PAXNET

AN INTRODUCTION

PAXNET

AN INTRODUCTION

PAXNET Report Class 1, No. 2,
Revision 2.00, October 1986.

KEYWORDS

PAXNET, Class 1, Introduction, Hardware components, Software structure, Development plans, Value-added services, Revision 2.00, October 1986.

ABSTRACT

This report is intended as an introduction to PAXNET. The main services are described and some technical aspects of the hardware and software components are introduced.

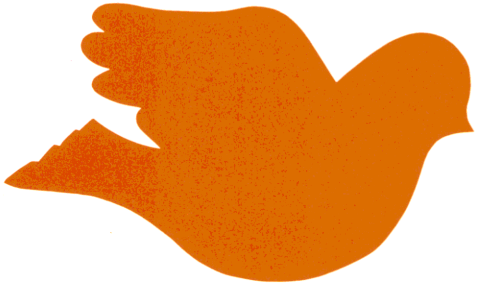


Table of Contents

Intended Reader Audience

This document is intended as a brief introduction to the PAXNET data communications system, for readers in quest of a survey of the PAXNET components and services. In this report the reader will be able to obtain the following information:

Scope of report

- A general survey of the PAXNET hardware and software components.
- An introduction to the basic services provided by PAXNET.
- A description of the protocols supported for terminal attachment and host computer interfacing.
- A description of the ISO/OSI protocols supported by PAXNET.
- A description of the PAXNET design concept and a statement of direction describing future services and components.

It is assumed that the reader audience has a general knowledge of informatics and some knowledge of data communications.

Readers in search of more detailed information on specific items may find this in the documentation describing the particular systems. Please refer to appendix B for a list of the currently available PAXNET documentation.

Introduction 1.

PAXNET is a versatile data communications system intended to provide efficient data communication services. The PAXNET product is primarily intended for public telecommunication providers, and private high capacity corporate networks.

The main service provided is a packet switching data transport system with access protocols as defined by the CCITT X.25 (and X.28) recommendations.

PAXNET also supports a number of industry standards and internationally standardized protocols, and is therefore the ideal foundation for important value-added and corporate network services. Furthermore PAXNET is committed to adhere to the ISO protocol standards for Open Systems Interconnection (OSI).

PAXNET incorporates the latest data communications technology to provide the optimal utilization of transmission media and techniques. The hardware consists of specially designed switching nodes. The software is developed in a high-level language, which provides resilient and maintainable software components.

This document is intended to provide an introduction to PAXNET. Initially, the history of PAXNET, the overall design considerations, and the current installment base will be described in chapters two to four of this report.

Outline of report

Chapter five describes how user equipment may be connected to PAXNET. The chapter enumerates the various protocols and interfaces supported by the PAXNET network access service.

Chapter six deals with the internal packet switching data transmission systems.

Chapter seven delineates the key issue of the Network Management facilities provided by PAXNET.

Chapter eight contains an introduction to the main hardware and software components of PAXNET.

Finally, chapter nine outlines the development plans and portrays the direction of the current development efforts in PAXNET.

The History of PAXNET 2.

Joint venture 1979

The PAXNET project was initially started in the autumn of 1979. It is a joint venture, comprising the two major Danish telephone companies, namely the **Copenhagen Telephone Company** (KTAS), the **Jutland Telephone Company** (JT), and the Danish computer manufacturer, Regnecentralen - internationally known as **RC Computer.**

PAXNET is operated and marketed nationally by the Danish telephone companies. International sales and customer support are carried out by RC Computer in cooperation with the Danish telephone companies.

RC Computer provides the packet switching hardware, the main part of the system software, and the network management system. System engineering and system design is performed jointly by RC computer and the telephone companies.

Lately the cooperation has been extended to include **CASE PLC,** the British manufacturer of data communications equipment. This cooperation is an indirect result of the ESPRIT project **CARLOS.** Within the PAXNET system CASE provides concentrators (Packet Assembler/Disassembler (PADs)) for the attachment of simple asynchronous terminal types to the X.25 service.

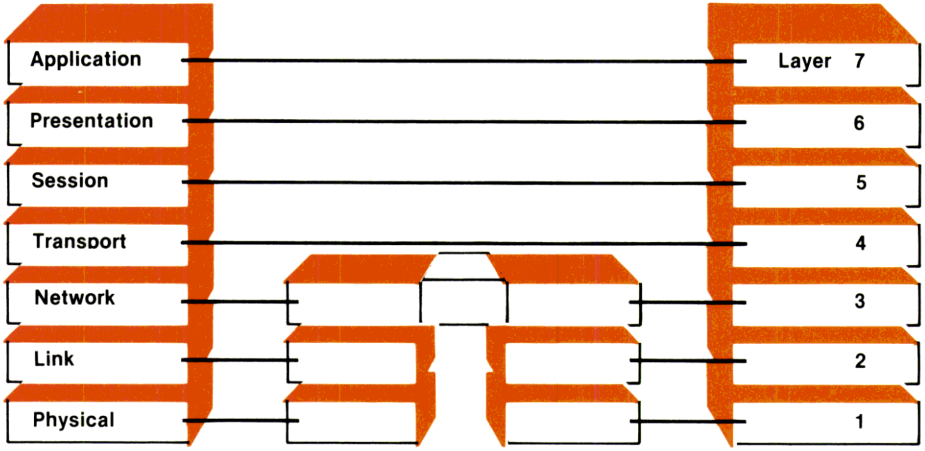
The PAXNET project was launched with the mission of providing an efficient data communications facility for internal use by the Danish telephone companies. It soon became apparent, however, that the resulting product had a wide market appeal. Therefore, the PAXNET product was marketed internationally in 1982.

To achieve the highest degree of vendor independence, strict adherence to CCITT and ISO international standards has been a natural requirement, whenever possible. As such, the software system is designed within the general framework of the ISO Reference Model for Open Systems Interconnection (OSI).

X.25 - 1981

As the name implies, the network belongs to the packet switching family. Therefore, the first phase of the project naturally included an initial network service with an X.25 access interface. The service is internally based on a highly efficient packet switching network, including facilities for end-to-end control of the internal data streams. This facility was completed in June 1981.

The next development step was completed at the end of 1982. This included an ECMA transport layer service and an ECMA session layer service. Advanced network management services were also implemented during this period. Based on these facilities a number of application systems have been launched.



ISO/OSI Reference Model framework for PAXNET architecture.

First application 1984

Among the first applications using the network during 1984 was a nationwide public Alarm Control Service intended for the transmission of service messages to and from private homes, offices, and industrial sites.

Terminal network 1986

As mentioned, one of the primary purposes of PAXNET was to provide an efficient, vendor independent, internal data communications infrastructure within the Danish telephone companies. By 1986 more than 1000 terminals, a number of different host computers, and various other equipment types (see chapter four) are interconnected by PAXNET.

Up to 1986, public data communication facilities have been provided by the Danish PTT, mainly as leased lines or through the Public X.21 circuit switched network (DATEX). Danish government regulations barred the telephone companies from providing public data communication services. In 1986 a new law was passed, and by 1987 PAXNET will be launched as a public data communications service in Denmark.

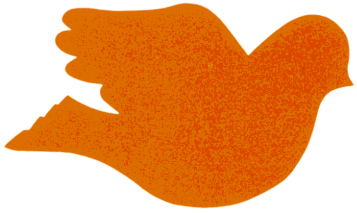
Public network services

PAXNET is also installed in Greenland, where it will be used both for the public X.25 service (KANUPAX) and for internal use within **Greenland Telecom.**

Initially, PAXNET will provide public X.25 and X.28 services. Current plans also include a number of value-added services, however, to be provided for public use, for instance 3270 terminal service, file transfer service, and electronic mail.

The forthcoming second generation Videotex system in Denmark will also utilize the X.25 service of PAXNET with access through special Videotex PADs.

As described in chapter four, the basis of these public services is a nation-wide installation of more than two hundred node computers operated by the regional telephone companies in Denmark.



ktas

Jydsk Telefon

Regnecentralen

The companies behind PAXNET.

Future trends

PAXNET will continue to evolve in response to new technologies and new user demands. This evolution is currently ensured by the following factors:

- PAXNET is designed, implemented and used by the Danish telephone companies. These companies are obliged to follow new standards from not only CCITT, but also CEPT and ISO. Furthermore the telephone companies are obliged to introduce new public services as for instance Message Handling (electronic mail), Videotex and FTAM. PAXNET will evolve in response to the demands imposed by these new service.

- The consortium members behind the PAXNET development have been awarded a two year development contract by the European Economic Community under the ESPRIT programme to enhance the data communications infrastructure of ESPRIT. The developments are a part of the Information Exchange Systems of ESPRIT. The project has been named CARLOS (Communication ARchitecture for Layered Open Systems). A short description may be found in reference (14). This places PAXNET in the mainstream of the European development within the field of data communications.

The Main Design Considerations 3.

This chapter provides an introduction to the fundamental design considerations behind the overall architecture of the PAXNET system.

The goal of the PAXNET architecture is to design and implement a data communications system with the following main characteristics and qualities:

Design highlights

- Access interfaces conforming to international standards and recommendations. This implies the implementation of CCITT recommendations, and ISO and ECMA standards.

- Access interfaces and gateway functions with support of the major industry standards for example IBM 3270 compatible devices.

- A highly efficient data communications network with dynamic adaptive routing, including internal end-to-end control mechanisms.

- A network management system integrated in all network components and modules, supervised by one or more Network Management Centres (NMC).

- A basic switching element (network node) which is small, flexible and of low cost, thus allowing a high degree of distribution and gradual extension of capacity.

- Hardware components which fit into the *telephony environment*, e.g. installation in telephone exchange racks, interconnection to Pulse Code Modulated (PCM) interfaces, etc.

- A software system which is easy to develop, maintain, and modify. This has led to an extremely modular design and the use of a high-level language at all software levels.

- Flexible hardware and software, based on modularity, to ensure that single components may be changed or upgraded.

- A user friendly interface to the network management system that may be expanded and modified in a simple manner.

Being based on these criteria of design and implementation, PAXNET has become a highly versatile and efficient data communications product.

PAXNET Installment Base 4.

PAXNET has been in daily operation since 1982. The current installment base of more than two hundred nodes in Denmark, vouches for the quality and the matureness of the PAXNET product. The daily operation of the network has provided the development team with invaluable experience and feedback to continously improve the quality of the PAXNET product.

Danish public data network

The first physical implementation of PAXNET networks was in the regions of Denmark covered by the two major Danish telephone companies, Copenhagen Telephone (KTAS) and Jutland Telephone (JTAS). The networks in these areas are continuously being expanded as new facilities are included and new groups of users are connected. Within the last years the network has been augmented to include the Funen Telephone company (FT), and to Greenland.

As mentioned above the current installment base entails more than two hundred network nodes. The relatively small size of the node processors has made this high degree of distribution possible, which in turn provides a number of advantages and opportunities. Especially the large number of network access points and the high degree of redundancy provided should be stressed.

For the moment the network provides the following services and interfaces:

- X.25 service according to the CCITT recommendations 1980 version (see section 9.1 for updates to 1984 version).
- X.28 start/stop terminal support with PADs according to the CCITT recommendations 1980 version (X.3, X.28, X.29).
- X.75 internetwork facility based on the CCITT recommendation 1980 version.

Current services

- 3270 support of terminal clusters and hosts. Currently used internally at the telephone companies approximately 1000 terminals and printers are connected via PAXNET to various hosts, e.g. IBM, Honeywell DPS8, CDC Cyber, Tandem, RC8000. Currently this connection is achieved by use of the 3270 BSC protocol; SNA/SDLC will be in operation by late 1987.

- A publically available Alarm Control Service, which employs the X.25 service to transfer alarms and control information.

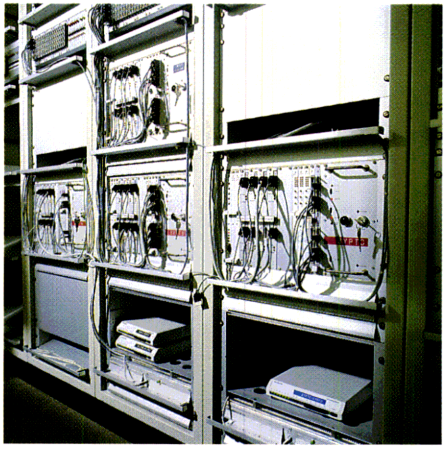
- A special X.25 version for use in connection with the Ericsson series of digital (AXE) telephone exchanges. This interface is used for supervision and maintenance of a large number of digital exchanges.

- CCITT Signalling System 7 interface (1980 version) used for supervision and for collection of account information from the digital DICON/DICEN series of telephone exchanges.

- A file transfer facility according to the UK *Blue Book* specification. The ISO File Transfer (FTAM) protocol is currently being implemented.

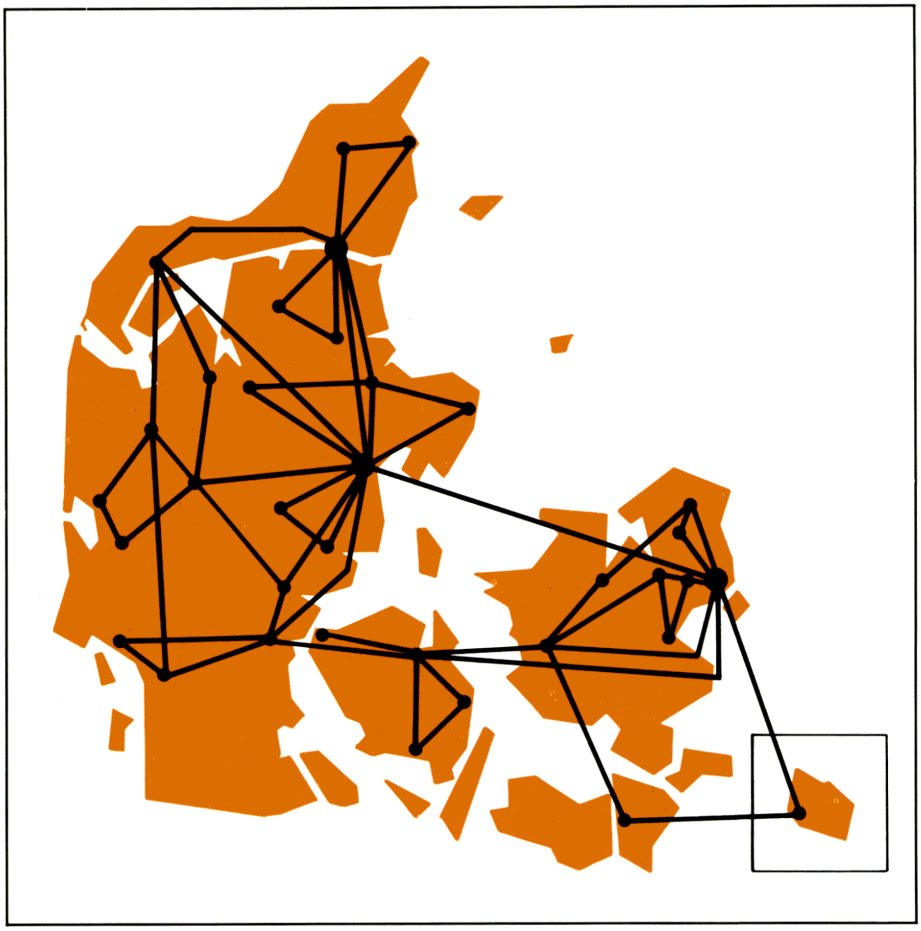
- A number of host interfaces towards various mainframe computers.

1 2



1. *Node installed at telephone exchange.*

2. *Network operations centre.*

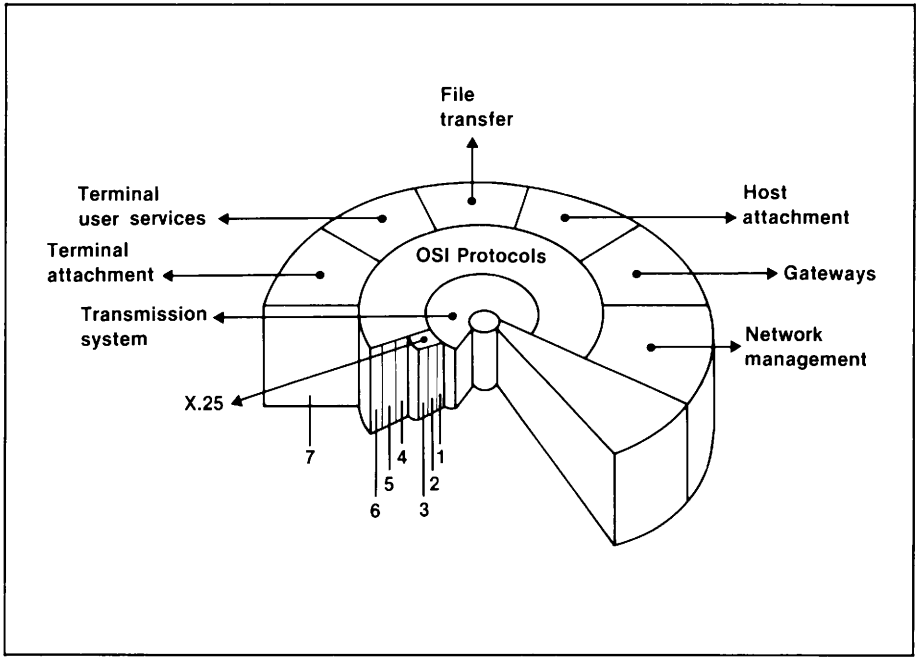


Topology of Danish network.

High availability is ensured by a number of Network Management Centres manned with network operators.

The current topology of PAXNET in Denmark is shown in the figure. The network configuration entails more than 200 network nodes geographically distributed in accordance with the user distribution.

Network Access Services 5.



PAXNET Value-added services.

Users may gain access to the PAXNET services through a number of different interfaces depending on the type of services required and the type of equipment in question. This chapter describes the various types of network access services provided by PAXNET.

Two distinct types of access services are available:

- Standard services as recommended by the standardization organizations, for instance CCITT, ISO, ECMA, etc.

- Services included to provide interconnection of vendor specific equipment.

Both types of services are important. The first because it provides an interface in accordance with widely accepted international standards and recommendations (X.25, X.28, etc.).

Value-adding

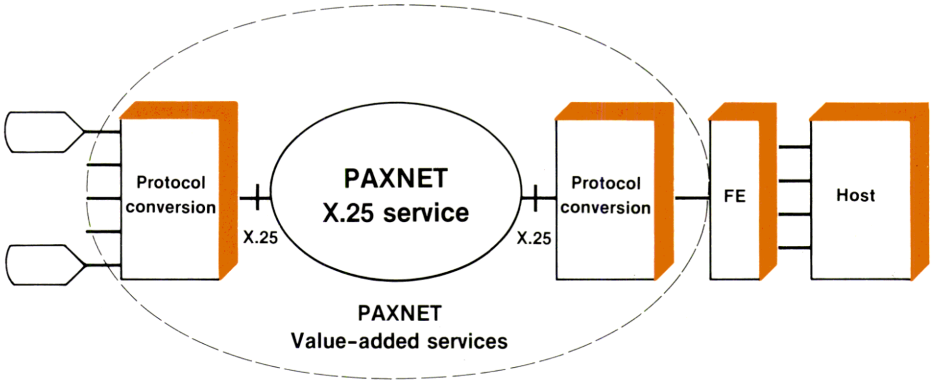
The second because most users quickly discover that a more intelligent, or value-added, service to provide interworking is required. One of the reasons for this is that most equipment available on the market today does not provide a standard communication interface. Therefore the user must extend his system with conversion software to conform to the interfaces provided by the network.

In case of a value-added network service, the network takes care of the protocol conversion, i.e. the conversion software is placed in the network instead of in the user equipment. This type of service is said to be value-added, because it *adds* to the basic task of interconnecting equipment facilities to ensure interworking of this equipment.

Currently the most important value-added services are used to provide interfaces towards vendor-specific protocols and systems. For example towards IBM 3270 compatible systems. Value-added services for enhanced network services in accordance with international standards for Electronic mail and file transfer will become more and more important within the next couple of years, however.

PAXNET also supports value-added services for access control, user validation terminal services and multiple simultanous sessions.

Protocol conversion as value-added service.



5.1 X.25 ACCESS SERVICE

PAXNET provides an X.25 access service according to the CCITT recommendation of 1980. The related CCITT recommendation X.2 describes a number of parameters and options which are applicable to the X.25 service. The technical details describing these parameter settings are described in detail in reference (5).

In short the X.25 service may be described as follows:

X.25 service (1980)

- Data is sent in packets with a predefined maximum length. The current default value is 128 bytes.

- User interconnection is established either through Switched Virtual Circuits (SVC) or Permanent Virtual Circuits (PVC).

- Users are identified by fourteen digit addresses as described in the CCITT recommendation X.121.

- A number of (additional) facilities may be subscribed, either for use during a certain period of time, or for request on a per call basis. These facilities described in the CCITT recommendation X.2 include:

  - closed user group,
  - non standard packet size,
  - reverse charging.

- Currently PAXNET supports all X.2 facilities marked "essential". Furthermore most facilities marked "additional" are available.

- The interconnection to other X.25 networks (national and private) is established through the service specified in the CCITT X.75 recommendation.

X.25 (1984)

The CCITT ratified late in 1984 a revised version of the X.25 protocol. The revised PAXNET software to support this version of X.25 will be completed by 1987.

5.2 X.28 START/STOP TERMINAL SERVICE

X.28 service (1980)

PAXNET provides an interface for X.28 start/stop (asynchronous) terminals in accordance with the CCITT recommendation of 1980. This service is implemented using autonomous PADs allowing a high degree of the geographical distribution of attachment points in response to the user distribution.

PAD service

In brief the main characteristics of the PAD service are:

- Support of start/stop mode terminals according to the X.28 recommendation.
- Support of call-in terminals connected via the Public Switched Telephone Network.
- Support of call-in/call-out terminals connected via leased lines.
- Support of bit rates from 50 to 19,200 bps with automatic clock setting up to 9,600 bps. However, service for terminals connected via the Public Switched Telephone Network is limited to the bit rates and modulation principles determined by the modem types in use.
- Support of the facilities described in recommendation X.3.
- Support of the exchange of control information and user data between the PAD and a packet mode DTE according to the X.29 recommendation.
- Support of Switched Virtual Circuits at the X.25 level.
- Support of Closed User Groups at the X.25 level.

X.28 (1984)

An updated version of the PAD software corresponding to the 1984 CCITT recommendations is planned to be completed by 1987.

5.3 VALUE-ADDED TERMINAL SERVICE

In addition to the support of standard user interfaces described in the preceeding section, one of the main objectives in the design of PAXNET has been to enable a wide variety of terminal types to connect to the network. Ideally each terminal should, regardless of type, be able to communicate meaningfully with all hosts connected to the network. The value-added terminal service of PAXNET is aimed at this goal in accordance with the OSI architecture for Virtual Terminal protocols.

Terminal support

The possibility for a terminal to connect to PAXNET depends on the particular native protocol of the terminal. PAXNET supports a growing number of native (vendor specific) terminal protocols, and more are expected in the future. Currently the list includes:

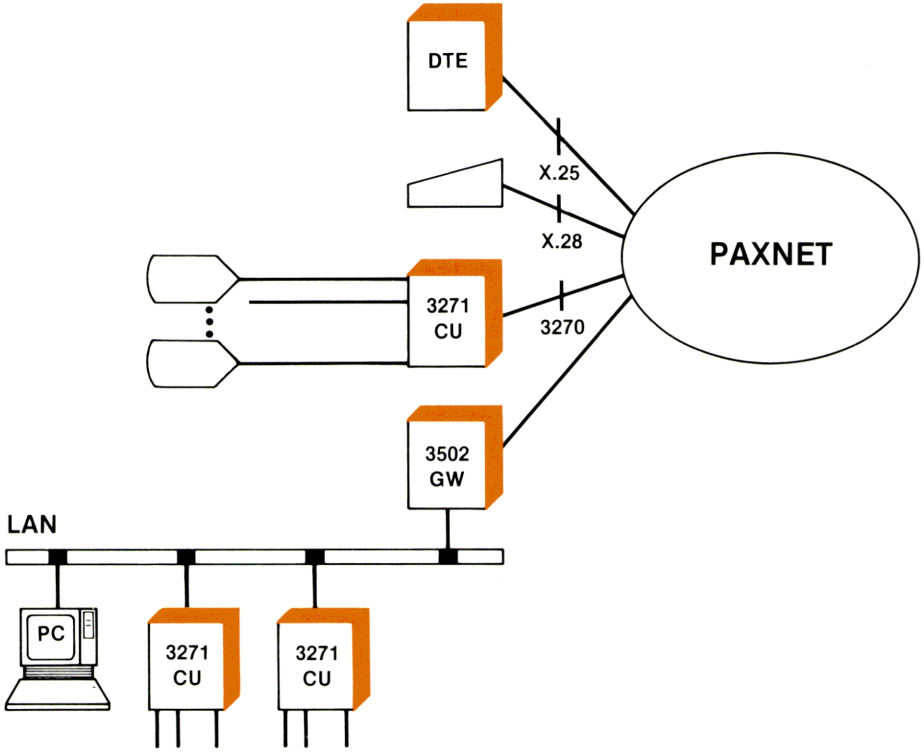
- IBM 327X BSC.
- TTY (start/stop).
- ECMA 48 (very similar to VT100).

This section depicts the general service provided, regardless of the physical terminal type and the native terminal protocol.

A terminal may operate in two dialogue modes.

The first one is a local dialogue between the terminal and PAXNET. This mode is called Terminal User Service mode, abbreviated TUS mode.

The second is called the Session (Connection) mode, where the terminal is connected to some counterpart by means of PAXNET.



Terminal access protocols.

Welcome prologue

Prior to entering one of the two modes the terminal will initially receive an optional welcome prologue. The welcome prologue contains an initial text presenting information like "Welcome to PAXNET", the current date and time, messages broadcasted from the Network Management Centre etc. After these service messages the terminal may be changed into one of the modes described above.

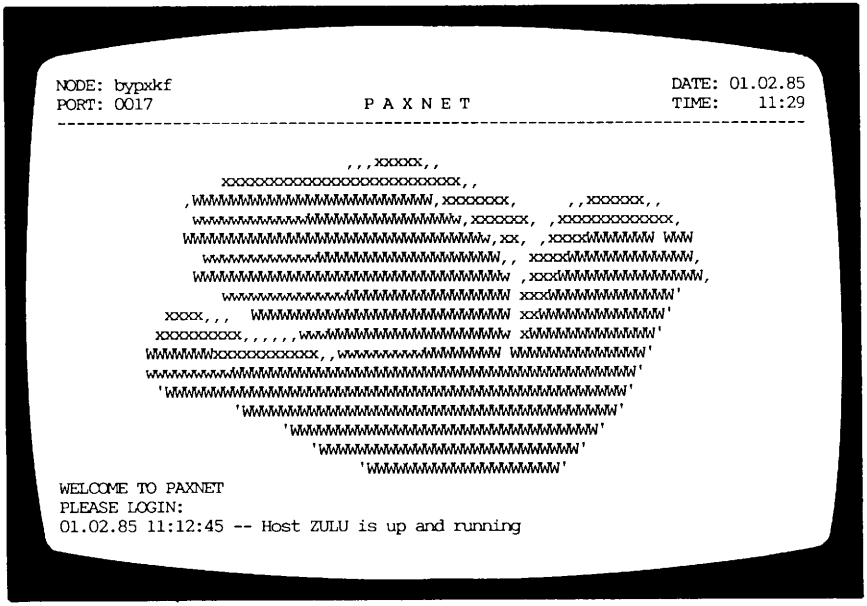
Terminal User Service (TUS) Mode

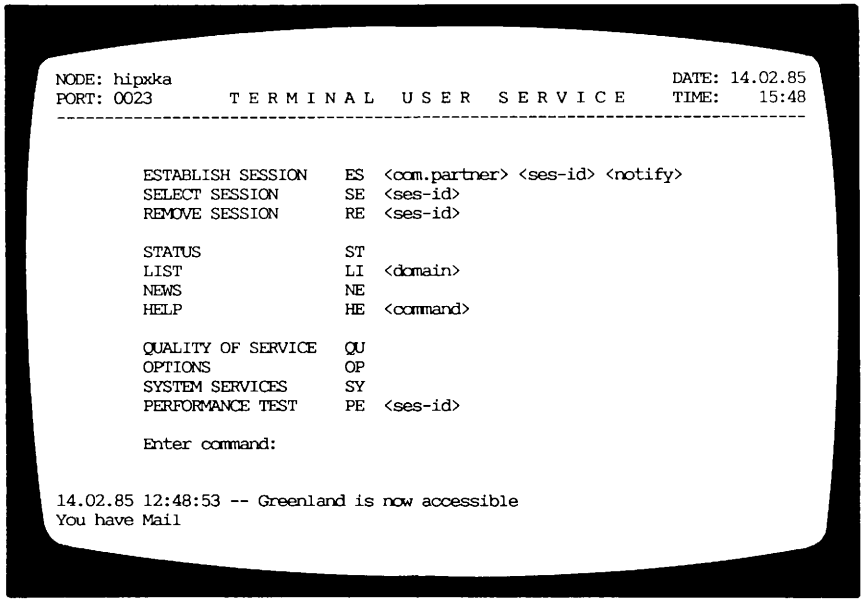
This mode may be described as a *local* conversation mode between the terminal user and PAXNET. Examples of actions which may be performed include:

TUS services

- Request of session establishment (possibly across the network) to a counterpart (for instance an application in a host computer or another terminal).
- Change of the profile definition (line width, page size, the use of function keys etc.) of the terminal.
- Selection among a number of already established sessions (windows).
- Removing a session.
- Choosing a certain level of service (for instance response times, number of simultaneous sessions etc.).

Example of welcome picture.





TUS dialogue picture.

5.4 VALUE-ADDED NAMING AND ADDRESSING

Titles & Network adresses

The identification of PAXNET users is an important aspect of the parameter setting. All application processes running in hosts connected to the network and all other active users are identified by a unique title independent of their physical network address. This enables an application to change network address (to be moved to another host) without changing its unique title.

The dynamic binding of a title to a network address occurs when the application becomes active, i.e. wants to create or receive calls from other users (terminals or other applications).

The unique title consists of a list of identifiers. Each identifier may be protected by a password.

Session Mode

Session mode services

After the parameter setting and the establishment of one or more sessions, the terminal is switched to Session mode by explicitly choosing one of the created sessions.

Once the session has been selected a virtual connection between the terminal user and the recipient will be established. This virtual connection will in many ways be indistinguishable from a dedicated physical circuit between the two parties.

If the called user is an operating system, the usual log on procedure with user name and password may now be carried out.

In Session mode the terminal may be switched back to TUS mode. Precisely how this is performed depends on the physical terminal, but this is typically achieved by pushing a predefined function key or on a more primitive terminal by using some escape sequence. The return to TUS mode will have no influence on the established session.

5.5 VALUE-ADDED CONTROL AND SECURITY

In many data communication systems, user validation and access control must be performed by the application itself. And indeed, each application should always support these functions and facilities, possibly even at numerous security levels.

For applications which may be accessed through a data communications network, the network should offer (supplementary) access control and possibly even user validation.

PAXNET offers basically two (independent) services to this end:

- access control, based on **physical** attachment points, and
- user validation, based on passwords.

Access rights

The PAXNET access control is based on *access rights* (capabilities) and *access filters*. When a virtual call is established in PAXNET (identified physically by the attachment point, the access right of the calling terminal is compared to the access filter of the called application. If they match the call will succeed, if not, the call will be rejected. The method may be viewed as a system of keys and locks.

Password

An optional facility may be provided based on a password mechanism. A unique password is allocated to every application title. (The application will typically have a further identification of the user based on a personal password).

Since the access right mechanism is related to the physical address (attachment point) it offers an extremely high degree of security. Passwords are potentially more vulnerable to careless human users. The two services, access control and user validation, however, supplement each other excellently to provide a very high degree of security when accessing PAXNET.

5.6 VALUE-ADDED HOST INTERFACE SERVICE

One of the goals of a data communications system like PAXNET is to enable various host computers to connect to the network. Host computers provide the data processing power shared by most of the users of the data communications service.

Heterogeneous host computers

Host computers are offered by a multitude of different manufacturers. These often have heterogeneous operating systems and different methods for representing data. For historical reasons many of these systems also use proprietary data communication protocols for system interconnection. These proprietary protocols are not standardized, and do not in general conform with the internationally standardized OSI protocols. The task of interconnecting these host computers therefore becomes a task of providing gateway functions.

Just a few years ago the task of providing gateways to conform with the wide varity of host computer access protocols was enormous. All through the seventies each major computer manufacturer invented proprietary protocols.

At the outset of the PAXNET project, a common denominator was beginning to emerge through the work on protocols for Open Systems Interconnection. The potential of these internationally standardized protocols lies in a dynamic reduction in the number of different types of gateways.

ISO/OSI interface

PAXNET is committed to conform to the OSI protocols as they emerge from the international standardization organization (ISO). The strategic impact of this commitment, is that host computers capable of supporting the ISO/OSI protocols may be connected directly to PAXNET as they emerge.

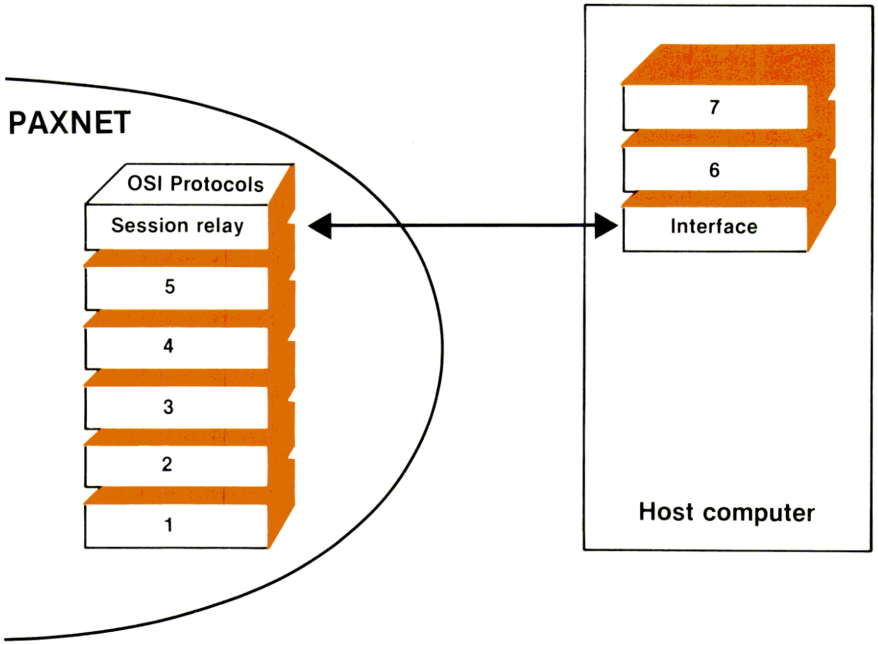
Many European and international initiatives to promote compliance with ISO/OSI seem to have considerable success. In a very few years a wide variety of host computers which support ISO/OSI are anticipated. PAXNET is designed to meet this challenge.

Session relay

Access to OSI host computers may be achieved by adhering to all protocol-layers as defined in the OSI standards. Thus both PAXNET and the host computer may be considered as OSI End Systems.

Access may also be achieved at an intermediate level where the upper layer protocols (layers six and seven - presentation and application) reside in the host while layers one to five reside in PAXNET. A session layer relay mechanism is currently being developed which provides the ISO session layer service across an HDLC based relay mechanism.

Session relay for non-OSI hosts.



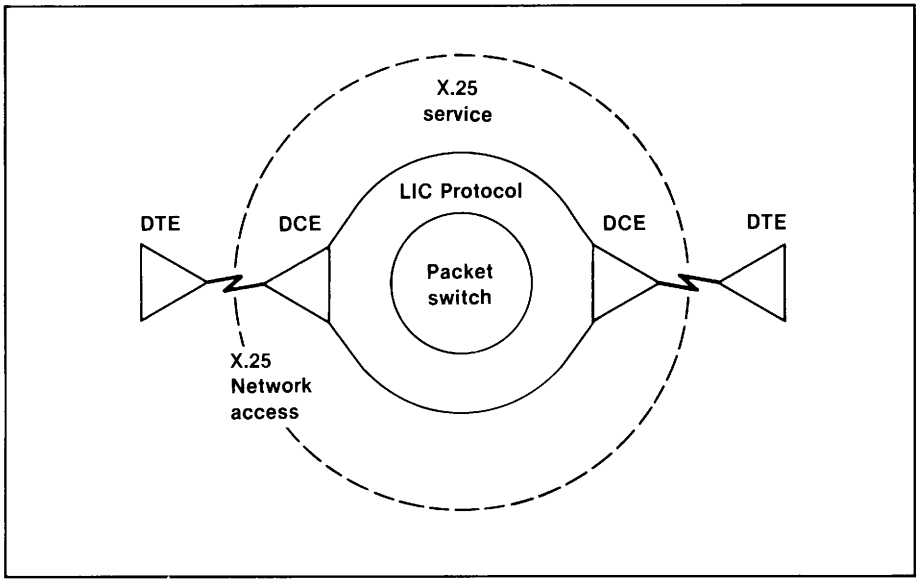
Hosts currently supported

In recognition of the current small number of hosts supporting ISO/OSI protocols, PAXNET supports a number of vendor specific host protocol gateways.

Currently special interfaces to the following hosts are available:

- RC 8000 — by emulating of a Front-End processor and mapping to the session layer service.
- CDC Cyber — running NAM (Network Access Method) by emulating CCP and mapping to the session layer service.
- IBM 43x1 and 30xx — via IBM 3705/3725 based on communication ports operating under the 3270 BSC protocol. Support of IBM/SNA is currently under development. Compliance with the PAXNET X.25 service is currently being tested.
- Honeywell Bull — based on a gateway from PAXNET to the DSA hosts Honeywell Bull DSA network environment.
- Tandem — using the 3270 BSC protocol, and through the PAXNET X.25 access service.

The Data Transmission System 6.



Transmission system protocols.

The very heart of the PAXNET data communications system is the efficient mechanism to move data quickly and safely between end user destinations. To accomplish this task a large number of data transmission techniques and media are applied, - and new ones will without doubt show up in the coming years. These new methods will allow for higher transmission speeds, better utilization and improved quality.

New transmission techniques

The rate at which new transmission techniques become available imply that it must be possible to modify the internal data transmission method in the network without changing the properties of the network access service. This independence, between the transport system and the access service, is vital in order to be able to reconfigure and optimize the data transport system.

The independence of the transport system and the user interface also implies that users need not deal with the properties of the transport network, e.g. alternative paths or reconnections in case of errors internally in the transport system.

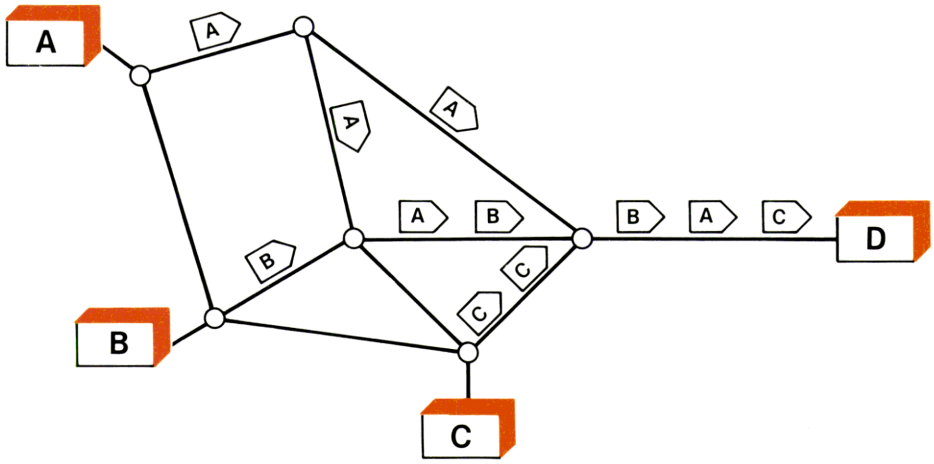
In the following sections the qualities of the PAXNET data transmission system are described.

6.1 THE PACKET SWITCH

Packet switching

The kernel system for the transmission of data is a packet switching network. Packets are sent from source (sender) to destination (receiver) based on address information (internal network address, not ultimate user address) placed in each packet as in all other packet switching systems.

Packets are sent and routed, independent of each other, based on a routing algorithm. Both an adaptive and a dynamic routing algorithm is used. The adaptive routing algorithm autonomously adapts to topological changes in the network, while the dynamic algorithm also takes the local load condition on each communication line into consideration. In reference (2) a detailed description of the routing methods may be found.



Basic principle of packet switching.

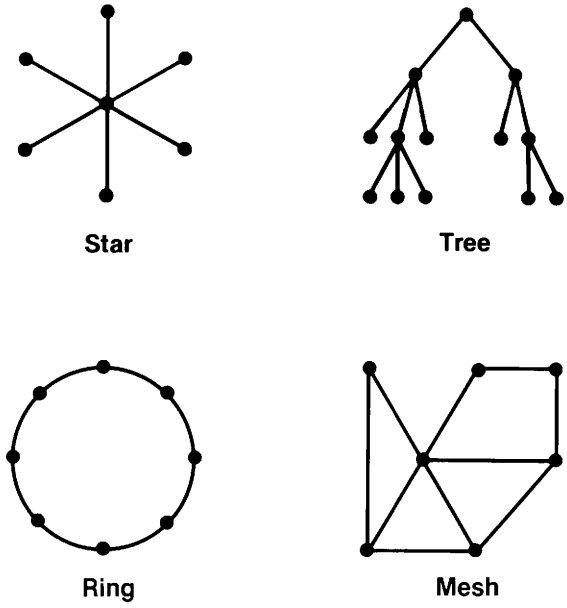
Routing

It is important to recognize that all network nodes are autonomous and selfcontained units. Each network node has an *up-to-date* knowledge of the network, which allows the switch to handle traffic even in case of break down of lines or nodes, without any predefined alternative routes and without any interference from the Network Management Centre. The information in the routing tables is based on information received from *neighbour* nodes and measurement of line transmission speeds.

Topology

There are no limits to the actual topology of the network. Thus networks may be of star, tree, ring, or mesh type. The mesh type network is the most widespread.

In the mesh configuration connections between the nodes are established in a non-restricted way, which means that links may be configured freely in response to the traffic volume, the back-up possibilities, and the speed of the existing communication lines.



Network topologies.

The mesh structure allows for easy reconfiguration and addition of new nodes, in response to changes or the need for increased capacity.

Transmission links

The nodes may be interconnected with a number of different communication media, e.g. 64 kbps digital trunk lines, PCM channels, or modem lines of various speeds and types. Satellite links may also be employed between the nodes. Alternatively, they may be coupled on 10 Mbps Local Area Networks using CSMA/CD access protocols.

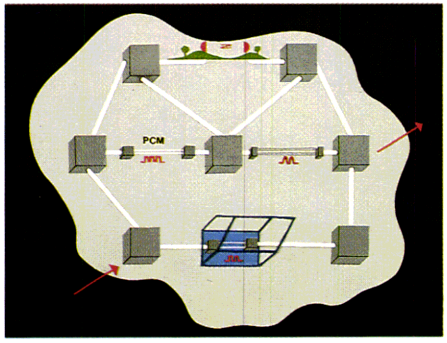
In sites where increased capacity is required, a number of processors may be combined to provide a node with the required switching capacity.

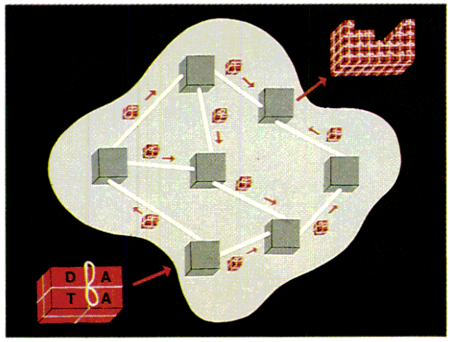
The advantages of gaining a high node capacity by combining a number of relatively small components in a close coupling are:

- The processors will be electrically independent. They all have their own power supply, and may therefore be serviced independently.
- The processors are functionally independent. Because of the distributed routing method they are able to transfer data independent of the state of their neighbours (traffic load sharing).
- The capacity may easily be increased in a site by adding processors to the configuration.

1 2

1. *Transmission techniques supported.*
2. *Principles of packet switching.*





Characteristics of the packet switch

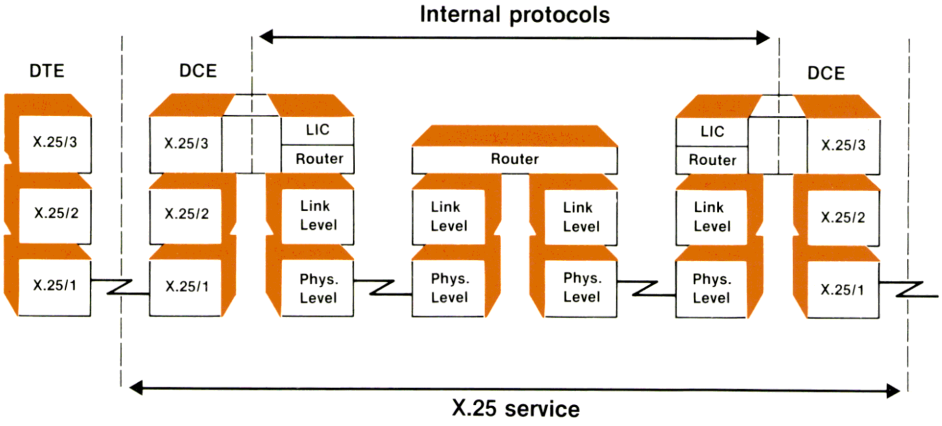
To summarize, the most important properties of the PAXNET packet switching network are:

- Automatic selection of *shortest* and most expedient path.
- Automatic adaption to topological changes, i.e. line up or down, node up or down, change of line speed, etc., without any human interference or interference from the network management system.
- Easy inclusion of new communication media such as Local Area Networks.
- Easy inclusion of new nodes with automatic adjustment of the routing tables.

6.2 TRANSPORT SYSTEM END-TO-END PROTOCOL

The internal packet switching network does not ensure end-to-end protection of data. To support this a protocol called the Logical Internal Channel (LIC) has been implemented. Details on this facility are found in reference (3).

The LIC protocol has been specially tailored to meet the requirements of the X.25 access service. The external function of the protocol correspond to the internal service provided by the LIC protocol layer, including window mechanisms, acknowledgement, expedited data, etc. The LIC protocol is applied as an end-to-end protocol for the protection of data transferred across the packet switching network. The packet switching network combined with the LIC protocol layer ensures a safe transport of X.25 data from entry point to exit point.



Protocol interaction.

LIC protocol

The LIC protocol ensures that X.25 Virtual Circuits will survive internal failures (of network nodes, or lines) in the packet switch.

The PAXNET LIC protocol is proprietary, mainly because it is an internal transport protocol which (like the routing protocol between the network nodes) is not generally available for the user. Furthermore the protocol preceeds the ISO Inter-net protocol which in functionality is similar to the LIC protocol. Currently, however, internetworking from PAXNET to other networks is only supported by the CCITT X.75 protocol intended for the interconnection of X.25 networks.

Network Management Service 7.

The purpose of the PAXNET network management system (NMS) is to ensure the long term and short term successful operation of the network. To this end the NMS operates *back-stage*, providing tools for the network operator to monitor and control the network. Ideally the NMS should be invisible to the individual user, at least as long as the network service operates in accordance with the guaranteed level of service.

At the operational level the NMS provides powerful and flexible tools for:

Operational level

- Monitoring the network (network log).
- Gathering statistics from the network.
- Fault management (identification, isolation and repair).
- Gathering of account information.
- Subscriber management.
- Control of the network.

At the tactical level the NMS provides facilities for:

Tactical level

- Configuration management (topology, software versions etc.).
- Monitoring the network availability.
- Capacity planning.
- Capacity adjustment.

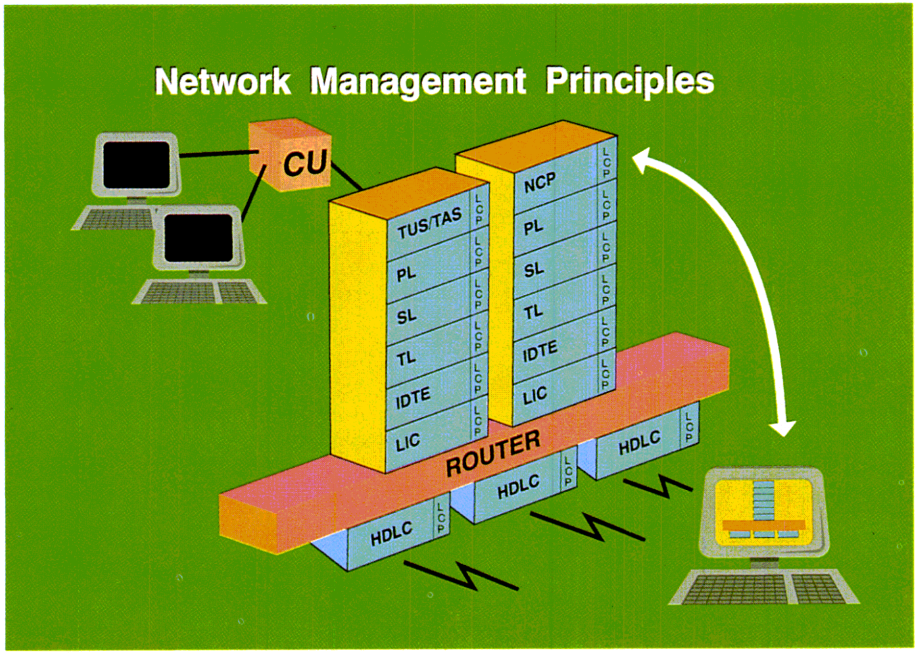
At the strategic level, new services and facilities are constantly under development in response to the experience gathered in the daily operation of the network.

A vital feature of the NMS is that it encompasses all PAXNET components. This implies that all system elements may be monitored and controlled by the NMS. Only in this way may the high service level of PAXNET be maintained all the way to the subscriber interface.

Decision support system

As the NMS reaches all system components, vast amounts of data may be collected. A key feature of the NMS is therefore the orderly presentation of these data to the operator. It is the goal of the NMS to provide the operator with a powerful decision support system where only the most relevant information is displayed. In short, the purpose of the NMS is to support the operators - not to confuse them!

Reference (7) contains further introduction to the NMS concept, and reference (8) elaborates on the details of the functions of the Network Management Center. The following section will briefly describe the NMS.

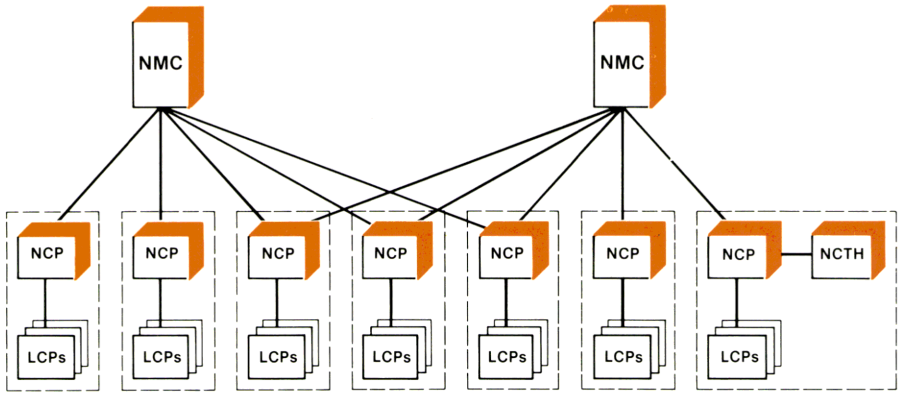


An overview of the main NMS components.

7.1 THE NETWORK MANAGEMENT ARCHITECTURE

Distributed capabilities

The NMS is designed and constructed as a distributed system where all functions have been fully distributed. The purpose of this distribution is to achieve precise monitoring and control facilities throughout the entire network. This implies that all elements (hardware and software modules) must contain NMS facilities.



NMS Architecture:

1. *Network level service.*
2. *Local systems level management.*
3. *Entity level management.*

LCP

In consequence all software modules have an interface to the NMS, and all software modules are able to perform local (entity) management functions accessed via the Local Control Probe (LCP) interface.

The information provided by the individual LCP is dependent on the actual software module which it monitors. Typical information is provided by counters describing various loads, errors, status information and events which occur.

NCP

Each network node (local system in ISO management terminology) supports a set of local system management functions accessed via the Network Control Probe (NCP). Local system management is performed by invoking one or more entity management functions through the LCP interface.

The NCP communicates with the LCPs by means of a native protocol, whereas the communication between the NCPs and the NMCs takes place on PAXNET session connections.

NMC

The Network Management Centre (NMC) provides the interface between the network operator and the network. It provides the vehicle for human interaction with the network and comprises the complex decision support part of the NMS.

A simple interface to the local system management is offered through the Network Control Terminal Handler (NCTH), an optional NMS module. The purpose of the NCTH is to offer a simple on-site NMS terminal interface, which may be used for local debugging and control without the support of the NMC.

7.2 NETWORK MANAGEMENT DESIGN PRINCIPLES

Flexibility

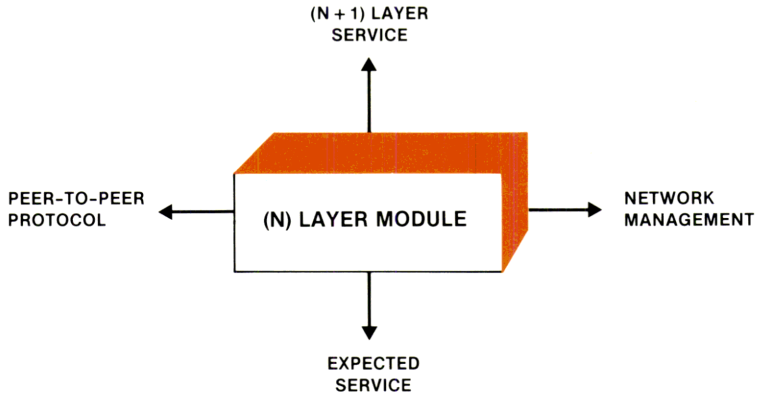
The major principle behind the NMS is to provide a framework, or set of tools which can either be used directly by human users interacting with the network, or extended to provide the required service automatically. This flexibility enables the users themselves to tailor the NMS functions to fit their exact needs.

This property is essential because of the multitude of different user groups with different requirements for network management and data presentation. These groups include network management operators, hardware technicians, system programmers, configuration personnel, help desk operators, performance analysts, and capacity planning personnel.

Modularity

Another major principle behind the NMS is the modularity of the design and implementation of the NMS software. This modularity enables new user facilities to be easily slotted into the NMS, and - particularly in the NMC framework - with a minimum of disturbance. In this way the NMS can keep pace with evolving network and operational requirements.

Finally the NMS has been extended to all PAXNET software modules by including an NMS interface in every software module. In this way all protocol modules support four types of interactions - as depicted in the *four-handle* model.



The four-handle model.

7.3 NETWORK MANAGEMENT CENTRE FUNCTIONALITY

NMC functions

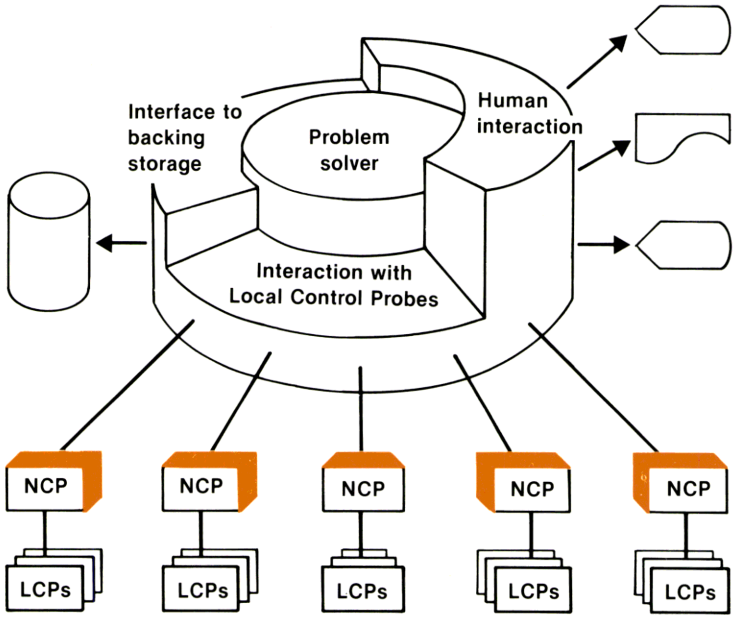
A complete description of the functionalities of the NMC is beyond the scope of this document. However, an introduction to the main functions may be found below.

The NMC comprises functions for:

- Monitoring the network.
- Controling the network.
- Administrating the network.

These functions of the NMC may be divided into a number of groups:

- Autonomous activities
  which are functions automatically executing a certain task invoked by an event from the network, e.g. down-line load of a node in case of a local malfunction.



NMC functionality.

- Operator initiated activities
  which are tasks activated in response to operator commands. An example of this type of activity is the line test facility, which upon operator request closes the suspected line for normal traffic, performs a test on the line, and then reports the diagnosis to the operator.

Monitoring

The NMC includes effective tools for **monitoring** the behavior and state of the different network elements. These tools provide the staff with *up-to-date* information from all parts of the network.

Functions in this category include:

- Generation of reports on hardware and software malfunctions.
- Presentation of information about new users connecting to the network.
- Presentation of the operator requested subset of the events generated by the LCPs.
- Presentation of on- and off-line statistical information.
- Presentation of the status of network elements.

Besides the passive tools for monitoring, the NMC includes means for changing the properties of the network elements.

Controling

The **control** functions include:

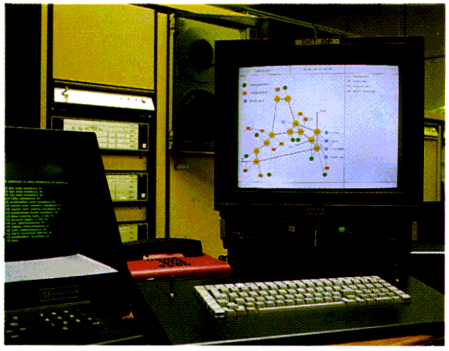
- Generation of commands to change the state of network elements.
- Down-line loading of software to a component.
- Generation of commands to execute tests in the network.

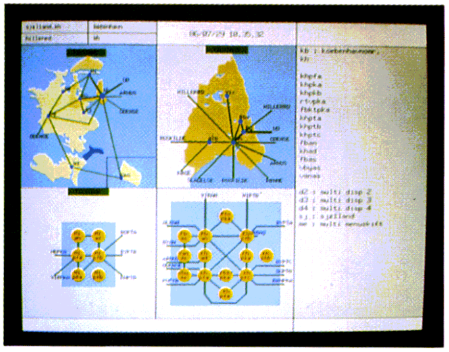
Administration

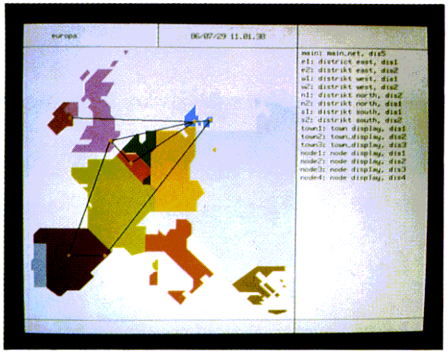
Furthermore it is possible to execute a number of **administrative** tasks not directly interacting with the network. These include:

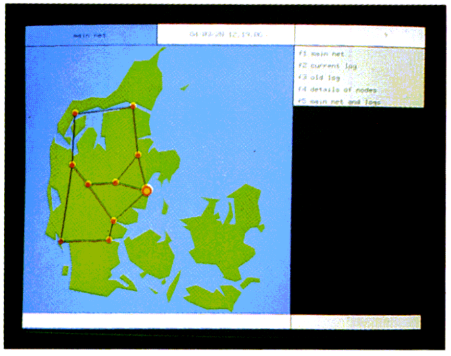
- Generation of software systems.
- Configuration updates.
- Collecting and saving statistics.
- Collecting and saving account information.
- Updating subscriber databases.

A description of the facilities (currently implemented) can be found in reference (15).









Examples of information displayed to the network operators.

7.4 OPERATOR INTERFACE TO THE NMC.

Operator interface

Considerable attention has been paid in the design of the human interface to the network management system. The interchange of information between the human operator and the NMC may be achieved through a number of different devices.

Access to the NMC is password protected. Various degrees of functionality may be accessed dependent upon the particular user identification.

Some of the devices which may be used for interchange of information between the operator and the NMC are:

Display systems

- Colour graphical display
  depicting the overall network configuration, or detailed information on smaller areas or single components, as described in reference (16).

- Monochrome or colour displays
  showing an operator a specified selection of events, with a multitude of mechanisms for selecting the set of presented events.

- Alarm printers
  providing a hardcopy of a selection of networks events.

- Ordinary network terminals
  providing access to a number of different NMC activities, e.g. facilities for fetching and displaying statistics, activating line tests, etc.

PAXNET System Components 8.

This chapter provides on overview of the hardware and software components utilized in PAXNET. It is not the intent of this chapter to provide detailed information pertinent to all system components. Please refer to the specific references mentioned in this chapter for further information.

8.1 THE HARDWARE STRUCTURE OF THE RC3502 PROCESSOR.

All nodes in the network are based on the same type of processor, namely the RC3502 minicomputer. The RC3502 may be used as a pure internal transit switch as well as a component both handling transit traffic and a number of network access services.

RC 3502 node processor

The main characteristics of the RC3502 are:

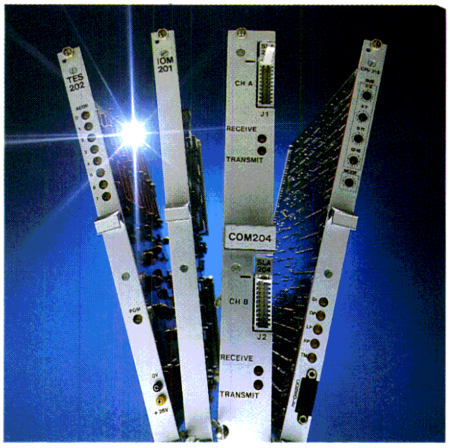
- A 16 bits CPU built around four 4 bits bitslice processor chips.
- An internal address space of 4 Mbytes.
- A total of 124 priority levels each with a set of registers facilitating fast change between real time processes.
- A stack oriented high-level instruction set, specially designed to support the Pascal language.
- An average instruction time of 3.0 microsec.
- A 20 Mbps capacity of the system bus.

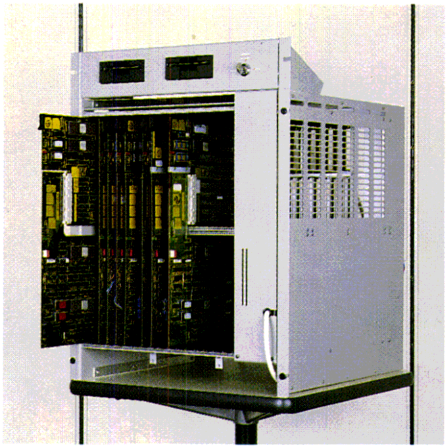
- A bootload facility of the basic system including selftest, which may be initiated either by system call, power up, manual activation on the front panel, or by a system watchdog facility.

- A memory expansion capability in modules of 256 kbytes and 1 Mbyte.

- A wide range of both simple and intelligent controllers and adaptors as described below.

1 2 3





1. *RC 3502 minicomputer.*

2. *RC 3502 controller cards.*

3. *CASE PAD hardware.*

The RC3502 cards are mounted in a 19 inch standard crate (DIN41494) which includes a power supply for 220V AC or 48V DC.

A number of RC3502s may be installed in the same rack or cabinet. The standard cabinet allows for 3 independent crates, but other types of racks or cabinets are available.

RC3502 may be interconnected by HDLC controllers, or in local configurations through a LAN, using 10 Mbps CSMA/CD controllers.

Link level hardware

Two types of HDLC controllers may be obtained both with automatic line speed adjustment and measurement. These are used internally between the network nodes, and externally to provide the X.25 access service.

A high speed version which handles two HDLC lines of 64 kbps each (or less). A variety of line interfaces is supported (PCM, V.35, etc.) by plug-in line adaptors.

Furthermore a low-speed HDLC controller which provides four channels of max. 9.6 kbps each. Line interfaces may be V.24/V.28 and X.21, (V.10/V.11).

Other interfaces may be established with a number of different controllers, among them an 8 line 3270/BSC adaptor for interconnecting 3270 devices, special host adaptors, etc. By late 1987 a 4-line SNA/SDLC controller will be available.

The RC3502 crate may also house 4-channel short distance modems (9.6 to 64 kbps) and 3-channel PCM emulators.

To allow a high degree of distribution of access points, the user interfaces for X.28 start/stop terminals are obtained with selfcontained PADs, which may either be situated in the RC3502 rack and connected directly to a HDLC controller, or placed remotely in another telephone exchange or on the subscriber's premises.

PAD hardware

The equipment used consists of two types of the CASE X.25 PADs (8160 and X-gate 2), characterized by:

- Speeds up to 19.2 kbps on the X.25 link with internal or external clock allowing direct connection or remote connection via modems.
- 8 to 64 asynchronous terminal ports, with speeds from 50 to 19.200 bps.
- Automatic bit rate adaption up to 9.600 bps, and 1200/75 and 75/1200 bps split speed.
- 76.8 kbps/2.3 Mbps aggregate input capacity.
- 220 V AC or 48 V DC power supply.

Further information on the RC3502 and the various interfaces may be found in references (10) and (11). In reference (13) some details on the present versions of the PAD are found.

RC 3502 software modularity

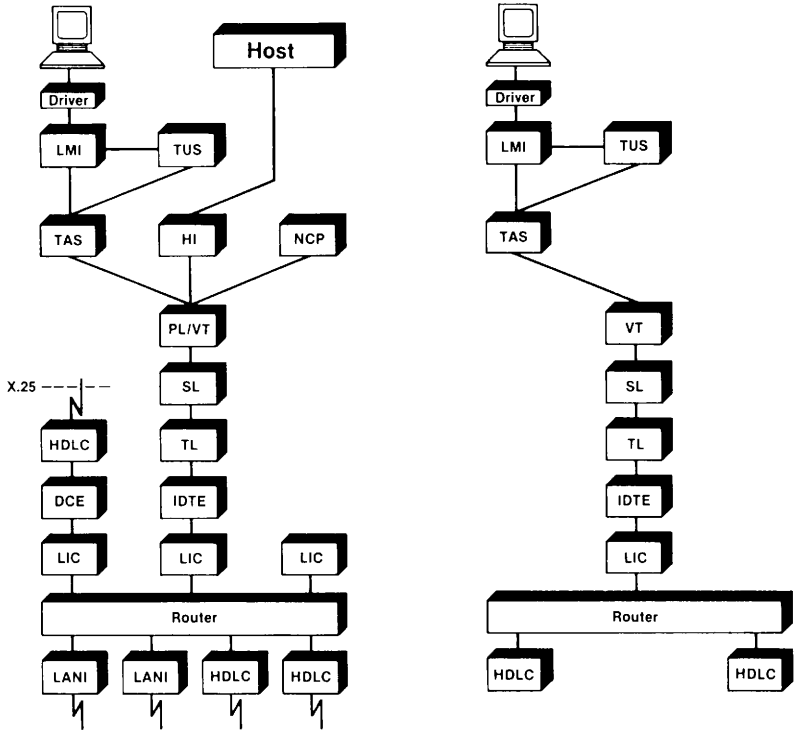
8.2 THE RC3502 SOFTWARE ENVIRONMENT.

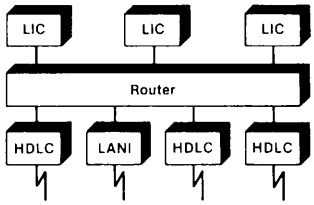
All software, including the operating system for the RC3502, is written in the high level language called *Real Time Pascal*. This language may be characterized as Pascal extended with facilities for administrating and synchronizing cooperating processes operating in parallel.

In the construction of the software systems for the RC3502 special care has been taken to obtain a modular structure. This to ensure that protocol layers, etc. can be replaced with new versions without affecting the total system. The figures illustrate the software modularity in various PAXNET configurations.

External access to the network is provided through dedicated service/protocol modules depending on the service of the LIC module.

Examples of software configurations in access nodes.





Software configuration for transit node.

X.25 service is implemented with a DCE module and an HDLC driver. As X.25 levels 1 and 2 are executed in the HDLC controller hardware/firmware, the DCE module only has to handle the X.25 level 3 (packet level). The DCE module is described in details in reference (4).

On top of the general purpose presentation layer module a number of different service modules are implemented - conceptually in the OSI layer 7.

Terminal access

Terminal connections are implemented by means of the Virtual Terminal concept (VT). Uniform sign-on procedures and various user assistance features (welcome prologue, etc.) are provided by the Terminal Attachment Service (TAS) and Terminal User Service (TUS) modules.

A mapping between the native communication protocol of the terminal in question takes place in the Local Mapping Interface (LMI). So for each new terminal type to be connected it is only necessary to program a new LMI.

The implementation of Host Interfaces (HI) on this level is manufacturer dependent, because of the differences in the communication facilities of the mainframes.

The functionality of the NCP is also illustrated in the figures. The NCP handles the local system management and performs the exchange of network management information as described in section 7.1, and makes use of the ordinary protocol modules for data transfer.

The protocols implemented so far are based on standards from ECMA. These are currently being changed to conform to the latest ISO standards. The current software implementation is based on the following standards:

Current OSI standards

Layer 4	ECMA-72,	Class 0 and 2.
Layer 5	ECMA-75,	Class A, B and D.
Layer 6	ECMA-86	

The Virtual Terminal (VT) supported is based on ECMA-87, and ECMA 88.

The revised implementation will be based on the ISO/OSI standards, please refer to section 9.2.

8.3 THE HARDWARE STRUCTURE OF THE RC8000 NMC

NMC hardware

The hardware used for the Network Management Centre is the RC8000 mini computer. This computer is also used for software compilation for the RC3502 node processor.

A variety of different RC8000 models are available allowing the hardware configuration of the RC8000 to vary between 0.2 MIPS for the smallest system and up to 3 MIPS for the fully equipped RC8000MP multi processor system.

Further information describing the RC8000 mini computer may be found in reference (12).

8.4 THE RC8000 SOFTWARE ENVIRONMENT

The RC8000 software environment is typical of a medium sized general purpose computer. The environment includes tools for safe software operation, implementation and testing.

The NMC application is constructed as a frame system in which a number of network/configuration specific activities operate. New facilities may easily be added, as the need arises. Both the frame system and the activities are programmed in an extended subset of the Algol 60 programming language.

Current Development Plans 9.

This section outlines the current development plans for both software and hardware components, scheduled to be completed before 1988.

Some of the subjects have already been mentioned. For the sake of readability a complete list of these items is repeated in this section.

9.1 CCITT RECOMMENDATIONS

CCITT recommendations (1984)

Currently all implementations of existing X recommendations are being updated to conform to the revised 1984 version as described in the *red books*. This process will be finished by mid 1987.

Implementation of the new X recommendations especially X.32, is currently being considered.

Concerning the X.400 message handling series of recommendations, it is currently being considered how a public service may be integrated in the PAXNET value-added set of services. This system may contain both MTAs and UAs. A prototype system for internal use is intended to be launched by 1987.

9.2 OSI STANDARDS

A major development task is currently under progress in order to support the latest versions of the OSI standards. This development will be completed by mid 1987, where PAXNET will comply with all the relevant ISO/OSI standards.

Specific development efforts include:

- Update of transport layer, session layer and presentation layer to conform to the latest version of ISO standards.

- Implementation of the ISO File Transfer Access and Management (FTAM).

In this way PAXNET will support the following OSI protocol standards:

OSI protocols

Layer 4	ISO	8073	Classes 0, 2 and 3
Layer 5	ISO	8327	BSS, BCS, and BAS
Layer 6	ISO	8823 and 8825	
Layer 7	ISO	9041	VT initial facility set.
Layer 7	ISO	8571	FTAM file transfer service class

9.3 VENDOR SPECIFIC IMPLEMENTATIONS

Host access

In recognition of the current lack of host computers supporting ISO/OSI protocols development of a number of vendor specific protocols is also under way. These include:

- Implementation of FTAM (only file transfer class) in RC3502, and access to the service from RC8000, IBM, Honeywell Bull computers.

- SNA/SDLC gateway development.

- Gateways to the following LANs:
  . Ungermann-Bass Net-One,
  . Sytek.

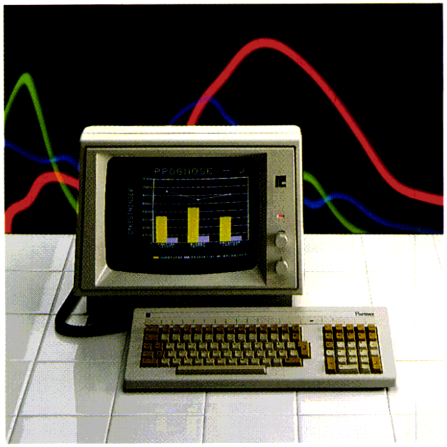
9.4 NETWORK MANAGEMENT

In response to the considerable experience gained from the daily operation of the Network Management Centre, and to incorporate the progress within ISO, a number of enhancements are under development:

- Extension of the colour graphical display system.

- Implementation of NMC functions in the RC3502.

- Implementation of NMC functions in a UNIX environment (RC39 computer line).



1 2

1. *The RC 750 PARTNER personal computer - the OSI-PC*

2. *The RC 39 mini-computer used for a UNIX based NMC.*

9.5 NEW COMPONENTS

Currently a number of new hardware and software components are planned. These include the following:

- OSI PAD, a component based on CASE hardware providing low cost terminal connections (VT100, 3270 BSC, etc.). This component is based on the OSI virtual terminal concept.

- OSI PC, a Personal Computer with support of all seven layers of OSI protocols. The first implementation will be in the RC750 PARTNER.

- RC3502-3 multiprocessor version of the RC3502. This product will be available 1986, and will provide improved price/performance of the node processor.

ISDN interface

- ISDN interface. The current plans for the introduction of ISDN in Denmark are quite advanced. In consequence a number of developments to integrate ISDN and PAXNET are under way. The first prototypes will be available by late 1986.

List of terms and acronyms 10.

Access Control: A mechanism used to prevent un-authorized users to gain access to a service or an application.

Adaptive Routing: Opposed to dynamic routing, an adaptive routing algorithm (see routing) only takes account of topological changes in the network.

Activity (Network Management Activity): An enterprise within the network management centre performing a logical group of functions and data manipulation.

Address: One or more characters designating a physical location (e.g. which is the origin or the destination of data being transmitted).

Analogue Signal: An analogue signal is one which can vary continously, taking any value between certain limits.

Application (Process): An enterprise within a computer system which performs the information processing functions for a particular application.

Application Layer: The uppermost layer within the OSI basic reference model, directly providing open communication facilities for use by application processes.

Application layer

Asynchronous line

Asynchronous Line: A physical line on which the time intervals between transmitted characters may be of varying and unequal length.

Asynchronous Terminal: Descriptive name for a group of terminals designed to operate over asynchronous lines. See also start/stop terminal.

Baud

Baud: One signalling element per second. A measure of the signalling rate on a data channel. The data transfer rate (measured in bits per second) is usually a simple multiple of this.

Binary Synchronous Protocol: A data link protocol that uses a defined set of control characters and control character sequences for synchronized transmission of binary coded data between stations in a data communications system. A widely used example is the IBM/BSC protocol for 3270 compatible devices.

Bit: The machine implementation of a binary digit, which can take the value 0 or 1.

Bitslice: A technique for computer construction, where a number of smaller processors (chips) are combined to provide an agregated processor (CPU).

Bootload: The initial load of software into an (empty) processor.

Bps: Bits per second. A measure of the data transfer rate of the data channel.

BSC: See binary synchronous protocol.

Byte: A group of bits, normally eight, which represent one data character.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection (CSMA/CD): A distributed channel-allocation procedure in which every station can receive the transmission of all other stations. Each station awaits an idle channel before transmitting, and each station can detect overlapping transmissions (collisions) by other stations.

CCITT: The International Telegraph and Telephone Consultative Committee, the technical committee of the International Telecommunications Union (ITU), which is responsible for the development of the recommendations regarding telecommunications, including data communications.

Channel: A data path logically joining two or more stations. A physical transmission media is often devided into a number of independently controlled channels by the applied data communications protocol or technique.

Channel

Circuit: A logical (sometimes physical) connection between peer entities in the lower three layers of the OSI basic reference model. The logical binding of X.25 subscribers is established by X.25 permanent or switched virtual circuits.

Circuit Switching: A technique of switching data in a network whereby a physical route or a fixed data path is dedicated to the two interconnected devices for the duration of the connection. Sometimes called line switching.

Controller: The hardware that controls a line, or any other physical device.

CPU: Central Processing Unit. A central part of a computer used to process data.

CSMA/CD: See Carrier Sense Multiple Access with Collision Detection.

Data Circuit-terminating Equipment (DCE): In public carrier communication services the equipment that provides the functions required to establish, maintain, and terminate a connection between DTEs (see below, under data terminal equipment).

DCE

Data Link Layer: The layer within the OSI basic reference model which is responsible for the transmission of data between systems between which there is a direct connection. This service is provided to the network layer, and depends on the service provided by the physical layer.

Data Terminal Equipment (DTE): The equipment, typically a computer system or terminal, that consists of a data source and sink connected to common carrier communication services. In plain terms the DTE usually represents the user's equipment.

DCE: See Data Circuit-terminating Equipment.

Digital Data Network: A network specially designed for the transmission of data, wherever possible in digital form, as distinct from analogue networks such as the telephone system, on which data transmission is an exception. (See Integrated Services Digital Network).

Digital Signal

Digital Signal: A digital signal is one which can only vary between two predefined levels. This opposed to analogue where the number of signal levels has no limits.

Downline Load: The process of sending a copy of a system image over a line to the memory of a target node.

Dynamic Routing: A special type of routing algorithm (see routing) taking account of the contemporary network topology and the actual transmission delay.

ECMA

ECMA: European Computer Manufacturers Association. An association of a number of European based computer manufacturers committed to providing common standards for vendor independent interworking.

Electronic Mail: See Message Handling.

End-to-end: The logical binding (across the network) between sender and receiver of data is termed as an end-to-end association. See session.

Error Control: The protocol function that ensures the reliable delivery of data. Typically it consists of sequencing, acknowledgement, and retransmission mechanisms.

Event (Network Management): An event is an unsolicited message generated in the network and sent to the network management centre, which contains information on the change of state of a network component or a resource.

FTAM

File Transfer, Access and Management (FTAM): An ISO term for that part of the application layer service which is concerned with the tasks of providing access to files, and facilities for transferring files between application processes.

Flow Control: A mechanism to control the orderly flow of data between a data source and a data sink to ensure that data is not lost, buffer deadlocks do not occur, and communication overhead is kept to a minimum.

Frame Level: Level 2 of the CCITT X.25 recommendation, which defines the link-access procedure for data exchange over the link between the DTE and DCE.

Gateway: A sub-system which is responsible for transforming the conventions used within one system (or network of interconnected systems) to the conventions used by another.

Gateway

HDLC: See High-Level Data Link Control.

HDLC

High-Level Data Link Control (HDLC): A widely used data link level protocol, defined by ISO and by CCITT in recommendation X.25 level 2.

Host (computer): A computer connected to a network. Typically the origin or receiver of data for processing.

IBM 3270: An IBM invented protocol for the attachment of synchronous terminal devices (and clustered terminals) to an IBM host computer. The early version is the IBM 3270/BSC version, which is gradually being replaced by IBM 3270 SNA/SDLC compatible terminals. These terminal protocols have been adopted by a large number of computer manufacturers.

Integrated Services Digital Network (ISDN): A set of services which may be provided on a public digital network, as described in the CCITT series of I recommendations.

International Standard: Within ISO, the final version of a standard on which international agreement has been reached.

ISDN: See Integrated Services Digital Network.

ISDN

ISO: The International Organization for Standardization, a body dedicated to the production of standards through international agreement.

Kbps: Kilo bits per second. A measure of the data transfer rate.

LAN: See Local Area Network.

LAN

Layer: A part of a hierarchically structured architecture, whose function is dependent on the layer below, and which provides a service to the layer above.

Leased Line: A non-switched circuit that a user (company or other institution) leases from a public utility company (public carrier) for exclusive use.

Leased Line

Line A

Line: A physical path that provides direct communication among a number of stations.

Local Area Network: A local area network (LAN) is one which spans a limited geographical area (usually within one building or site) and interconnects a variety of computers and terminals, usually at very high data rates.

LCP

Local Control Probe (LCP): An LCP is a remote agent of the NMC responsible for controlling and monitoring a specific (hardware/software) module. The LCP is invoked through the NCP.

Logical Channel: An association between an X.25 DTE and its DCE for a given virtual circuit.

Mbps: Mega bits per second. A measure of the data transfer rate.

MHS

Message Handling (switching): A data communications technique in which a complete message is stored and then forwarded to one or more destinations when the required destination(s) are free to receive traffic. Often applied to document interchange and electronic mail systems.

MHS: See Message Handling.

Modem: A contraction of the term "modulator-demodulator". A modem converts the serial digital data from a transmitting terminal into a form suitable for tranmission over the analogue telephone channel. A second unit reconverts this signal to serial digital data for acceptance by the receiving terminal.

Multiplexer: A multiplexer divides a data channel into two or more independent fixed data channels of lower speed.

Native Protocol

Native Protocol: A manufacturer, or device specific, protocol or interface. Some of these have been widely adopted by a large number of manufacturers. These are often termed de-facto, or industry, standards.

NCP: See Network Control Probe.

NCTH: See Network Control Terminal Handler.

Neighbour Node: A network node removed from another node by a single communication link.

Neighbour Node

Network Access: The user entry point to a network service defined by an interface description, typically a protocol. Often defined on the borderline between the DCE/DTE in public networks.

Network Address: In an X.25 network the identification (X.121 number) of the subscriber. Typically pin-points a specific DCE and the DTE.

Network Control Probe (NCP): The NCP is the focal point of the local system management functions situated in each node. The NCP executes the communication with the network management centre and invokes local system management functions through the Local Control Probe (LCP) interface of the software modules.

NCP

Network Control Terminal Handler (NCTH): An optional facility used to offer an on-site network management terminal interface for local debugging and control.

Network Layer: That layer within the OSI basic reference model which is responsible for the transfer of data between arbitrary systems, and in particular for choosing a suitable route to follow. This service is provided entities within the transport layer, and depends on the service provided by the data link layer.

Network Management: The collection of tools and services intended to ensure the long term and short term operation of a network.

Network Management Centre: The focal point (or one of many) where network management information is collected and processed prior to presentation to the network operator. Also the origin of control information intended for the network.

NMC

Network Operator: See Operator.

NMC: See Network Management Centre.

Node (Network Node): A communication processor, or a group of processors, that support the PAXNET routing methods and forms the basic switching element in the packet switching system. A node in PAXNET is implemented by an RC3502 mini computer.

OSI

OSI Basic Reference Model: An OSI standard (IS 7498), which describes the conceptual structure of systems which are to communicate with one another.

OSI Standard: Any standard which fits into the conceptual structure described by the OSI basic reference model, and which apply to processes of communication between systems.

Open System: Within the OSI basic reference model a system which obeys OSI standards in its communication with other systems.

Operator (Network Operator): The human user who controls and monitors the network by means of the facilities provided by the network management centre.

Packet

Packet: A unit of data, of bounded size, with complete address information to allow it to be routed from a source node to a destination node.

Packet Level: Level 3 of the CCITT X.25 recommendation, which defines the packet format and control procedures for the exchange of packets.

Packet Switching: A technique for switching data in a network whereby individual data blocks or *packets* of controlled size and format are accepted by the network and routed independently to their destination. The equipment making up the network is shared by all users at all times, packets from different terminals being interleaved throughout the network.

PAD

PAD: Packet assembly/disassembly device. A PAD permits terminals which do not have an interface suitable for direct connection to a packet switched network to access such a network. As well as converting the terminal's usual data flow to and from packets, the PAD handles all aspects of call set up and addressing. Primarily used to allow asynchronous terminals to communicate over a packet switching service.

Path: A route from source node to destination node. The path can comprise a sequence of connected nodes between the source and destination nodes.

Permanent Virtual Circuit (PVC): A virtual circuit between two X.25 DTEs that is always established. A logical channel is permanently allocated at each DTE/DCE interface to a PVC.

Physical Layer: That layer within the OSI basic reference model which is responsible for activating and deactivating physical connections between systems, and for transmitting elementary units of data over these connections. This service is provided to the data link layer, and depends on the nature of the physical medium used to implement the connection.

Physical layer

Presentation Layer: That layer within the OSI basic reference model which is responsible for the representation of data to be transferred between systems in a form acceptable to the application entities within those systems. This service is provided to the application layer, and depends on the service provided by the session layer.

Protocol: A set of rules for the interaction of two or more parties engaged in data transmission or data communications.

PSDN: Public Switched Data Network. Typically a digital network especially suitable for data communications.

PSTN: Public Switched Telephone Network. The familiar (voice) telephone system over which calls may be dialled.

Pulse Code Modulation (PCM): A standardized technique for high speed transfer of many data and/or digital voice channels often used between telephone exchanges.

PCM

PVC: See Permanent Virtual Circuit.

Routing: In a packet switching network the algorithm by which the node autonomously derives the optimal path towards the intended receiver.

Routing

Service: In the OSI basic reference model, the facilities offered by one layer to the layer above. In the context of a data communications network, the service provided by the network.

Session: In PAXNET, and in many other network architectures, the logical binding - typically across the network - of a sender and a receiver of data.

Session Layer: That layer within the OSI basic reference model which is responsible for the organization and synchronization of dialogues between presentation entities. This service depends on the service provided by the transport layer.

Session

Signalling System 7

Signalling System 7: A CCITT defined protocol and service for the exchange of signalling (control) information between telephone exchanges.

System Network Architecture (SNA): A network architecture concieved by IBM, but widely adopted by a number of computer manufacturers.

Start/Stop (terminal): A serial data transmission method in which each character is transmitted as a self contained unit of information needing no additional timing information. See also *asynchronous.*

SVC: See Switched Virtual Circuit.

Switched Network: A network which is shared among many users any one of which can potentially establish communications with any other when required.

SVC

Switched Virtual Circuit: In a packet switched network a connection between two stations, which is created only when it is required, following a call set up procedure.

Synchronous Terminal: A terminal requiring timing information from its associated modem for the proper reception and transmission of data. Usually more efficient than a *start-stop* terminal.

Terminal: A device for sending and/or receiving data on a communication channel.

TAS

Terminal Attachment Service (TAS): In PAXNET a common platform for the support of various terminal types.

TUS

Terminal User Service (TUS): In PAXNET a number of services and assistance tools available to a terminal user, connected to PAXNET.

Title: In PAXNET the identification of objects independent of their current physical address. Typically used to identify application (processes) operating in host computers attached to the network.

Transmission: The process of sending (for example, data) from one place to another.

Transport Layer: That layer within the OSI basic reference model which is responsible for providing transfer of data between arbitrary systems, with control on an end-to-end basis. This service is provided to entities within the session layer, and depends on the service provided by the network layer. Transport layer

Trunk Line: Typically a high capacity permanent (leased) line between two network nodes.

User: The term is used to describe the following, depending on the context in question: User

. Network user - a subscriber. An individual or a company which makes use of the network provided services through some type of computer equipment. The border line between the network and the user is typically the DTE/DCE interface.

. Terminal user. Typically a human operator utilizing a terminal connected (in some way) to the network.

Value-added Network (VAN): A network (access) service which apart from data transmission also offers some additional *value* such as protocol conversion, store- and forward messaging, gateways and so on. VAN

Virtual Circuit: A temporary connection between a data source and a sink in a network. Virtual circuits typically guarantee delivery and sequentiality of client data.

V. Recommendation (CCITT): A series of CCITT recommendations covering data transmission over the public switched telephone network. Of particular relevance:

V.10 Electrical characteristics for unbalanced double-current interchange circuit for general use with integrated circuit equipment in the field of data communications.
V.11 Ditto, but for balanced double-current interchange circuits.
V.22 1200 bps full-duplex 2-wire modem standardized for use in the general switched telephone network.
V.22 bis 2400 bps full-duplex 2-wire modem standardized for use in the general switched telephone network
V.23 600/1200 bps modem standardized for use in the general switched telephone network.
V.24 List of definitions for interchange circuit between data terminal equipment and data circuit-terminating equipment (i.e. modem).
V.28 Electrical characteristics for unbalanced double-current interchange circuit.
V.35 Data transmission at 48 kBps (or more) using 60-108 kHz group band circuits.

Virtual Terminal

Virtual Terminal: An idealised terminal which contains many of the features of real terminals presented in a standardized form.

Virtual terminal Protocol: A protocol within the application layer which provides application processes with facilities for the transfer of data to and from data objects which have the form of virtual terminals.

Virtual Terminal Service: The service provided to application processes which have access to a virtual terminal protocol.

VT: Virtual Terminal (q.v.).

VT100 Terminal: A widely adopted asynchronous terminal protocol and display system defined by Digital Equipment Corporation. The protocol is an extended subset of the ECMA-48 standard and ISO 6429 despite a number of differences.

Watchdog

Watchdog: A nickname for a hardware/software device which monitors a node to detect system errors, and to take the necessary actions in response to errors.

X. Recommendations (CCITT): A series of CCITT recommendations covering data transmission over the public switched data network. Of particular relevance:

X.1 International user classes of services in public data networks.
X.2 International user facilities in public data networks.
X.3 Packet assembly/disassembly facilities (PAD) in a public data network.
X.21 General purposes interface between data terminal equipment and data circuit-terminating equipment for synchronous operation on public data networks.
X.21 bis Use of public data networks of data terminal equipment which are designed for interfacing to synchronous V-series modems.
X.24 List of definitions of interchange circuits between data terminal equipment and data circuit-terminating equipment on public data networks.
X.25 DTE/DCE interface for packet mode access.
X.28 DTE/DCE interface for a start/stop mode data terminal equipment accessing the packet assembly/disassembly facility (PAD) on a public network.
X.29 Procedures for exchange of control information and user data between a packet mode DTE and a packet assembly/disassembly facility (PAD).
X.32 Describing dial-up access to X.25 services.
X.75 Covering interconnection of X.25 networks.
X.121 International numbering Scheme for public data communication services.
X.200 A series of recommendations describing OSI services for CCITT telematic applications.
X.400 A series of recommendations for public message handling systems.

Appendix A.

List of References

(1) An introduction to PAXNET
PAXNET report class 1, no.2, rev.1.10, July 1984

(2) Router Description
PAXNET report class 3, no.1, rev.1.00, November 1980

(3) LIC Description of PAXNET
PAXNET report class 2, no.10, rev.1.00, November 1980

(4) RC3502 DCE Description
PAXNET report class 3, no.2, rev.1.00, November 1980

(5) X.25 Service, Technical Description
PAXNET report class 1, no.1 rev.1.01 December 1984

(6) Session Layer Service, Introduction
PAXNET report class 2, no.4, rev.1.00, March 1983

(7) Network Management System, Introduction
PAXNET report class 2, no.2 rev.1.00, March 1983

(8) Network Management System, General Description
PAXNET report class 2, no.3, rev.4.00, September 1986

(9) Down Line Load, General Description,
PAXNET report class 2, no.6 rev.1.00, June 1983

(10) RC3502, High Speed Communication
Processor. RC Publication RCSL 42-i2393

(11) RC3502/2, Operating Guide
RC Publication RCSL 99-0 771

(12) RC8000, System Architecture
RC Publication RCSL 42-i1221

(13) PAD User Guide,
CASE Publication X.340 - 300051, rev.3.00

(14) Communication Architecture for Layered Open Systems, CARLOS,
Technical Description,
PAXNET report class 7, no.3, rev.1.00, March 1985

(15) Network Operator's Manual, RC8000 NMC
(NMC GEN No.2)
PAXNET report class 4, no.2, rev.1.00, March 1984

(16) General Introduction and Specification of DILA,
PAXNET report class 2, no.11, rev.2.00, May 1984

(17) File Transfer Access and Management,
File Service Definition
PAXNET report class 2, no.5, rev.1.00, December 1985

Appendix B.

List of currently available PAXNET Documents

Class 1

NO	REV	TITLE	DATE
1	1.00	X.25 Præciseringer (Danish Language) Teknisk Beskrivelse	Dec. 1983
1	1.01	X.25 Service Technical Description	Dec. 1984
2	1.10	An Introduction to PAXNET	July 1984

Class 2

NO	REV	TITLE	DATE
2	1.00	Network Management System Introduction	Mar. 1983
4	1.00	Session Layer Service Introduction	Mar. 1983
5	1.00	File Transfer Access and Management File Service Definition	Dec. 1985
6	1.00	Down Line Load General Description	June 1983
10	1.00	LIC Description of PAXNET	Nov. 1980
11	2.00	General Introduction to and Specification of DILA	May 1984

Class 3

NO	REV	TITLE	DATE
1	1.00	Router Description of PAXNET	Nov. 1980
2	1.00	RC3502 DCE Description	Nov. 1980
5	1.00	RC8000 Network Management Center Construction Manual (Tentative Version) (GEN No.1)	Feb. 1984
8	1.00	File Transfer Service Construction Manual	Jan. 1983

Class 4

NO	REV	TITLE	DATE
2	1.00	Network Operator's Manual RC8000 NMC (NMC GEN No. 2)	Mar. 1984
3	1.00	RC8000 NMC Operating Guide (NMC GEN No. 3)	May 1984

Class 5
Class 6

Documents in classes 5 and 6 are not generally available.

Class 7

NO	REV	TITLE	DATE
1	1.00	Analyse af TELETEX Datalogisk Praktik ved DIKU (Danish Language)	Dec. 1982
2	1.00	Network Management Datalogisk Speciale ved DIKU DIKU rapport 84/17, ISSN 0107-8283 (Danish Language)	July 1984
3	1.00	Communication Architecture for Layered Open Systems, CARLOS Technical Description	Mar. 1985
4	1.00	Introduktion til lokalnet Udviklingsafdelingen, KTAS (Danish Language)	Apr. 1986

NOTES

NOTES

COPYRIGHT

The PAXNET project is a joint venture between the following members:

- JTAS
  the Jutland Telephone Company.
- KTAS
  the Copenhagen Telephone Company.
- RC COMPUTER
  the Danish computer manufacturer and software house, A/S Regnecentralen af 1979.

Further information regarding the project may be requested from the individual organizations in the joint venture. The following contact addresses may be used:

- PAXNET group, KTAS, Noerregade 21, DK-1199, Copenhagen, Denmark.
- PAXNET group, JTAS, Sletvej 30, DK-8310, Tranbjerg J, Denmark.
- RC COMPUTER, A/S Regnecentralen af 1979, Klamsagervej 19, DK-8230, Aabyhoej, Denmark.

Printed in 1986.

PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE
PAXNET PAXNET PAXNET PAXNET PAXNET PAXNET PAXNE