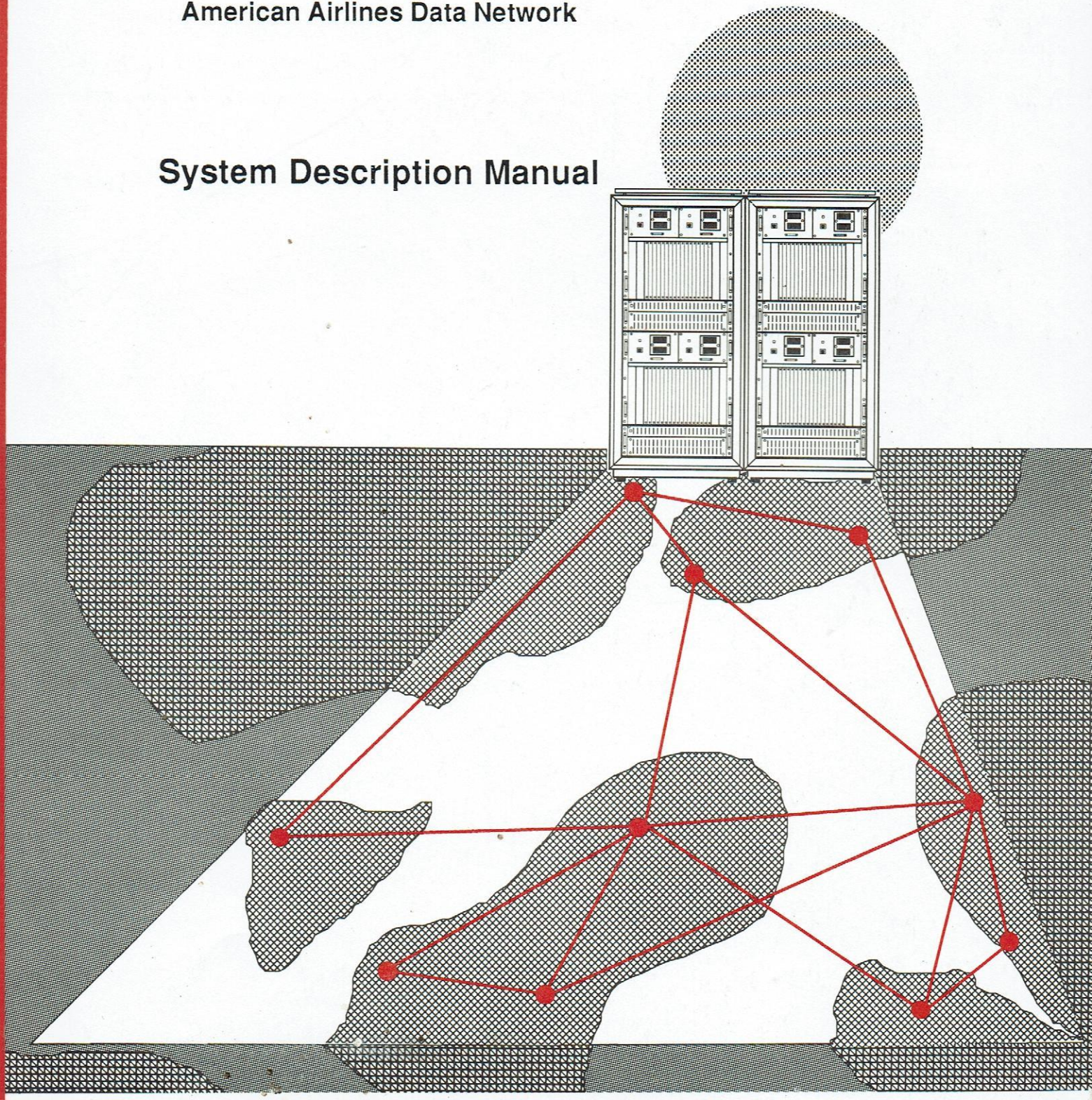
American Airlines Data Network

System Description Manual



CR Systems

American Airlines Data Network

System Description Manual

DOCUMENT: AADN/USM/0001

ISSUE: 3.0 **BY/DATE:** LTO/870810 **LAST PAGE:** 62

This document reflects the design and functionality of the Corporate Resource Sharing Network (CRSN) at the time the documentation was written. Since CRSN systems are subject to a continuous process of development and improvement, CR retains the right to improve, add or modify design and functional features without the obligation of CR to provide notification (to notify any person or organization) of such improvements, additions or modifications.

PREFACE

The AADN System Description Manual serves as a general introduction to the American Airlines Data Network. Primarily, it addresses managers and administrative personnel needing a brief overview of the system. The AADN terms and network characteristics are discussed; the network topology, components and interfaces are described and depicted. Furthermore, the functional and operational capabilities of the network are discussed in broad terms to give an overview of the network impact on the AA environment.

The Fig.s illustrating displays on an operator terminal must be taken as examples only. The actual displays can be modified according to customer needs.

OVERVIEW

The first part of the manual deals with AA's data network needs and the network solution as provided by CR. The following part (Chapters 2, 3 and 4) describes the Corporate Resource Sharing Network (CRSN) product in terms of its architecture and capabilities. The last chapter deals briefly with system maintenance.

SUMMARY

This manual provides an overview of the network hardware, software, and system functionality. It is useful as a stand-alone introduction, but may also be a valuable entry to the AADN Operating Manual and other AADN descriptions.

CONTENTS PAGE

1 INTRODUCTION TO AADN

This chapter contains a brief description of what a data network is. It also explains the relation between the Corporate Resource Sharing Network (CRSN) and The American Airlines Data Network (AADN) as a customized version of the CRSN. Environments connected to AADN are also covered in this chapter.

CONTENTS PAGE

1.1 Data Networks

A data network consists of a number of interconnected computers and terminals. The primary objective of the network is to provide connectivity between any two end-users, e.g. a data terminal and a computer, and to do so cost effectively. This goal is achieved when many users are able to share expensive transmission lines and host computer services.

The basic idea of a 'transparent' network system is to enable many end-users to communicate as though they were all directly connected to each other, irrespective of make and type. The American Airlines Data Network (AADN) is a customized version of the Corporate Resource Sharing Network (CRSN). CRSN is an integrated system of hardware and software designed to be compatible with resources of various makes. The CRSN also includes network management of resources constituting the CRSN itself, and of the resources connected to the CRSN.

The CRSN is a product designed and developed at Christian Rovsing A/S af 1984 in Denmark and in the USA. The AADN is described in the following sections with full functionality and compatibility, i. e. the final delivery (Version 3) of the network.

1.2 Overview of AADN

The American Airlines Data Network (AADN) is based on the CRSN. It is a meshed network which consists of 14 computer Nodes at sites distributed across the U.S. These sites are connected via internodal trunk lines as illustrated in Fig. 1.2-1.

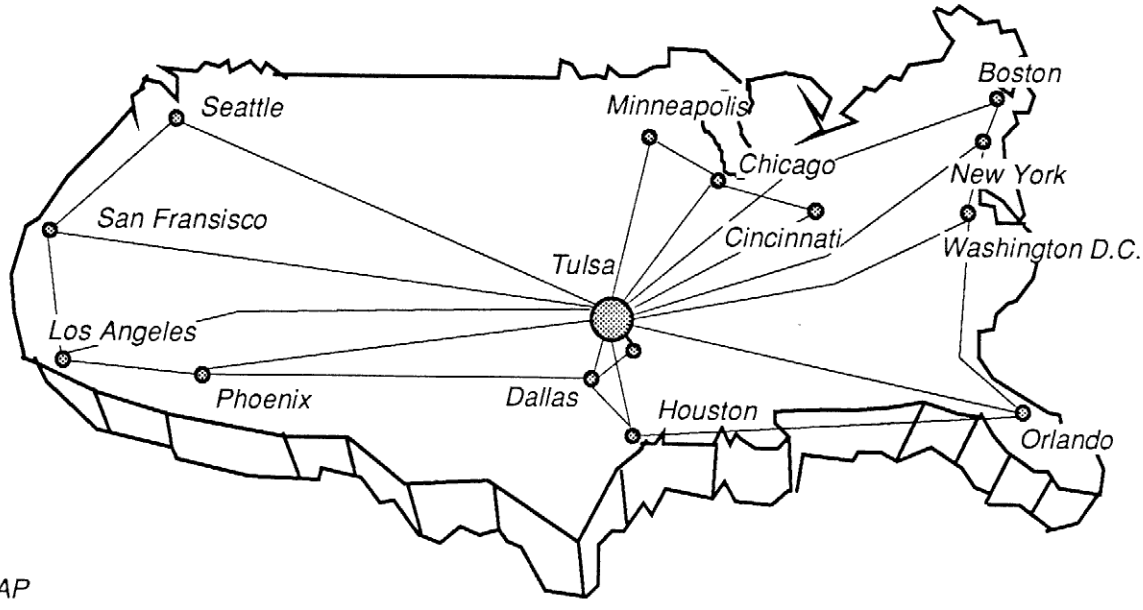


Fig. 1.2-1 AADN Geographical Network Topology

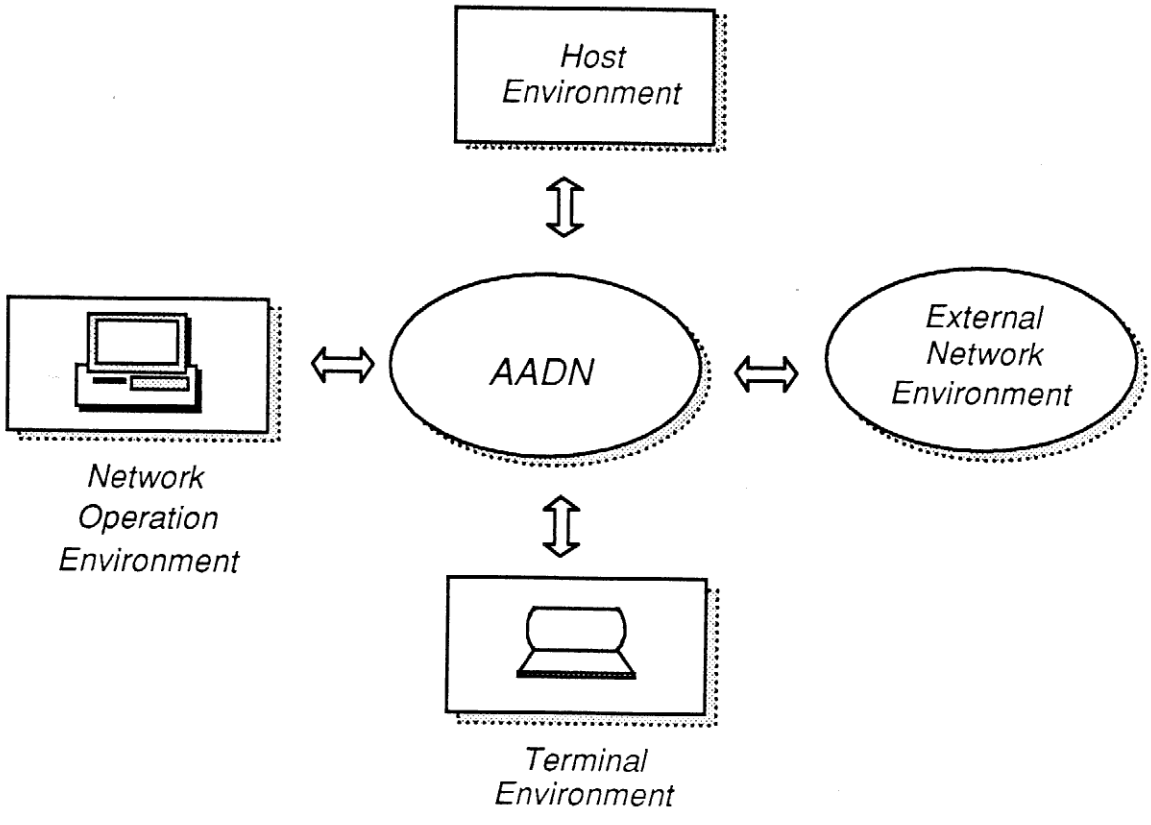
The central site is located in Tulsa, Oklahoma, from where the entire AADN is controlled. All hosts and external networks are connected to the central site, whereas end-user terminals are connected to the distributed sites via access lines.

AADN Connectivity

The AADN connects the American Airlines' widely distributed terminal population with its computer facility (hosts). Connections to several external networks and other airlines' computer facilities are also supported.

Four environments are connected to the AADN (Fig. 1.2-2):

- The terminal environment
- The host environment
- The external network environment
- The network operation environment



CON3

Fig. 1.2-2 AADN Environments

The Terminal Environment

The terminal environment includes two types of devices - visual display units (VDU terminals) and printers. The AADN provides an interface to the following devices:

- Semi-Automatic Business Reservation Environment (SABRE)
- IBM SNA
- Asynchronous TTY

SABRE devices are connected to the network via modems, concentrators, interchanges, and access lines. SABRE devices constitute the majority of user terminals connected to the AADN.

IBM SNA terminals and printers can be connected to the network via cluster controllers and access lines. Asynchronous TTY devices attached to a Public Data Network (PDN) can also be included as a part of the terminal environment. (Fig. 1.2-3).

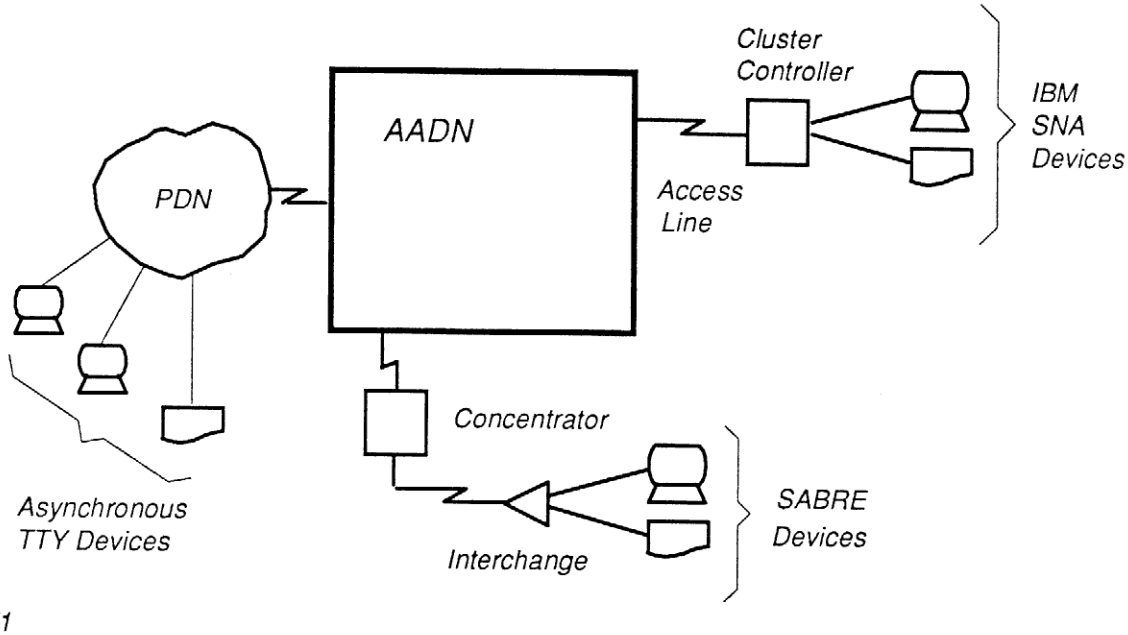


Fig. 1.2-3 AADN Terminal Environment

The Host Environment

AADN supports three different host environments (Fig. 1.2-4):

- Realtime hosts
- Commercial hosts
- Virtual Machine (VM) test hosts

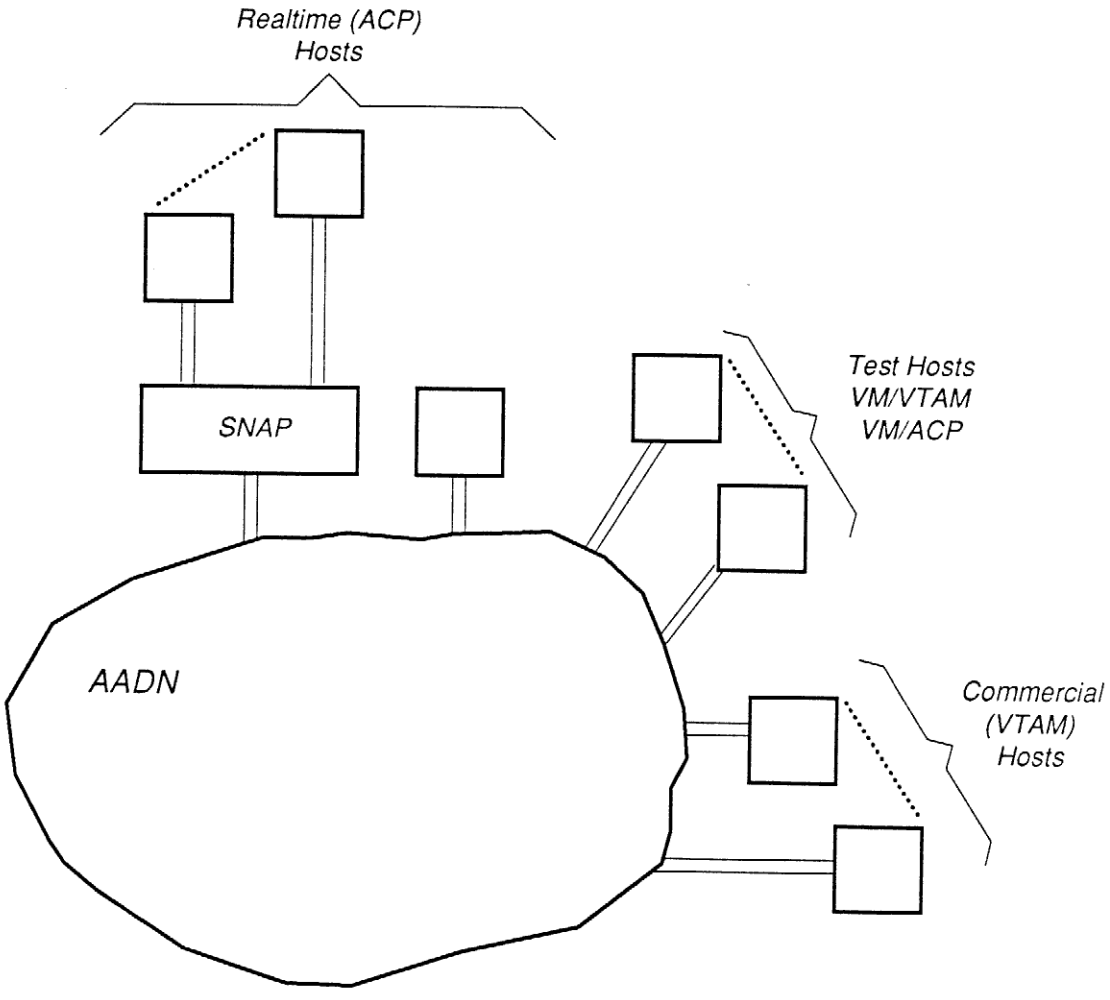


Fig. 1.2-4 AADN Host Environment

The Realtime host is an IBM compatible mainframe running the AA version of the Airline Control Program (ACP). It supports applications such as:

- Reservations (RES)
- Flight and Traffic Statistics (FATS)
- Freight (FRT)
- Flight Operating System (FOS)
- Dispatch Environmental Control System (DECS)

By means of the SABRE Network of ACP Processor (SNAP), it is possible to run the same application on more than one host simultaneously. The traffic from the terminals to, e.g. the RES application, can be shared between the hosts running the same application. The routing to the various hosts is transparent to the users.

Commercial hosts are standard IBM (or IBM compatible) mainframes which operate in an IBM VTAM environment. The commercial hosts run applications such as

- Time Sharing Option (TSO)
- Information Management System (IMS)
- Conversation Monitor Session (CMS) (on VM test hosts)

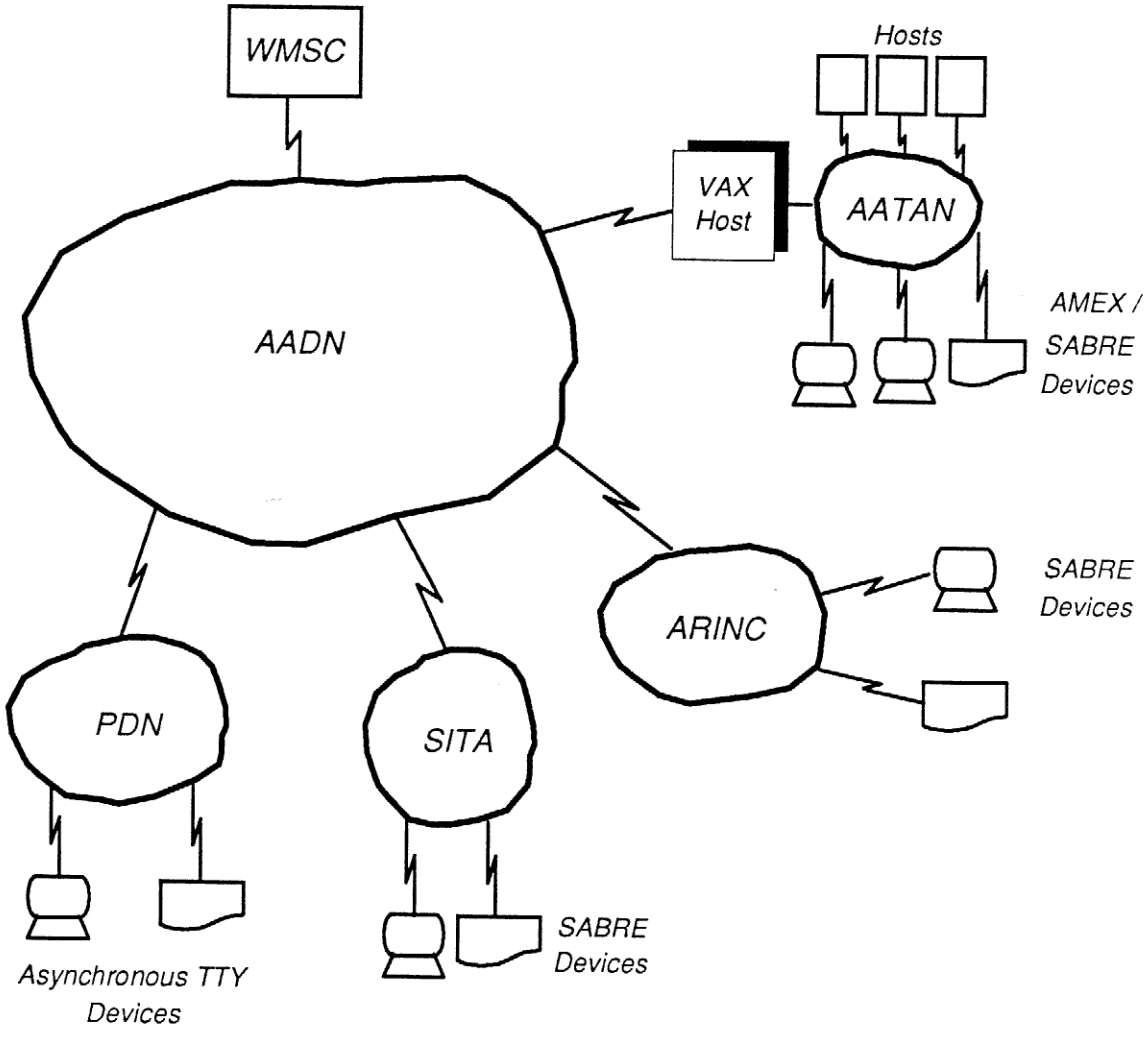
American Airlines VM test hosts can operate in an ACP or IBM VTAM environment.

The External Network Environment

AADN provides interfaces to a number of external networks (Fig. 1.2-5):

- ARINC (The Aeronautic Radio Inc.)
- SITA (Societe Internationale de Telecommunications Aeronautiques)
- AATAN (American Airlines Total Access Network)

- WMSC (Weather Message Switching Center)
- PDN (Public Data Network)



SDM/D/3

Fig. 1.2-5 External Network Environment

The external network ARINC provides ARINC-connected terminals access to AADN Realtime hosts. SITA connects SABRE devices outside the North American continent. These devices can communicate with AADN Realtime hosts in the same way as SABRE terminals directly connected to the network.

The AATAN allows AADN-connected SABRE terminals to communicate with the reservation computers (Hosts) of a number of other airlines, e.g. British Airways, and likewise provides AATAN-connected American Express (AMEX) terminals access to the ACP host environment. The AATAN interface is a Virtual Address Extension (VAX) host.

The connection to WMSC through a gateway processor supplies AA with weather condition information.

Finally, the PDN connection to the AADN will give PDN's terminals access to the IBM commercial host services.

The Operating Environment

The Network Control Center (NCC) in Tulsa is the network operator's interface to the AADN. The NCC contains the operator terminals (the operator's consoles, VDUs, and PCs), printers, tape stations, Intelligent Database Machines (IDM), etc. The main tasks of monitoring and controlling the network, taking preventive and corrective actions, and re-configuring the network is done within this area. Figure 1.2-6 shows the operator's environment and schematically illustrates the equipment at the operator's disposal.

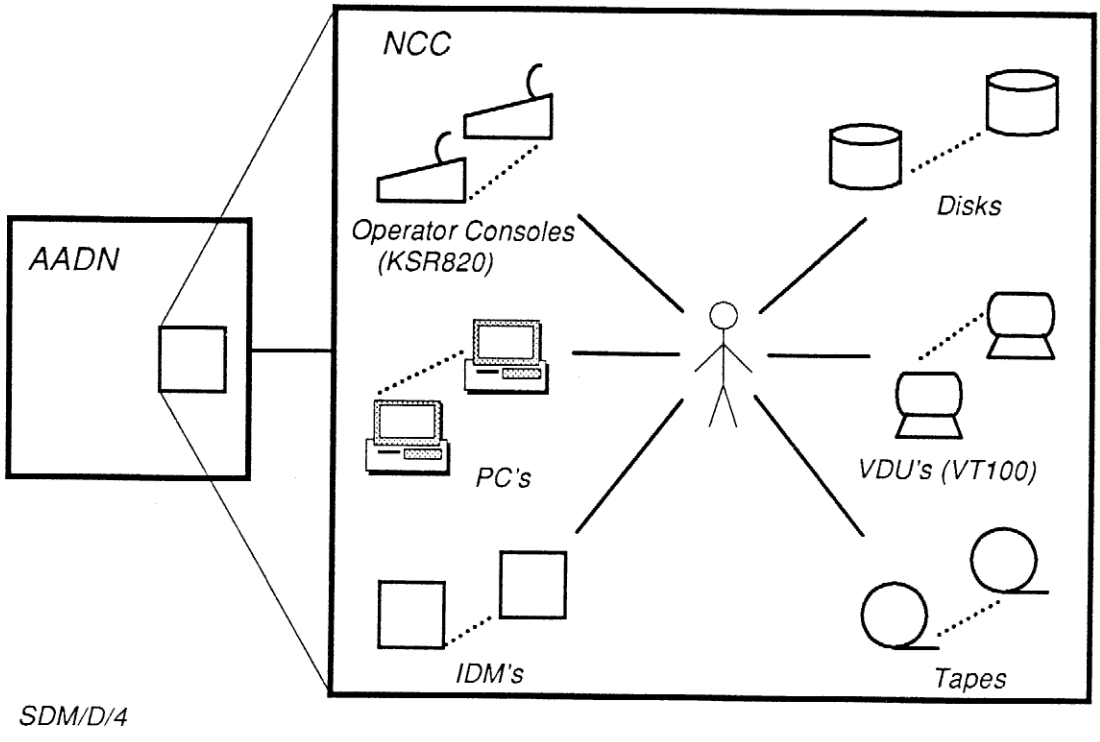


Fig. 1.2-6 The NCC and The Operating Environment

In Fig. 1.2-7 the entire AADN is depicted. AADN constitutes the interconnected Nodes to which the terminal, host, network operation and external network environments are interfaced.

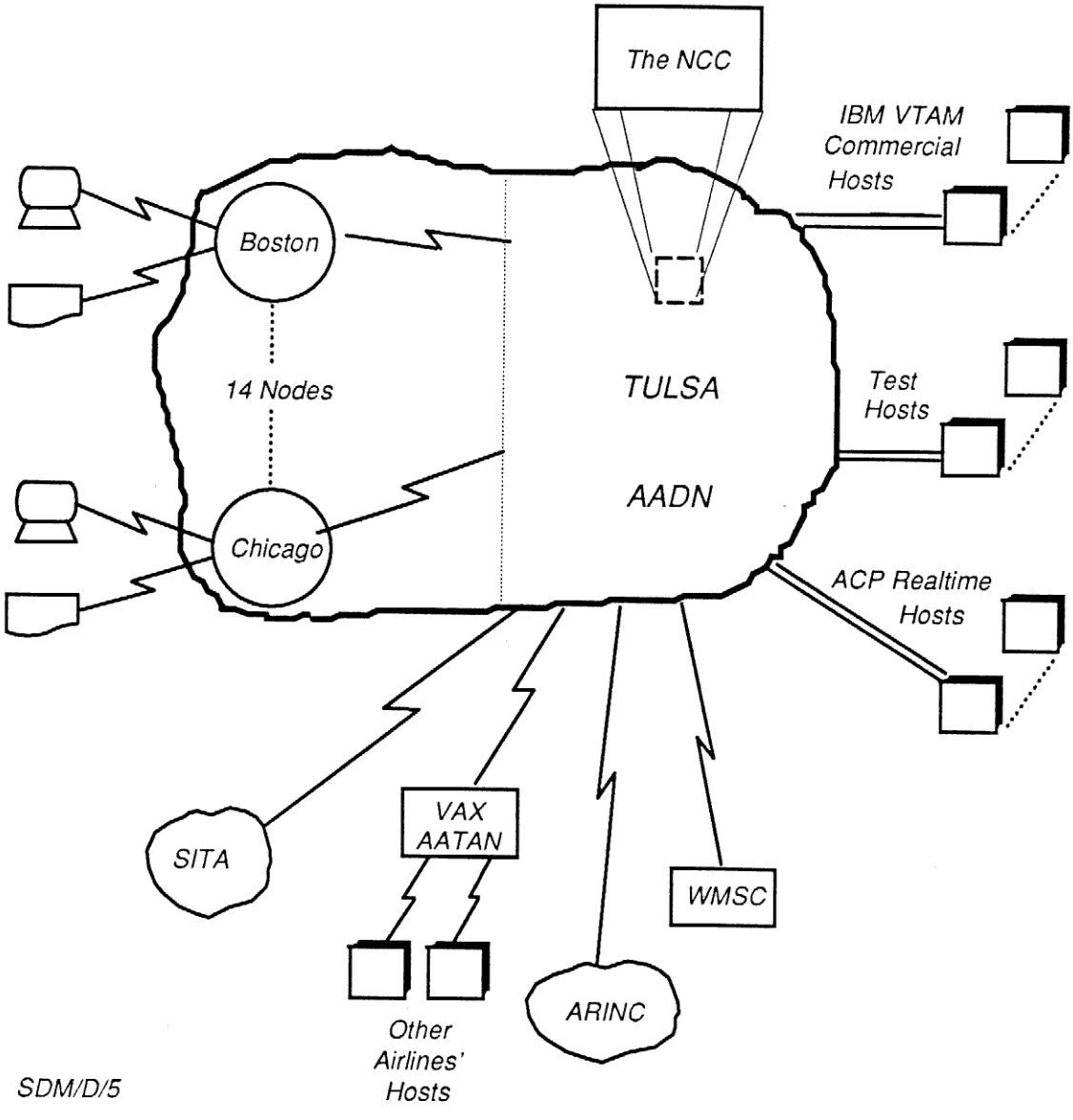


Fig. 1.2-7 AADN connections.

2 CRSN ARCHITECTURE

This chapter describes and depicts the Corporate Resource Sharing Network (CRSN) architecture in terms of its hardware and software components.

CONTENTS PAGE

2.1 Hardware

The main hardware components in CRSN are the Processing Units (PUs) and the Channel Units (CUs). The PU and CU crates are mounted in racks, which may also contain peripherals, such as disk drives, tape stations and Intelligent Database Machines (IDMs). Each PU or CU Crate contains front and rear modules. The crate is also equipt with a power supply and it is cooled by a fan unit beneath the crate.
Fig. 2.1-1 illustrates three racks equipt with crates and peripherals.

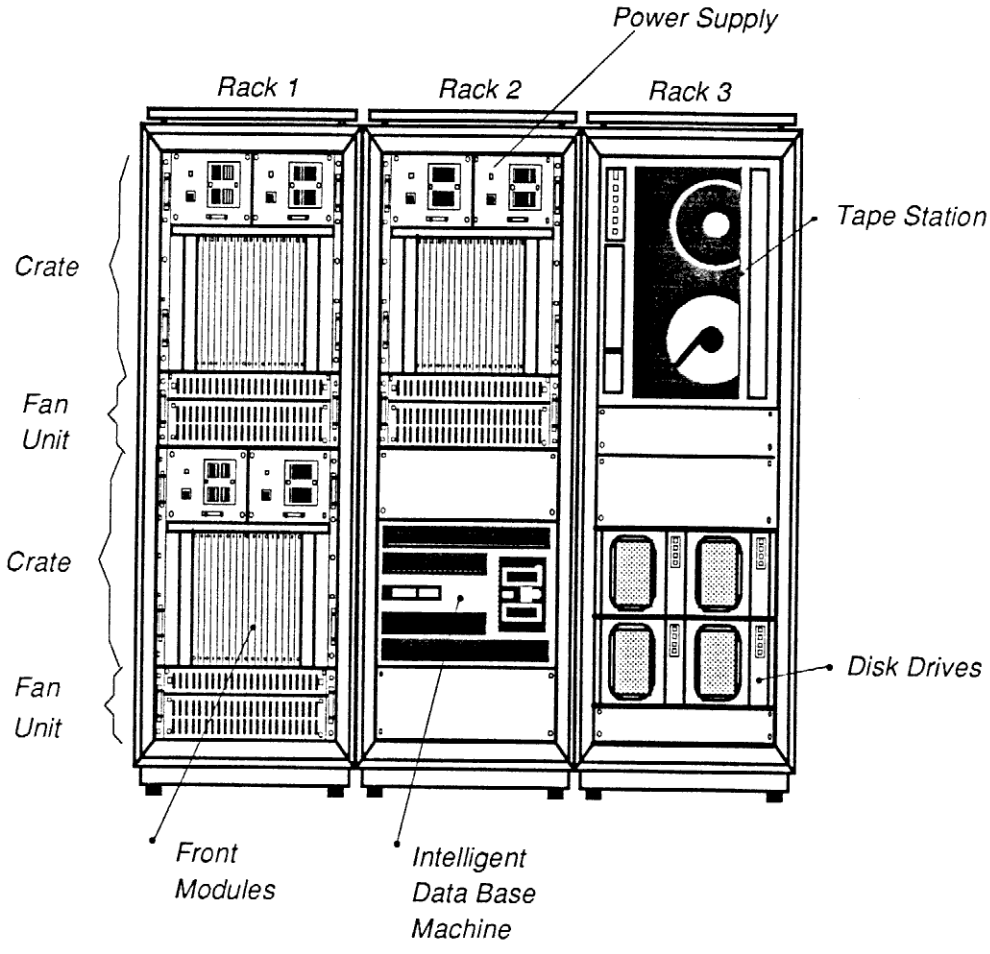


Fig. 2.1-1 CRSN Racks

Fig.2.1-2 CRSN Racks - Front View

PUs and CUs are connected via the Data Channel. Up to Up to 12 CUs can be attached to one PU, but usually no more than 5 CUs will be connected to the same PU. The CU has a dual bus system, allowing one CU to be connected to two different PUs via separate Data Channels.PUs exchange information across the S-Net (Suprabus Net) which consists of two serial transmission cables. One S-Net can handle up to 64 PUs. Fig. 2.1- 3 shows a rear view of a rack.

Opposite: *A rear view of a rack containing a dualized PU (at the top) and a CU. The power supplies are at the top and in the center of the rack. The S-net (coax cables) and the Data Channels (twisted flat cable) are connected to the rear modules.*

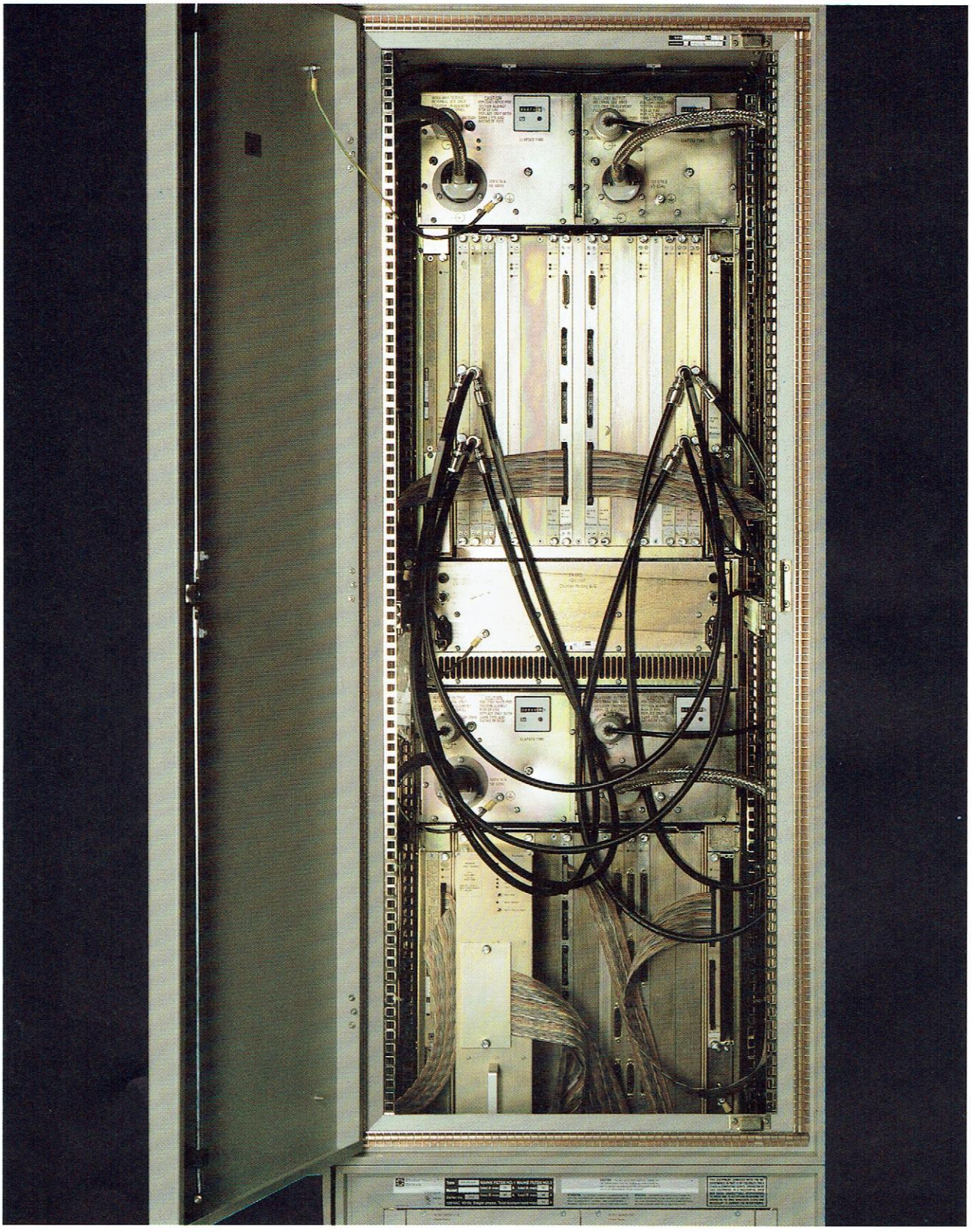


Fig. 2.1-3 CRSN Rack - Rear View

Processing Unit

The PU stores data programs and interfaces to other PUs via The S-Net. Usually the PU crate contains two PUs, where one is active and the other is standby. The main modules in the PU are

- o CMR CPU MAP RAM. This module performs the central processing, the MAP function and has 256 K words of RAM
- o SNI S-NET interface which interfaces CMR to the S-NET
- o MIC Main Bus and Interrupt Controller, which distributes the workload between The CMRs and interfaces to the Data Channel

Channel Unit

The CU functions as the interface to peripherals such as communication lines, hosts channels, disk drives, etc. via the I/O modules.
The CUs may also contain CMRs (Fig. 2.1-4), whereby more processing can be done in the CU. The main modules in the CU are

- o LTU Line Termination Units, which interfaces to access lines and internodal Trunk Lines
- o ICT ICM Channel Interface
- o MIC Main Bus and Interrupt Controller

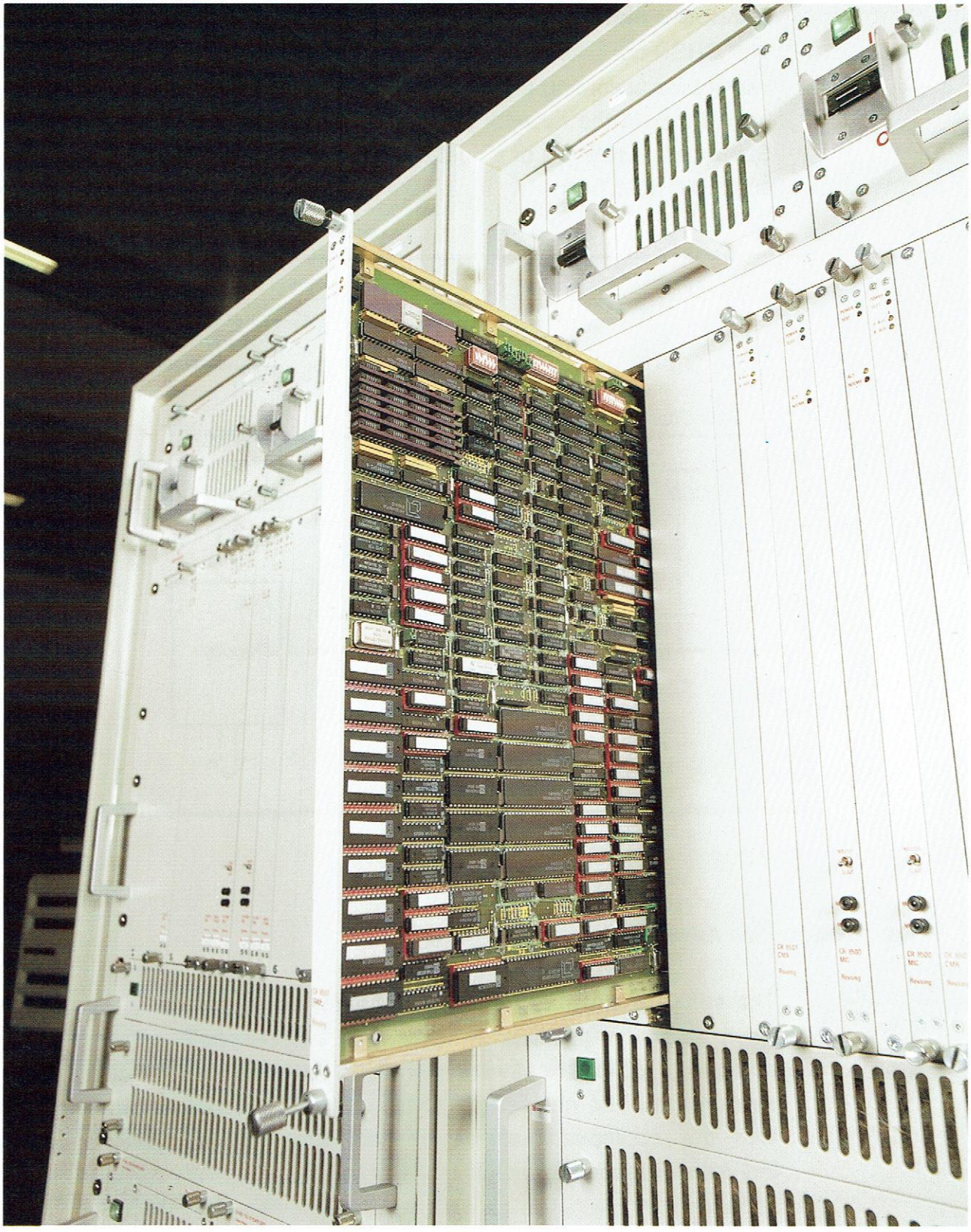
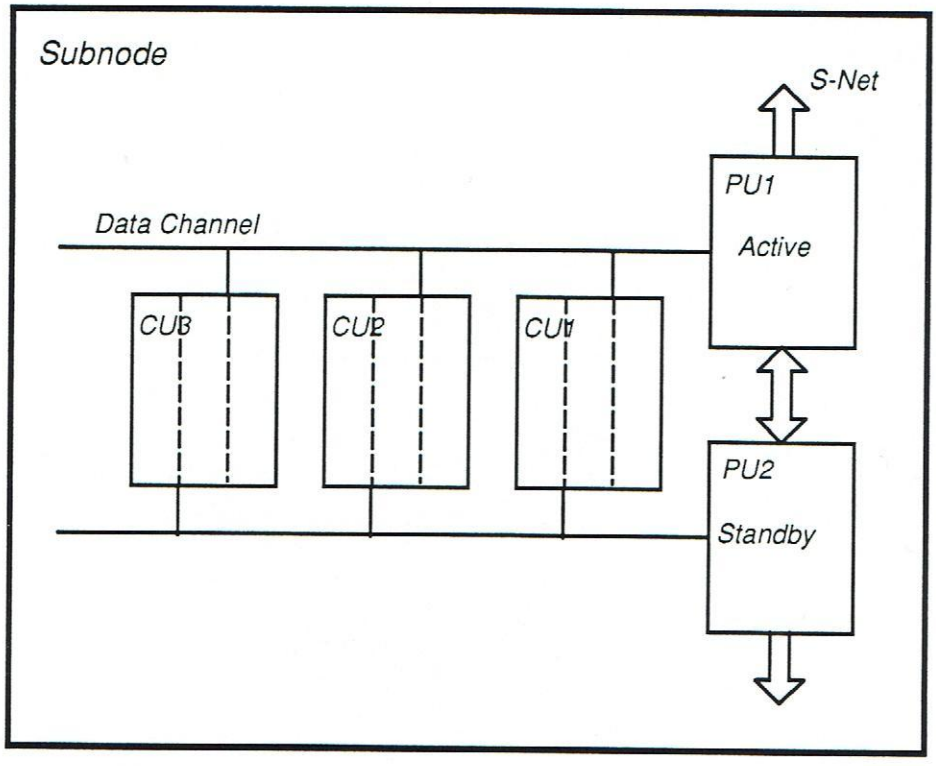


Fig. 2.1-4 A CMR Module

Subnodes and Nodes

The CRSN consists of building blocks (hardware and software) which are assembled according to their function in the network. The Subnode is the basic block in the network and the hardware structure is identical for all Subnodes. It consists of a dualized set of PUs and one or more connected CUs (Fig. 2.1-5).



SDM/D/13

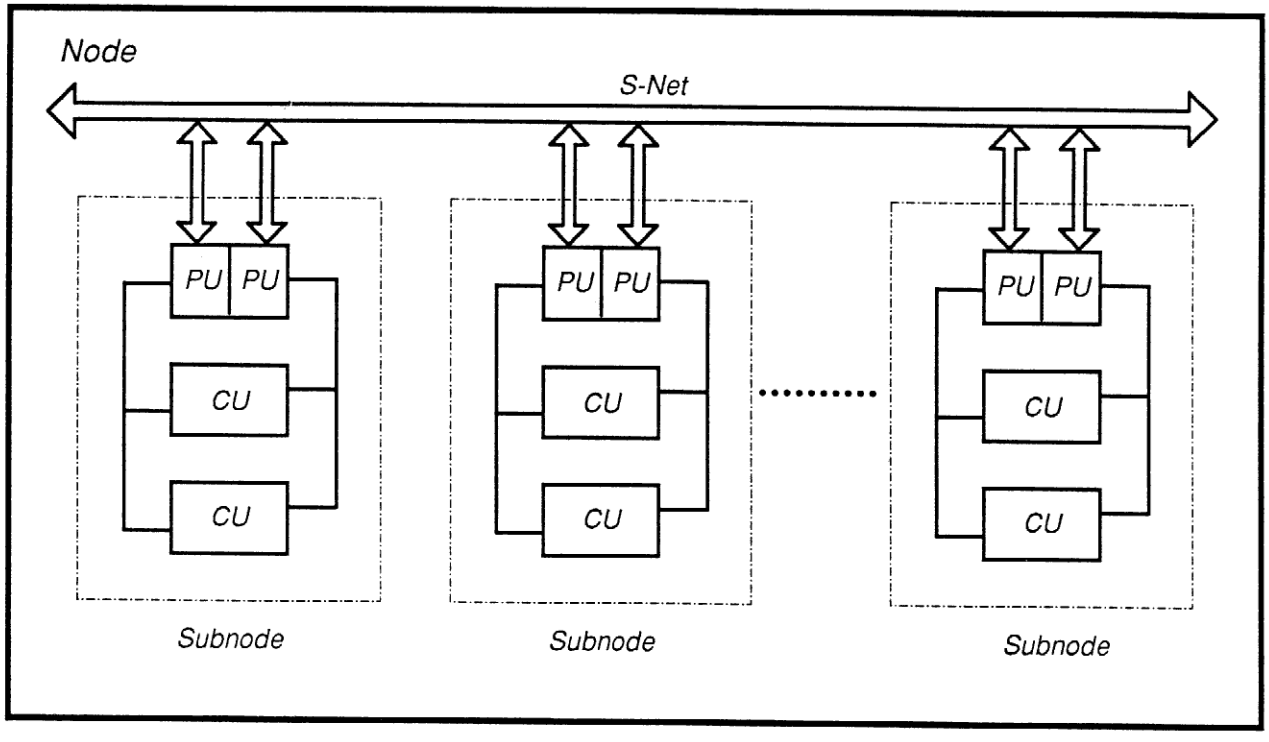
Fig. 2.1-5 Subnode Architecture

The software structure is also identical for any Subnode in the network. Each Subnode contains a portion of indispensable software and a number of optional software packages (software will be dealt with in section 2.2). The choice and combination of optional software together with the appropriate choice of hardware modules, determines the individual Subnode's function in the network.

Subnodes can interface to hosts, other Subnodes, access lines (to terminals) etc., and the CRSN flexibility allows for many configuration

possibilities. The AADN specific design will be described in the following section.

The term Node is a logical term which denotes a number of interconnected Subnodes (interconnected via the S-Net) as shown in Fig. 2.1-6.



CR80-TDS/D/6

Fig. 2.1-6 Node Architecture

The Host Interface Processor Complex

The building blocks in AADN are configured so that all terminals are connected to the Secondary Nodes (14 in all). The Secondary Nodes, the host environment and the external network environment are all connected to the Primary Node's Host Interface Processor (HIP) complex (Fig. 2.1-7). The Network Control Center (NCC) is also a part of the Primary Node.

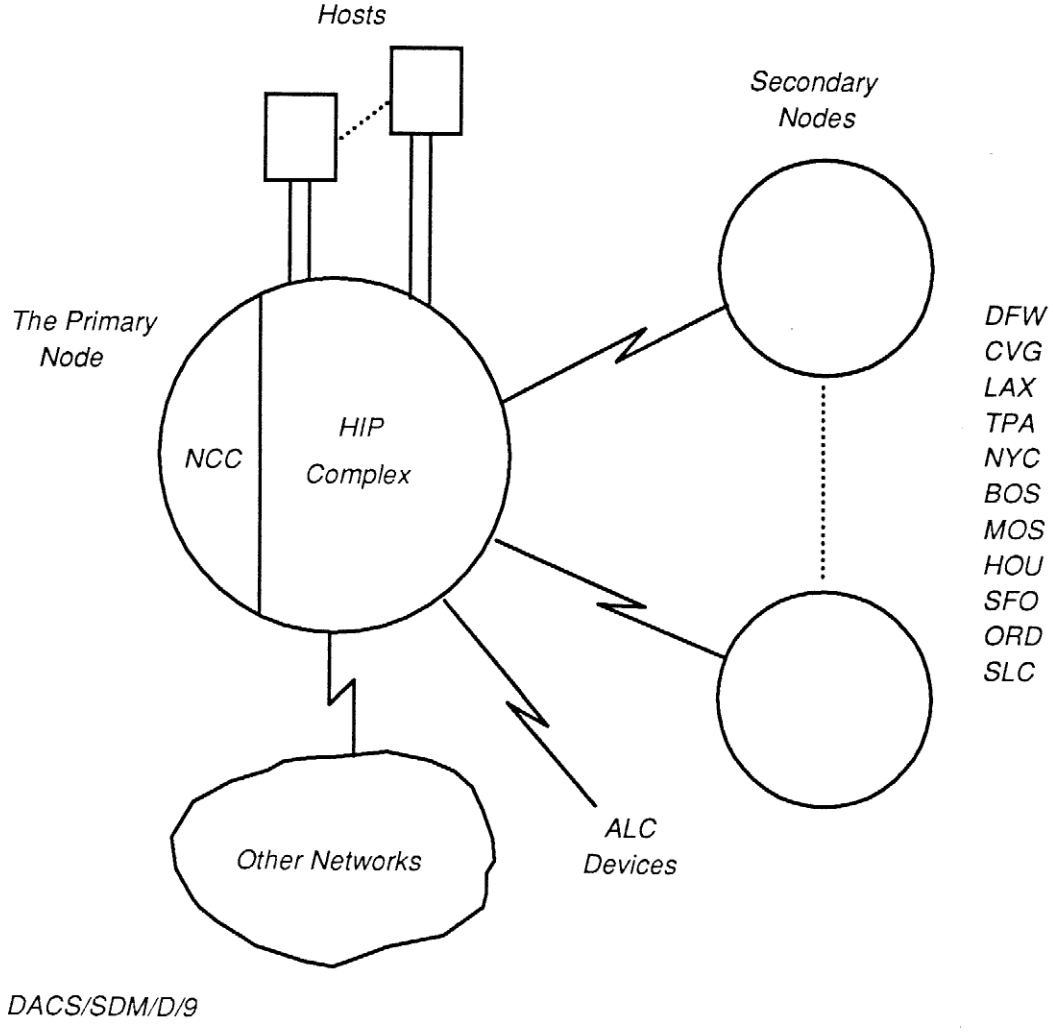
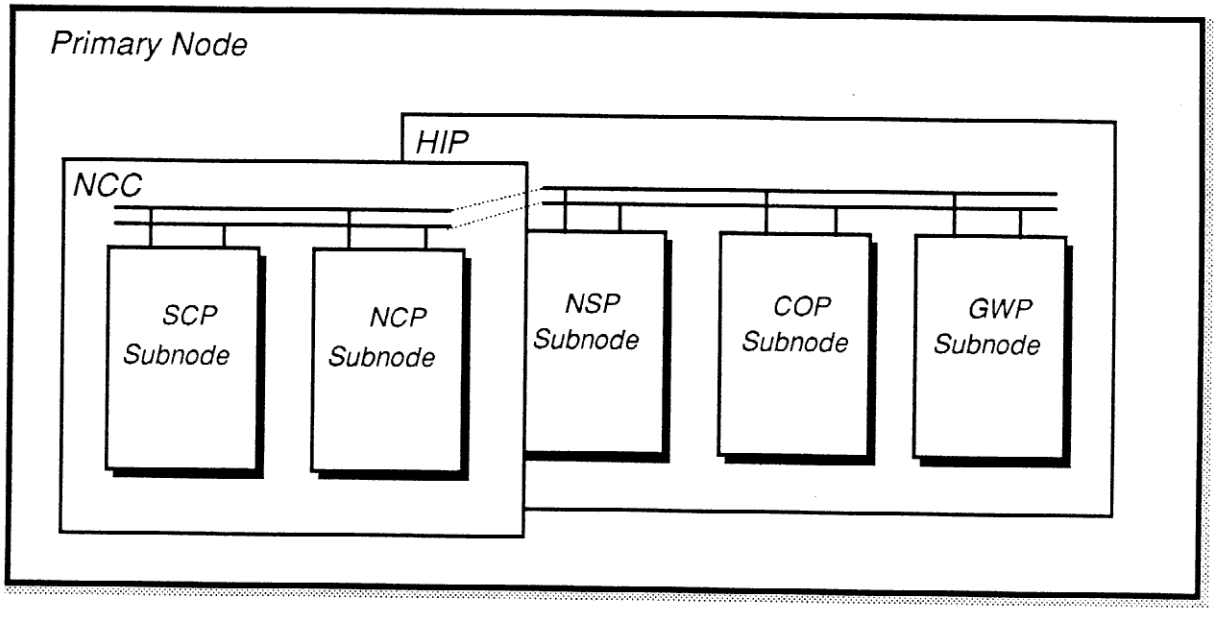


Fig. 2.1-7 AADN's Primary and Secondary Nodes

The NCC provides the Network Management function and contains the Global Network Database (GNDB) which stores all network software and the network configuration. The NCC functions as the operator's interface to the network.

The HIP complex establishes an interface between internodal trunk lines and the ACP and VTAM hosts.

The Primary Node also provides the interface to other networks, primarily through the Gateway system. It consists of a number of Subnodes, each performing a specific task, as illustrated in Fig. 2.1-8.



OPM/D/5

Fig. 2.1-8 The NCC and HIP Complex.

NCC

System Control Processor (SCP)

The SCP is attached to the Global Network Database (GNDB) which maintains files for boot-loading of Subnodes in Primary and Secondary Nodes. Therefore, the SCP is the source of all network software. The Local Area Network (LAN) interface is also provided by the SCP.

Network Control Processor (NCP)

The NCP implements central network control functions such as Global Network Database management, statistics collection, and event processing. The NCP controls the Global Network Data Base.

HIP Complex

Nodal switching Processor (NSP)

The NSP handles the traffic between the incoming internodal trunk lines and the ACP host environment.

Commercial Processor (COP)

The COP manages the traffic between the SNA terminal environment and the commercial VTAM host environment.

Gateway Processor (GWP)

The GWP handles the traffic between external networks, Total Access, and the ACP host environment.

Connectivity and Expandability

Version 3 of the AADN will, as a minimum, support the following connectivity (this is only a partial list):

- **SABRE/ACP**

  - o 85,000 terminals
  - o 41,000 printers
  - o 1 SNAP complex of 8 real-time hosts
  - o 1 FOS host
  - o 3 VM test hosts

- **IBM SNA/VTAM**

  - o SNA terminals
  - o SNA printers
  - o 4 commercial hosts

- **An External Network Environment**

  - o 400 ARINC and AMEX devices

By addition of hardware and with some software changes, it will be possible to expand the AADN connectivity.

2.2 Software

CRSN software consists of a number of subsystems, ordered in a hierarchial structure, where each subsystem supports specific functions. The software structure as shown on fig. 2.2-1 is identical for any Subnode; each Subnode contains the following network elements:

- Network Management (NM)
- Transport Network (TN)
- System Control (SC)
- Access Resource Handlers (ARHs)

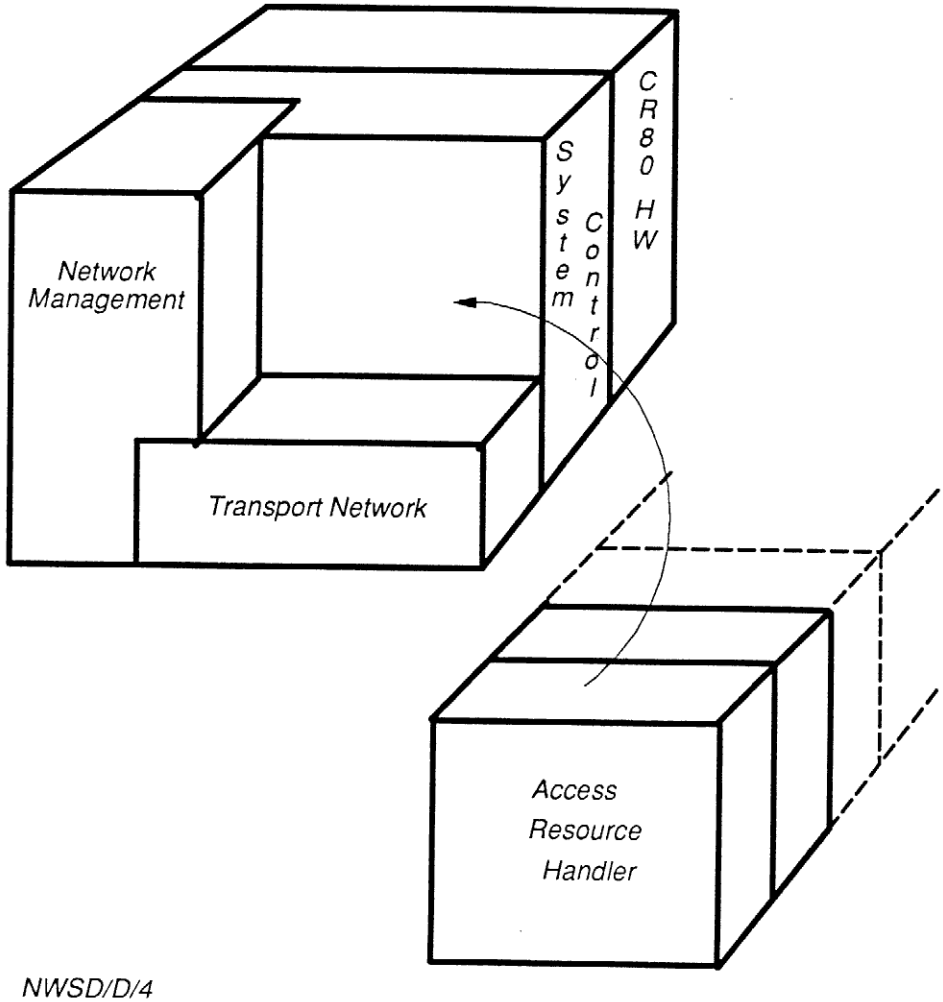


Fig. 2.2-1 CRSN Subnode Software Architecture

Together they form a complex with a number of common aims:

- To provide external resources (hosts, terminals, and other networks) with the ability to communicate with each other through a transparent network.
- To transfer data between Subnodes.
- To monitor and control the data flow and the network resources.

The standard software in a Subnode is composed of NM, TN and SC. The Subnode can be configured to contain a variety of ARHs, which are responsible for the connectivity and access services towards external equipment. In a deeper level of the software structure lies the operating system. It manages hardware resources, including peripherals such as terminals and disk drives. It is also responsible for file management, process control, real time clock, and an efficient queue driven Basic Communication service, used as the main interface vehicle between the processes.

Network Management

NM is responsible for the overall management of the network. The following areas represent the main NM functions:

- Configuration Management
  - Offline Configuration Management
  - Online Configuration Management
- Network Monitoring
  - Event Handling
  - Status Presentation
- Statistics
  - Statistics Collection
  - Report Generation

- Diagnostics
  - Hardware Test Programs
  - Software Diagnostic Tools
- Access Control
- Operator's Interface
- Line Switch Management

Transport Network

The TN provides and controls the transport service between Subnodes. The TN uses hardware resources such as S-Nets, internodal trunk lines, or PDN links. TN selects an alternative route if a transport resource fails.

System Control

SC is the high-level operating system of the Subnode, creating a general software environment for all other subsystems/Resource Handlers. SC supports hardware unit/module switch-over in case of failure.

Access Resource Handlers

ARHs manage the interfaces to various external resources. Access Resource Handlers may be divided into two groups:

- Terminal Access Subsystem (TAS)
  The TAS controls the interfaces to Terminal Access Networks. There is one TAS residing in a Subnode for each type of terminal environment, e.g. SABRE or SNA.

- Host Access Subsystem (HAS)
  The HAS handles channel or link interfaces towards hosts and applications. There is one HAS residing in a Subnode for each type of connected host computer, e.g. ACP or VTAM.

3 FUNCTIONAL AND OPERATIONAL CAPABILITIES

This chapter deals with the network capabilities with regard to access control, network configuration and operation.

CONTENTS PAGE

3.1 Network Configuration Maintenance

There are two phases in network configuration maintenance: the actual planning, (i.e. considering what network configuration changes are necessary), and implementing required changes. Some re-configuration can be done online (e.g. inserting or deleting terminals) while other changes must be made in the Offline Configuration Database (e.g. adding an internodal line).

The Database

The information used during network operation and known to the online system is stored in the online network database.

The database consists of three databases (Fig. 3.1-1):

- The Online Software Database ONSW contains the software necessary to boot-load the network.
- The Online Configuration (ONC) contains resource records for every resource in the network (applications, hosts, Resource Handlers, etc.).
- The Online Access Control (ONAC) database contains the information necessary to validate end-users (terminals/users or hosts) trying to gain access to the network/host applications.

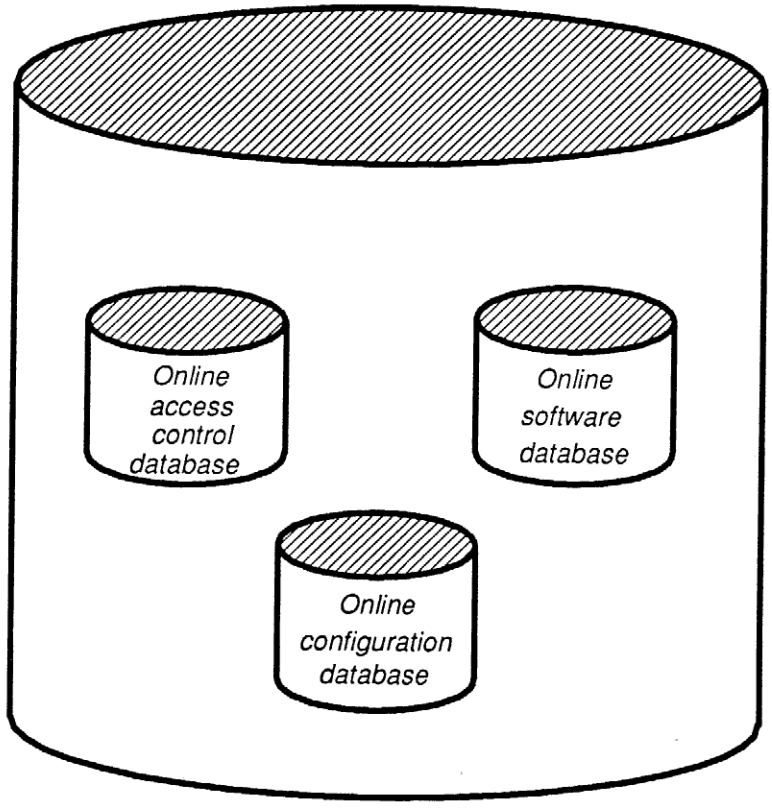


Fig. 3.1-1 The Online Database

Online and Offline Versions

On the online system, one database serves as the 'current' version, i.e. the version which reflects the present network and in use when the system is running. The online configuration database and the online software database can exist in two other versions on the online system. One of them can become the 'current' version when changes have been made in the network, which must be reflected in the database.

The database versions present on the online system are selected from the pool of versions maintained in the offline database. Up to 15 offline configuration versions (OFC) and 4 offline software versions (OFSW) can exist simultaneously. There is only one version of the online and offline access control (OFAC) database at a time. Figure 3.1-2 illustrates the offline and online database versions.

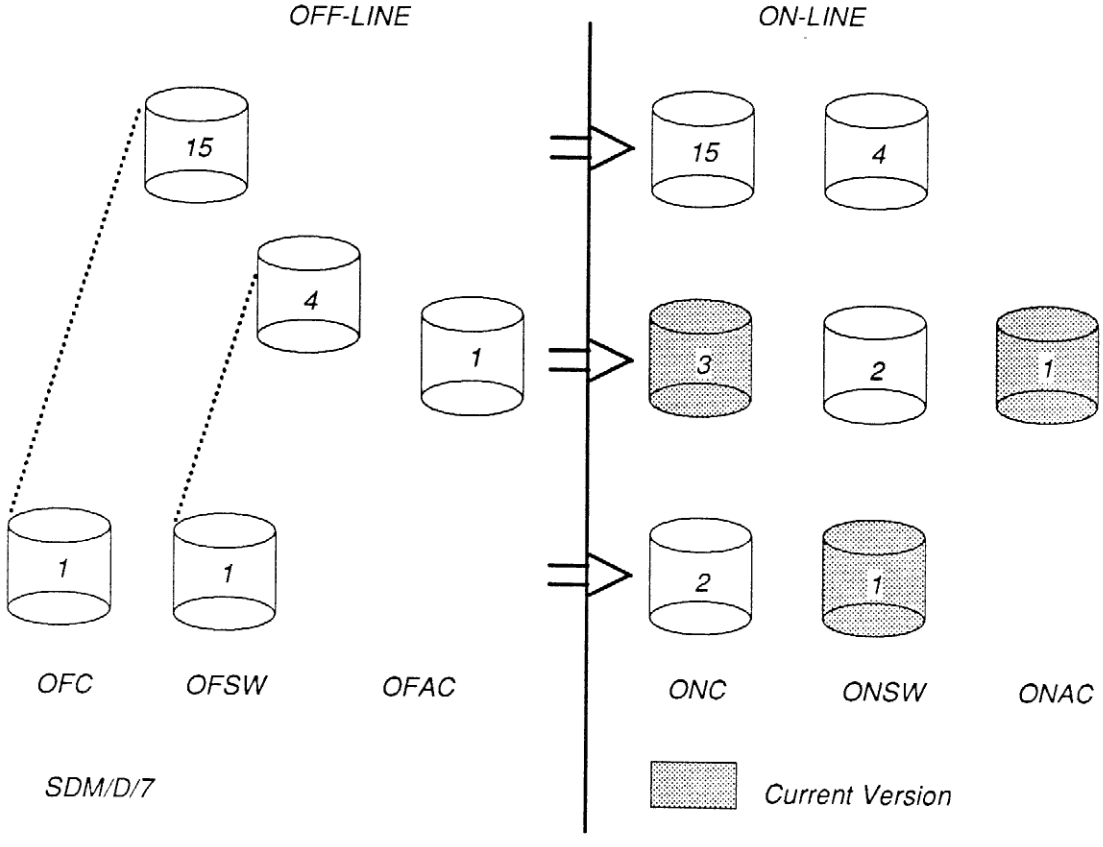
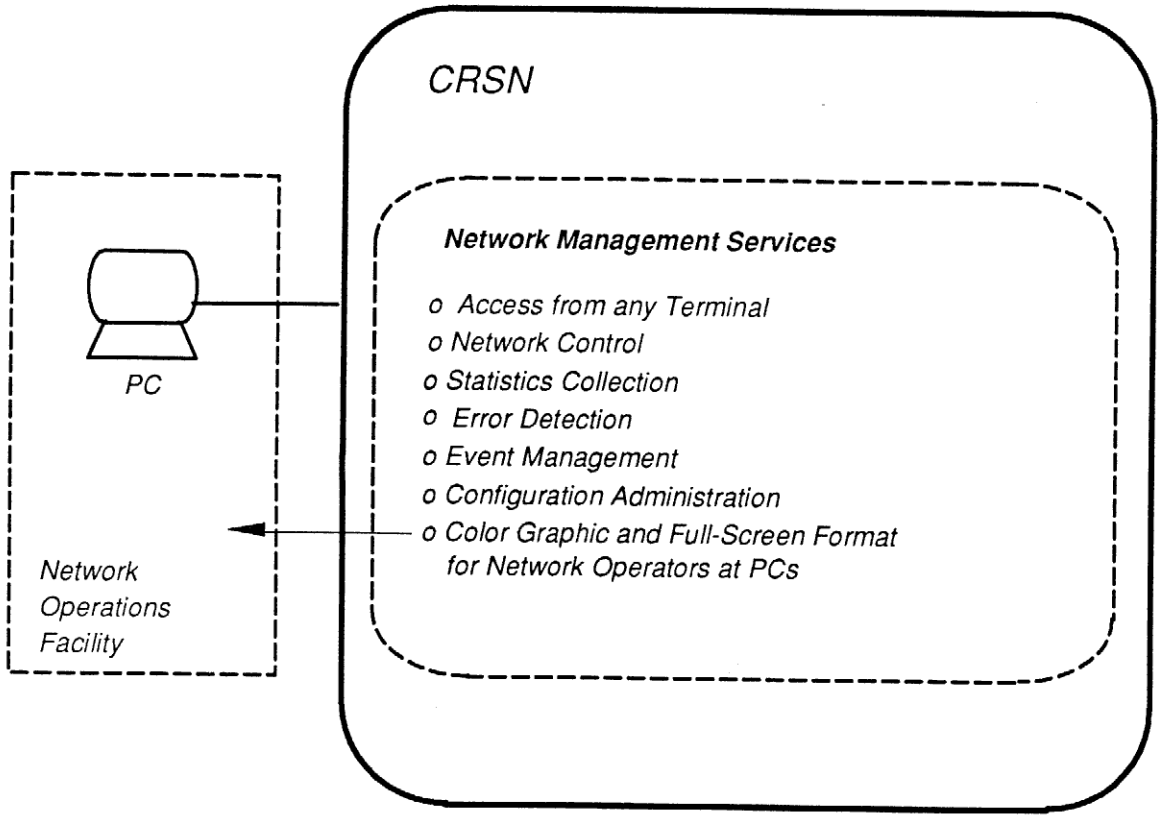


Fig. 3.1-2 Offline - Online Database Versions

3.2 Network Operation Functions

The Network Control Center is the primary center for monitoring and controlling the network. The network operator has a number of 'tools' available which can be classified as hardware or software tools. The hardware tools comprise operator terminals, disks, tape stations, printers, IDMs, etc., whereas the software tools are the operator commands.

Most of the operator's work can be done from a PC (or a VT100 terminal). The PCs are connected to the AADN via a Local Area Network (LAN). This is the operator's interface to the network, or, more specifically, to Network Management, (Fig. 3.2-1).



SDM/D/20

Fig. 3.2-1 Network Management Services

The network services provided by AADN are implemented as a set of commands divided into logical groups called command classes. The actual grouping and the number of commands classes may be changed according to needs.

All network commands can be issued from the PC either as a text command or via a menu-driven command entry facility (Fig. 3.2-2, 3.2-3, 3.2-4, 3.2-5).

Opposite top: *The top menu lists the command classes from which the operator may make his first selection.*

Opposite bottom: *Command Fill-in Panels illustrating all parameter fields.*

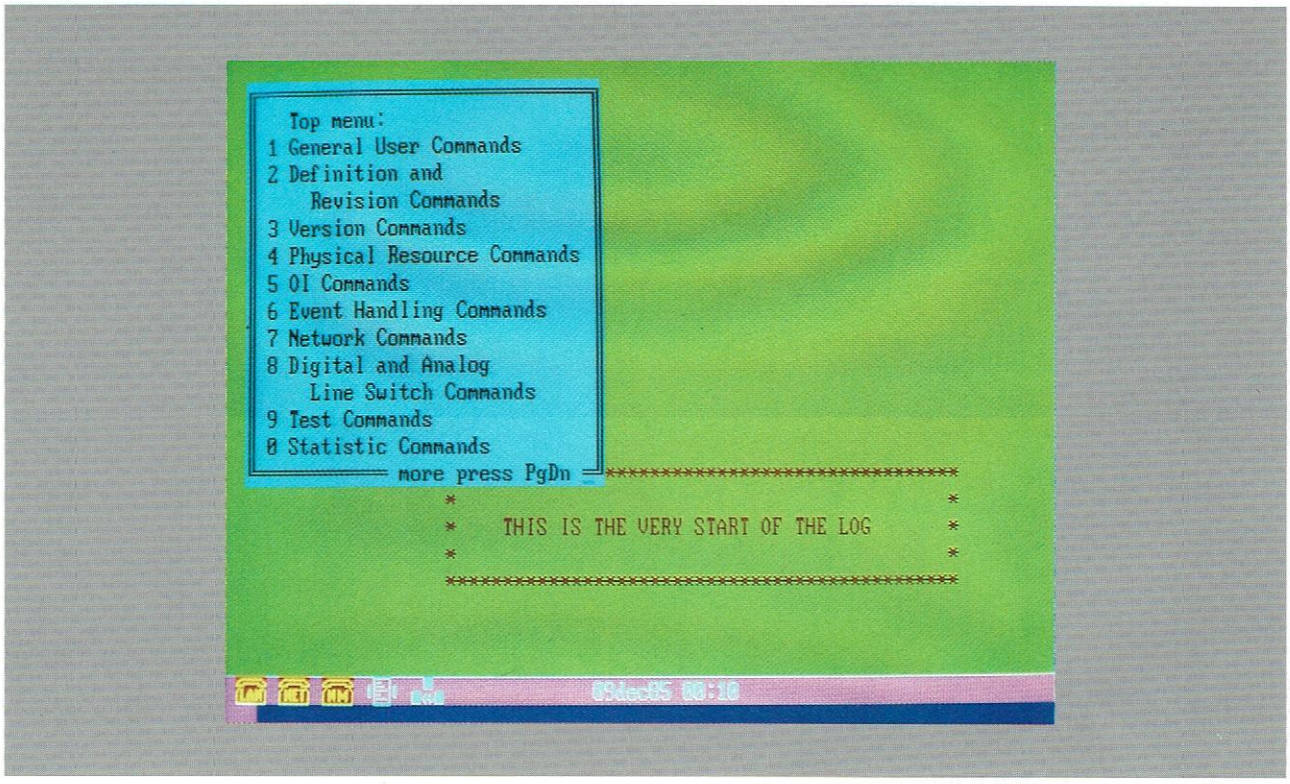


Fig. 3.2-2 Top Menu

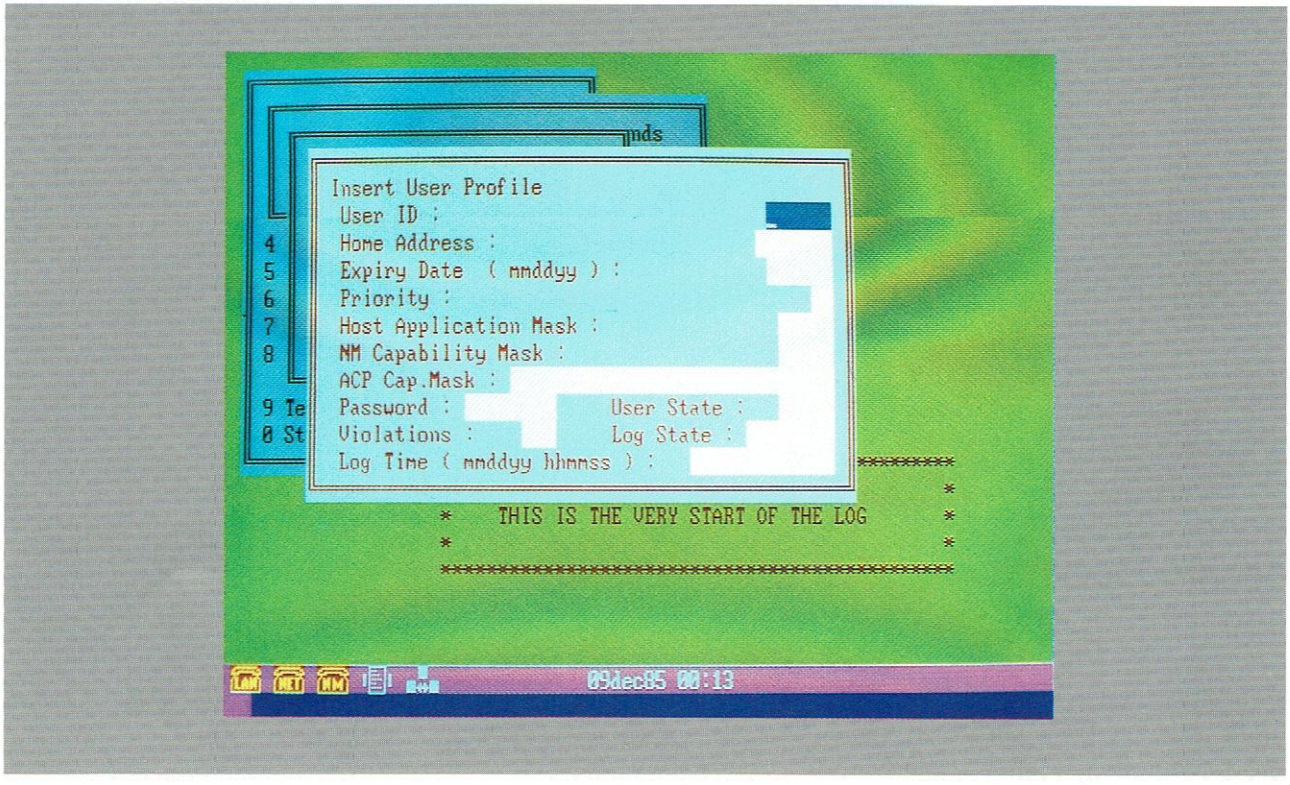


Fig. 3.2-3 Command with Fill-in Panel

Opposite top and bottom: *Command Fill-in Panels illustrating all parameter fields.*

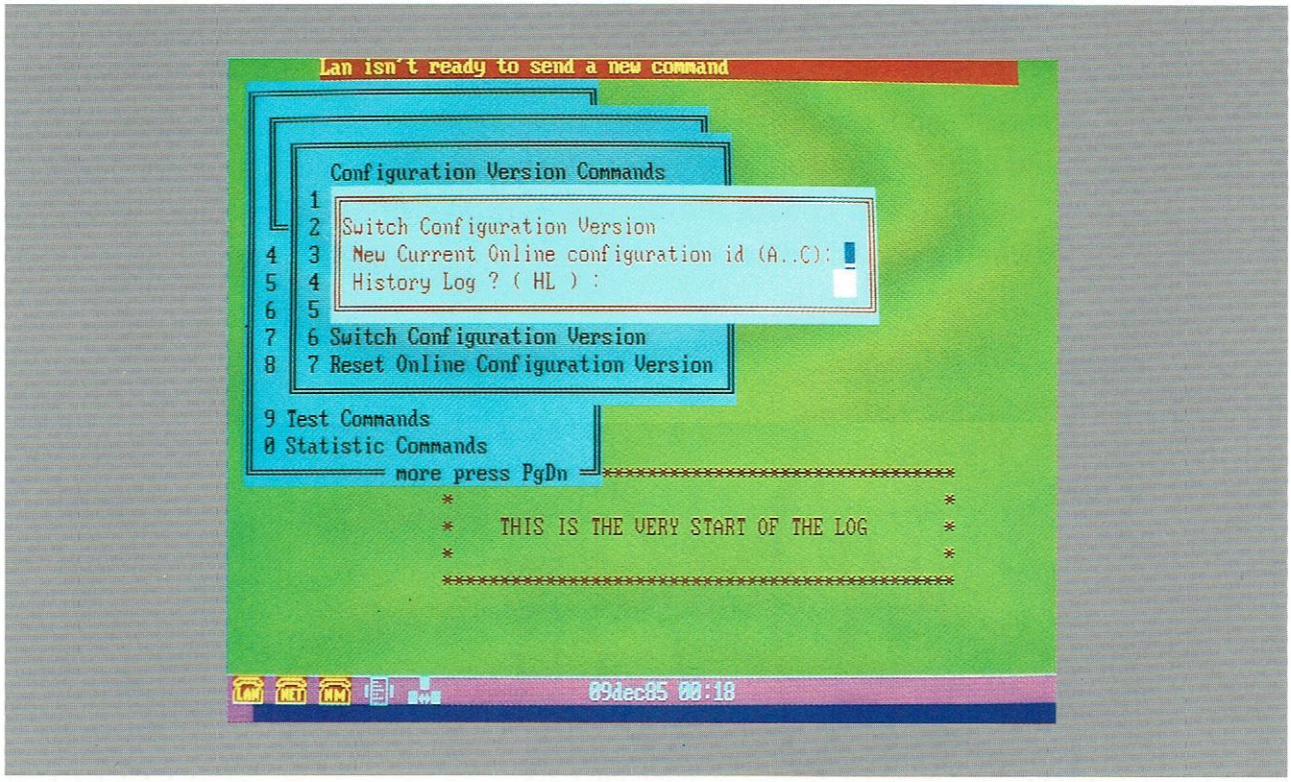


Fig. 3.2-4 Switch Configuration Version Command

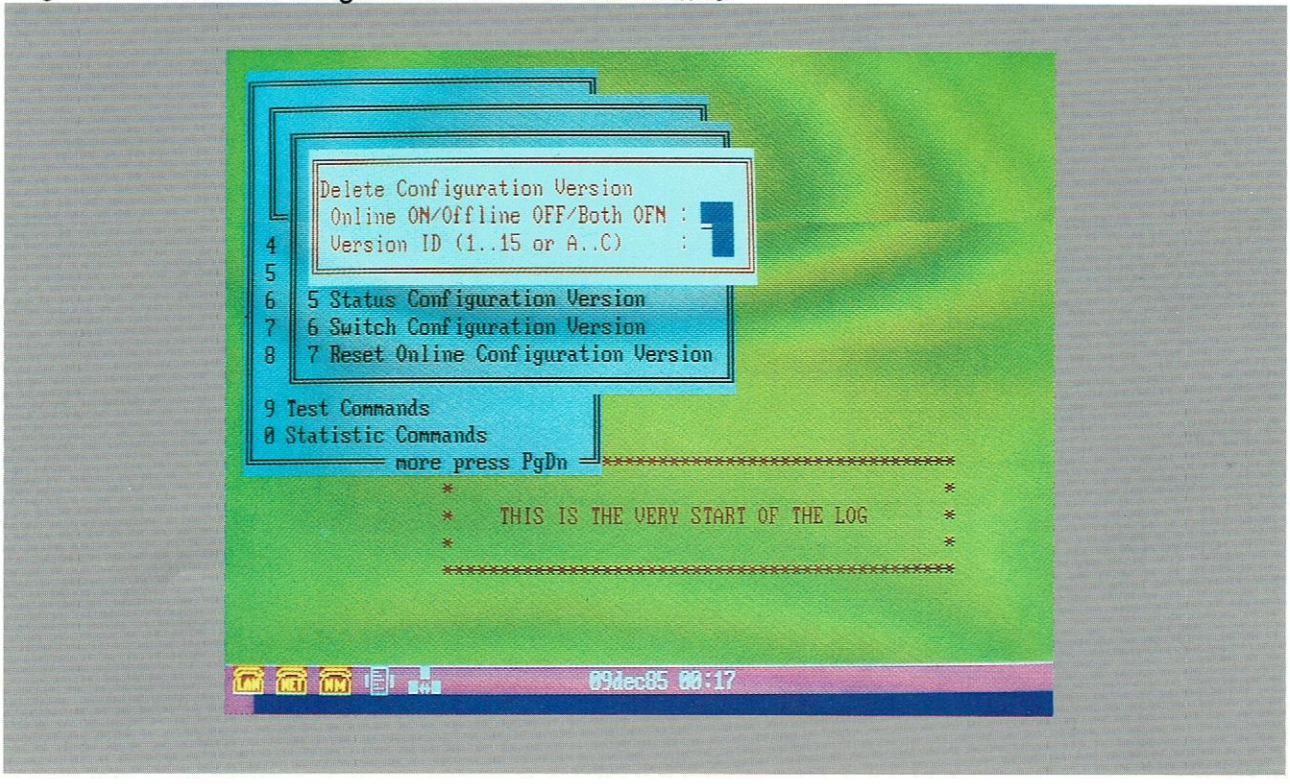
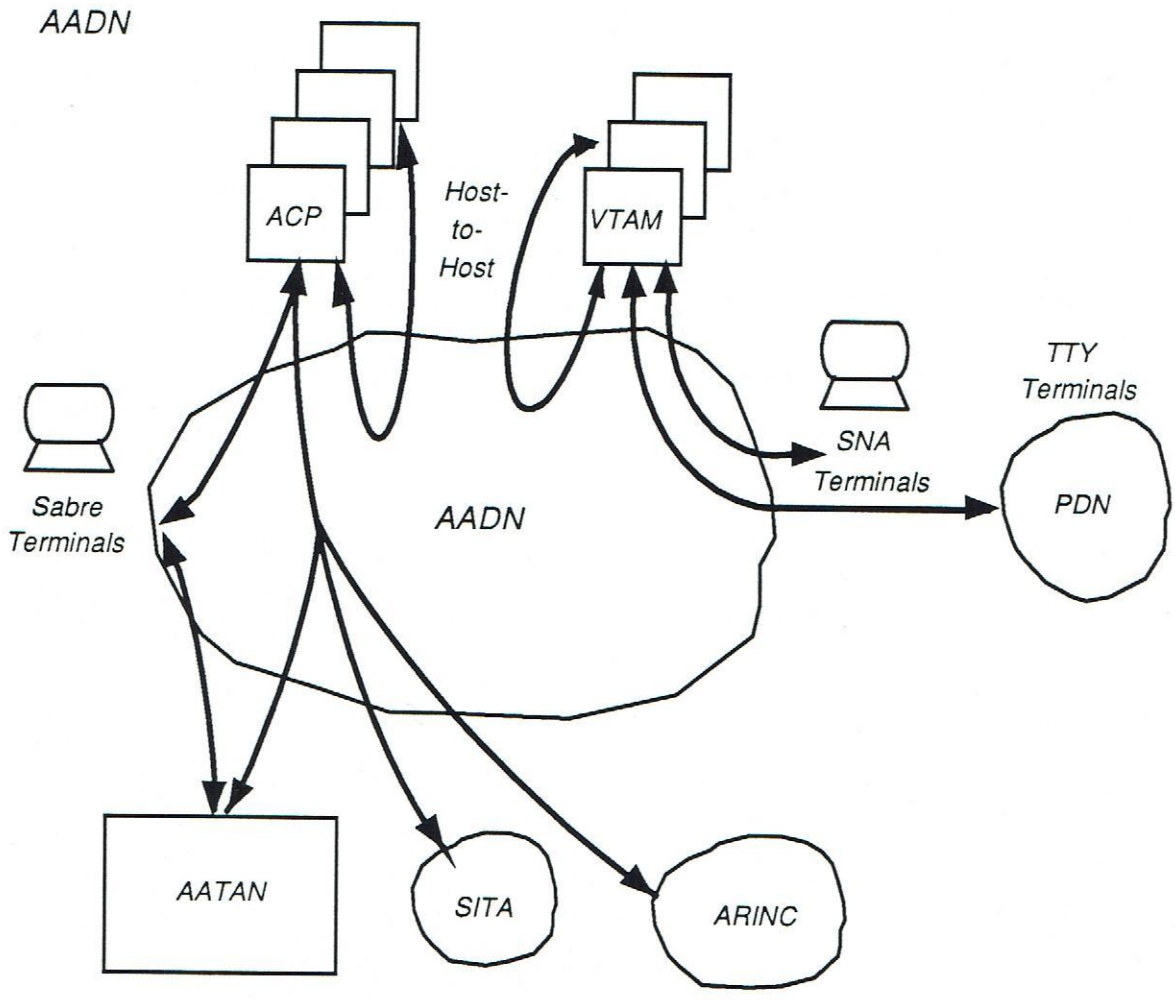


Fig. 3.2-5 Delete Configuration Version Command

From a network operations point of view, there are two primary tasks in operating the network. The first is related to the Network Control Center itself and concerns installing databases, making online updates to the database, printing files, starting command files, etc. The second task is to monitor and control the access networks and the sessions which have been established between end-users (Fig. 3.2-6).



SDM/D18

Fig. 3.2-6 End-User Sessions

3.3 The Network Control Center

Network monitoring is primarily done by means of the PC's color-graphic resource status pictures. (Fig. 3.3-1). These status displays indicate the nature and location of failures or problems.

Three levels of detail may be displayed in the status pictures:

- The entire network in overview.
- A selected resource and its neighboring resources.
- The internodal trunk lines connecting the Nodes.

It is also possible to obtain information on end-user sessions in the form of status pictures.

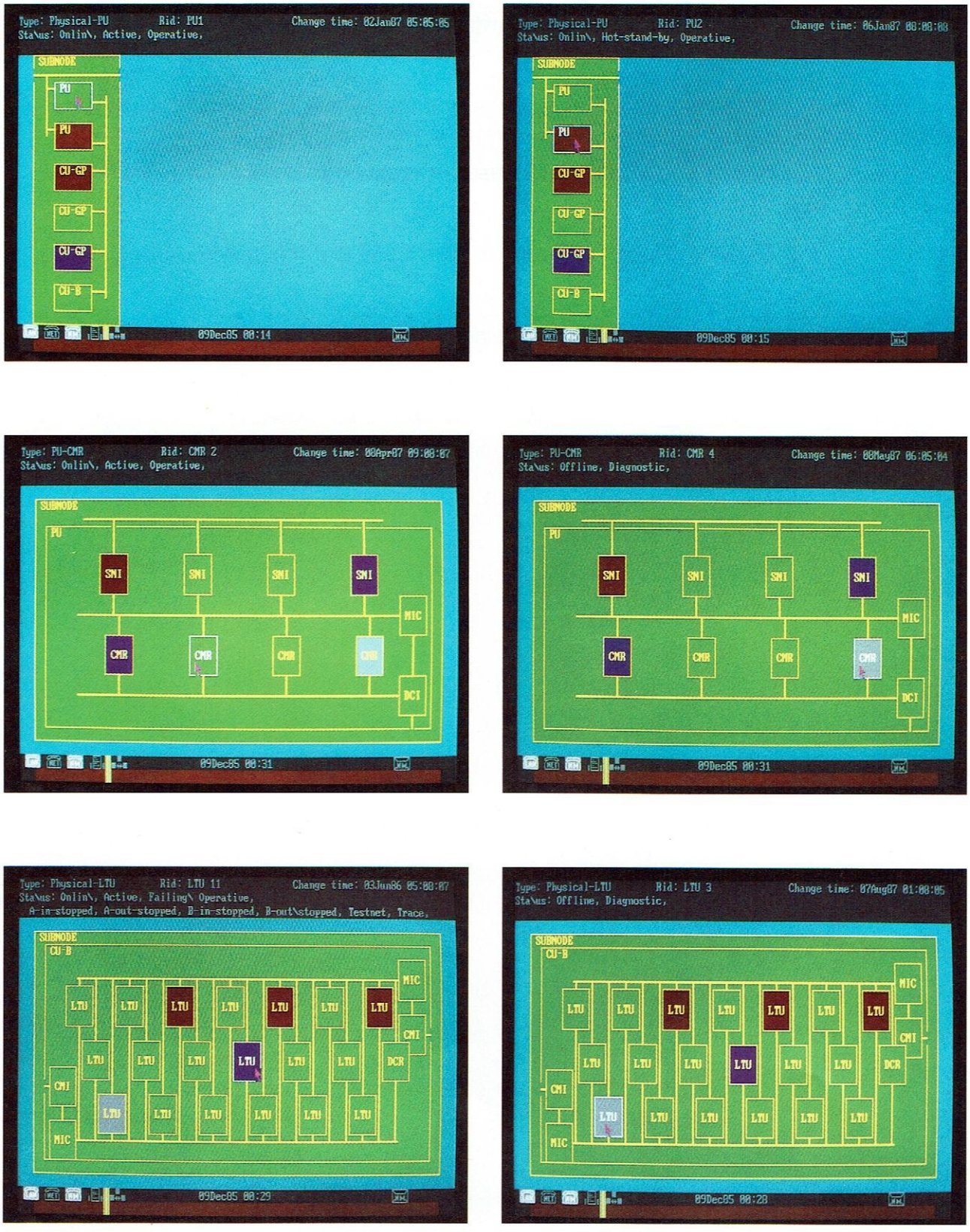


Fig. 3.3-1 Color Graphic Status Displays

Statistical information on traffic and network performance is available on either a permanent on temporary basis; permanent statistics are collected continually at predefined intervals, while temporary statistics are collected upon operator request. Both types are stored and accessible to the operator at any time. The operator can also issue statistical reports based on information collected within the last 24 hours.

Events are generated throughout the network when resource states change unexpectedly, when resource limits are reached and when hardware or software errors are detected.

Events may be subject to time or frequency filtering, so that minor irregularities are not reported. Only if the problem continues, will it result in an event being generated. All events are classified as an alarm, an alert, or a notice, and assigned a priority according to resource type.

3.4 Access Control

The Access Control Database contains a record or profile for each user, terminal and application in the network. It is on the basis of the user profile and the terminal profile that access control of terminal end-users is performed. A default session with a host application may be set up for SABRE and IBM SNA terminals. But these terminals, as well as PCs and VT100s, may also be subject to access control checks.

A user can have two types of session (Fig. 3.4-1):

- A network session, which is established by a LOGON command, enabling the user to communicate with the network. A network operator must log-on in order to issue network commands.
- A user session initiated by means of a SIGNON command, which enables the user to establish a session with a host application or with network management.

For each of the two types of sessions the user must be validated. Among other things, this includes checks for:

- Correct user-id and password (only a limited number of logon attempts are allowed before the user-id is closed)
- Expired user profile
- Valid terminal cutover date (i.e. the date from which the terminal may be used)
- The user's rights to use a specific terminal
- The user's and terminal's rights to access specific host applications
- The user's and terminal's rights to invoke specific network commands

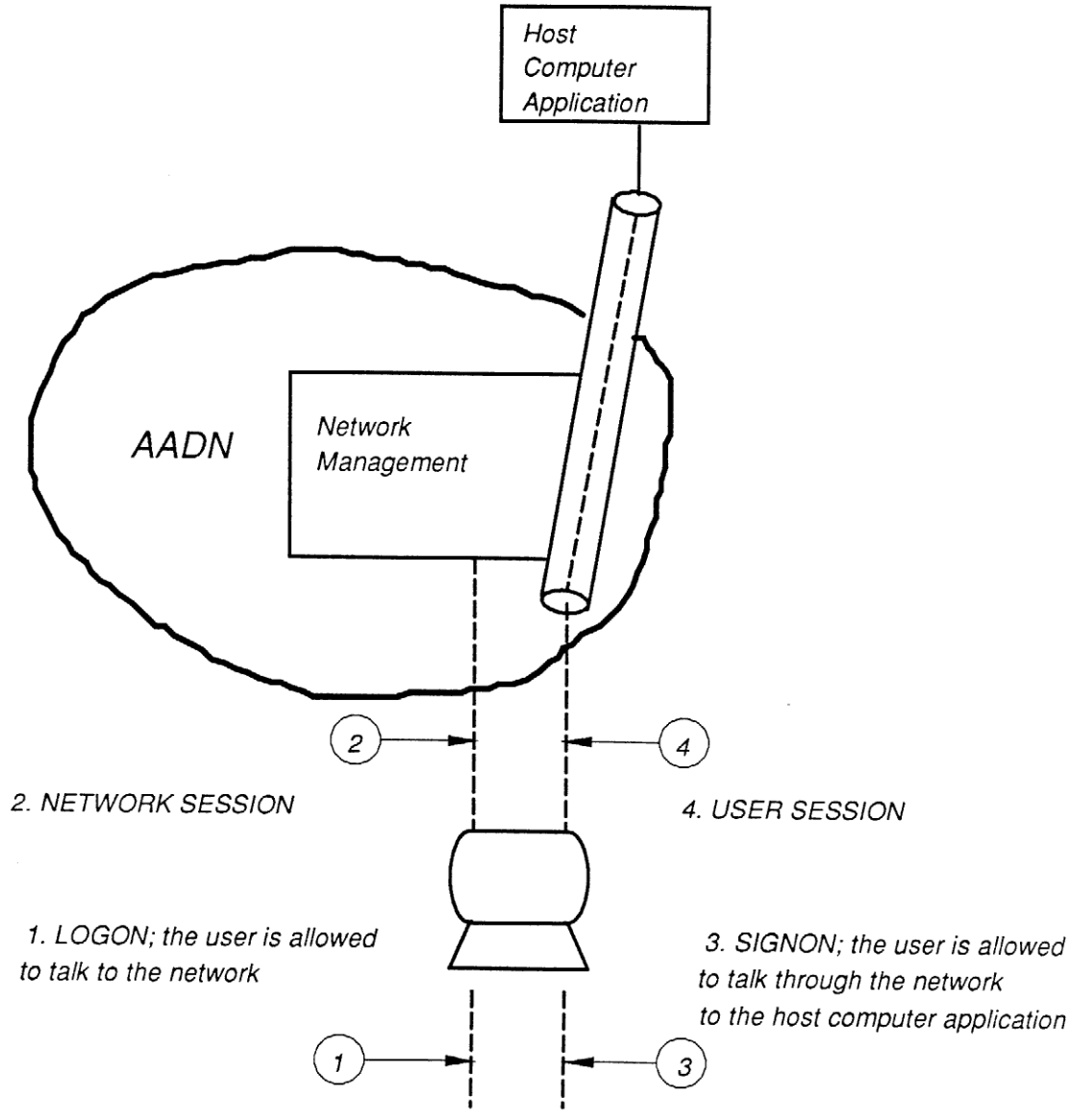


Fig. 3.4-1 Network and User sessions.

4 RECOVERY

This chapter deals with the recovery mechanisms and facilities of the Corporate Resource Sharing Network (CRSN).

CONTENTS PAGE

The aim of the recovery mechanism is to allow the network to survive a hardware or software failure. The software is designed to function despite a failure. And errors are detected immediately (by the software and the hardware). Finally, vital status information on the network state is retained through a check-pointing mechanism, which continually updates the hot standby PU (i.e. a standby PU which is ready to take over immediately) with vital information.

The main areas which must be recovered are:

- The NCC
- Primary Nodes
- The Secondary Node
- Internodal trunks and lines
- Host channels
- The LTUs and CU-CMRs

4.1 Redundancy

To provide high availability, the CRSN is designed with several levels of redundancy. Spare equipment can in many cases replace failed equipment.

On module level, system availability can be increased by adding one or more spare Line Termination Units (LTUs) online. On Subnode level, one PU in a PU-pair is active while the other is hot standby. If a failure occurs in the active PU, an automatic switch-over will take place. The hot standby PU is check pointed to memory which keeps it in a state identical to the active one before the error occurred. This keeps recovery time and loss of data traffic at a minimum. As an extra safety precaution, the Primary Node contains a spare Subnode which can be loaded if a PU switch-over should fail.

The redundancy principle also applies to the S-net which connects the Subnodes. To increase the traffic volume flow between the Subnodes up to four S-nets can be used in a Subnode-to-Subnode connection. If one S-net fails, the traffic is automatically taken over by the remaining S-net(s).

A high degree of redundancy is present in the connections between the Primary Node and the Secondary Nodes. The internodal trunk lines connecting the Nodes consist of several lines. If an error occurs on one or more lines, the remaining line(s) can still ensure a connection between the Nodes. If all the lines in a trunk line fail, a secondary route to the Primary or Secondary Node (via an intermediate Node) will be used.

Fig. 4.1-1 illustrates the various levels of redundancy which are possible in the CRSN.

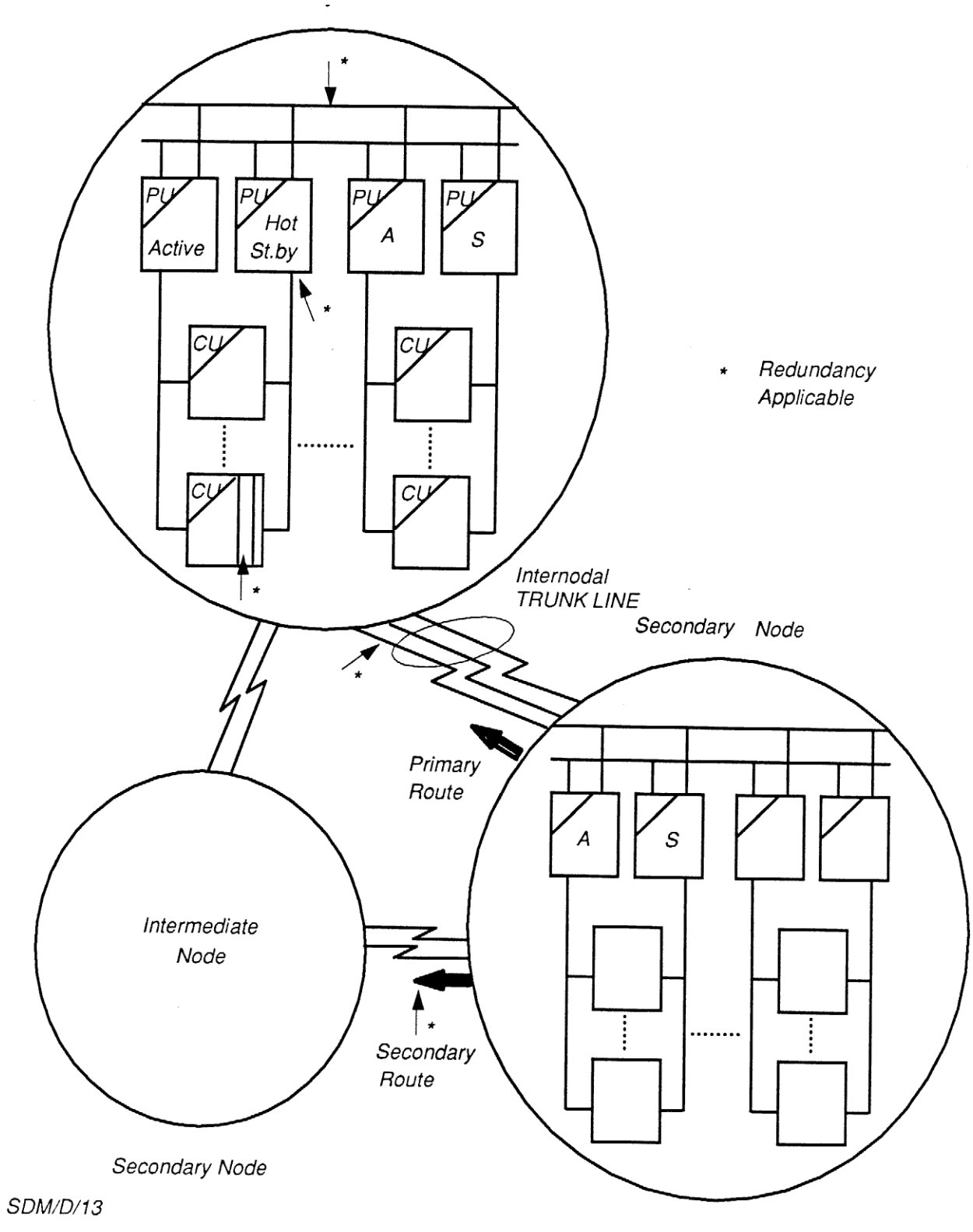


Fig. 4.1-1 Redundancy Principles

4.2 Recovery Actions

When an error is detected, there are in principle three ways to recover from it:

- Local Recovery
- Switch-over or Reload
- Re-initialization

Local recovery is performed by the software detecting a minor error. It does not involve switching over to standby equipment, reloading memory or restarting processes. If a problem persists (e.g. data transmission errors) the operator will be notified by an event message.

Switch-over or reload will return the system almost to the state it had before the error occurred, without operator intervention. This condition will result in the generation of an event message.

Re-initialization is performed manually if automatic switch-over or reload are impossible, and this will bring the recovered system component back to the state it had immediately after system start-up.

The latter recovery action is associated with a complete subnode, whereas automatic switch-over and/or reload concerns three elements:

- PU (switch-over)
- CU-CMR (switch-over/reload)
- LTU (switch-over/reload)

4.3 Session Clean-Up

During recovery no attempt is made to recover user sessions and these sessions are not checkpointed. Still, not all cases of recovery result in loss of sessions.

A PU switch-over will result in the loss of all user sessions of a terminal/user connected to the Subnode in which the switch-over takes place. LTU recovery will not in itself cause session loss but sessions might be terminated e.g. by host applications due to loss of data. Commercial host channel failures will result in loss of user sessions. With regard to the real-time SNAP hosts, sessions are not lost in case of channel failure or PU failure; Network Management will find another host (logical host) which can take over the session.

If sessions are lost, clean-up facilities exist to prevent non-existing sessions from "hanging". The appropriate Resource Handler informs Network Management, whereafter these sessions can be removed.

5 SYSTEM MAINTENANCE

5.1 Software Maintenance

The enhancement of the Corporate Resource Sharing Network (CRSN) in terms of new connectivity or new services requires the customizing or development of an Access Resource Handler. For this purpose the system is delivered with a large amount of system software and utilities, such as programming languages and test tools. CRSN programs are developed in the following languages:

- Pascal
- C
- Swell (a CR developed language)

The software is developed on CR80 computers. Development and test can be performed on a dedicated Test and Development System or directly on a Subnode in the online network.

CR supplies software maintenance for one year after the Network Acceptance Test, which will take place upon delivery of Version 3 of the AADN.

5.2 Hardware Maintenance

Hardware maintenance will be supplied by the Radio Corporation of America (RCA).

A DOCUMENTS FOR REFERENCE

System Requirement Specification	AADN/SRS/0001 (3.0), 830809
Man Machine Interface Reference Manual	NM/RFM/0001 (1.0), 870322
ACP I/F	AADN/ICD/0002 (4.0), 830809
IBM VTAM I/F	AADN/ICD/0003 (3.0), 830809
SABRE I/F	AADN/ICD/0004 (4.0), 830809
IBM Standard Terminal Support	AADN/ICD/0005 (4.0), 830809
ARINC I/F	AADN/ICD/0006 (3.0), 830809
Total Access I/F	AADN/ICD/0007 (5.0), 850331
Kansas City Weather I/F	AADN/ICD/0008 (4,0), 830809
Digital Line Switch I/F	AADN/ICD/0010 (3.0), 850331
Analog Line Switch I/F	AADN/ICD/0011 (3.0), 850331
Modem Control I/F	AADN/ICD/0012 (2.0), 830809
CCI Gateway I/F	AADN/ICD/0013 (2.0), 830809
Other Airlines I/F	AADN/ICD/0014 (4.0), 830809
Internodal Line I/F	AADN/ICD/0015 (2.0), 830809
SLC I/F	AADN/ICD/0016 (4.0), 830809
Physical I/F	AADN/ICD/0017 (2.0), 830809
Digital Test Equipment	AADN/ICD/0018 (1.0), 850331

B TERMS AND ABBREVIATIONS

AADN American Airlines Data Network based on a customized version of the CRSN.

AATAN AA Total Access Network

ACCESS LINE Denotes a communication line which connects a **Subnode** in the AADN to one of the following:

- o SABRE concentrators or interchanges
- o IBM 3270 cluster controllers
- o Total Access Network
- o Other Airlines
- o ARINC
- o Weather systems
- o Test equipment
- o PDN

ACP Airlines Control Program - specialized operating software residing in AA real-time host that supports the reservations and flight information applications at AA.

Active State of **online** resource indicating that it is part of the live environment, and intended to be operative.

AMEX American Express

Application A software program residing in a participant host processor. An application program may provide services to a user.

ARINC

Aeronautical Radio Inc. - An organization, of North American airlines and foreign airlines operating in the US. The ARINC network is used for the routing of messages between airlines.

Automatic Recovery

Indicates that **recovery** from a failure situation will be achieved without manual intervention.

Automatic Switch-Over

Indicates that **switch-over** of a failed component to a standby component is accomplished without operator intervention.

Checkpointing

Copying a coherent set of state variables (i.e. resource status information for a subsystem), which describes a state from which a restart might be done.

CMR

CPU-MAP-RAM. Hardware module of a PU or CU.

Cold (Re)start

Cold (re)start refers to the start-up of a resource from a situation where the software is reloaded and has to be (re-)initialized, tables built, etc.

Commercial Hosts

The AA host processor complex that performs all processing except for the Reservations, Flight Information systems and their associated Test Systems. It consists of standard IBM (or IBM compatible) hardware and standard IBM operating systems and software.

Commercial Processor (COP)

A Subnode in the **Primary Node** whose primary function is to provide connections to commercial hosts.

Configuration

The description of hardware and software resources and their interconnections including all parameters necessary for proper operation.

Congestion Control Procedures for

- o Control of the network in such a way that congestion is unlikely to occur;
- o Resolving congestion, once it has occurred.

COP Equivalent to **Commercial Processor.**

CR Christian Rovsing A/S af 1984.

CRSN Corporate Resource Sharing Network. The CRSN is a generic network in the sense that it is not a deliverable network, but a template for the development of a deliverable network.

CU Channel Unit. Hardware component of a Subnode.

DECS Dispatch Environmental Control System - Realtime application residing on an ACP host processor.

Down Time The period that elapses between the time a system fails and until the system is returned to normal operating conditions.

End User An external point to which the AADN provides services.

End-User-Session A logical association which allows two **end-users** to exchange information.

Event The detected occurrence of an incident such as:

- o A security violation.
- o A change in the state of an internal or external resource.
- o A threshold being exceeded.

Event Message

Message issued as a result of an **event**.
The event message contains the following information:

- resource identification
- event code
- time of occurrence
- event specific information

Event Priority

Number between 0 and 15.

External Network

A network interfacing the AADN for which AA does not have total responsibility or control, e.g. SITA or ARINC.

FOS

The PAID identifying the Flight Operating System residing in an ACP host.

Gateway

A gateway is a facility interconnecting two networks. The AADN includes gateways to a number of networks:

- Total Access
- SITA
- ARINC
- Other Airlines
- Weather
- PDN

Gateway Processor

A **Subnode** in the **Primary node** whose primary function is to provide **gateway** capabilities.

Global Network Database

Generic database which consists of the following entities

- Network Configuration Database.
- Access Control Database.
- Software Data Base.

GWP — Equivalent to **Gateway Processor.**

HIP — Host Interface Processor.

Hip Complex — The AADN node attached to the real-time hosts, the commercial host and the test host environment, either by channel connection or remote communication lines and which supports communication with external networks.

Host — Generally a larger computer system; in AADN used for AA's real-time and commercial IBM compatible computer systems.

Hot Standby — Indicates that the status of the standby **resource** is loaded, initialized, and up-to-date, ready to take-over the functions of the active resource for which it is back-up.

IDM — Intelligent Database Machine.

Initialization — The transition of a system from reset state into operational state. Will be based on the current Global Network Database Configuration.

Inoperative — Indicates that an **online resource** is not available although included in the active network, e.g. due to a permanent error situation.

Internodal Line — Data transmission line directly interconnecting one **Node** to another **Node.**

Internodal Trunk Line — Group of **internodal lines.**

Line Termination Unit — An input/output module in the CU in which access lines terminate.

Log-off

The process whereby a **user** declares an intention to terminate the use of the services of the network.

Log-on

The process whereby a **user** declares an intention to use the services of the network.

MX-AMOS

Mapped Extended Advanced Multiprocessor Operating System. An operating system in the CR computers.

NCC

Network Control Center.

Network Configuration

Comprises the descriptions of terminals, hosts and nodes. This includes the different physical and logical relations available from one unit to another. E.g. host, channel, node, LTU, internodal trunk line, concentrator, line, terminal.

Network Configuration Data-base

Part of the **Global Network Data Base** containing the **network configuration**.

Network Operator

A **user category** without access right restrictions performing network control.

Network Session

A logical association which allows an **end-user** to exchange information with AADN.

Nodal Switch Processor (NSP)

Subnode whose primary function is to switch messages. The nodal switch processor is the end point of the **internodal trunk** lines.

NM

Network Management. The software subsystem which is responsible for monitoring and controlling the network statistics collection, presenting of status, on-line and off-line configuration, etc.

Offline	Logical state of **resource** indicating that it is not serviced by the network.
Online	Logical state of a **resource** indicating that is serviced by the network.
PAID	Process Area Identifier - This is the term given to identify a host application in the Real-Time Host Environment.
PDN	Public Data Network.
Primary Node	The Node containing the NCC and the HIP complex.
Profile	Those parameters of a resource (terminal, application or user) used by the network to perform access control.
PU	Processor Unit. Hardware component of a subnode.
Realtime Host	IBM compatible host operating ACP; includes AA's RES, FOS and VM test systems.
Recovery	Re-establishment of service provided by a given **resource** from a failure condition; recovery may imply **switch-over** to back-up equipment.
Resource	A network element (hardware or software) which is known to the network by its resource identification.
RES	The PAID identifying the Reservation application residing in the ACP hosts.
SABRE	Semi-Automatic Business Reservation Environment.

Secondary Node

Two or more NSP subnodes interconnected via a S-Net. The Secondary Nodes are connected to the Primary Node by internodal trunk lines.

Sign-Off

The process of terminating a user session.

Sign-On

The process of establishing a user session with a specified application.

SITA

Societe Internationale de Telecommunications Aeronautiques.

SNA

IBM's System Network Architecture, a protocol supported by the commercial host.

SNAP

SABRE Network of ACP Processors - This is the name given to modifications made to the ACP by AA to allow the ACP to execute the same application on more than one host simultaneously.

S-Net

Physical connection between two or more **Subnodes** in a **Primary** or **Secondary Node.**

Subnode

Component of a Node. The Subnode hardware consists of one active PU and optionally a standby PU, and a number of CUs. The Subnode types are:

- ***SCP***
- ***NCP***
- ***NSP***
- ***GWP***
- ***COP***

Switch-Over

The act of switching from an active component to a back-up component, usually in the event of a failure.

System Control Processor (SCP)	A Subnode in the **Primary Node** whose primary function is the loading, initialization and control of the CRSN systems constituting the other Subnodes of the Primary Node and Secondary Nodes.
Total Access Network	A communications system allowing SABRE terminals to communicate directly with **hosts** external to AADN, and allowing **AMEX** terminals to communicate directly with AADN **ACP hosts.**
TSO	IBM's Time Sharing Option - This is an application program that runs under MVS (an operating system) on an IBM compatible mainframe and provides time sharing services.
TTY	Teletype terminal or a device compatible herewith, i.e. an ASCII async terminal.
VAX	Virtual Address Extension.
VTAM	Virtual Terminal Access Method - IBM program product, running in the commercial and test hosts.
WMSC	Weather Message Switching Center - a Kansas City, Missouri, facility operated by the Federal Aviation Administration (FAA) for the distribution of surface weather data.

CR Systems