AUGUST 1984

CRSN SYSTEM DESCRIPTION

Issue 1.0

AUGUST 1984

The information contained in this publication is subject to continual re-evaluation. Christian Rovsing A/S therefore reserves the right to update this information accordingly.

Please consult your Christian Rovsing representative for further advice on using any information contained herein.

Issue 1.0

CRSN SYSTEM DESCRIPTION

TABLE OF CONTENTS

TABLE OF CONTENTS, cont.

1.0 INTRODUCTION

1.1 THE ORGANIZATION OF TODAY'S NETWORKS

Many corporations today maintain multiple data processing facilities. In many cases, separate networks also exist, organized along geographical as well as functional lines.

Many companies, for price/performance reasons, have also taken a heterogenous approach to their data processing facilities. Today, it is quite common to have a range of computer systems - such as DEC, Univac, Honeywell, ICL and H.P. - alongside IBM hosts.

Other organizations have chosen an IBM orientation in order to maintain some consistency and compatibility. However, this approach intrinsically implies a total commitment to the rigid structural protocol limitations of IBM's systems network architecture.

How, then, are the diverse communication procedures of these totally different vendors to be integrated into one total resource? Where do local area networks fit in? What about office automation, private voice conferencing, teletex, videotex... What do international standards mean to vendor offerings?

1.2 THE CHRISTIAN ROVSING NETWORK SOLUTION

Benefiting from our unique experience in designing highly complex and sophisticated data networks - for example, for NATO, Barclays Bank, American Airlines and Air Canada - Christian Rovsing has developed a Network Solution: The Corporate Resource Sharing Network (CRSN).

The CRSN solution is fully capable of meeting the high demand for expandability, flexibility and availability required by todays carrier.

The solution resolves the data communication problems caused by separate networks. CRSN is the only solution that can completely replace exisiting front-end equipment with state-of-the-art technology. It provides Value Added Services such as Protected Message Switching/Electronic Mail, Videotex, EFT/POS transaction switching and authorization; all services which are directly implemented into the Network Nodes.

Moreover, CRSN creates a modular DP environment specifically structured for smooth migrations to future technological advantages, this assured by having CRSN to be more than just a product but also being a network concept.

2.0 CRSN CONCEPTS

2.1 BASIC DESIGN OBJECTIVES

The Corporate Resource Sharing Network is designed to meet two principal objectives within the realm of digital data communication:

- To provide connectivity between any two end-users, thus enabling meaningful exchange of digital information in real time;

- To manage an organization's DP resources so that optimal usage, through sharing, is achieved.

The first objective generates requirements for compatibility with any connected resource, as well as for conversion facilities to allow end-users belonging to different families to communicate. In order to keep the number of different conversions to a minimum, a requirement for standardization within CRSN is clearly recognized.

The second objective, resource management, has two aspects. Firstly, the resources constituting CRSN itself must be effectively managed; Network Management is thus extremely important. Secondly, a distinction exists between end-users. Some end-users connected to CRSN provide services to other end-users. Information about these services, their location and availability, must be maintained by CRSN to enable end-users to share these services.

The objectives and requirements discussed above clearly indicate that the resource sharing network plays a central role within the corporation. This is reflected in Figure 2.1-1, which shows CRSN as a homogeneus central entity, annotated with the principal requirements for:

- Effective resource management;

- End-user connectivity;

- Compatibility with connected resources;

and the derived requirements for:

- Standardized communication service;

- Value-added services, which can most effectively be placed in the network so as to be accessible to all end-users within the corporation.

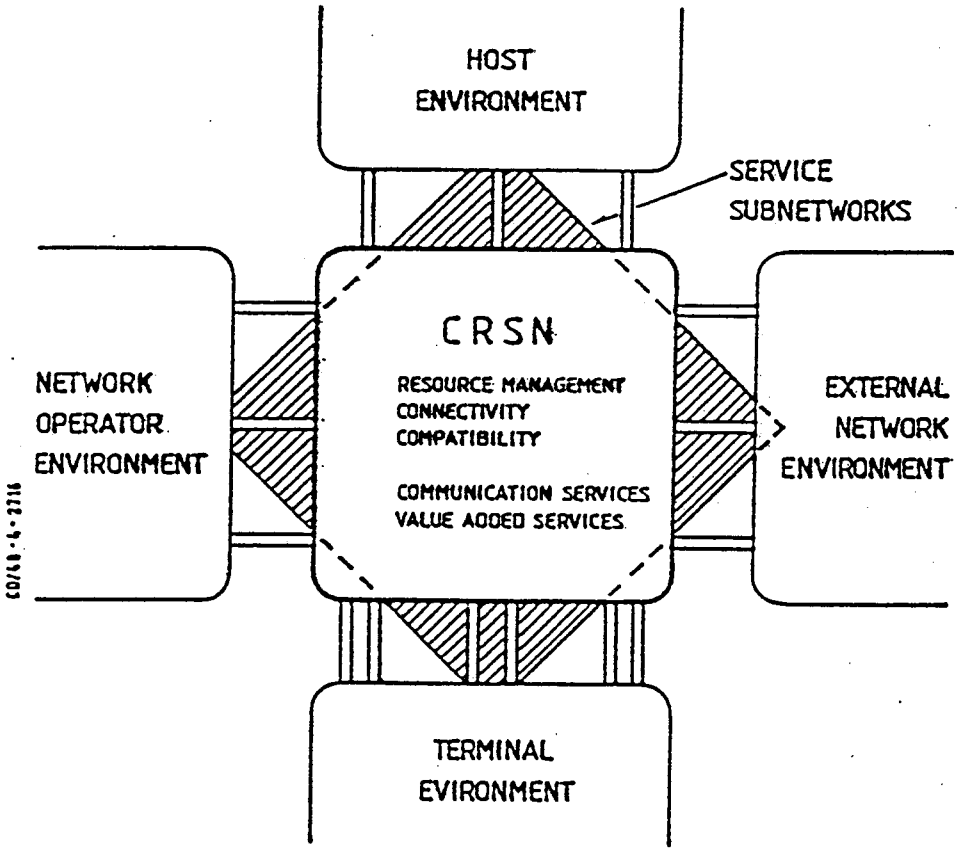

Figure 2.1-1 CRSN Environment

CRSN operates within a set of identifiable environments which are classified into four categories:

- Network Operator Environment;
- Host Environment;
- Terminal Environment;
- External Network Environment.

This classsification, based on physical characterisitics, is explained and further refined in the next section.

Communication between CRSN and one of the environments can either be achieved by some direct means peculiar to the environment, or it can happen via some services provided by a general facility. Such a collection of standardized facilities (e.g. virtual circuits), which at some level provide transparent transfer of data, are referred to as a service subnetwork.

2.2 DP ENVIRONMENTS

CRSN serves the four DP environments which constitute a company's total DP environment:

- The Network Operator Environment;
- The Host Environment;
- The Terminal Environment.

CRSN provides a migration path for integrating, by the same data communication network, present as well as future computer and terminal facilities from the four environments.

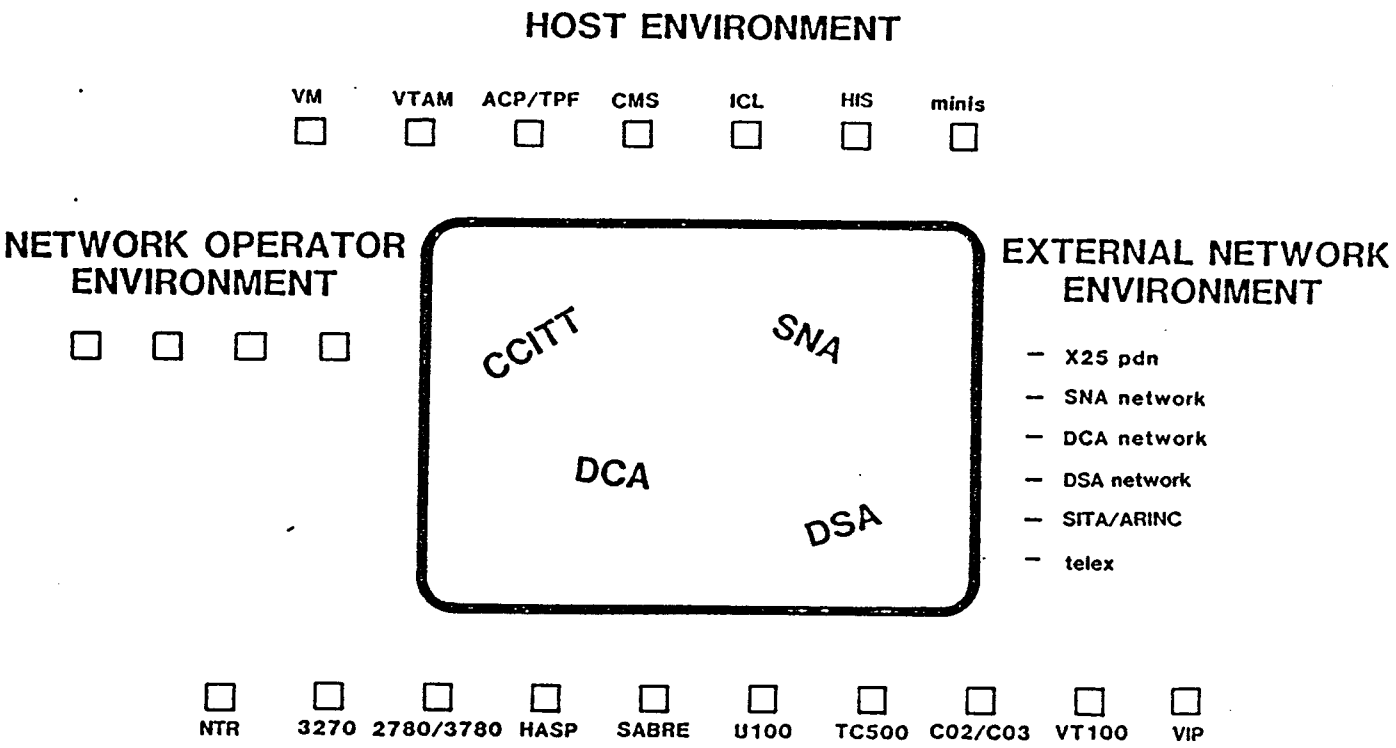

Figure 2.2-1 CRSN Integrates Heterogenous DP Environment

The end-users, host applications and terminal operators use a combination of the facilities implemented in the Host, Network and Terminal Environments, together with those of the network. The network interconnects the external environments and provides a level of integration which makes the actual network topology and application allocation transparent to the end-user.

End-user is the general term for the ultimate source or destination of any information exchange. There are two types of end-users: the human end-user, referred to as user or a programmed user. A special case of a user is a network operator.

End-users access CRSN via access paths formed by a succession of external resources, such as access line, cluster controller and terminal.

The last resource element in the access path can be an application in a host computer, a minicomputer, a personal computer (PC), or a terminal.

Applications can be connected as participants. A participant adds value to the network by providing some identifiable services which may be shared amongst the end-users. CRSN will cooperate closely with participants in order to monitor availability of services and direct requests for a service to the appropriate participant.

Minicomputers, PC's and terminals can be connected as attachments. An attachment is a resource, known to CRSN, through which an end-user can access the services provided by participants or CRSN itself, or which can establish a session with another attachment.

Network Operator Environment

The Network Operator Environment is composed of those users who can influence the behavior of CRSN. Through this environment, they may issue commands to the CRSN which directly affect its operation; or they may request a display of status information.

The operators may use designated color graphic displays, contained directly in the Network Operator Environment; or they may use ordinary devices contained in one of the other environments.

Host Environment

The Host Environment is characterized either by relatively few host processors or by application subsystems (participants) which are tightly coupled with CRSN to allow high data-exchange rates. The relationship with the participants of the Host Environment is normally trusted, i.e. no access control is performed on participants.

Participants will often act as masters in the protocols with CRSN; however, CRSN will try to counteract this tendency.

Terminal Environment

The Terminal Environment usually contains a large number of geographically dispersed devices (attachments) which are configured with specific access paths and characteristics to CRSN.

The CRSN normally has total control over all resources in the Terminal Environment. Access paths between attachments and participants can either be static or dynamic (switched). By default, any end-user can access CRSN through the Terminal Environment and obtain access to a predefined set of participants. An access control scheme allows a differentiation of individual end-user capabilities.

External Network Environment

The External Network Environment contains a mixture of participants and attachments.

The physical configuration of the resources remains unknown to CRSN. Instead, it communicates with the External Network Environment on peer level protocols to convey the identity of the end-users and to control access to and from the External Network Environment.

2.3 THE CRSN ARCHITECTURE

CRSN is conceived as consisting of five interrelated functional environments. The five environments are designated as:

- Network Interface Environment
- Communication User Environment
- Data Transmission Environment
- Data Link Environment
- Network Services Environment.

The above environments broadly relate to contemporary layered architecture, like SNA, Digital Network Architecture (DNA), Honeywell's Distributed Systems Architecture (DSA), and the Open Systems Interconnection reference model.

The proposed architecture is mapped on the OSI as follows:

- application layer	Network Interface Environment
- presentation layer	
- session layer	Communication User Environment
- transport layer	Data Transmission Environment
- network layer	
- link layer	Data Link Environment
- physical layer	

The Network Interface Environment provides the physical and logical interface with attachments and participants of the external environments. It relieves the interconnected equipment of the burden of providing the appearance expected by either end of a connection.

The Communication User Environment consists of components that establish and maintain an orderly exchange of information between two end-users.

The Data Transmission Environment consists of components that provide the actual communication path through CRSN supporting the dialogue between two users. This environment supports both connection-less as well as connections, subject to end-to-end assured delivery.

The Data Link Environment consists of firmware components which transport data over physical internodal links.

The Network Service Environment consists of components which provide network control and management to the network operations staff, as well as the provision of value-added services to network users.

The Network Control and Management Services are provided to the network operation staff. The following facilities are made available through these:

- Network Definition;
- Dynamic Resource Management;
- Statistics Collection;
- Event Management.

Value-added services provided by CRSN include access control facilities, which ensure that only authorized users have access to the participant services provided by CRSN.

3.0 FUNCTIONALITY OVERVIEW

CRSN implements a number of services with a set of software/hardware elements, each based upon functionality and a requirement of "minimal" interface with other packages.

Figure 3-1 illustrates the functional areas assigned to the two important generic elements, the Network Control Center (NCC) and the Node. The shells illustrate the layered structure of the CRSN-OSI environment, meaning that outer shells require the services provided by the inner shells.

The functional areas are:

HAS - Host Access Services;

TAS - Terminal Access Services;

ENAS - External Network Access Services;

NMS - Network Management Services;

LNMS - Local Network Management Services;

VAS - Value-Added Services;

NSS - Nodal Switching Services;

SCS - System Control Services;

BCS - Basic Communication Services.

Each service is implemented in a specific software package. The software elements within a node are linked by the Basic Communication Services (BCS) of the CR80 Operating System, MXAMOS.

The hardware elements of CRSN all belong to the Christian Rovsing CR80 minicomputer family.

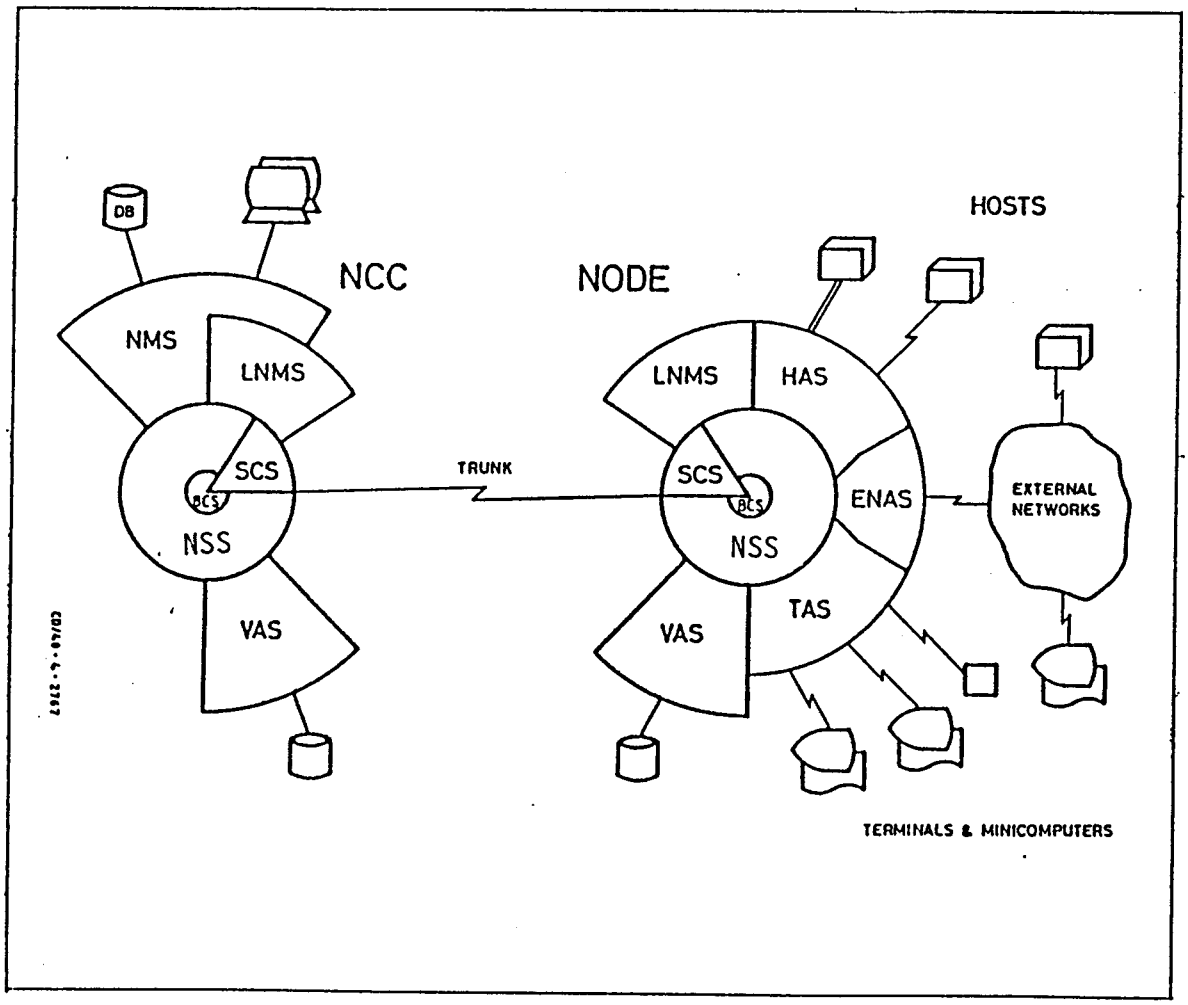

Figure 3-1 Functional Areas within CRSN

3.1 HARDWARE MAPPING

CRSN is realized by means of primary and secondary nodal systems, referred to as nodes, together with a Network Control Center system, and - where applicable - dedicated systems implementing value-added functionality.

All systems are based on the same computer, the Christian Rovsing CR80. This leads to substantial logistics savings, derived from using the same equipment throughout the network.

The Network Interface Environment and the Communications Environment are implemented (in hardware terms) by sharing the same nodal processing equipment. Figure 3.1-1 illustrates a single network node implementing several different services all in one CR80 configuration.

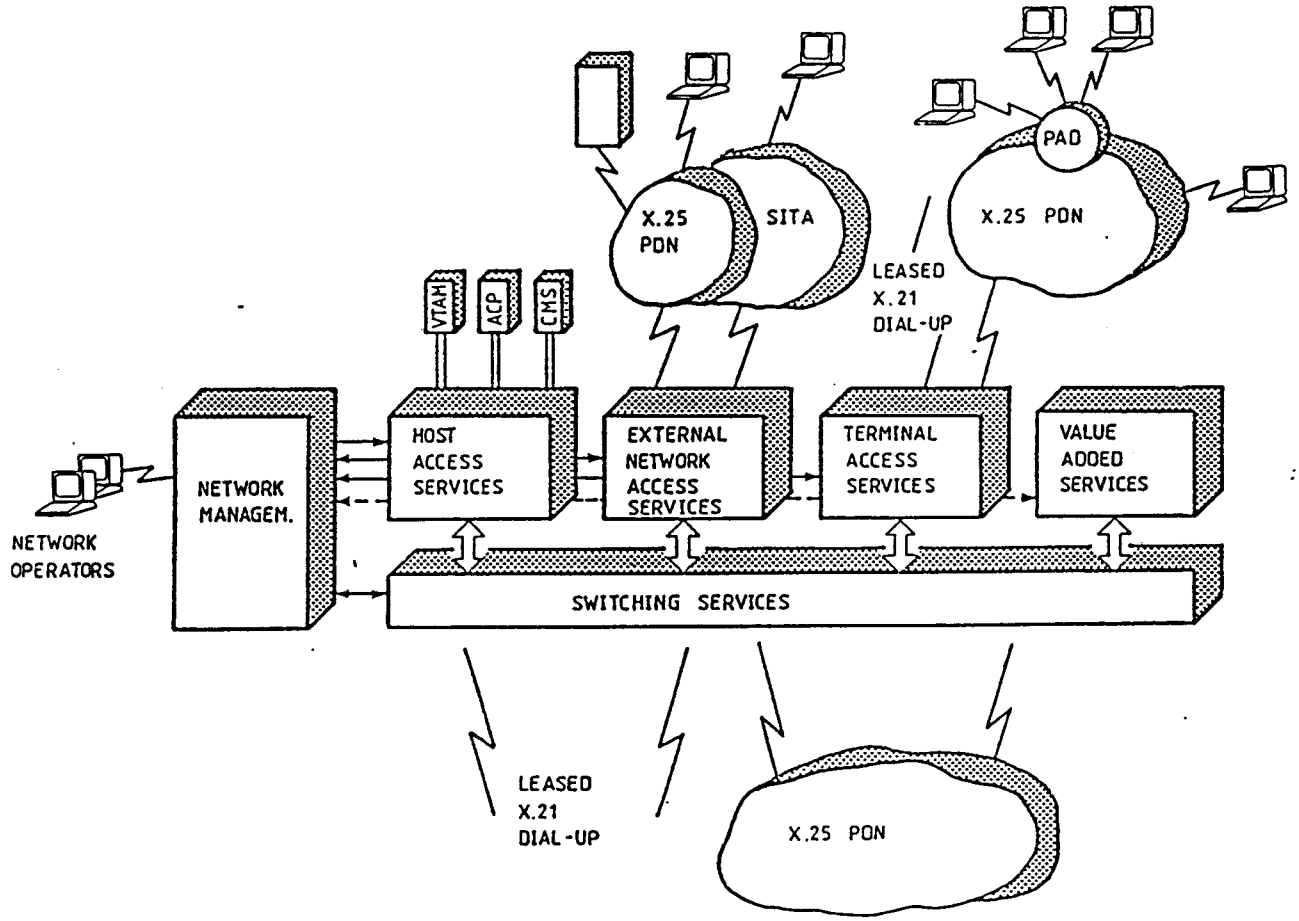

Figure 3.1-1 CRSN - Nodal Services

The specific interfacing may be conceived as implemented by multiple Host Interface Processors (HIPs), Terminal Interface Processors (TIPs) and Gateway Processors (GWPs) interconnected by a common high speed bus, the data channel. The Data Transmission and Data Link Environments are implemented by Transport Network (TN) Processors which provide interface to internodal lines connected to other nodes. Each of these processors operates independently of, and is controlled by a dualized nodal switch processor (NSP); the main task performed by the NSP is exchanging data, generally in the form of full messages, between the processors. The entity described above defines an NSP subnode.

One or more co-located subnodes may be interconnected by means of a highspeed bus complex, the S-net into a Node. Primary Node subnodes are controlled locally by a redundant System Control Processor (SCP) subnode, whereas secondary nodes are controlled remotely from the SCP in a primary node.

This is illustrated in Figure 3.1-2. The actual hardware implementation by the CR80 reflects and fully supports this open-ended architecture.

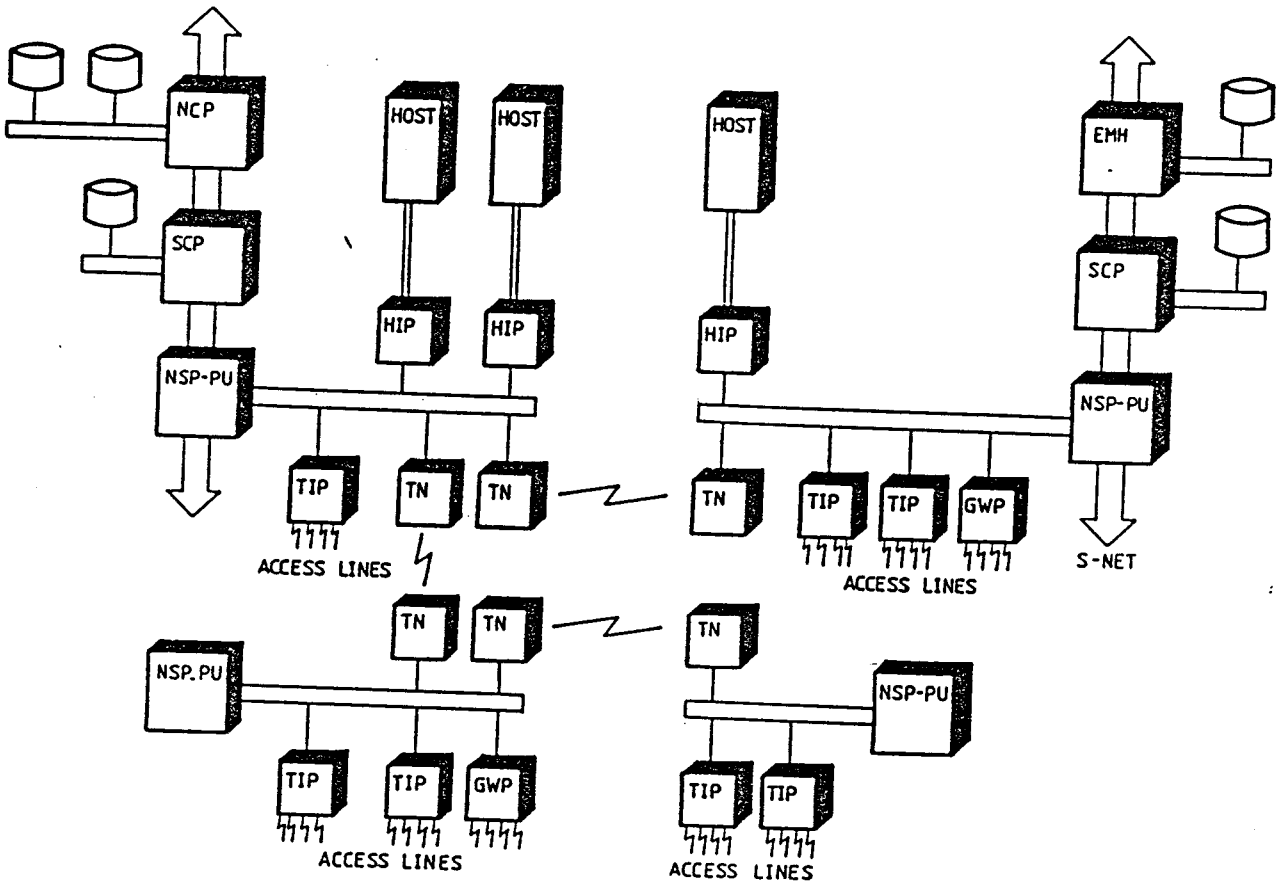

Figure 3.1-2 CRSN Network Realization

Nodes provide the termination points to equipment of external environments, whether in the form of host data channels or communication access lines to terminals and to other networks.

The nodes are mutually interconnected by groups of 9.6 up to 72 Kbps internodal lines. These lines are the physical transmission media used by the Data Link Environment.

The Network Service Environment is implemented on a number of processors, each dedicated to a specific set of services.

A Network Control Center (NCC) implements the network management facilities to designated network operators, referred to as network supervisors. The services provided by the NCC are available on a network-wide basis.

An Electronic Mail Host (EMH) implements the hardware required to provide protected message service (PMS), as well as proper distribution of multiaddressed messages. The EMH provides centralized protected storage for the PMS traffic, in the form of mirrored disk equipment, while long-term storage is provided in the form of moveable disk packs and magnetic tape.

A Videotex Host (VTH) implements the hardware required to support a videotex data base. CRSN can support multiple such hosts thereby facilitating a distributed Videotex application.

An EFT/POS Host implements the hardware to support transaction switching and authorization including a high performance data base system.

3.2 NETWORK ACCESS SERVICES

The Network Access Services provide the direct physical and logical interface to the CRSN environments.

These services consist of the interfacing hardware and software required to support integration with external elements, actively in the form of e.g., participating hosts providing services and co-operating with the network; passively, in the form of attachments, e.g., the terminal equipment.

The elements implementing these capabilities are:

- Host Access Services (HAS);
- Terminal Access Services (TAS);
- External Network Access Services (ENAS).

The hardware implementing these capabilities are:

- Host Interface Processor (HIP);
- Terminal Interface Processor (TIP);
- Gateway Processor (GWP).

3.2.1 HOST ACCESS SERVICES

The primary characteristics of the Host Access Services (HAS) are:

- High performance, tight coupling with many parallel sessions;
- Management of few external resources, but with a high degree of state awareness;
- Via trusted connection, interface to host and to trusted end-users in the host.

The interface to hosts is fully compatible with the native network architecture of the host at the network level as well as at a terminal interface level. This is extremely important since it guarantees that CRSN will benefit from future enhancements in the hosts' network implementation.

The HAS implement access methods which operate at mainframe channel speed and, towards the host, make the network appear as a front-end representation native to that host. As such, the HAS implements the adaption required for a host to integrate as a participant.

The following host interfaces are currently supported:

- IBM 30XX, 43XX, 370/-with Block or Byte Multiplexer channels towards VTAM;
- IBM 3705 via SDLC link as remote NCP;
- Univac 1100 mainframe with high-speed channel;

- Univac 1100 mainframes as remote DCP;
- ICL 29XX mainframes with high-speed channel;
- ICL 29XX mainframe via CO3;
- Honeywell via HDLC link to Datanet 8 (FEP).

The HAS implements compatibility with the following network architectures: SNA (IBM), DCA (Univac), DSA (Honeywell).

3.2.2 TERMINAL ACCESS SERVICES

The primary characteristics of the Terminal Access Services (TAS) are:

- Connectivity to a large population of external devices;
- Support for both static and dynamic (switched) connections;
- Facilities to control and diagnose the external devices.

The TAS implement access methods which operate with communication lines towards terminal equipment. Furthermore, TAS may convert the features of a wide variety of terminals into terminal features recognized by the hosts.

By supplying this broad-range compatibility, TAS enables any network user to use any application on any network host, virtually irrespective of host or terminal vendor.

Data transmission route assignments are automatic and require no special action by the user, other than the user's identifying the desired host processor.

An important Network Access Service roll is to give an end-user access to a participating host by endowing the user with the appearance of a valid end-user native to that host. This transparancy is implemented by transforming, where applicable, the user's data into a format better suited to the particular host.

The HAS and TAS participate in establishing and maintaining connections between two end-users. Both are subdivided into entities, with one such entity for each type of host or terminal. They share the resources of the subnode equipment.

The application of direct channel attachments, replacing existing front-end processors, allows a cost-efficient connection to be established with host processors.

Some terminal protocols that are currently supported by TAS are:

- TTY with Async. protocol;
- TTY compatible terminals including VDUs;
- IBM 3270 BSC, 3270 SNA or compatible;
- IBM 2780/3780;
- HASP work station;
- IBM 3770/3790 RJE;
- IBM 3767 SNA;
- UNIVAC UNISCOPE 100/200, UTS 400/4000;
- UNIVAC NTR.

3.2.3 EXTERNAL NETWORK ACCESS SERVICES

The External Network Access Services (ENAS) are characterized by:

- Capacity for a vast amount of end-users, of whom relatively few are active at any time, and
- Facilities for distinguishing between attachments and participants, and for providing higher level functions similar to TAS and HAS.

The ENAS supports interface to:

- X.25 PDNs;
- SNA Networks;
- DCA Networks;
- DSA Networks;
- SITA/ARINC (airline networks);
- Telex.

3.3 NETWORK MANAGEMENT SERVICES

The Network Management Services (NMS) play a key role in maintaining the integrity of the network. They provide sophisticated maintenance and control facilities, which are a prerequisite for safe operation of a large data communication network.

Network-wide resource and control facilities are provided by Network Management Services of the Network Control Processor (NCP), supported by local NMS and System Control Services (SCS), located in the nodes. The SCS implements local system-wide resource management in the local System Control Processor, assisted by resource management entities in the local node equipment.

The control software, in the form of the NMS and SCS, may be considered as participants, since neither supports transmission of user data; instead they control network and local resources respectively. The NMS uses permanently allocated connections and resources in the network to establish its control of the remaining part of the network topology.

The NMS uses network access software packages as a source to achieve and retrieve configuration control information, events and statistics. The NMS/SCS plays an active role in re-establishing of connections between users (sessions) when such a connection has been temporarily lost.

3.4 VALUE-ADDED SERVICES

The CRSN can also incorporate commercial services developed by the user, other vendors, or by Christian Rovsing A/S in-house.

The CRSN is not only fully receptive to additions of current Value-Added Services, but can also accept enhancements as new technology becomes available - without requiring new computers or new inventions. Virtually without restriction, CRSN can grow with new revenue-producing commercial services.

Some of the currently available optional Christian Rovsing Value-Added Services which can be incorporated into CRSN are:

- Protected Message Switching;
- Electronic Mail;
- Videotex.
- EFT/POS Message Switch and Data Base.

Other services in the form of administrative billing and planning and dedicated development capabilities can also be offered by CRSN. Development capabilities are provided by standard development tools, using processor equipment of a Test Drive System (TDS).

3.5 NODAL SWITCHING SERVICES

The Nodal Switching Services (NSS) implements a bridge between the different entities of the various network access services, HAS, TAS, and ENAS as well as with value-added network application.

The NSS is devided into

- The Transport Network (TN), which interconnects individual CR80 Systems, and
- The Basic Communication Services (BCS), which is used for internal transportation of data within a CR80 configuration.

NSS is implemented by mutually interconnected Nodal Switch Software executed in the Nodal Switch Processors and the Transport Network Processors.

The following essential service types are provided by the NSS to the entities of the Access Services:

- Datagram type of service (connection-less type);
- Switched virtual connection;
- Permanent virtual connection;
- Priority;
- End-to-end acknowledge;
- No end-to-end acknowledge.

The transportation provided by NSS is carried out by means of transmission units in the form of packets transmitted between nodes on internodal trunk groups. The routing of data is handled by providing each message/packet with a routing header and employment of an efficient routing strategy. A multi-link procedure applied on groups of 72 Kbps lines, facilitates a very high use of high-speed, inter-nodal communication lines without sacrificing the end-user service level.

4.0 NETWORK ACCESS SERVICES

This section describes the Network Access Services provided by CRSN in different environments of host and terminal equipment. It also describes the general Access Control procedure and the connectivity features of CRSN.

4.1 SNA ENVIRONMENT

CRSN provides complete replacement of existing 37X5 front-end processors.

The host access services for VTAM hosts are provided by:

- Emulation of a shared local 37X5 running NCP;
- Emulation of a non-shared remote 37X5 running NCP;
- Emulation of the Cross Domain Resource manager for communication with VTAM.

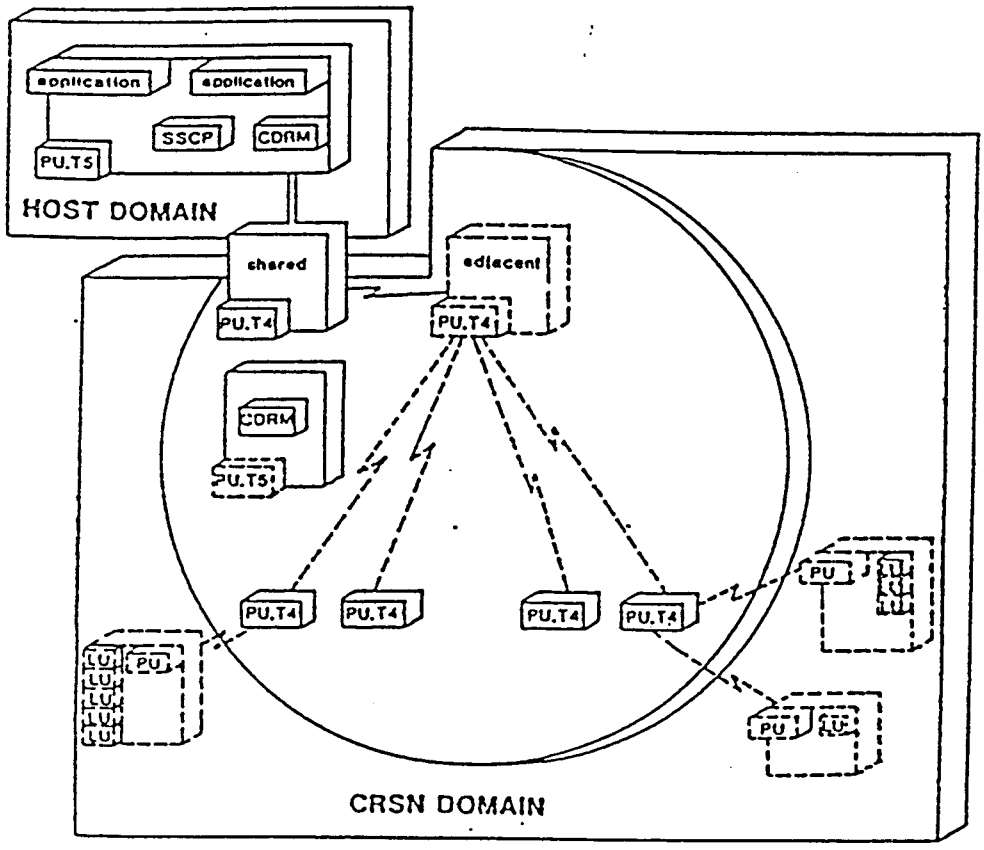

Figure 4.1-1 CRSN Domain Appearance Towards VTAM Hosts

The appearance of CRSN to the SNA hosts is much like an SNA Communication Management Configuration (CMC), wherein one domain, controlled by the CMC host, contains all the SNA (and non-SNA) resources (except for resources resident in other hosts).

The important difference is in the implementation of domain control. The CMC host performs all domain control, including session management; whereas CRSN distributes domain control to the Network Access Services. Only overall SNA-independent central control is maintained in Network Management Services. This prevents overloading of the Network Management Services. Availability is improved, because sessions are not affected by any Network Management Services failure.

The major characteristics of this integration with SNA are:

- Minimal VTAM/NCP definition, i.e. freed host resources;
- Minimal host dependency;
- Configuration awareness;
- Channel or link connection;
- Recovery facilities;
- Status awareness;
- Use of SNA sessions as communication channels.

Except for very limited VTAM host control operations on the emulated NCP, all communications flow across a domain boundary. This means the host is shielded from any knowledge of the network's physical configuration. It only knows the identity of some Logical Units and the existence of some paths ("explicit routes" in SNA terms) to the CRSN and to other IBM hosts. The CRSN HAS is aware of host LUs which can be used by other participants.

Once the connection to the host is activated, the HAS will constantly monitor the status of the defined participant Logical Units, so that the CRSN Access Control can route requests for service to the proper LU.

For transactional traffic, a set of permanent SNA sessions from HAS to host can serve as communication channels, through which transactional traffic from different end-users can be multiplexed. However, this facility requires cooperation from the host application to allow identification of unsolicited transactions. The multiplexing of transactions is based on implementing IBM's SLU type P (Programmable) in the HAS, which is supported by IMS and especially used in the IMS Fast Path Version.

The Terminal Access Services (TAS) support SNA devices of the following characteristics:

- PU Type 1 and 2, and

- LU Type 0, 1, 2, 3 and 4

The TAS handles the SSCP-PU and SSCP-LU sessions towards the SNA devices and provides the necessary Boundary Functions.

Besides supporting native LU-LU sessions with SNA applications, appropriate Primary Logical Unit support is provided for running standard sessions (virtual protocol) with non-SNA applications.

The TAS allow as well, non-SNA devices to access the SNA host applications by performing cross-emulation thereby mapping non-SNA devices into SNA LU appearance.

4.2 VM ENVIRONMENT

The support of VM host processors offers a significant off-load in the hosts; yet the front-end supports many more concurrent SNA-VM sessions than could normally be supported.

The host access services for an IBM VM Host support:

- Emulation of a channel-attached 37X5, and

- Subchannels in NCP and/or EP mode for multiple Virtual Machines running VTAM, CMS and RSCS.

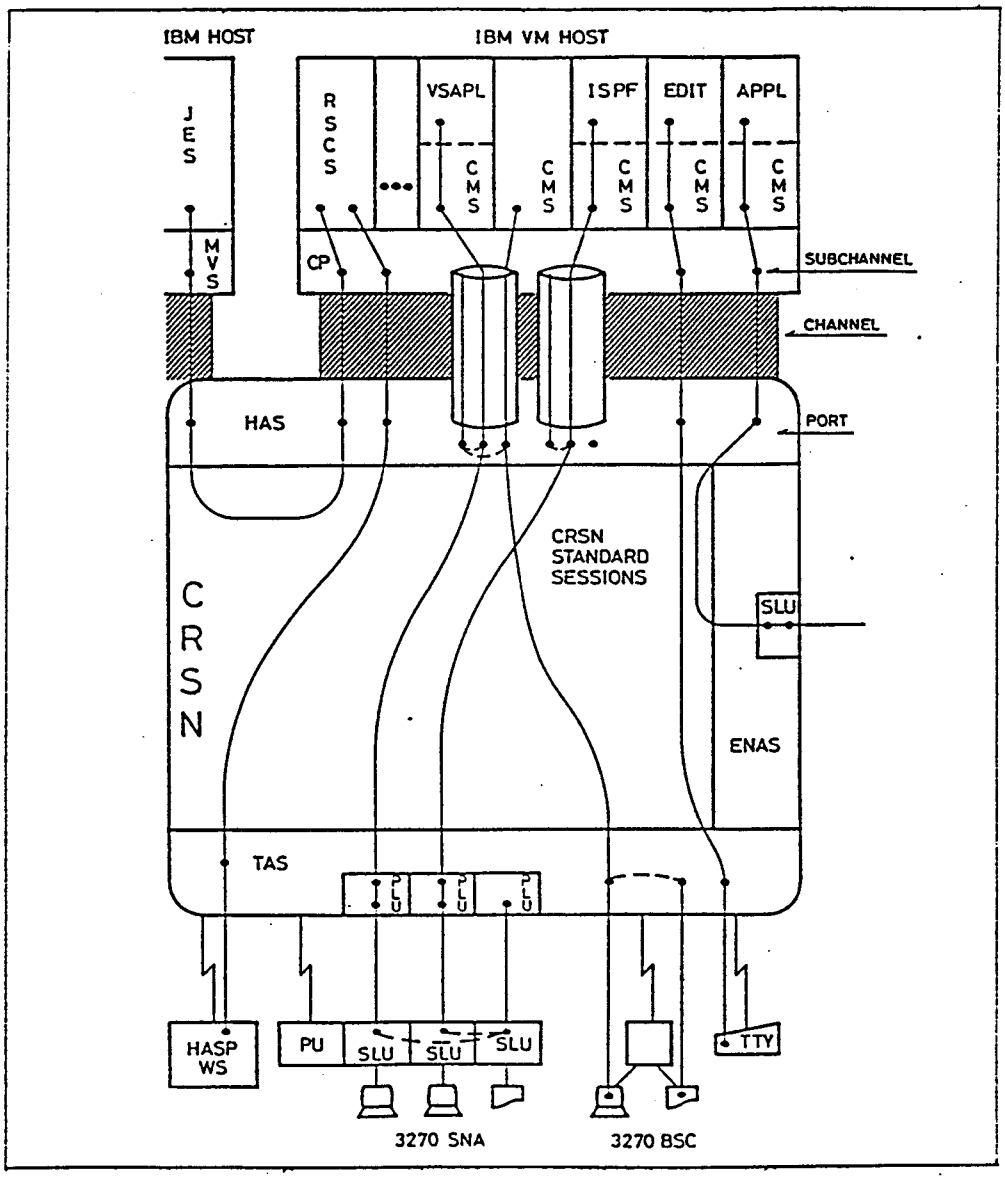

Figure 4.2-1 IBM VM Host Connectivity

The CRSN HAS interfacing with a VM host is via a single channel, as in an IBM 3705 running NCP/PEP. Each subchannel in EP mode represents an access line to CP. On each of these virtual access lines, the HAS maintains a number of ports:

- A multileaving line contains one port;
- A BSC line contains a number of 3270 display and printer ports, as defined both to CP and the HAS, and
- An asynchronous line contains one TTY port.

The association between real devices and ports is only at the session level. This means that no relation exists between the link level protocol, the configuration and the addressing used for the virtual lines and the real terminal.

Via standard sessions through CRSN, ports may be dynamically connected to other access resources.

A multileaving port is associated with RSCS and can connect to:

- An HASP Workstation;
- JES within a non-VTAM host;
- Another RSCS.

CRSN manages the data flow, but does not in any way interpret the data on such a port.

A 3270 display port is associated with a Virtual Machine running CMS and is connected to the 3270 display terminal which started the Virtual Machine.

The display terminal may be SNA or BSC type. If the terminal is an SNA type, the SNA session is terminated by a PLU function in the TAS. Via an available virtual BSC port, data is then passed through a standard session/internal connection to the host.

Note: This scheme eliminates the need for a VTAM service machine (VTAM, VCNA, OS/VS1), thereby significantly offloading the host and allowing many more concurrent SNA-VM sessions.

Applications under CMS may either use the terminal in line mode or in full screen mode.

A 3270 printer port is used to support the CP copy function. Traffic on the printer port is routed on the session for the corresponding display, so that the TAS can ensure further routing to the appropriate real printer.

A TTY port is associated with a Virtual Machine running CMS and is connected to the TTY terminal or IBM 3767 SNA terminal which started the Virtual Machine. The applications under CMS must use line mode only.

4.3 ACP ENVIRONMENT

CRSN supports the ACP Environment with its ACP or ACP/TPF host processors and ALC - whether SABRE type or P1006 type, BSC - and SDLC terminals.

Also supported are ACP/TPF hosts implementing Network Extension Facility (NEF) to access ALC terminals via SNA and ACP/TPF hosts running in a Computer Network environment using ACF.

The host access services for ACP/TPF are provided by:

- Emulation of a channel-attached 3705;
- Emulation of the 3705 Partitioned Emulation Program (PEP);
- Emulation of NEF supported by ALC terminals.

Because the CRSN HAS allows for the attachment of several hosts (ACP or other) communication between hosts may be at mainframe channel speed rather than at link speed.

To avoid host polls received by the HAS being propagated to terminals attached to the Terminal Access Services (TAS), remote polling is implemented. The TAS polls the terminals. The HAS responds to the host polls and only in the case of a data transfer in either direction is a message sent between the HAS and the TAS.

Also available is a dual routing capability to facilitate copying live data from any access line to any VM-based ACP/TPF test machine. This feature is especially useful when new ACP applications are tested in a near-to-live environment without using simulated data.

Statistics on any access line can be collected as a basis for network planning.

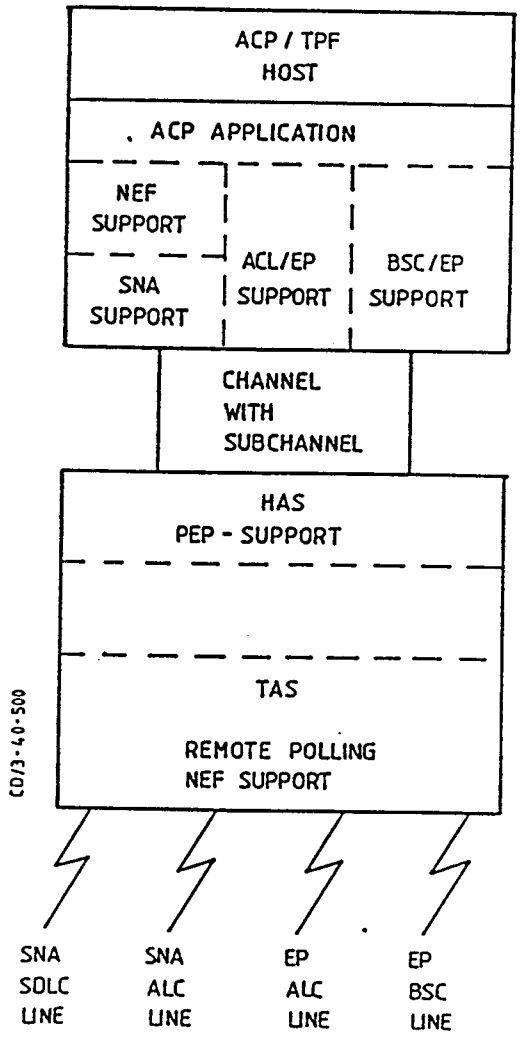

Figure 4.3-1 IBM ACP Host Connectivity

Extensive event monitoring and filtering are provided. Error conditions are reported as event messages to Network Management. An event filtering mechanism ensures that only "stable" error conditions are reported.

CRSN extends applications available to ALC terminal users by enabling access to MVS-based applications in other domains. Through cross-emulation in the TAS, the ALC terminal appears as an SNA terminal able to access the MVS host through a cross-domain session.

4.4 SPERRY (UNIVAC) ENVIRONMENTS

The CRSN HAS/TAS fully supports Univac 1100-series host processors and the typically U100-based transaction terminal population.

Host Access Services are provided for Sperry (Univac) 1100/XX mainframes, running Distributed Network Architecture (DCA). This is implemented with TELCON running on DCP/40 and the Communication Management System (CMS-1100) module in Univac 1100 hosts.

DCA reflects the stratified reference model of the ISO Open Systems Interconnection (OSI). A message is transferred from one end-user to another via a system session.

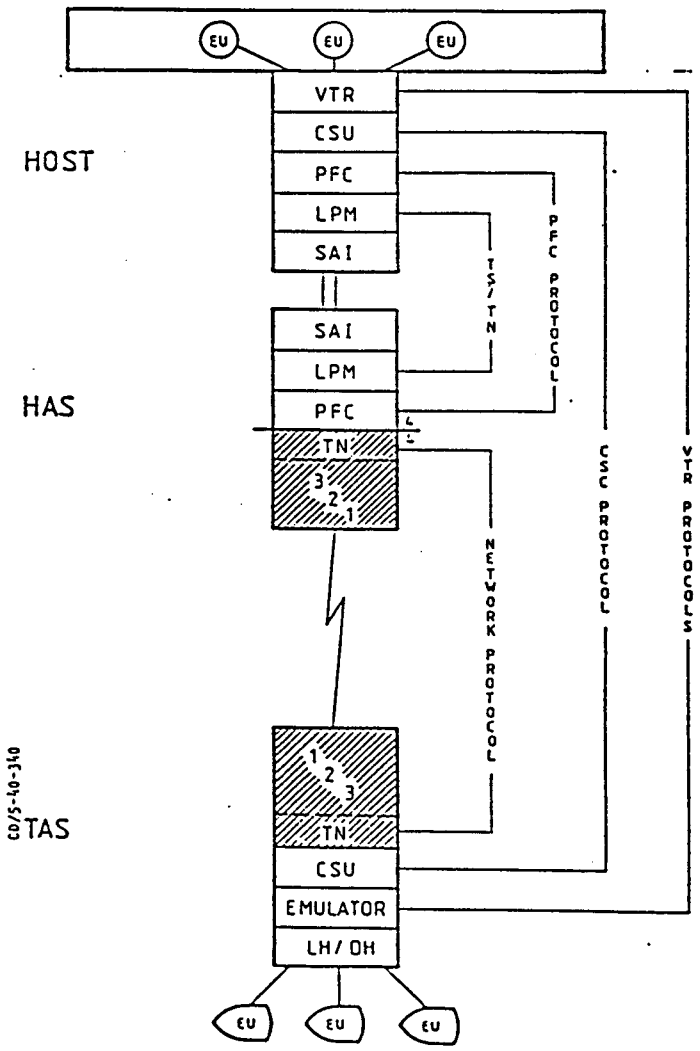

Figure 4.4-1 CRSN Support of Univac DCA

CRSN supports three different connection alternatives towards CMS-1100 hosts:

- Directly, via the Host Access Service (HAS) interface, with the HAS connected to the 1100/XX by a word channel interface.

  With this approach, the protocol layers in the HAS are:

  - Virtual to real (VTR) RB-2, INT-1,
  - Communication system user (CSU),
  - Logical port multiplexer (LPM) as a TS/TN interface,
  - Sub-architectural interface (SAI).

- Via DCP/40, acting as an FEP through the HAS. The HAS are locally connected to DCP/40 or through UDLC links for remote locations.

  With this approach, the protocol layers are the same as above; the HAS appears as an external terminal system (TS) to a DCP/40 FEP.

- Via a pre-existing TELCON network using a remote DCP/40 concentrator.

  With this approach, the protocol layers in the HAS appear as a DCP/40 FEP to the DCP/40 remote concentrator.

  The protocol layers are:

  - Data unit control (DUC), and
  - Route trunk control (RTC).

The HAS functions are monitored and controlled by the Network Control and Management Services Center.

The CRSN network offers the following advantages over the pure Sperry (Univac) TELCON environment:

- Even resources not supported by TELCON can access a Univac host.

- Comprehensive status display, including current status and statistics.

- Color graphics status display, showing the current network configuration and resources' status.

- Performance test facilities for measuring trip delays in the network.

- Any terminal in the network can be used as an operator console, without having to predefine it to perform network management functions.

  Events can be assigned to different categories - e.g nodal, resource name, resource type - or to any number of terminals.

- Separate logs for system command/response, events and statistics.

- Flexible on-line configurator modification facilities.

- Dynamic switchover to a completely new configuration.

- Comprehensive on-line test dump and debug facility.

- Allows multiple application session for one terminal.

- Permits open-ended growth.

4.5 EXTERNAL NETWORK ENVIRONMENTS

The External Network Access Services (ENAS) of CRSN provide services for access to and from networks external to the network environment directly controlled by CRSN:

- X.25 PDN;
- SNA Networks;
- DCA Networks;
- DSA Networks;
- SITA/ARINC;
- Telex.

Public Data Networks can be interfaced according to the CCITT Recommendation X.25, Yellow Book, Geneva 1980. The ENAS communicates as a Data Terminal Equipment (DTE) towards the PDN Data Circuit-terminating Equipment (DCE).

Optionally, PDNs can be interfaced via an X.75 connection. The X.75 is the CCITT recommendation for an internetwork protocol, very similar to X.25. The ENAS provides the full support for the Signaling Terminal (STE), as specified by X.75, which connects to an STE implemented in the PDN. However, not all PDNs support X.75 and the administration of public data networks may not allow this connection; in these cases the X.25 DTE connection will have to be used.

The ARINC Network is interfaced according to the rules laid down in the ATA/IATA SLC procedure. The SITA Network is interfaced according to P1024. Both Type A and Type B traffic are supported.

SNA and DCA networks are supported by ENAS in a manner functionally similar to the support given by the Host Access Services (HAS). The important difference is caused by the different characteristics of the environments: HAS is intended to support a tight coupling, mainly to a few participants, whereas ENAS is intended to support a looser coupling to many resources within the SNA/DCA networks.

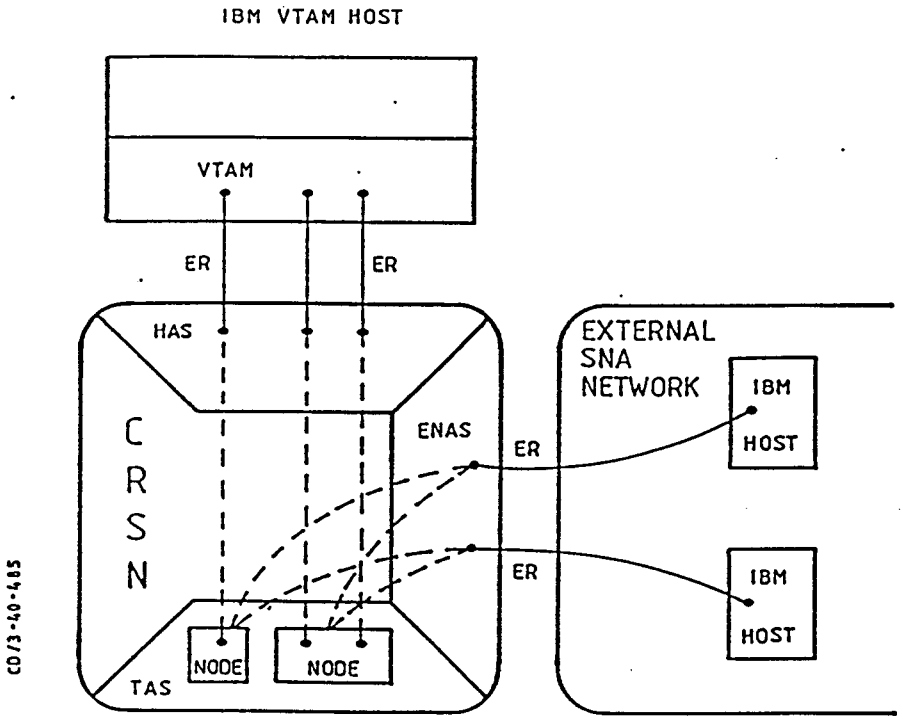

Figure 4.5-1 HAS and ENAS Connectivity with SNA Hosts

Figure 4.5-1 illustrates the HAS and ENAS interfacing SNA hosts. There are three areas where the ENAS SNA support differs from the HAS SNA support:

- Resource names in CRSN and the SNA networks may be different.
- Complete freedom in definition of subareas which represent resources controlled by the front-end.
- Recovery only at the session and host level.

Participating hosts and participating Logical Units must be defined to ENAS, whereas attachment LUs in the SNA networks need not be defined. The defined resources must have unique names in the CRSN, but can also have another name which identifies the resources in the SNA network. In the latter case, ENAS provide name translations whenever needed.

The tight coupling in HAS requires that each host interface is defined to the host as one or more subareas. The ability to map more subareas to a host interface is of considerable benefit since all subareas in an SNA network must have address spaces of the same size. However, especially in a migration situation, subarea numbers are scarce. Therefore, one or more subareas can be defined in ENAS to cover all the front-end resources. The number only depends on the total address space required to identify all simultaneously active sessions.

ENAS provides a looser, but simpler and more flexible connection to SNA networks.

4.6 CONNECTIVITY

This section describes the possibilities for establishing data paths through the CRSN for exchanging data between end-users.

We define an end-user session as an end-user to end-user path with end-to-end significance.

In addition to paths between end-users, the network also provides a path between a terminal and a command processor within the CRSN. This is called a network session. The network session can e.g., be used by a terminal operator to request the termination of an end-user session.

A terminal may, in general, be engaged in only one end-user session at a time. A switchover to the network session while engaged in an end-user session will in general be possible, but may require the use of a customer-defined switchover procedure.

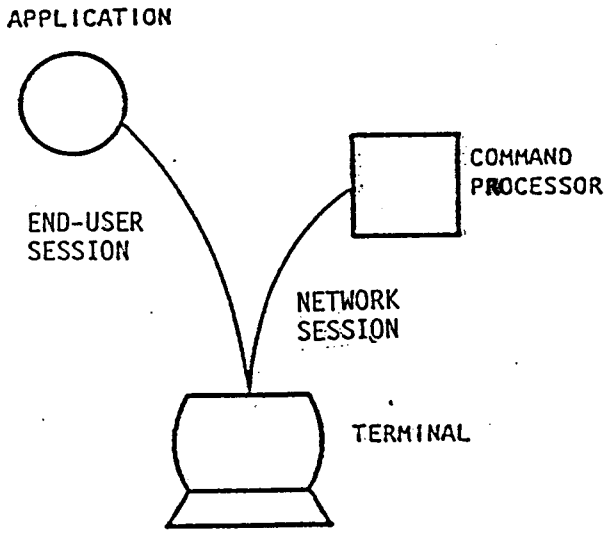

Figure 4.6-1 End-User and Network Sessions

End-user sessions may be in the form of native sessions, in which case the end-users use protocols from the same architecture (e.g. 3270 SNA session with VTAM application), and these protocols are carried through CRSN rather than being converted into a CRSN-specific protocol.

End-user sessions may involve a mapping provided by the network. For example, a terminal type not supported by a certain host computer may be mapped into a protocol supported by this host. The mapping of protocols is performed by cross-emulation programs which are an integral part of the Network Access Services.

A typical end-user session would involve a terminal and an application residing in a participant host. End-user sessions may also be set up between for example, two applications in different hosts or between a terminal and an application residing in the network (a network application).

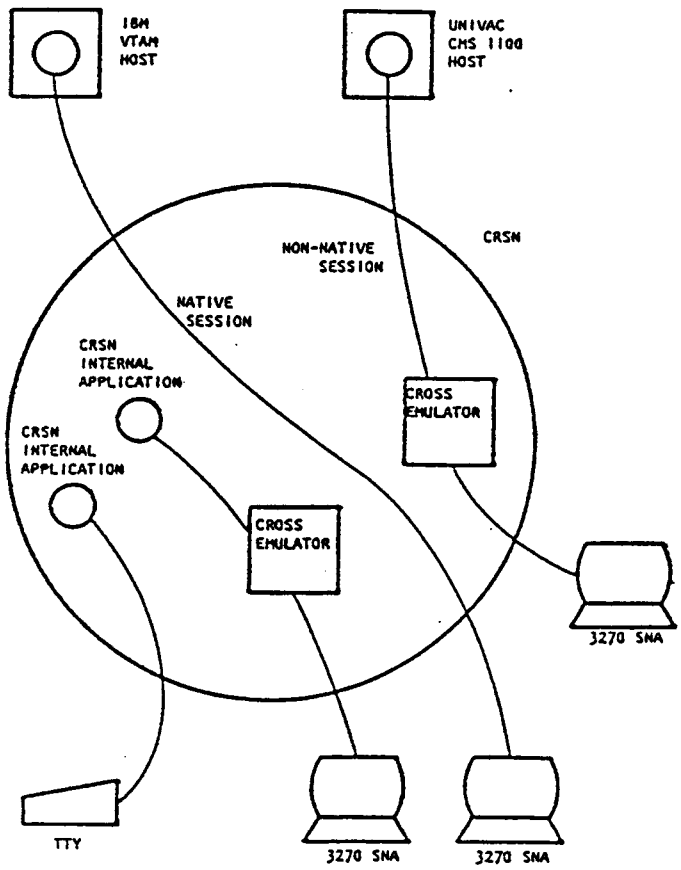

Figure 4.6-2 Example of Native and Non-Native Sessions

Network sessions, which are used by all end-users in CRSN, require a standardization both of the session level and the presentation level. This is achieved via the CRSN Standard Session protocol, which provides a Virtual Terminal Service (VTS) running a simple line-oriented Virtual Terminal Protocol (VTP) on top of the network session.

The Standard Session protocol is also provided for the transaction sessions, which uses the session multiplexing facility in the HAS towards IMS Fast Path (see Section 4.1).

Attachment-to-attachment sessions (e.g. terminal-to-terminal sessions), can be optionally provided by CRSN. This facility also performs mapping of protocols to a standard line-oriented protocol using the ASCII character set.

The following tables provide an overview of connectivity matrices for possible end-user sessions. It covers native sessions as well as non-native sessions involving cross-emulator programs. The description is arranged according to host types.

CRSN CONNECTIVITY MATRICES

1. IBM VTAM Hosts

Terminal	Support
IBM 3270 SNA	Full
IBM 3270 BSC	SNA 3270 LU.TO Appearance
IBM 3767 SNA	Full
Other SNA PU.T2	Full
U100/U200	3767 SNA Appearnace
UTS 400	Do
UTS 4000	Do
TTY	Do
IBM 2780/3780	SNA RJE Appearance
HASP BSC Work Station	Do

Other Host	
IBM VTAM	Transparent

2. IBM VM Hosts

Terminal	Support
IBM 3270 SNA	3270 BSC Appearance
IBM 3270 BSC	Full

3. IBM ACP Hosts

Terminal	Support
ALC Terminals	Full
IBM 3270 SNA	ALC Terminal Appearance
IBM 3270 BSC	Do

CRSN CONNECTIVITY MATRICES, Cont.

4. UNIVAC CMS1100 Hosts

Terminal	Support
IBM 3270 SNA	DCT 1000 Appearance
IBM 3270 BSC	Do
IBM 3767 SNA	Do
U100/U200	Full
UTS400	Full
UTS4000	Full
TTY	DCT 1000 Appearance
NTR	Full
IBM 2780/3780	NTR Appearance
HASP BSC Work Station	Do

4.7 ACCESS CONTROL

Access Control is a standard feature of CRSN. Access control protects DP resources against "penetration".

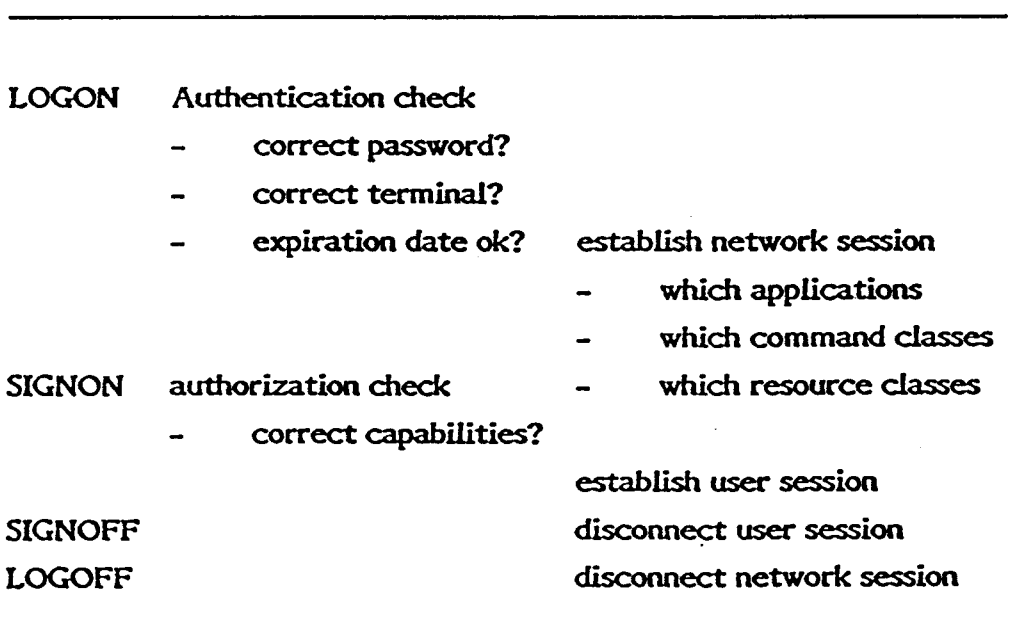

Figure 4.7-1 CRSN Access Control

Authentication

An end-user must be logged-on to the network in order to get access to the services provided via the network.

An important part of network log-on is an authentication based on checks of the security and capability sections of a predefined profile of the user and the terminal.

Unsuccessful multiple attempts to log-on will result in a blocked terminal, requiring network operator interference to unblock.

A successful log-on establishes a network session. The network session lasts until either the user or the network operator issues a log-off command or the network operator terminates the session.

Authorization

The network session authorizes the user for access to a set of network commands and a set of services. This is granted after controlling a combination of the user's security profile with those associated with the terminal.

The result of a successful log-on is the establishment of a network session profile identifying the user's access rights.

During a network session, a user may use commands from only those categories of network commands granted in the session profile. Furthermore, the user is only authorized to have access to those services flagged in the session profile.

By using a special command, the user may sign-on to one or more of the granted services.

The result of a successful sign-on is the establishment of an end-user session, a logical connection between user and service.

An end-user session lasts until the user issues a sign-off, the network operator forces a sign-off, or the application forces a sign-off.

Default Session

A default session exists to support a migration from an existing network environment into the full access control provided by CRSN.

Multi-Session Support

CRSN can optionally provide multi-session support in a transaction oriented environment. It enables a user, who has signed-on to several services simultaneously, to route data to the proper application.

The user may choose whether he wants to switch between applications for each transaction or to route all data to a specific application until he decides otherwise.

5.0 TRANSPORT NETWORK

The Transport Network (TN) provides a reliable data transmission media for the function subsystems in CRSN. The transport network acts entirely transparent to the information transmitted - without involving itself in the semantics of the data.

The transport network provides a well defined "surface" to the higher level subsystems, so that the latter can communicate with one another irrespective of their location in CRSN. These higher level subsystems may be access subsystems or functional subsystems.

All traffic handled by the Transport Network has a source/destination address. The destination address forms the basis for routing of individual traffic to the appropriate destination, i.e. to the next higher functional subsystem; further address resolution is their responsibility.

The service interface provided by the Transport Network encompasses classes and each class has various grades of services.

For the lower level subnetwork, the Transport Network embeds a datagram subnetwork which provides a basic packet transport mechanism which supports all data traffic in CRSN.

The datagram subnetwork is designed to provide resilient internodal routing so that the total capacity and the topology of the underlying backbone internodal lines are exploited optimally.

The network executes network command from and delivers statistics to the network control. Furthermore, it is directly involved in the bootload of adjacent nodes.

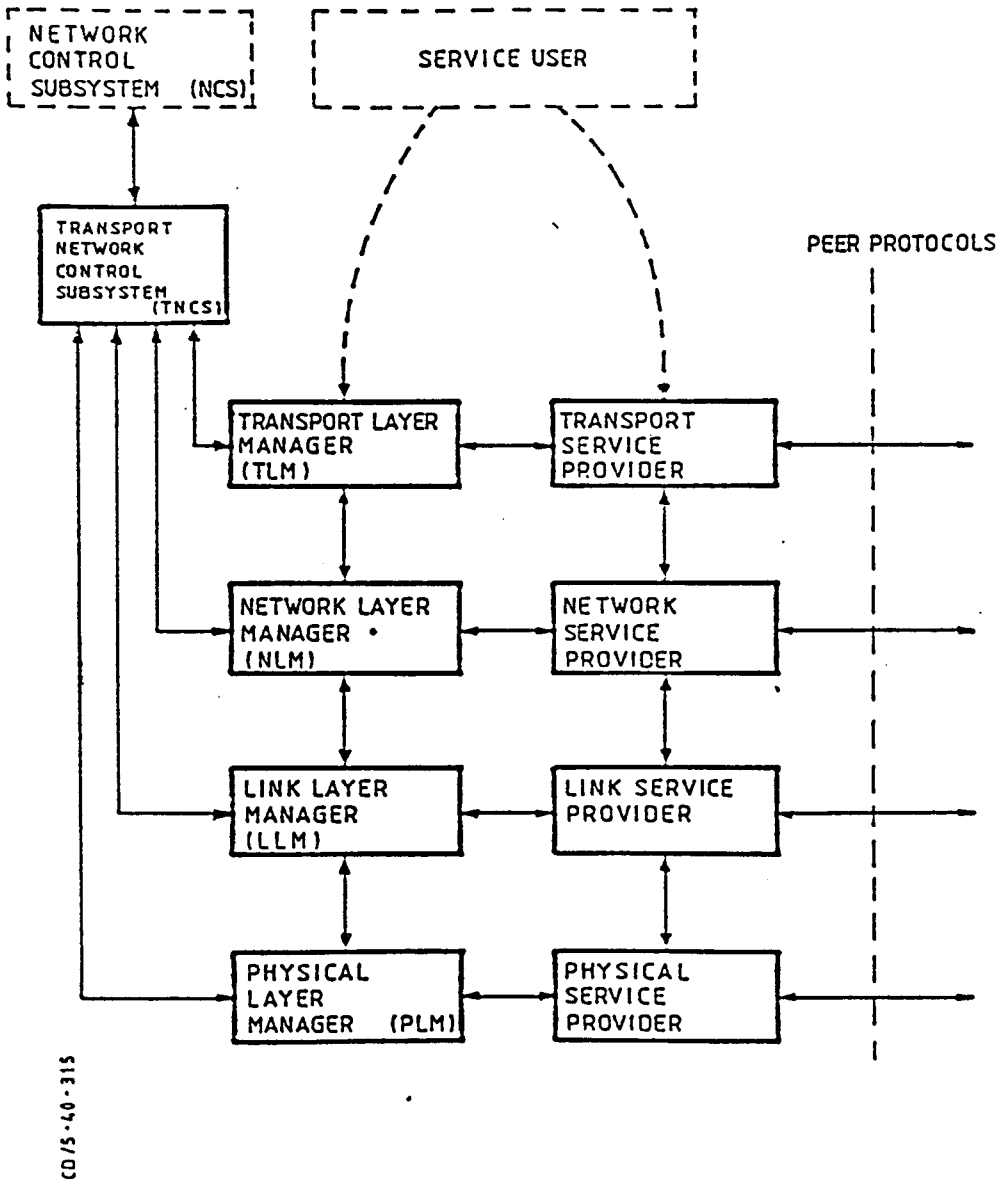

Figure 5-1 The Layer Entities of the Transport Network

The following subsections present a list of functional capabilities of the Transport Network. The functional breakdown of the TN is shown in Figure 5-1, which defines the following functional entities:

- Transport Layer;
- Network Layer;
- Link Layer;
- Physical Layer;
- Management and Control.

5.1 TRANSPORT LAYER

The Transport Layer maintains the fundamental end-to-end characteristics of the underlying network elements, by enhancements of Quality of Service including aspects of cost optimization. The Transport Layer provides Connection Oriented Services (based on ECMA 72) as well as Transaction Oriented Service; the latter in the form of individual data units - messagegrams. The two service modes are co-existent and the service is provided by running the transport layer protocol. The Transport Protocol provides the functions (which are tranparent to the user) listed below.

Protocol Functions for the Connection-Oriented Service:

- Connection Establishment and Termination;
- Sequencing;
- Detection of Duplicates;
- Retransmission;
- Segmentation/Reassembly;
- Flow Control;
- Acknowledgements.

Protocol Functions for the Transaction-Oriented Service:

- Segmentation/Reassembly;
- Confirmed Delivery;
- Non-Delivery Indication;
- Detection of Duplicates.

5.2 NETWORK LAYER

The Network Layer is primarily concerned with routing of datagrams. This is implemented by a Centralized Adaptive Routing scheme where routing tables are calculated (at the Transport Network Control Subsystem) and distributed to the Network Layer. The latter will base its routing ability on these tables; although it takes reported events (such as trunk failures) into account instantly.

The centralized Routing Table Calculation takes the following parameters into account:

- Current topology of network;
- Trunk speeds - Line speeds;
- Weighting factors;
- Cost measurements (the criteria of minimum delay is used);
- Throughput measurements;
- Possible congestion areas in the network.

Furthermore, loadsharing on the trunks is included in the calculations.

The Network Layer functions include:

- Establishment termination of datagram endpoints;
- Detection of availability of other nodes;
- Use of link level endpoints;
- Loadsharing on trunk resources;
- Providing congestion-avoidance resolution;
- Monitoring and measurements of trunk throughput and delays;
- Maintain statistical information on the trunks;
- Network layer resource supervision and control;
- Interface to network layer manager.

5.3 LINK LAYER

The Data Link Layer maintains data transmission over the physical circuits connecting the nodes. The Link Layer provides the means for synchronous, full duplex transmission of frames. It runs the resilient LAPB protocol for each physical circuit to ensure the throughput, a number of links are connected to one logical link by running multilink procedures.

In addition to the procedures defined in the LAPB recommendation, the link-level unit takes an active role in the activities for monitoring unmanned remote nodes. Such procedures are necessary to perform remote master clearing and remote loading.

The main functions of the Link Layer protocol are:

- Provide Link Connection Establishment and Disconnect for the Balanced Node, and
- Provide Full Duplex Data Transmission, Including Sequencing, Error Detection and Recovery.
- Ensure Data Consistency
- Provide Reset Procedures for the Link

- Provide Multilink Procedures for a Group of Individual Lines
- Maintain Status and Statistic Information of Links and Multilinks
- Detect Special Frames Used to Control Remote Nodes (Remote Loading) and Transfer them to the LLM
- Link Test Capability.

5.4 PHYSICAL LAYER

The Physical Layer has facilities for full duplex serial bit transmission over physical circuits, comprised of leased lines. The Physical Layer has the means for controlled establishment of the line and primitive error recovery.

5.5 MANAGEMENT AND CONTROL

This instance of the Transport Network relates to the management and control activities regarding the resources possessed by the Transport Network.

This set of functionality is located in the part of the Transport Network referred to as the Transport Network Control Subsystem (TNCS) and will be distributed among various layer managers (refer to Fig. 5-1), as appropriate.

The management and control functions are implemented partly as functions having effect on a local node, or as functions having effect on a network-wide basis. The latter is accomplished by specific layer management protocols.

Major Management and Control Functions are:

- Event/Error reporting;
- Status/statistic collection and manipulation;
- Execute commands received from the Network Management;
- Calculate and distribute routing tables;
- Interact on specific layer service providers;
- Performance measurements and optimization;
- Configuration management;
- User administration;
- Test and Loop Facilities.

5.6 TN BASIC SERVICES

Having described the major functionality of the Transport Network, this section focuses on the properties of the interface between the TN and the TN users.

Messagegram Service will be provided whereby higher level subsystems can exchange "single-shot" messagegrams.

Each messagegram is transported through the TN and delivered individually. Messagegrams may be up to 4 Kbytes long. Even though transmission of such messagegrams is based on (smaller) datagram packets, they are delivered as a complete entity to the addressed sybsystem.

Connection-Oriented Service is provided for transmitting continuous streams of data. During such transmissions, the two end-point subsystems will be associated via a transport connection. Sequencing and automatic retransmission guarantee the data integrity of the data transmitted via this service.

5.7 QUALITY OF SERVICES

Within the two major classes of services described above, there will be a number of variations. These variations will be based on different combinations of service attributes.

Service attributes are grouped in three types:

1. Common Attributes

   All attributes which are common to all the variations of a service are included in this group.

   Following is a list of such attributes. (M) or (C) after the attribute indicates the relevance to Messagegram Service or Connection-Oriented Service.

   - Protocol Guarantee (M)

     No variations within Messagegram Service provides end-to-end guarantee, in the sense that TN retransmits messagegrams if they are lost.

   - Sequencing (M/C)

     No Messagegram Service provides sequencing. All connection-oriented Services provide sequencing of messages sent with a Transport Connection.

   - Flow Control (M/C)

     All Messagegram Services are subject only to local interface flow control procedures, the latter being negotiable at connection setup time.

   - Message Size (M/C)

     All variations are subject to a specific maximum size of message (4000 bytes). Message sizes in Connection-oriented Services are negotiable between peer subsystems but must be within the above specified maximum.

2. Graded Attributes

   All attributes which are common to all the variations of a service, but may not be graded in intensity, are included in this group.

The following is a list of such attributes:

- Service Priority (M/C)

  All variations will have an implied service priority. This is the priority by which TN undertakes to service a particular variation of a service.

- Resilience Priority (M/C)

  All variations will have an implied resilience priority. This is the priority indicating the importance of the data-contents within a message. This priority will be used by TN internally to affect a control on the total traffic flowing through the subnetwork.

3. Optional Attributes

   - Protocol Guarantee (C)

     Any variation of the Connection-Oriented Service may be specified to include an end-to-end guarantee or no guarantee.

6.0 NETWORK MANAGEMENT SERVICES

The Network Management Services (NMS) provide sophisticated maintenace and control facilities which play a key role in maintaining the integrity of the CRSN network.

The NMS consists of software components resident in the Network Control Processor, also referred to as the Network Control Center (NCC), cooperating with distributed software components in the primary and secondary nodes. The NMS software uses the disks at the primary nodes, whereas secondary nodes are operated without disks, in order to increase availability in an unattended environment.

The key facilities of NMS include:

- Access from any terminal connected to CRSN;
- Support for individual user capabilites;
- User friendly man-machine interface;
- Support for bilingual interface;
- On-line and off-line configuration management;
- Control, test and monitoring of external and internal resources;
- Event handling, statistics collection and report generation;
- Graphics status displays;
- Support for geographically dualized NCC.

6.1 MAN-MACHINE INTERFACE FACILITIES

NMS Access

Network Management Services facilities can be accessed from any terminal connected to the network and possessing a proper set of capabilities. Depending on the capabilities assigned to the user and the terminal, a subset or a full set of operational procedures can be accessed by the user.

A bilingual interface can be provided allowing the user to choose the language in which he wants to communicate with the services.

The man-machine interface is generally user-driven, but in certain areas menues will be used as the vehicle, mainly for network definition. Furthermore, commands can be prerecorded in command files for more effective operation, or be automatically executed at pre-defined time intervals.

Commands may be specified for automatic logging, thereby providing an audit trail. Commands are logged with date and time with the user's and terminal's identification.

A script language provides the operator with facilities for on-line definition of new reports. The language contains facilities for extracting selected data items, for arithmetical and conditional operations, and for conditional execution.

Status Displays

Color graphics status displays give the network operators facilities for closely monitoring the network. The screens give different levels of detail on the current status of specified network parts. One picture shows the entire network in an overview form, giving the status of hosts and other major network elements; another picture shows the status of a single node and associated access lines. Colors are used to indicate the resources' different states. Additionally, a color-form editor is provided with facilities for defining these schematic network diagrams.

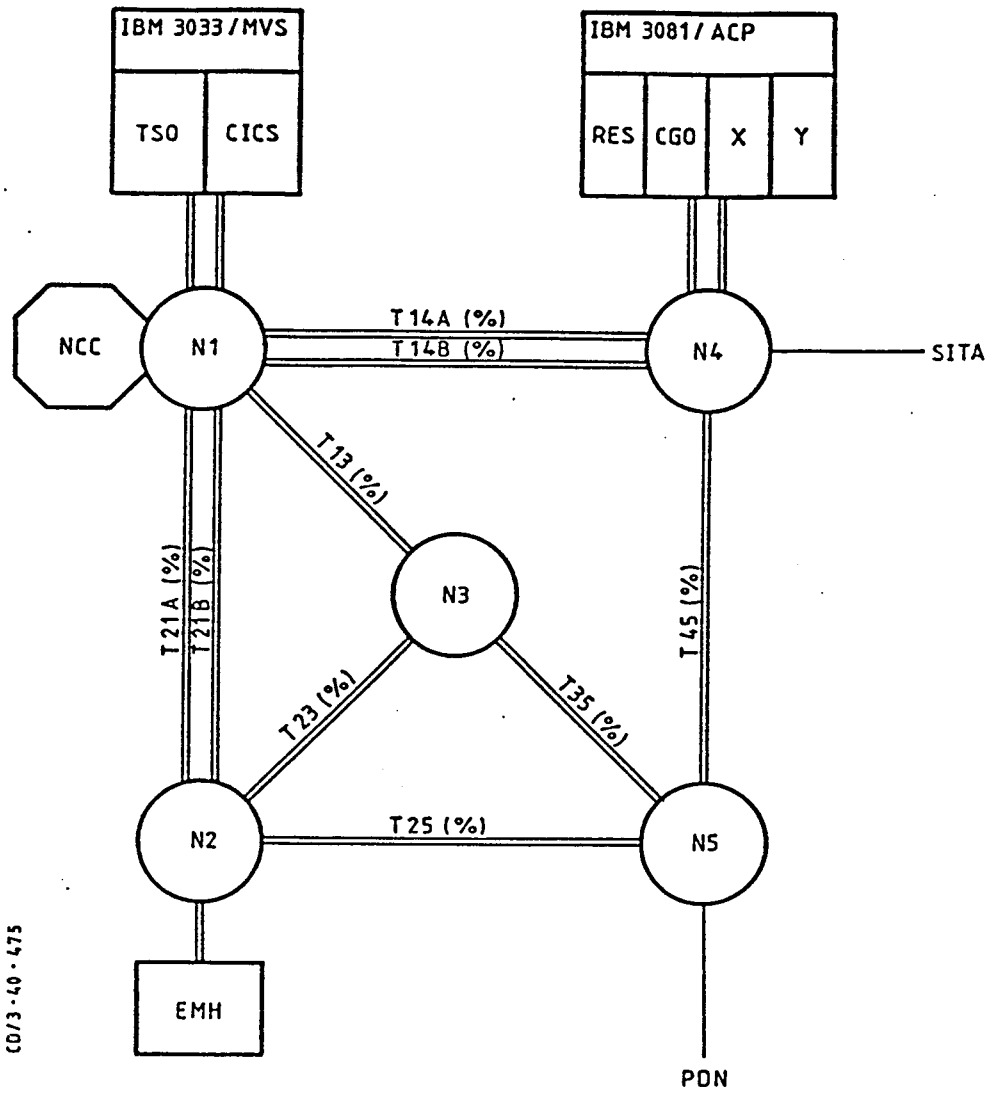

Figure 6.1-1 Network Overview Provided by Graphics Displays; Colors are Used to Indicate Status of Resources

6.2 CONFIGURATION MANAGEMENT

An extremely important Network Management feature is its ability to define and maintain the overall network configuration. Network Management provides full on-line capabilities in this area. Parameters of the line network's existing resources can be modified; terminal/printers, concentrators and access lines can be added to existing configurations. Furthermore, new configurations defined off-line can be activated without taking the network down.

Full support for network operators is provided by three on-line versions of the configuration; one of which may be the current, one the next-to-current, and one the under-update. The available switching capabilities provide a safe fall-back for network operators.

The key features are:

- Support for up to 16 off-line and 3 active versions;
- Update by color form editors;
- On-line update of terminals, concentrators and access lines;
- Support for on-line switching between versions;
- History log for on-line updates.

Global Network Data Base

Resource definition is kept in a set of data bases. The main data base is the Global Network Data Base (GNDB), which contains the following:

- Software Data Base (SWDB), containing all software required for operating the network;
- Network Configuration Data Base (NCDB), containing all configuration data, hierarchically structured to reflect the hierarchy of resources (hardware, Transport Network and Access Resources) within CRSN;

- Profile Data Base (PRDB), containing the access profile definition required for operating the network. Three resource types may assume the end-user role: terminals, applications and users; each of them have an associated profile definition;

- Recorded Information Data Base (RIDB), containing information constantly being collected throughout the network. The information is recorded in sequential files in the order of arrival.

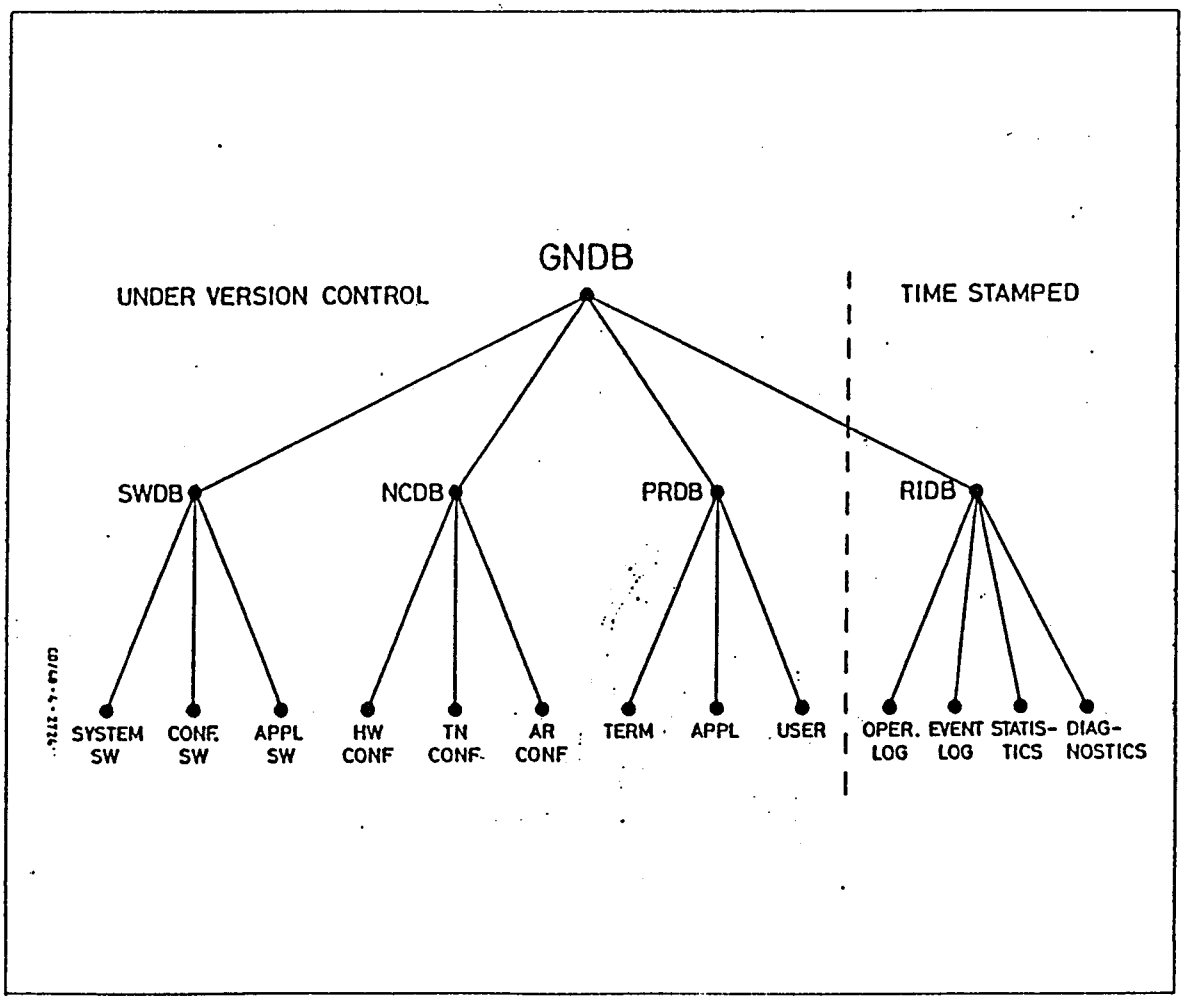

Figure 6.2-1 Organization of the Global Network Data Base

Network Configuration

The network configuration is defined and maintained by using:

- On-Line handling for:

  Modifying parameters of existing resources and for adding terminals/printers, new concentrators, and access lines to the existing network configuration.

- Off-Line definitions:

  Facilities are provided for adding and deleting resources to/from the Network Configuration Data Base. Utilities are provided which validate uniqueness, existence and configuration constraints on the resources.

Source Library

The Global Network Data Base is a source library which allows for multiple versions of the data bases.

Network Management enables the network operators to activate any of the "off-line" data bases by a copying to one of the three on-line versions, which may exist in the system. On-line versions are candidates for being loaded into memory.

Facilities are provided which allow the network operators to activate any of the three on-line versions. Network Management activates the same version in all network systems to protect network integrity.

The software is responsible for protecting existing users who have retained their old network definitions; this includes a version update mechanism which generally leaves unaffected sessions undisturbed. Network users are thus basically transparent to system upgrades.

6.3 RESOURCE CONTROL AND MONITORING

A multitude of facilities and commands for controlling and monitoring resources are provided by the Network Management Services. These include:

- Inclusion/exclusion of resource in/from the network;
- Initialization/restart of resources;
- Status of resources;
- Traffic control;
- Session control;
- Event management;
- Statistics collection;
- Report generation.

HOST-STATUS OF <res-id-1> <IN/EX>

MAX-NO-OF-SESSIONS	:	<number>
SESSION-LIMIT	:	<number>
NO-OF-SESSION	:	<number>

RESOURCE	INC/EXC	OPE/ERR	REASON
CHANNEL	<IN/EX>	<OP/ER>	<reason>
CHANNEL-HDL	<IN/EX<	<OP/ER>	<reason>

APPLICATION & APPLICATION SUBSYSTEM STATUS

NAME	STATE	MAX	LIM	NO
<appl-id>	<state>	<max-no>	<limit>	<no. of secs>

END STATUS OF <res-id-1> . <date-time>

Figure 6.3-1 Example of Resource Status

Facilities' Procedures

The procedures for controlling and monitoring network resources permit users, especially network operators, to conduct secure network operation.

Most facilities aim at manual control of resources, such as including a terminal (putting it on-line), stopping input on an interface (e.g. skip polling of a line), taking the status of a host channel, or terminating a session. However, several other facilities exist which are no less important. Among these are event management and statistics and report generation.

Session Control

Network Management supports network users in session establishment and status awareness of sessions. On request, the users are kept informed of the status and availability of a requested service.

The high availability of internal network resources is achieved by automatic switchover to redundant hardware components when required. To a certain extent, sessions are not effected by resource failures, provided that the system is able either to recover from the failure or to switch to standby equipment. The local Network Management uses its stored session data to provide this recovery service. Failing to re-establish a session causes Network Management to inform the network operators.

Event Management

An event message is generated whenever an error-condition occurs. An event-filtering mechanism, based upon established process control technology, ensures that only "stable" error conditions are reported. Event-messages are sent to Network Management for storage/processing.

Events are divided, according to priority, into a number of event types. Events belonging to the event type with the highest priority are called alarms; those with the lowest priority are notices; and the rest are alerts.

Three logical queues exist; the active, the pending and the closed queue. Notices are directly inserted in the closed queue; the others are inserted in the active queue. Active event messages have to be acknowledged, either automatically or manually, before they are inserted in the pending or closed queue. Events inserted in the pending queue return to the active queue after a specified time, unless they have been acknowledged to the closed queue.

Each network operator can be assigned a specifiable subset of network resources and event types to control and monitor, enabling an orderly distribution of Network Managment adapted to specific organizational needs. The event-base is organized in such a way that all events associated with a given resource can be easily traced. Color-graphics displays are used to improve the control and monitoring of event queues.

6.4 STATISTICS

Two types of statistics exist: permanent and temporary statistics. The permanent statistics are collected continuously and saved on permanent storage at regular time intervals. These consist mainly of data required for network planning. Temporary statistics will only be collected on request.

Network Management is responsible for synchronizing the collection, activation/deactivation of temporary statistics, and storing statistics to the disk; first locally at the primary node, then centrally at the NCC.

A script language facility exists for report generation. The language permits the user to access Network Management data and to define and produce reports.

6.5 DIAGNOSTICS AND TEST TOOLS

The Network Management Services are provided with various diagnostic and test facilities, including:

- Monitoring of traffic on external interfaces;
- Loop-back;
- Message bouncing;
- Dual message routing;
- Protocol tracing;
- Memory dumping;
- On-line test modes;
- Synthetic traffic generator;
- Equipment diagnostics.

Testing and Dignostics

Network Management provides built-in support for various test and diagnostic facilities.

These facilities include provision for monitoring traffic on access lines, host channels and internodal trunk lines. Also included are capabilities for loop-back, message bouncing, dual message routing, protocol traces and memory dumping.

Dual message routing is an especially useful tool for testing and development. Live data may be dually routed to both a live and a test application, thereby enabling a real-life test without interference in the operational environment.

Online Testing

Two kinds of on-line test modes exist. Test Mode 1 supports the routing of test messages through the live network between test end-users.

Test Mode 2 makes it possible to run tests on redundant resources without interfering with the live network.

In both modes, a synthetic traffic generator may be activated to test specific message sequences or to perform load tests on the network.

CR80 Test Capabilities

The network operators or service technicians can invoke specific diagnostic sequences on CR80 equipment for:

- CPU testing;
- RAM testing;
- LTU testing;
- Disk testing.

Such tests may be invoked without interfering in the operational environment. Diagnostic results will be displayed on the operator's terminal.

In addition, the events and statistics collected by the NMS provide a comprehensive means for fault diagnosis. Statistics for access lines include items such as the number of time-outs and the number of NAKs received.

6.6 GEOGRAPHICALLY DUALIZED NCC

Dualized NCC equipment can be provided. This increases survivability and facilitates distributed Network Control. Only one NCC is active at a time (only one master in the network); the other NCC is standby, ready to go active.

The NCC may be in one of three states: off-line, standby and active. The off-line state means the NCC is not able to perform NCC functions.

The standby state means the NCC is fully operational and ready to take control. All reports and monitoring functions are active and all network reporting is sent to the active, as well as to the standby, NCC. The standby NCC "listens" to the network and keeps an up-to-date picture of the network status, but is unable to perform network control.

The Active state means that the NCC is able to monitor as well as to control the network.

Normal operation will assume an active NCC and a standby NCC. The state transitions are controlled by operator commands as well as automatically. In order to ensure network control integrity, the NCCs communicate mutually by an "inter-NCC handshake" protocol, which is an inherent part of the NCC.

The network is resilient enough to survive a temporary loss of all NCC services. When an NCC is repaired and brought back to active operation, it will automatically update to the current network status by polling network status from the primary nodes.

7.0 VALUE-ADDED SERVICES

The CRSN network can provide integration of Value-Added Services into any primary node. The software package can run on the hardware by sharing the processor with other network services or the hardware configuration can be expanded with dedicated processors for Value-Added Services.

7.1 PMS/ELECTRONIC MAIL

The optional Electronic Mail facility provides full Electronic Mail Services (EMS) to all users connected to CRSN. In addition, Protected Message Switching (PMS) can be provided for message handling, i.e. receipt, protection (long-term storage) and distribution.

Currently the EMS/PMS supports the airline ATA/IATA message format. However, the general design ensures easy modification to other message formats.

EMS Functions

Electronic Mail performs a number of functions on the messages passing through the Electronic Mail Service. The message is validated according to the conventional message format, and queued for repair or rejection of invalid messages.

The mnemonic address indicators are resolved into network addresses used for internal routing. Each mnemonic address can refer to one or more destination resources.

Message-type is checked for consistancy with destination resource type capability. Human-originated messages are checked for capability.

Separate input and output catalogues are maintained for all resources originating or receiving messages.

Message information is logged. On request, for each message leaving Electronic Mail, these logs are collected and forwarded to a network management position for statistics purposes.

Messages are distributed or queued up according to address multiplicity.

Protected Message Switching

In the delivery phase, the PMS handles a multitude of destinations: hosts, external networks, terminals and printers. The PMS maintains status awareness of these destinations and queue-up messages, per device and per priority for all devices which are declared "down".

For all devices declared "up", the PMS issues the message immediately after protection. When a delivery ACK is returned from the destination resource, the PMS regards the message as delivered.

If a NAK, or "no ACK", is returned from the destination resource, the message is retransmitted up to a device (configurable several times) before the device is declared "down".

Additional User Services

The Electronic Mail Service provides a number of additional user services. These services may be accessed from any authorized user in the network.

The following groups of services are provided:

- Interactive Message Entry;
- Message Repair;
- On-line Routing Control;
- Message and Catalogue retrieval for both delivered and undelivered messages;
- Electronic Mail file and queue handling.

7.2 VIDEOTEX

Christian Rovsing can offer a private Videotex service as a value-added service integrated with the CRSN.

Videotex, also known as Viewdata, is a facility for retrieving information from computer data bases. The information is stored in "pages" in the Videotex system or may be optionally retrieved from external data bases.

Videotex enables a data processing environment to use low-cost and standardized terminals to interface with different data bases in a manner oriented to the user.

Videotex Capabilities

Videotex offers the following capabilities:

- Retrieval of Videotex images;
- Message service;
- Generation/modification of Videotex images;
- Generation of primary keywords;
- Maintenance of user catalogue;
- Provision for generating user groups from users;
- Password maintenance;
- Three different access methods:
    - Hierarchical search,
    - Direct page selection,
    - Selection by keyword.

Phone Access

Terminals can acquire access to the Videotex system by a call via a public telephone network.

This is a useful facility because it allows a "public" entry point to such value-added services. An external subscriber, whether a small travel agent or a company, could dial this service. All the user needs in order to use this facility is a normal television set, modified with a low-cost circuit board and provided with a low-cost modem so it can function as a terminal.

After the user has acquired access to the system, a log-on image is presented. The user has to key-in his user number and associated password. Once authentication is made, the user may choose individual Videotex applications.

Videotex Applications

Applications for Videotex are virtually unlimited. Here are a few examples:

Travel and Tourist Information

- Time tables (local and global);
- Information on destinations (domestic and foreign);
- Local transportation schedules;
- Local entertainment guides.

News Media

- News briefings;
- Stock exchange reports;
- Weather forecasts;
- Restaurant guides;
- Public events, attractions, entertainment;
- Advertising

7.3 EFT/POS MESSAGE SWITCH

The EFT/POS message switch option is based on the Danish national debit card system, developed by Christian Rovsing for the Danish banks and savings banks. The system will support 60,000 terminals and 3,000,000 debit card users. The transaction capacity of the central on-line CR80 computer system is 700 transactions per second with an availability of 99.98%.

Switching and Transaction Authorization

The EFT/POS system may act both as a high speed transaction switch and also as a stand-in processor. The stand-in processing is provided when permission to perform transaction authorization is issued from a host. The stand-in facility can be used as a backup scheme or it may be used as an independent central computer system for transaction authorization.

The system can be configured to handle 700 transactions per second. This is achieved by a distributed data-base system, where the most-used search keys are stored in a "Megastore" containing up to 64 Mb core memory.

Standard Message Format

The message switch maps vendor specific message formats to a standard internal switching (network) format following the ISO specification in "The International Message Standard for Electronic Funds Transfer (EFT) Transactions."

Incoming messages are converted to the standard internal format, and then sent to a central message router. Outgoing messages are converted to the appropriate external message format and are then sent to the designated terminal and network. The implications are that future needed device protocols (message formats) can be incorporated into the EFT system without modification to the system software itself.

Security

Verification of the card owners validity is done by checking that the card number is not blocked and that the Personal Identification Number (PIN) is correct.

All PINs sent to the switch are encrypted in accordance to the Data Encryption Standard (DES). The system offers hardware security modules for DES encryption. Line encryption devices can be installed to protect messages in transit within the network.

In addition, security is enhanced with audit reports, which can quickly expose any unauthorized attempts to access the network.

Test Facilities

The system is provided with test facilities that permit simulation of the EFT network in order to fully test the switching software.

The system can simulate virtually any valid or invalid transaction. Test messages can be routed into the network just as though they had come from a real terminal or network. This ensures thorough end-to-end testing of the EFT software.

8.0 EQUIPMENT

The nodal equipment of CRSN is based on the Christian Rovsing CR80 minicomputer which is described in the following pages. However, to properly evaluate the advantages of the architecture in this specific environment, the software view is presented first.

8.1 A SOFTWARE VIEW

Figure 8.1-1 illustrates the software view of a subnode, a generic term used for a tightly coupled CR80 subsystem. A CR80 node may expand into multiple loosely-coupled subnodes, to exploit the full potential of the CR80 architecture and be capable of supporting more than 2,000 transactions per second.

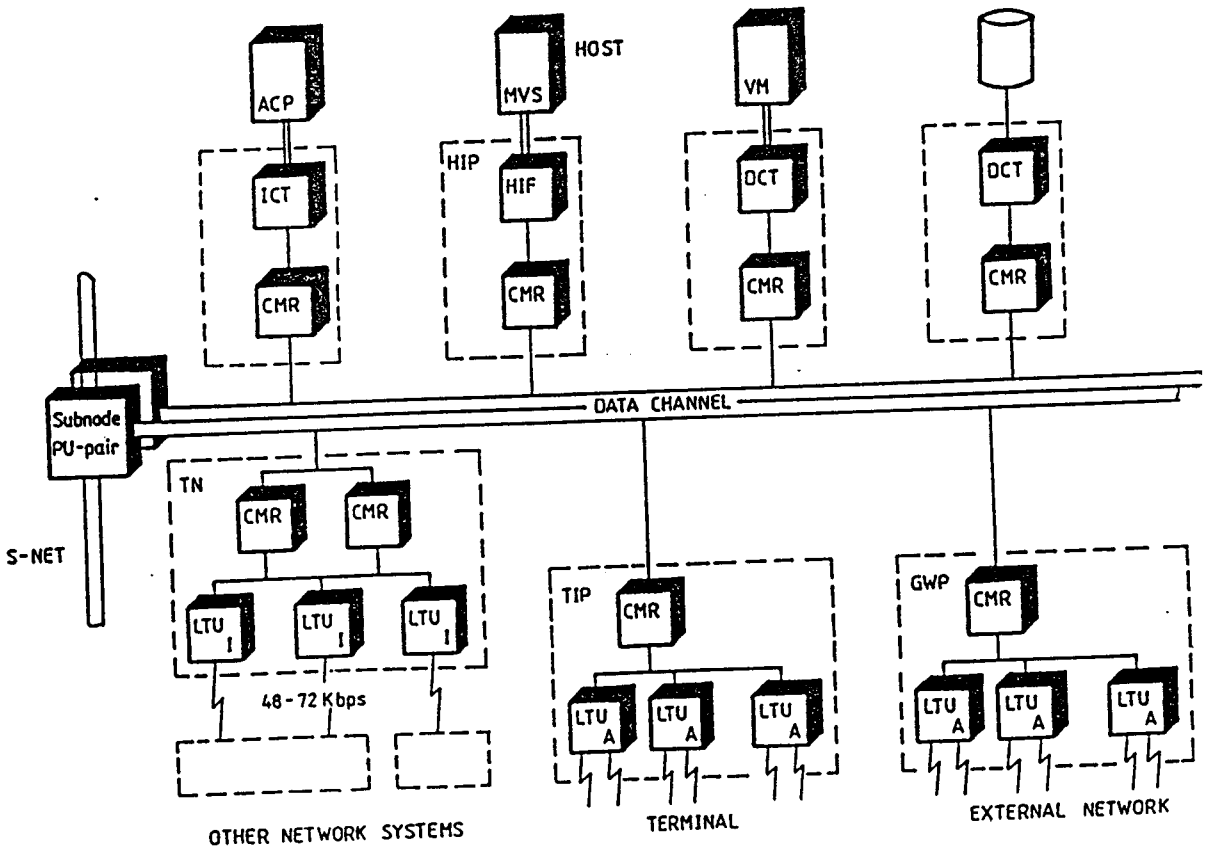

Figure 8.1-1 Software View of a CR80 Subnode

Specific Interfaces

The specific interfaces to the environments served externally can be conceived of as multiple virtual processors bound together into a tightly coupled system, a CR80.

Host Interface Processors (HIP) supply Host Access Services (HAS); they appear as host-specific front-ends. This emulation enables complete replacement of existing 37X5 and DCP/40 front-ends, either channel-attached or remote.

Terminal Interface Processors (TIP) supply Terminal Access Services (TAS) which convert the features of a wide variety of terminals into terminal features recognized by the hosts.

With this broad-range compatibility, any network user may access any network host, irrespective of the host or the terminal vendor. Data transmission route assignments are automatic and require no special action by the user, other than the user's identifying the application.

Gateway Processors supply External Network Access Services (ENAS) and, during migration, to an existing SNA and DCA network.

Transport Network Processors enable communication with remote CR80 nodal systems.

Note: Only a few basic CR80 printed circuit cards, CMRs (CPU-MAP-RAM), ICTs (IBM Controller), UCTs (Univac Controller) and LTUs (Line Terminating Unit) are needed to implement the above virtual processing elements. Each one operates as a single virtual machine with its own dedicated MXAMOS operating system.

Processor Unit (PU)

The Processor Unit-pair, with its redundant data channel, binds the subnode into a tightly coupled system.

Each PU is equipped with CMR-processors indentical to the above virtual processors. Their primary role is to move processed data, e.g. an inquiry from a Terminal Interface Processor to a Host Interface Processor and then move the response back in the opposite direction.

Furthermore, the PU-pair provides the processing power and memory required to support network and system control.

A hot stand-by PU, combined with a proper check-point to disk philosophy, protects against session loss during most failure situations; this also ensures a fast recovery.

8.2 CR80 HARDWARE

The CRSN nodes are based on the CR80 minicomputer product line specifically designed for optimal performance in advanced data communication systems.

Developed and produced by Christian Rovsing A/S, the CR80 is a modular multiprocessor minicomputer system which, due to modularity on both Unit Level (Processor Unit, Channel Unit) and module level (Printed Circuit Board), can be configured to fulfill all requirements for processing power, memory capacity, communication ports and host channels.

A CR80 system consists of a number of Processor Units (PU) and Channel Units (CU) interconnected by high performance data communication buses. Using this bus structure based on the modular and distributed CR80 processing design with a microprocessor associated to each communication port and host channel, the system is prepared for advanced technology - for the installation of the future - simply by inserting new modules.

A CR80 nodal system can contain from one to 32 subnodes with each subnode upgradable to a capacity of more than 500 packets per second and more than 500 communication line terminations. This is accomplished simply by installing the required number of modules in the system.

The host interface is equally flexible and supports simultaneous multiple host data channel connections.

Because redundancy is designed into the system, a high availability is ensured. Several redundancy principles are implemented, as described below:

On the PU level, a complete, dualized principle is used, with one PU assigned as hot stand-by for another. This dualized configuration also allows for load-sharing between the two PUs.

Intercommunication between PUs is performed via the S-Net. The S-Net consists of up to four independent transfer buses, each with a transfer capacity of more than one megabyte per second, thereby producing redundant paths.

On the CU level, all modules are dual-ported, i.e. interfaced to two PUs via the Data Channels. This means that a single point failure cannot stop the PU service for the CU.

High availability with low line costs is achieved by having a single line termination module as a spare for a number of modules (N out of N+1 redundancy).

Monitoring and control of the complete configuration is performed by the integrated watchdog system, which reports whenever a failing module is recognized and performs the proper switching actions.

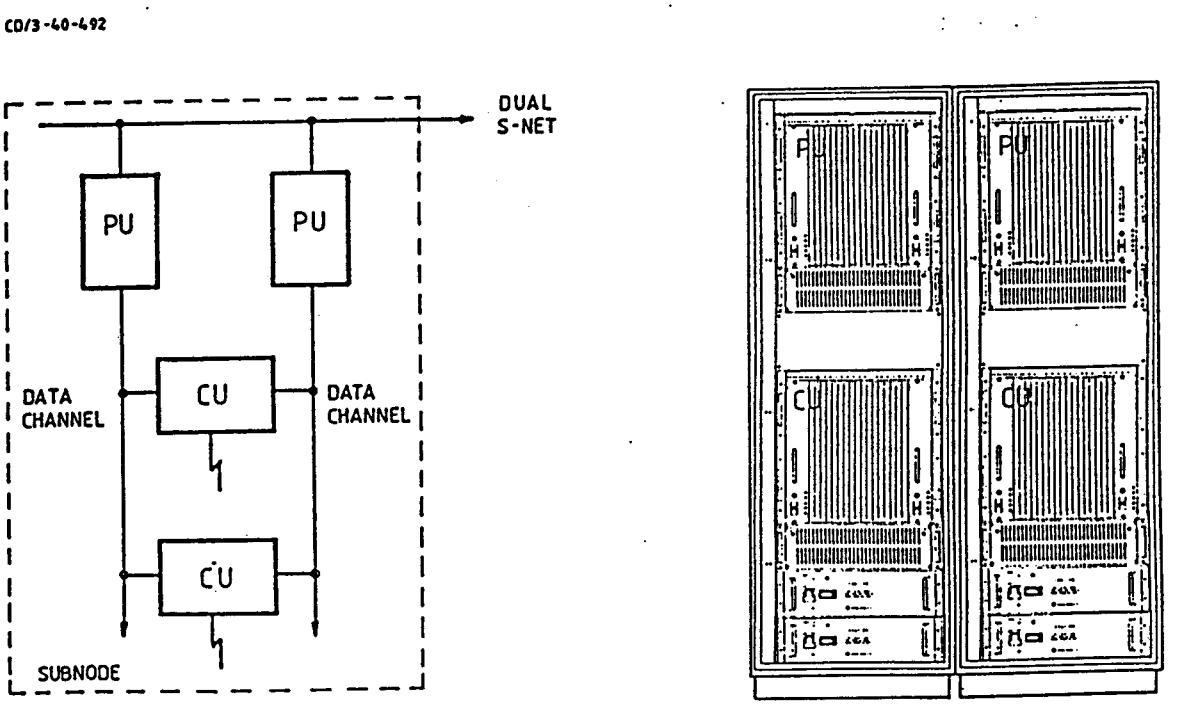

Figure 8.2-1 CR80 Building Blocks and Physical Layout

System repairs are easily performed by replacing the failed module and including the new module in the system configuration.

Expansion of the system is accomplished as if a repair, without interrupting any on-line processing.

8.3 THE TECHNOLOGY

To ensure the quality and cost-effectiveness of the CR80 system, Christian Rovsing uses the latest technology and processes in producing the system's equipment. This means extensive reliance on, for example, CAD-CAM, large scale integrated components (LSI), and very large scale integrated components (VLSI).

In designing circuits and in developing the equipment for the CR80, computer-aid designs are used to produce high quality, uniform documentation upon which production is based.

Computer-aided tools are then used throughout the production cycle, including the component insertion and test phases.

A modular system architecture and the extensive use of the latest technology combine to produce a system of high uniform quality, offering cost-effectiveness through advantages such as simple module replacement (using printed circuit boards).

Christian Rovsing A/S possesses a production line fully capable of manufacturing highly reliable, high quality components, designed to meet even strict military and space agency specifications.

All of these sophisticated resources remain at the disposal of our private sector projects.

9.0 OPEN ENDED EXPANDABILITY

The CRSN concept combined with the modular CR80 architecture gives the CRSN network a growth capability which is virtually open-ended. The expandability of CRSN allows for dynamic growth in:

- Connectivity;
- Processing power;
- Functionality
- Technology.

Hardware

The modular CR80 architecture, as previously described in the Equipment chapter of this document, allow a CR80 subnode to connect more than 500 communication lines and several channel-attached mainframes. Furthermore, up to 32 subnodes can be interconnected to form one CR80 nodal system.

Processing power can be expanded by adding additonal CMRs (CPU-Memory-Ram) to either the PUs (Processing Units) or the CUs (Channel Units). The processing power can reach beyond 2000 transactions per second.

Software

For very large systems, the System Control Services and the Network Management Services can operate on separate processing unit pairs to increase capacity. Smaller systems can be built by operating several services on the same processors. It is even possible to combine Transport Network or Network Access Services into the System Control Services Processor Unit.

The layered architecture of CRSN and especially the general internal inter-processes Basic Communication Services (BCS) allow easy implementation and integration of new software services.

Value-Added Services

Additional functionality can be added to the CRSN network in the form of optional service. The most important of these; Electronic Mail, Videotex and EFT/POS Message Switch, are described in this document.

Accepts Latest Technology

The CR80 also permits the adoption of new technology. Because of the modular design of the CR80, modules designed and based on the newest technology can be readily integrated into an existing system simply by inserting the printed circuit boards in the CU or PU crates.