the position of an apparent image on the front with the



=①=



=②=



=③=

[Drawing] To transmit a manuscript (1) by means of concealed transmission, (2) is superimposed on (1) and transmitted; the output of this transmission is shown in (3).

hidden image on the back. Thus, by reversing the arrangement order of the front and the back, the image on the front becomes scrambled while the image on the back becomes unscrambled. The concealed image may consist of a superposition of several sheets of images or just a single sheet. In the case of a single sheet of image, the key section of the document such as the signature may be scrambled and scattered in the form of garbles somewhere in the document.

Certification may be cited as another effective application of the concealed image transmission method. Certification is a process of confirming receipt of a document by the receiver. An additional scrambled image is superimposed onto the scrambled signals of the document which is being transmitted. After the rightful receiver has decoded the scrambled signals with an appropriate key, the reproduced additional image is then sent back to the original sender. Thus, certification can be carried out smoothly if the sender and the receiver make arrangements beforehand.

The high speed facsimile machines used today are standardized by the CCITT as G-III (Group III). The next generation of G-IV facsimile machines reportedly will be facsimile machines with an internal memory. The purpose of having a memory is to increase the effective utilization of the circuit and to transmit a larger volume at a higher speed. With the memory function available, the technique of superimposing several images which is essential in the concealed image method can be introduced easily and the application of software for confidential transmission can be accomplished. Furthermore, in the future, when all documents and information are stored in the computer memory and the so-called "paperless office" is a reality, the equipment itself can be shared by everyone, with the confidential and non-confidential documents intermixed. In such circumstances, the document management can be easily carried out by takint appropriate secret protection measures in accordance with the degree of confidentiality. Meanwhile, communication by such means as microwave and millimeter wave is expected to grow in the future because of the low equipment cost per circuit. Aside from military secret communications, other users of communications via electronic waves are beginning to attach importance to the concealed communication technique.

Finally, this group plan to present a paper describing their results at the "International Symposium on Image and Document Communications" in Paris in November.

9113
CSO: 4106/11

ITALY

MODULAR EQUIPMENT FOR PACKET SWITCHED DATA NETWORKS

Turin ELETTRONICA E TELECOMMUNICAZIONI in Italian May-Jun 81 pp 126-130

[Article by N. Corsi and L. Musumeci*]

[Test] Summary--Modular Equipment for Packet Switched Data Networks. This paper points out the basic choices for the design of network equipment to be used in packet switched networks. Considering the wide range of system requirements, the approach based on the availability of modular blocks has been chosen and investigated. The paper shows how it is possible to interconnect the building blocks in order to best fulfill network requirements. A packet adapter concentrator (ACP) for X28 and X25 data traffic has been developed and tested. The ACP is a single processor equipment based on a general purpose CPU and dedicated communication units. The ACP is described in more detail from the hardware and software point of view.

1. Introduction

The first Public Data Networks, based on the packet-switching technique, went into service in the second half of the 1970's. The standardization activity successfully carried out by the concerned international organisms, particularly by the ISO (International Standard [as published] Organization) and by the ICCTT (International Consultative Committee for Telegraphy and Telephony), has made it possible to obtain a range of Recommendations that have created the premises for having available, in the near future, a world-level Data Network, like what has come about for the telephone service and the telex service.

These decidedly positive results have led several Administrations in Europe to adopt the packet technique for constructing Data Networks, to be opened to public service in the beginning of the 1980's.

The packet networks furnish "Virtual Circuits" that can be defined as logical associations between pairs of terminals, by means of which it is possible to exchange, through the network, packet-structured data information.

---

* Doctor of Engineering Norberto Corsi of the CSELT (Telecommunications Research and Study Center), Turin; Doctor of Engineering Luigi Musumeci of ITALTEL. Typescript received 12 February 1981. Paper presented to the 28th International Communications Conference of Genoa.

The characteristics of the virtual circuits are defined by Recommendation X25. Two basic communication services are offered in particular by means of virtual circuits:

1) Virtual Calling, by which, and analogously to what happens in circuit switching, a virtual circuit is temporarily established between two terminals by means of exchange of suitable signaling packets with the network.

2) Permanent Virtual Circuit, by which two terminals are permanently associated through a virtual circuit. This service is similar to that offered by means of dedicated connections of point-to-point type.

While on the one hand there is a growing demand for data services, on the other hand, users are having to cope with problems today relative to exchange of information between terminals having different formats, codes, transmission speeds, etc.

Because of its intrinsic nature, which involves "store and forward," the packet-switching technique seems to be the most flexible, in terms both of performance characteristics and cost, for solving these problems.

This article describes how, starting with appropriately chosen modular structures, it is possible to construct the network equipment necessary for providing a packet-switching service open to the ongoing technological development and to the use requirements in terms of new applications.

The solutions described make reference to the results of studies and experimentation carried out in collaboration between the CSELT and ITALTEL.

2. Network Configuration

In the Data Network, the essential functions to be performed are those of concentration and switching. In addition to these, it is also necessary to take into account the functions of management and control, which make it possible to keep, in time, the available resources at a high level of efficiency and to manage the development of the network in a coordinated manner.

Generally speaking, the concentration function is carried out in the peripheral part of the network so as to achieve savings in the transmission lines. This function is often associated with that of adaptation of the nonpacket terminals; this makes it possible to transfer into the access network the heavy task of support of the various protocols and thus to lighten the load on the nodes with which it is most convenient to interface with unified protocols of type X25.

The nodes--both terminals and transit nodes--provide for switching the packets and directing them to the destination requested in accordance with the routing strategy chosen.

The management and control philosophy depends fundamentally on the dimensions of the network and on its architecture. In the context of a public network with broad geographical coverage and organized in at least a two-level hierarchy, it is considered more advantageous to go with a hierarchical structure, in which various peripheral centers are available, coordinated by one or two primary centers positioned at the highest level of the network. In short, the control and management functions pro-

vide for gathering and transporting to the center the data for carrying out the operations of charging, continual testing of the state of the network, gathering of data for statistics, and signaling of breakdowns occurring in the equipment.

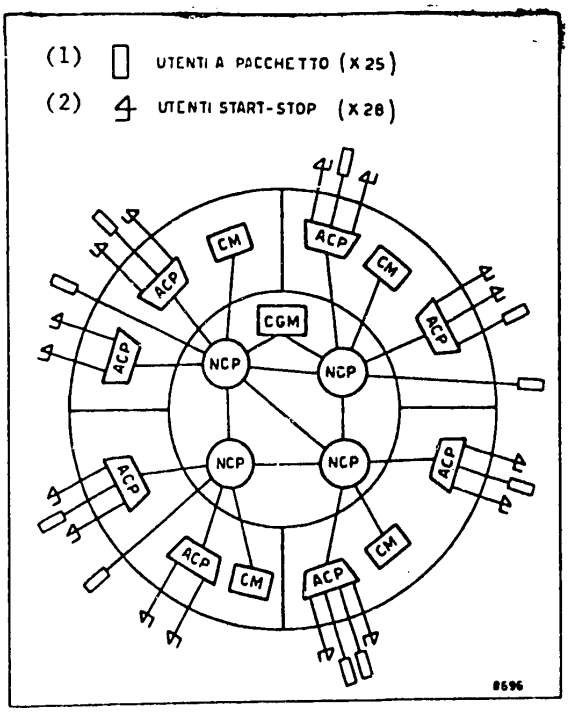


Figure 1. General structure of the network referred to. ACP = Packet Adapter Concentrator; NCP = Packet-Switching Node; CM = Maintenance Center; CGM = Management and Maintenance Center.

Key:
1. Packet users
2. Start-stop users

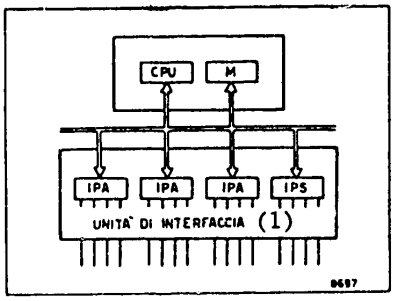


Figure 2. Monoprocessor structure. CPU = Central Processing Unit; M = Memory; IPA = Asynchronous Protocols Interface; IPS = Synchronous Protocols Interface.

Key:
1. Interface units

In addition, the management centers are capable of carrying out operations relative to topological changes and network reconfiguration owing to breakdowns and overloads.

Figure 1 shows the reference-network structure. The equipment considered can be classified as follows:

1) Packet Adapter Concentrators (ACP), normally placed in the access network and to which the user lines are connected;

2) Packet-Switching Nodes (NCP): terminal switches or transit switches for the purpose of being able to construct different network structures;

3) peripheral Maintenance Centers (CM) and primary Management and Maintenance Centers (CGM).

3. Structure of the Network Equipment

A structure-design objective for achieving the functions required of packet-switching networks should provide for a single "system" with such flexibility as to be able to configure all the necessary items of equipment with the capacity desired. The technical and economic advantage resulting from a solution of this type is indeed quite obvious.

The present state of the technology, which has introduced the microprocessor on a vast scale and has enormously reduced the cost of memories, has made this approach possible. The availability of processing units at extremely low cost has oriented design toward objectives such as:

a) functional modularity, for the construction of distributed and therefore flexible systems;

b) modularity of the processing capacity, for construction of economically viable systems, of both small and large dimensions;

c) modularity of the reliability assignable to the systems, by providing them with the quantity of redundance required by the degree of service of the particular application.

In short, the technical solution that meets with greatest favor today provides for development of units based on microprocessors specialized for handling particular functions (for example, management of a particular protocol, switching of individual packets, etc) and interconnected in a wide variety of configurations.

In our case, the aforesaid units constitute the "basic subsystems," comprising a processor, the memory related to it, and the associated terminals and interfaces (Figure 2).

The fundamental component was chosen in accordance with the criterion of being able to develop the ACP equipment with a single subsystem and to use a large number of subsystems, appropriately interconnected, for higher-level functions and greater traffic capacity. This is because of the fact that it was considered advantageous to exploit the economy and efficiency of single-processor structures in the peripheral area of the network where the traffic is less concentrated.

As regards the Central Processing Unit adopted, products of the PDP 11 family of microprocessors were decided on, while the Interface Units for the various line terminations were specially designed for the purpose. This structure makes it possible to manage up to 64 user terminals, with a mixed traffic of characters and packets up to 40 packets/sec (on the assumption that each packet is made up of 64 characters).

This modularity permits a vast range of applications in the peripheral area of the Data Network. Interconnection of several subsystems (modules provided with CPU, memories, and appropriate interfaces) makes it possible to obtain increasingly complex structures so as to construct equipment that can be used as terminal nodes and as transit nodes for processing capacities of several hundred packets per second.

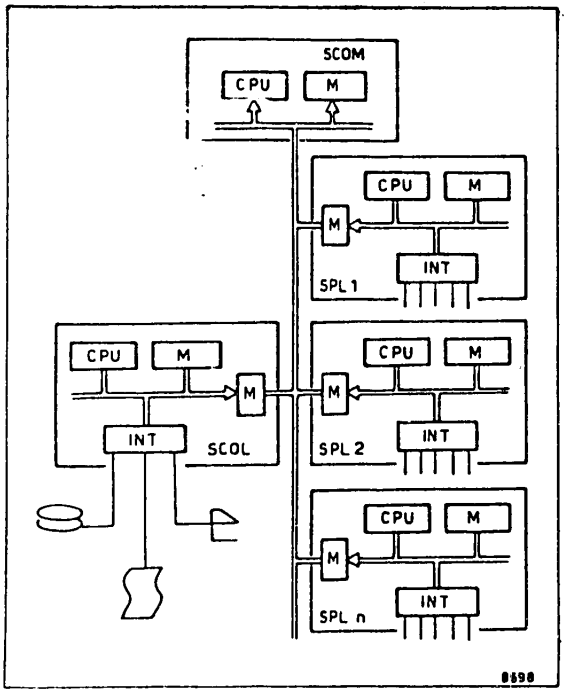


Figure 3. Multiprocessor structure. SCOM = Communication Subsystem; SCOL = Subsystem for Management of Connections; SPL = Subsystem for Handling Line Protocols; INT = Line Interface.

The most important aspect in the designing of a system of this type (multiprocessor) is to assign the functions to be carried out to the various subsystems in such a way as to optimize the traffic handled. In particular, in order to achieve, within acceptable limits, a linear growth of traffic capacity manageable with the growth of the number of subsystems involved, it is necessary to keep the processes with a high degree of information exchange within the subsystem itself as much as possible.

Figure 3 presents the block diagram of a multiprocessor structure whose subsystems can be reduced to the following three types:

1) Subsystems for Handling the Line Protocols (SPL): it is obviously necessary to use a large number of SPL's, with the load distributed uniformly so as to optimize the utilization of the available resources.

2) Subsystem for Management of Connections and for control and management of the network (SCOL). These functions are not critical from the point of view of processing capacity, but they do require considerable memory capacity and can be centralized in a single subsystem.

3) Communication Subsystem (SCOM) for interconnection of the SPL's with one another and with the SCOL subsystem. This function can be fulfilled in a satisfactory manner through the use of a processor-type control. This solution was considered an efficient one by comparison with other methods such as the use of a global common memory, which entails excessive access conflicts when the traffic is high, or the use of the common-bus TDM technique, which involves a rather complex logic in the individual SPL's.

In order to ensure high availability of the system, redundance elements must necessarily be introduced; in particular:

1) full duplication, of the "hot stand-by" type, of the centralized subsystems (SCOL and SCOM);

2) SPL-subsystems redundancy of the n + 1 type.

Redundancy between the duplicated subsystems is provided for by means of parallel interfaces directly connected for transfer of synchronization and exchange messages.

The interconnection of the SPL and SCOL subsystems with the communication subsystem (SCOM) is by means of exchange of packets on a common memory. The duplicated structures are connected to the unduplicated subsystems through appropriate bus switches of very high reliability.

4. First Prototypes

The definition of the structure described above was achieved by use of the results of the following work:

1) simulation of the procedures in increasingly complex structures;

2) development of the most important modules of the software structure;

3) fabrication of the ACP, which, as stated earlier, constitutes the basic subsystem of the architecture proposed.

Further work will be related to development of nonpacket synchronous protocols, the making of multiprocessor prototypes, development of remote-management centers. More detailed information on the ACP already developed is given below.

The ACP is an apparatus composed of a Central Processing Unit (CPU) of general-purpose type and specialized Communication Units which, under the control of the software, carry out the functions of adaptation of the user data to the packet protocol of the network and of concentration of these data at the junctions for connection to the node.

The ACP was built in two equipment layouts. The first makes it possible to hook up 64 asynchronous lines up to the speed of 1,200 bits/sec, for a maximum traffic ca-

pacity (throughput) of 15 packets/sec; the second makes it possible to hook up 48 asynchronous lines of the above type and 4 synchronous lines up to the speed of 9,600 bits/sec, for a maximum capacity of 40 packets/sec. Various mixed equipment layouts are possible, within the limits of the maximum traffic capacities, simply by variations in the wiring of the apparatus.

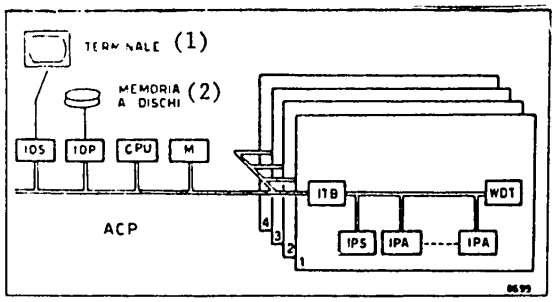


Figure 4. Block diagram of the Packet Adapter Concnetrator (ACP). IOS = Serial Input/Output Interface; IOP = Parallel Input/Output Interface; ITB = Bus Interface; IPS = Synchronous Protocols Interface; IPA = Asynchronous Protocols Interface; WDT = alarm circuit (Watch-Dog).

Key:
1. Terminal
2. Disc memory

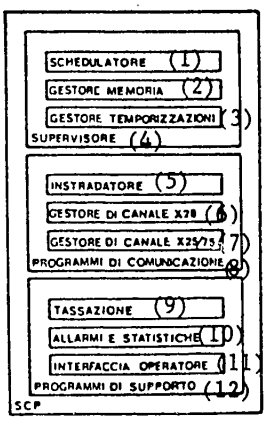


Figure 5. The software system for Packet-Switching (SCP) of the ACP.

Key:
1. Scheduler
2. Memory manager
3. Time-sharing manager
4. Supervisor
5. Router
6. X28 channel manager
7. X25/75 channel manager
8. Communication programs
9. Charging
10. Alarms and statistics
11. Operator interface
12. Support programs

Transfer of data between user terminals and ACP is by use of protocols conforming, respectively, to Recommendation X28 for asynchronous terminals and Recommendation X25 for synchronous terminals. For both installations, the connection to the switching node involved is by means of 4 junction lines of synchronous type with maximum speed of 9,600 bits/sec. Transfer of data between ACP and Node is by use of a protocol based on Recommendation X75 of the ICCTT.

The following units are shown in the block diagram of the ACP in Figure 4:

1) Central Processing Unit (CPU), for all the data-processing and communications-management functions. It consists of a Digital PDP 11/23 miniprocessor that permits interconnection of external units on its own internal bus;

2) Communication Units, for the data input/output functions and for the lower-level processing provided for by the protocols. They consist of modules, organized in 4 groups which, by means of appropriate bus extension plates (ITB), are connected directly to the bus of the Central Unit. Each module can terminate 4, 2 or 1 lines or junctions, depending on the type of protocol used on the line and the type of access to the central memory. In particular, there are 4-line modules for asynchronous interfaces, 2-line modules for synchronous interfaces with interrupt access, and 1-line modules for synchronous interfaces with direct memory access.

The software of the ACP equipment group is composed of two systems:

1) the Packet-Switching Software (SCP) system for real-time execution of the network functions residing in the ACP itself;

2) the Maintenance system (M) for off-line execution of diagnostic and testing procedures.

The SCP system (Figure 5), in turn, is designed in terms of three subsystems:

a) Supervisor, for management of the resources and coordination of the processes;

b) Communication Programs for traffic management;

c) Support Programs for supervision of the ACP and for network-management functions.

The Supervisor comprises the following modules:

1) the Scheduler, which provides for synchronization of the processes and assignment of the CPU's time to the processes themselves;

2) the Memory Manager, which provides for dynamic assignment of the memory areas for temporary memorization of the characters and packets as well as of the data exchanged between processes;

3) the Time-Sharing Manager, which provides for management of the meters associated with the time-sharings put into the ACP.

The Communication programs comprise:

1) the Channel Managers: program modules for management of the virtual connections (formation and killing) and for control of the data flow through the connection itself;

2) the Router: program module responsible for association between input and output lines for each of the virtual connections required, and depositary of the configuration of the ACP (lines hooked up, in service, out of service, etc).

The Channel Managers so far developed relate to the X28 protocol for asynchronous terminals, the X25 protocol for packet terminals, and the X75 protocol for junction lines: the program modules reproduce, as regards structure also, the typical multilevel structure of the recommendations involved. The Channel Managers communicate with one another through internal interfaces; the mechanism that provides for these interfaces is a code system to which the managers accede through the Scheduler.

Finally, as regards the Support Programs, the following modules have been provided:

1) the Charging-Block Manager: the data used for generation of the charging blocks are detected by the Channel Managers and transferred to the Network Management and Maintenance Center, using a logical channel devoted to this purpose;

2) Alarms and Statistics Managers: provides for collecting information on the state of the ACP and forwarding it to the operator (local or remote) or to the Management and Maintenance Center;

3) Man-Machine Interface: this module manages the operator-machine dialogue, which can be both local and remote (from a Maintenance Center [CM] or from the Management and Maintenance Center [CGM]--see Figure 1).

5. Conclusions

The choices made for constructing equipment to be used within the framework of Packet Switched Data Networks have been illustrated. The basic structure, already built with a single processor, is that which carries out the function of adaptation of nonpacket terminals and of concentration of the data traffic. Multiprocessor structures can be built, starting with the basic structure, in accordance with the guidelines discussed in this paper and with a modular approach, for both the hardware and the software, covering the entire spectrum of functions and capacities required even by networks of considerable complexity and large dimensions.

BIBLIOGRAPHY

1. ICCTT Recommendations X3, X25, X28, X75; Study Group VII, Geneva, February 1980.

2. Roberts, L.G., "Packet Network Design--The Third Generation," IFIP Congress 77.

3. Kelly, P.T.F., "Public Packet Switched Data Networks, International Plans and Standards," PROCEEDINGS OF IEEE, Vol 66, No 11, November 1978.

4. Halsey, J.R., Hardy, L.E., and Powning, L.F., "Public Data Networks: Their Evolution, Interfaces and Status," IBM SYSTEMS JOURNAL, Vol 18-2, 1979.

5. Micciarelli, A., and Mossotto, C., "Technical Aspects in the Implementation of a Public Switched Network for Data," International Switching Symposium, Paris, 1979.

11267
CSO: 5500/2311

END