IBM

International Technical Support Centers

APPN / SUBAREA NETWORKING DESIGN AND INTERCONNECTION CONSIDERATIONS

GG24-3364-00

APPN / SUBAREA NETWORKING DESIGN AND INTERCONNECTION CONSIDERATIONS

Document Number GG24-3364-00

May 30th, 1989

International Technical Support Center
Department 985, Building 657
Raleigh, North Carolina

FIRST EDITION (May 1989)

This edition applies to VTAM V3 R2, NCP V4 R3, NCP V5 R2 for use with the MVS/370, MVS/XA, VSE, and VM/SP Operating Systems and also for use with AS/400 R1.2.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this document is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

The information contained in this document has not been submitted to any formal IBM test and is distributed on 'As Is' basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Publications are not stocked at the address given below. Requests for IBM publications should be made to the IBM branch office serving your locality.

A form for reader's comments is provided at the back of this publication. If the form has been removed, comments may be addressed to:

IBM Corporation (985A/B657)
International Technical Support Center - Raleigh
PO Box 12195
Research Triangle Park, NC 27709, USA

IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Acknowledgments

The author of this document is:

- Hans Neecke - IBM The Netherlands

Project advisor:

- Paul Berdowski - ITSC Raleigh

The contribution of the following persons are gratefully acknowledged:

- Ger Roovers - ITSC Raleigh
- Roland Peschke - ITSC Raleigh
- Fred Fletcher - CPD Raleigh
- John Drake - CPD Raleigh.
- John Zeiger - CPD Raleigh.
- Gary Schultz - CPD Raleigh.
- Marcia Peters - CPD Raleigh.
- Gregg Sunday - CPD Raleigh.
- Jim Fletcher - CPD Raleigh.
- Rick Mcgee - CPD Raleigh.

Abstract

This document is a guide for planning interconnection of APPN and SNA subarea networks. It is intended for systems engineers who are involved in planning the connection of APPN to SNA subarea networks.

Products involved:

- AS/400
- VTAM V3R2
- NCP V5R2/V4R3.

CSYS (81 pages)

Preface

The purpose of this document is to provide information about the APPN extensions and connection of current APPN networks with SNA subarea networks. This includes:

- Connection of APPN networks to subarea networks
- Design considerations for building mixed APPN subarea networks.

The document is structured to provide the following information:

- SNA T2.1 node structure
- Description of the APPN extensions
- APPN compared with SNA subarea networking
- SNA T2.1 support implemented in VTAM and NCP
- APPN implementation in the AS/400
- Interconnection of APPN networks and SNA subarea networks
- Design criteria in a mixed APPN/subarea environment
- SNADS and DDM in a mixed APPN/subarea network.

Table of Contents

List of Illustrations

1.0 SNA T2.1 and APPN Node Structure

1.1 Introduction

The purpose of this chapter is to give an overview of the components and functions of the SNA T2.1 node and the SNA T2.1 node with the APPN extensions for the purpose of a general discussion of the APPN[1] extensions. The APPN extensions are product unique features based upon the SNA T2.1 node and are implemented today in the System/36[1] and the AS/400 [1].

From here on an SNA T2.1 node is referred to as a T2.1 node. The term APPN network is a generic one meaning the implementation of the APPN extensions and implies no particular relationship with an IBM product.

1.2 T2.1 Node Overview

T 2.1 peer protocols provide a mean of communication between adjacent peer-to-peer connected distributed processors. A T2.1 node can also be attached to a subarea node with boundary function (BF), also called a boundary node. In this way the physical and session level connectivity required for support of LU 6.2 as well as other LU types through a boundary node is provided.

Two types of LUs can be distinguished:

- An independent LU is able to activate an LU-LU session without assistance from an SSCP. Only an LU 6.2 can be an independent LU. A T2.1 node supports independent LU protocols to other adjacent T2.1 nodes as well as to a boundary node.
- A dependent LU requires the assistance of the SSCP to activate an LU-LU session. Dependent LU protocols are supported from the T2.1 node only to boundary nodes.

The T2.1 node consists of the following components:

- Node Operator Facility (NOF)
- Control Point (CP)
  - Session Services (SS)
  - Configuration Services (CS)
  - Address Space Manager (ASM)
- Logical Unit (LU)
- Path Control (PC)
- Data Link Control (DLC).

Figure 1 on page 2 outlines the T2.1 components.

---

[1] trademark of IBM

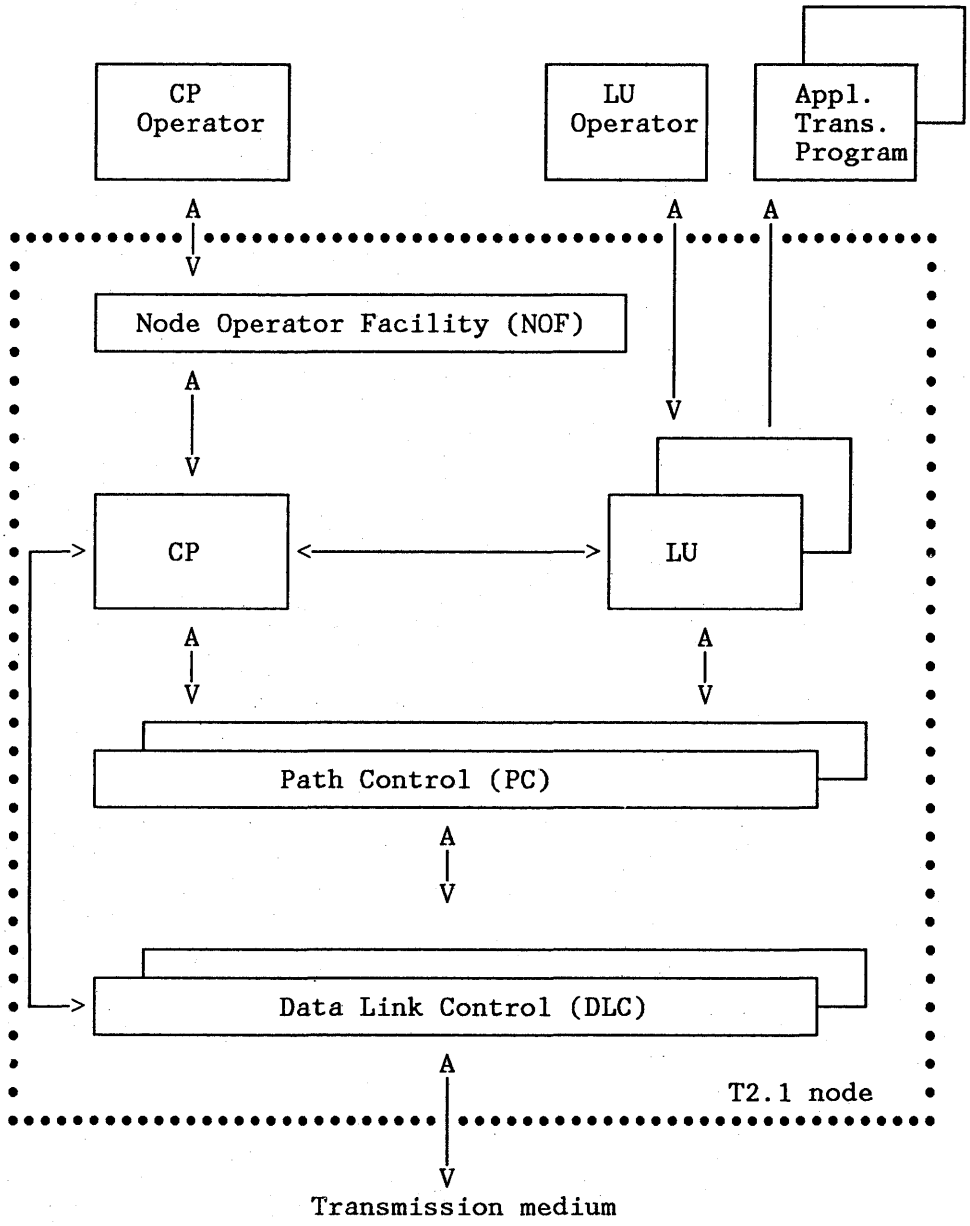


Figure 1. T2.1 Node Components

1.2.1 Node Operator Facility (NOF)

NOF acts as the user interface to the node. This interface can be human as well as programmed. NOF functions are:

- Activation/deactivation of the node, resulting in creation of the control point, which in turn creates the control point components when the node is activated. The control point is responsible for the management of the T2.1 node's resources.
- Operator-initiated link-related commands (link activation/deactivation). During node startup link activation is performed by the control point.

- Operator- initiated activation/deactivation of LUs.

1.2.2 Control Point

The control point (CP) manages the resources of the node, for example applications and communication links. At node activation time, the control point activates the links by starting up path control and data link control elements serving each link. The control point also assists independent LUs to initiate and terminate sessions. This is done by the following components:

- Session services
- Configuration services
- Address space manager

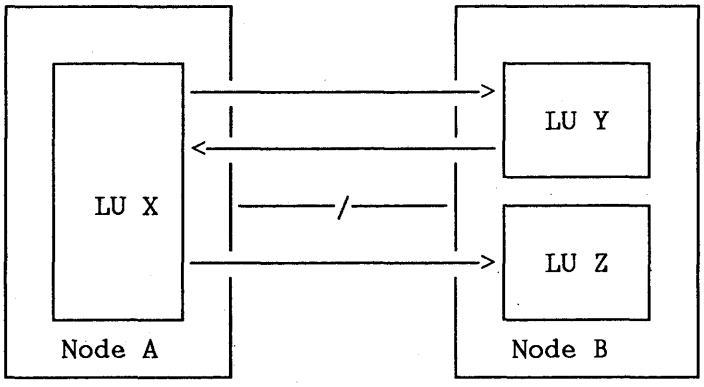
1.2.2.1 Session Services

The session services component assists independent and dependent LUs with session initiation. For this it maintains a directory that maps a destination LU name to its corresponding control point name and link. If the link is not yet activated, session services makes use of the service of another component, configuration services, to activate the link. If the link is active, session services relates the LU session to a path control/data link control port.

T2.1 nodes support LUs that can both initiate sessions and can respond to session initiation requests; an independent LU in a T2.1 node is able to both send and receive BINDs. The LU sending the BIND is called the primary LU (PLU); the one receiving the BIND is called the secondary LU (SLU).

Independent LUs can have multiple sessions and are able to manage their session limits themselves. A dependent LU can act as an SLU only and has an LU-LU session limit of one (managed by the SSCP).

In Figure 2, LU X has parallel sessions with LU Y and multiple sessions with LU Z and LU Y.



Key
-/- represents a link between nodes
—— represents a session between LUs (arrow points to SLU)

Figure 2. Session Capabilities

1.2.2.2 Configuration Services (CS)

The configuration services component of the control point is responsible for activation, deactivation and management of the link(s) to the adjacent node(s). It creates the path control instances and

relates them with links when they are activated. The adjacent node is identified by exchange of XID protocols. T2.1 nodes use XID3 protocols. During XID3 processing information about the node characteristics, such as node type, buffersize and link station role, is exchanged.

1.2.3 Address Space Manager (ASM)

Each session between adjacent nodes is associated with a session address. This address consists of a two-byte combination of the local address and the remote address (OAF-DAF pair). This information enables path control to correlate the half-session in the node with the route to the data link control components and is stored in the local format session identifier (LFSID). The ASM residing in the physical unit where the request originates assigns the LFSID and manages the LFSID pool for all the active links and half sessions in the node.

The address space managers in adjacent nodes may assign LFSIDs when starting sessions from their node. To avoid the assignment of identical LFSIDs, the address spaces in the nodes are kept independently by using a bit in the LFSID. This bit is called the OAF-DAF assignor indicator (ODAI). The bit is set during XID processing. The bit is set to zero for the primary station and set to one for the secondary station.

ASM also performs several functions associated with the session-activation and deactivation requests and responses and is involved in the BIND and UNBIND processing.

1.2.4 Logical Unit (LU)

The logical unit serves as a port to the path control network and enables transaction programs to communicate on a peer-to-peer basis. The logical unit contains instances of the following SNA layers:

- Transaction services (for example SNADS, DIA)
- Presentation services
- Data flow control
- Transmission control.

The interface between the LU and the transaction program (protocol boundary) consists of the LU 6.2 command interface.

1.2.5 Path Control (PC)

The primary role of the path control (PC) component of a T2.1 node is to deliver message units between LUs in the node and other LUs outside or within the node. Path control provides the transmission priority function for outgoing message units. There are four transmission priorities: network, high, medium and low. One path control instance per link exists and maintains four queues for the link and outgoing messages. According to their priority these are queued for transmission by data link control.

PC uses the local format session identifier (LFSID) to route messages between DLC and the LU half session.

1.2.6 Data Link Control (DLC)

DLC is responsible for performing the communication over the link using DLC protocols. Currently supported protocols are:

- SDLC

    - leased point-to-point
    - leased multipoint
    - switched
- X.25
- Token-Ring
- Ethernet (RT PC [2] only).

Data link control used between two T2.1 nodes or between a T2.1 node and a boundary node may be any one of a number of mentioned DLCs.

A T2.1 node can have links to multiple adjacent T2.1 nodes or subarea nodes. This is illustrated in Figure 3. Communication between node B and C can be provided through an application level function in node A or through the APPN [3] feature.

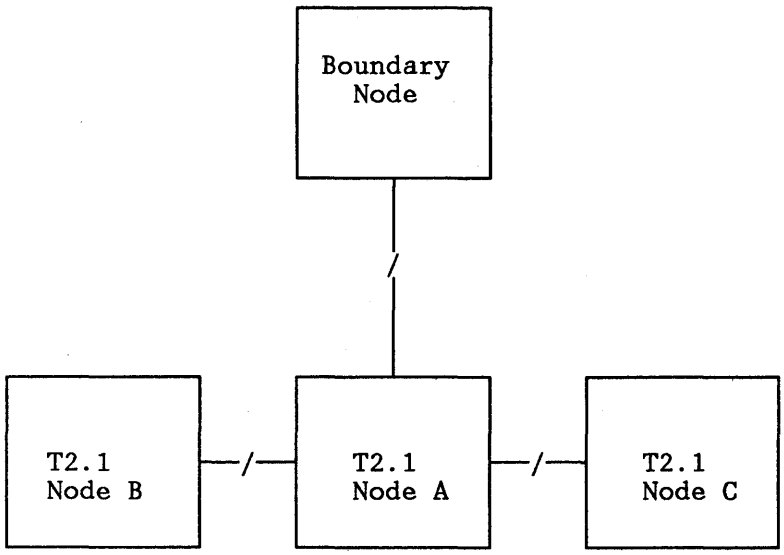


Figure 3. A T2.1 Node Attached to a Boundary Node and Multiple 2.1 Nodes

Two T2.1 nodes, both attached to the same subarea network, may have sessions between their respective LUs as if their nodes were adjacent. The session may span multiple subareas. In this case the session has to connect independent LUs. For dependent LUs only T2.1-to-subarea LU-LU sessions are possible through the boundary node. Figure 4 on page 6 illustrates this.

[2] trademark of IBM

[3] trademark of IBM

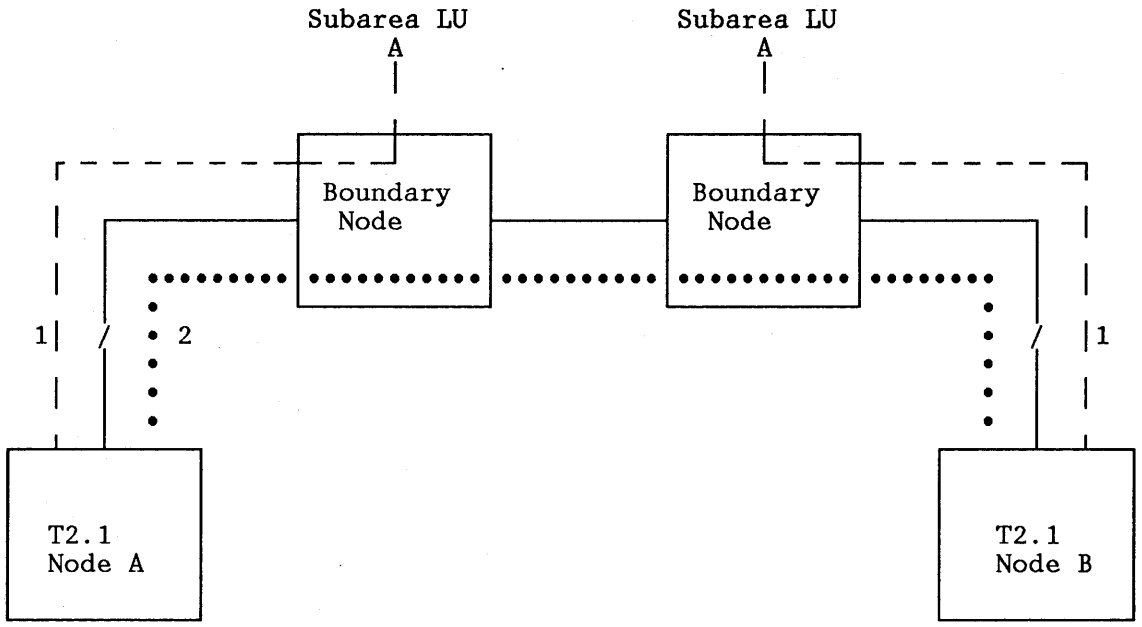


Figure 4. A T2.1 Node Attached to Boundary Nodes: 1: dependent LU-LU sessions; 2: independent LU-LU session

1.3 APPN Extensions

As discussed before, T2.1 nodes only support connections between adjacent nodes. Each T2.1 node manages its own local resources. Within a T2.1 node all remote resources with which sessions will be established, have to be defined.

Adding the APPN capability to communicate through the network with other non-adjacent nodes without the burden to system-define the entire network topology in each node means that the control point must have the ability to dynamically locate other resources in the network. Also the network has to keep track of changes in its topology in a dynamic way; the network has to be "self learning". To allow this to happen, the network nodes must exchange information about their local resources. This information exchange takes place by means of control sessions between the nodes on both sides of the link. The control session is started during node and link activation and remains active until deactivation of one of the nodes or links. A control session consists of two half-duplex LU 6.2 sessions between the control points and constitutes in this way a full-duplex connection.

Also the nodes should have a directory with the node's local configuration, which is accessible by other nodes. After having located a resource, the optimum route to that resource must be calculated. This implies that topology information must be available also. Figure 5 on page 7 illustrates this concept. The actual route between A and B could pass any intermediate node, depending on the route selection criteria. For example depending on node and link characteristics, the selected path could be the route via node 2, node 3 and node 6. "Topology and Routing Services (TRS)" on page 9 provides more information about route selection.

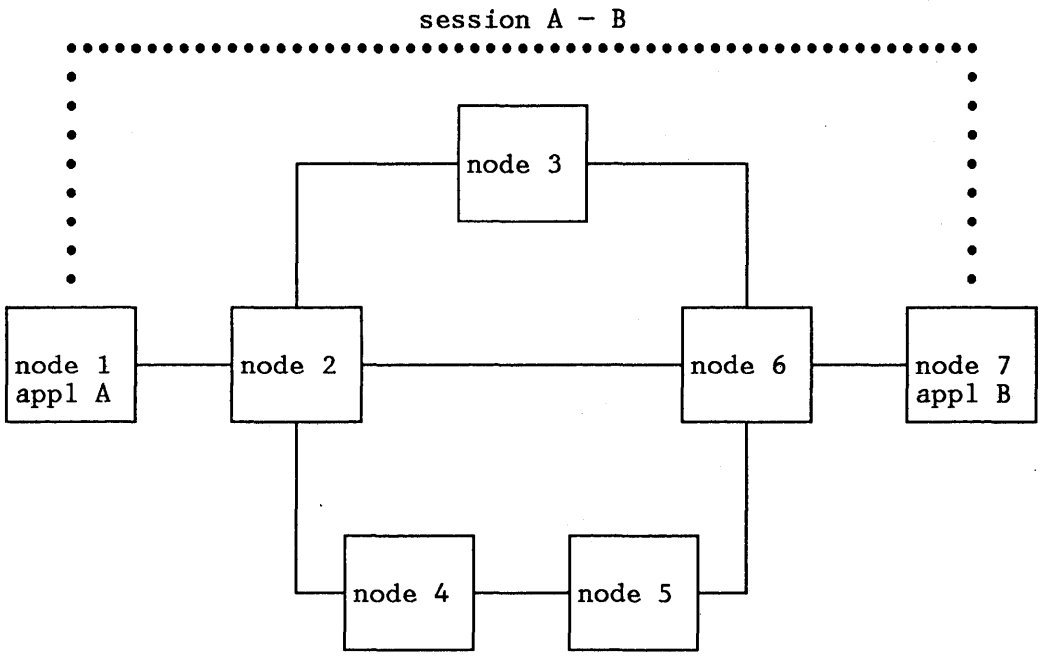


Figure 5. Session Between Non-adjacent Nodes

The functions mentioned above are implemented as a product extension to the T2.1 node architecture. These functions are described in an IEEE paper of May 1985. The extensions are:

- Dynamic topology changes
- Distributed, dynamic routing
- Intermediate session routing (including intermediate adaptive pacing and segmenting and reassembly).

1.3.1 Node Types

Three different node types can be distinguished. All are T2.1 nodes, but the APPN nodes are product extensions to the basic T2.1 node architecture.

- ***APPN Network Node (NN)***

  The network node role is to act as an intermediate node and as a server for attached APPN end nodes (EN). Server functions for the end node are routing, session and directory service. The collection of APPN end nodes attached to the network node for which it acts as server are includeded in the network node's *domain.* In Figure 6 on page 8 the nodes EN1a, EN1b, EN1c, NN2 and EN6, NN5 constitute two network node domains as shown. APPN end nodes have control sessions with the server network node. Network nodes have control sessions with the adjacent network nodes. Sessions can have end points in either network nodes or APPN end nodes.

- ***APPN end Node (EN)***

  The APPN end node can only provide directory and session services for its own LUs. For services beyond the scope of the APPN end node, the APPN end node relies on its serving network node. An APPN end node has a control session only with its server and can have links to other network nodes. Afterwards the APPN end node can change the network node server by selecting another network node from the server list. This may happen in case of a link failure or server outage. An APPN end node has the option to have no control session with the network node. When the

APPN end node is connected to the network node via a public switched network, it is preferable to have no control session.

- ***Low-Entry Networking (LEN) End Node (EN)***

  A LEN end node is a T2.1 node that does not have the APPN extensions implemented. The LEN end node only has the knowledge of the link to its adjacent node and is therefore not able to set up a control session with its adjacent network node. So there is no way to exchange directory information. The adjacent network node has no knowledge of the LEN end node configuration. The LUs in the LEN end node also have to be system-defined in the network node; in this sense, they are also in the network node's domain.

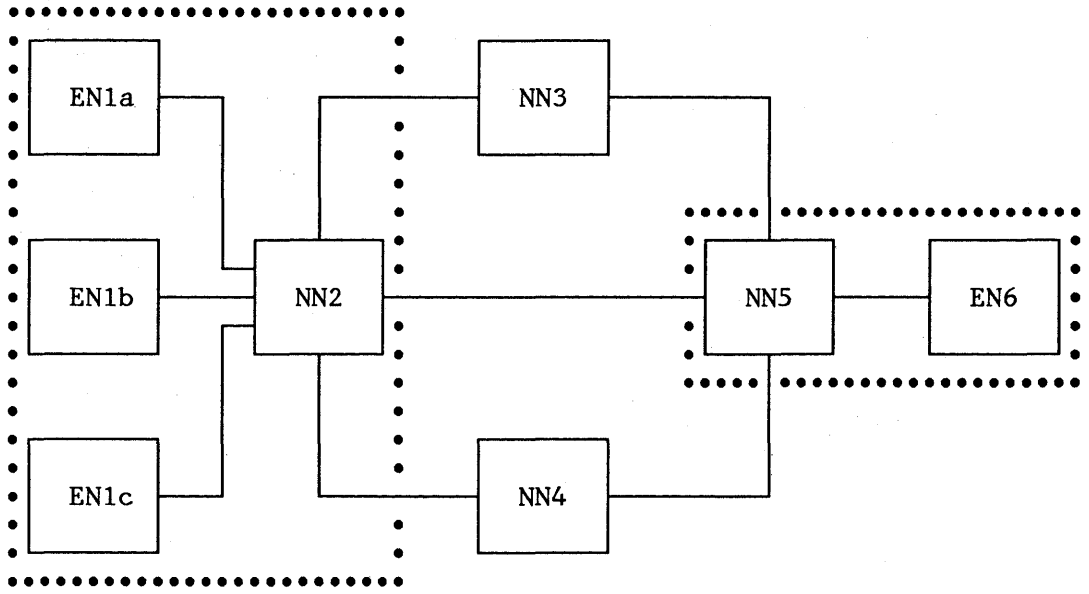


Figure 6. Network Node Serving APPN End Nodes in its Domain

1.3.2 Control Point Components

1.3.2.1 Configuration Services

This function is found in NN, APPN EN and LEN EN.

Adjacent T2.1 nodes exchange XID3 protocols as part of link activation. The XID3 information consists of node name, NETID, node type (EN or NN), capability to support control sessions, link station role (primary or secondary), maximum BTU length and receive buffer size.

XID3 exchange on an active link, called non-activation XID3, takes place to let the adjacent node know that the control point or SSCP name has been changed. This may also happen if the existing control session is disrupted. If the link is not affected by the interrupt, a non-activation XID3 is needed to re-establish the control session.

Non-activation XID3 exchange also allows an APPN end node to change its server. For example consider the following configuration:

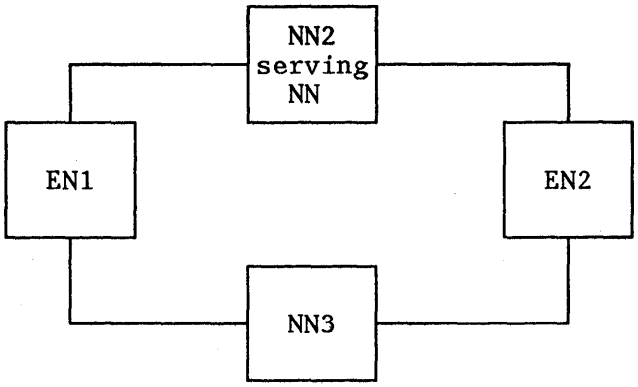


Figure 7. APPN EN Connected to Multiple NNs

EN1 has a control session with NN2. NN2 is the actual network node server for EN1. If contact with NN2 is lost, EN1 can automatically inform NN3 that it has to take over the network node server role. In such a case EN1 sends a non-activation XID3 to NN3.

1.3.2.2 Session Services (SS)

This function is found in NN, APPN EN and LEN EN

Session services are extended to initiate/stop sessions between session partners located in the network and to manage the control session. From the T2.1 node perspective, a control session is just another LU 6.2 session. To set up the session through the network, other services such as topology and routing services, address space manager and directory services are invoked. The directory services component is used to locate the target session partner.

The process of finding the destination LU is explained in "Directory Services (DS)" on page 10.

The preferred route is now calculated by the network node server's topology and routing services. The route is an ordered sequence of hops that represents a path from the origin APPN end node to the destination APPN end node and is represented by control vectors. Control vectors consist of a list of links and intermediate nodes. The route selection control vector (RSCV) is added to the BIND.

When using the sample in Figure 8 on page 11, the RSCV for a session from application A to application B could look like: EN1-NN2-LK1-NN3-LK5-NN5-EN6 or EN1-NN2-LK2-NN5-EN6 depending on link/node characteristics. The session path does not need to go through the network node server. The requesting APPN end node informs the network node server about its configuration. If there is a link between the APPN end node and another network node, the network node server could calculate the following path: EN1-LK4-NN4-LK6-NN5-EN6 (see Figure 8 on page 11).

A session is identified by a network-wide unique token, called a fully qualified procedure correlation ID (FQPCID). The FQPCID contains the network identifier and the control point name of the node that created the FQPCID.

1.3.2.3 Topology and Routing Services (TRS)

This function is found in NN.

In an APPN network multiple routes between any two nodes in a network can exist. The function of TRS is to sort out the best route to take. Route selection is based on two kinds of information:

1. Topology data base

2. Class of service table.

The topology data base contains information about network nodes and links between them with their respective characteristics. Each node contains a topology data base which is updated each time a new node or link is activated in the network or when node or link characteristics change. Updates are sent between nodes via the control session. Route selection is always performed in the network node server of the APPN end node of the originating (primary) LU. If an APPN end node sends a directory request to the network node, the network node locates the destination LU and computes a route which is represented by the route selection control vector (RSCV). The RSCV is returned to the APPN end node which attaches the RSCV to the BIND. The BIND is sent to the destination LU. In contrast with an APPN end node, a LEN end node sends a BIND directly to the network node; the network node computes the RSCV after directory search, appends the RSCV to the BIND and sends it to the next node indicated in the RSCV.

It is possible to assign a relative preference for certain characteristics of a link or node in a class-of-service table (COS). These characteristics can be encrypted links for secure transport, line speeds for low, medium or high priority transport and a threshold for load on a node to prevent overloading due to intermediate routing. At session establishment TRS uses these sources of information to calculate a weight factor for each node and link. Based on these factors the preferred route is calculated. In summary, TRS provides the following APPN functions:

- Topology data base
- Route selection
- Class of service.

1.3.2.4 Directory Services (DS)

This function is found in APPN EN, LEN EN (local significance) and NN.

Directory services maintains the directory data base, which consists of a local directory and a distributed directory. The directory contains information about network resources; these are LUs used by end users and network services. All resources are identified by NETID.NAU name. The NETID identifies the APPN network. An APPN end node manages its own local data base describing the node's local resources, which are manually defined. The network node maintains a local domain directory. The directory contains information about all resources in the domain. These are resources belonging to the APPN end nodes for which the network node acts as an serving node and the local network node resources. The APPN end node informs the serving network node about its resources when a control session is established. For LEN end nodes, all resources have to be manually defined at the serving network node. The network node also maintains the distributed directory. The distributed directory data base also contains a cache. The cache can be updated via system definitions or dynamically by caching the result of successful search operations. If a cache entry is found for a destination, a direct search to the destination LU is used to verify the validity of the cache entry. In other cases a broadcast search is used.

The advantage of caching information is that for resources with cached entries, no broadcast search takes place every time that resource is requested for session set up.

The search operation is performed as follows:

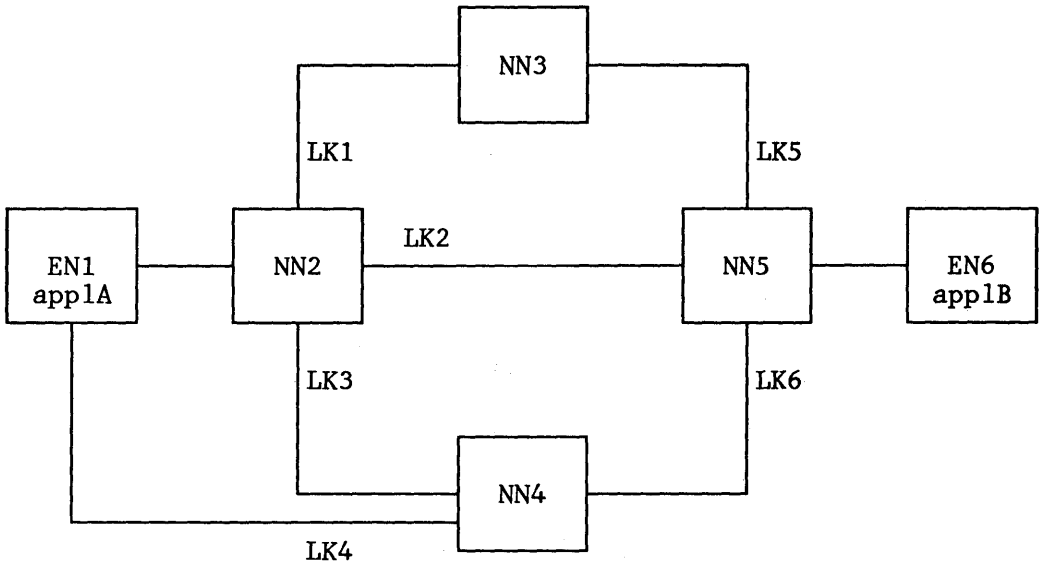


Figure 8. Sample Directory Search

- Application A located in EN1 wants a session with application B.
- The local directory of EN1 is searched; application B is unknown in EN1.
- EN1 issues a locate request and provides NN2 with information about its links to other nodes. NN2 searches its domain directory and cache; if a hit in the cache was found, NN2 issues a direct search to NN5 to find out if application B still is in EN6.
- If there is no cache entry, NN2 issues a "broadcast search" resulting in search requests from:
  - NN2 to NN3 and NN4
  - NN3 to NN5
  - NN4 to NN5
  - NN5 to NN3 or NN4 (depending on from which node the search request is received first).
- NN5 finds out that application B is in its domain, in EN6.
- The search request is propagated to EN6. If the resource is available, EN6 sends a positive reply including information about its links to other nodes.
- NN2 is informed about the location of application B by NN5.
- TRS computes, based on COS table information, the most appropriate route (RSCV) from EN1 to EN6.
- This information is cached and returned to EN1.
- EN1 adds the RSCV to the BIND and issues the BIND.

1.3.2.5 Address Space Manager(ASM)

This function is found in APPN EN, LEN EN and NN.

ASM is responsible for assigning and maintaining the pool with identifiers which correlate the LU half session with the link (DLC components). A session in APPN network hops from node to node to the destination node. The end-to-end session consists of a number of node-to-node *session stages*. The session stages are interconnected in the intermediate nodes by assigning a session identification (LFSID).

1.3.2.6 Management Services (MS)

Network management is divided into the following major categories:

- Problem management
- Performance and accounting management
- Configuration management
- Change management.

Network management processes may be distributed across different nodes with different responsibilities depending on how the network management hierarchy is organized. Though APPN provides peer-to-peer networking, the management of a peer-to-peer network needs some form of a hierarchy.

The network information about the behavior of the network elements is gathered and sent to a central place. There the data is processed and correlated to determine which action can be taken. The entry points where network management data originates send this information upwards to a central focal point (FP).

In an APPN network a focal point provides a particular category of management services to a set of entry points. An entry point can have different focal points for different categories of services. An entry point can send alerts to FP1 and use FP2 for performance and accounting data. A focal point can have a higher level FP; this is called nested focal points. Filtered information can be sent upwards. A higher hierarchy FP cannot directly exchange information with an entry point.

The sphere of control (SOC) defines how management services is organized. A focal point for a management services category has an SOC table, listing the APPN and/or subarea nodes for which it is to be focal point. The normal case is for the nodes in a focal point SOC table to be network nodes. The network node and its served end nodes are treated as one unit from a focal point's perspective. An APPN end node may however appear directly in a focal point's SOC table.

The management services applications in the APPN nodes maintain LU 6.2 sessions with each other to exchange network management data.

1.3.2.7 Intermediate Session Routing (ISR)

This function is found in NN.

A network node acts as an intermediate node in a session route. It uses the FID2 transmission header. The inbound and outbound session stages are connected by a session connector; the session connector creates a path between the inbound and outgoing link. Figure 9 on page 13 illustrates this. The connection is made based on address swapping at each intermediate node. Each session stage has a different address, represented by the local form session identifier (LFSID). The fully qualified procedure correlation identifier (FQPCID) is used to identify the session and is carried in the BIND.

Pacing during the session is performed on the session stage basis. Each session stage is paced separately. Adaptive session pacing allocates the intermediate node's session resources dynamically. The receiving node determines the pacing window size. The initial window size is determined during BIND processing.

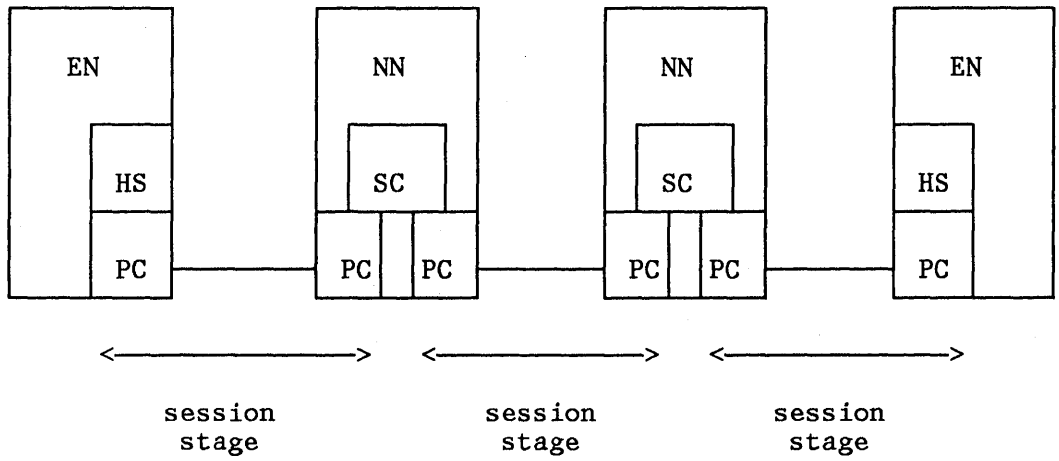


Figure 9. Session Stages: HS: Half Session; SC: Session Connector

2.0 APPN Compared with Subarea Networking

2.1 Characteristics

In the following sections APPN is compared with the subarea networking techniques as they exist today. When discussing APPN and subarea networks, the following aspects will be considered:

- Flexibility
- Large networks
- Network management
- Costs
- Performance
- Availability
- Efficiency.

2.1.1 Subarea Networks

Though subarea networks are providing peer-to-peer connections, the network is basically of a hierarchical nature. The systems services control point (SSCP) in a host system provides central control for a group of network resources. It is responsible for directory services and operator function. Also the nodes in the network fit into a hierarchy. Communication controllers, terminal controllers and terminals depend on the host node. This structure suits the communication needs of end users with host-based applications. Communication between SNA end users (terminal users and applications) however has to take place with the involvement of at least one host system.

The subarea network hierarchy is a perfect platform for network management functions which can be distributed through the network. Decentralized systems perform data collection and first line actions. A central point receives filtered information about the network's behavior and processes accounting and performance data for problem determination and planning purposes.

Another property of a subarea network is the predefined structure. The relationship between the components and links is generated in the host systems involved. A session path is system-defined, while in an APPN network the session path is determined during session initialization. In both cases the route is selected according to COS table definitions. A subarea COS table contains fixed, predefined paths while APPN dynamically selects the optimum route according to selection criteria defined in the COS table.

There is of course, flexibility to modify individual pieces of the network without the need to rebuild the definition of the entire network when changes are required. VTAM Version 3 Release 2 provides functions for dynamic VTAM table replacement, dynamic path update and dynamic reconfiguration.

However when the environment changes, management of network resources may become difficult, especially in a distributed systems environment where a large expansion is expected in the future. The development of intelligent workstations, personal computers and departmental systems has led to end-user to end-user communication in an unpredictable pattern. Personal and departmental

systems are in most cases managed by the end user. This requires a network infrastructure which allows for any-to-any communication and dynamic adaptation of network configuration changes.

In situations were the network configuration is relatively stable, subarea networks deliver high performance and efficiency. Backbone networks interconnecting terminal networks and peripheral networks (APPN networks) are a good example of a stable environment.

Also subarea networks prove to be able to handle high volumes of traffic in very large networks very efficiently. Pre-definition of network resources allows fast session set-up which can be an important factor in a large network.

2.1.2 APPN Networks

The main characteristic of an APPN network is that there is no hierarchy. All nodes are independent and communicate on a peer-to peer-basis with each other. APPN networks support the requirement of any-to-any communication with dynamic adjustment to the topology of the network. As explained in detail in the previous chapter, APPN provides these functions. All changes, for example the addition of a new node, are made available to all other nodes (and thus users) in the network without human intervention. The addresses of network resources such as applications are kept current by APPN directory services in each node, so at any time each APPN node knows exactly the state of the network. The use of APPN can establish highly dynamic SNA networks where nodes can join and leave as needed and session routes can be selected according to the situation prevailing at the time.

Though APPN offers a maximum of ease of use because of the ability to dynamically adjust the topology of the network, one could imagine a situation where a lot of terminals always have access to the same application. In such a case you would system-define parts of the network, which results in efficient session initialization.

Session set up and hardware usage are not the only parameters when measuring the efficiency of a network. Network efficiency is a trade off between hardware, software and support personnel costs. APPN networks require minimal definition effort. However in an environment with large and complex networks there are more processor resources needed for session set up (locating the session partner and calculating the route) than in a subarea network.

Today's APPN networks can interconnect via a subarea backbone network. This combines the advantage of dynamic and flexible networking with the performance and efficiency of subarea networking.

Figure 10 on page 17 summarizes the differences in the way both are defined.

Resource	SA definition	APPN definition
Host	SSCP PU	CP
Subarea	Host NCP	
Session Path	PATH-ER VR	
Session Path Selection	COS	COS
Session Characteristics	MODETAB	MODE Description
Cross Domain Resources	CDRM CDRSC ADJSSCP	CP (AS/400)
Network resources	LU name	LU name

Figure 10. Overview Definition Subarea/APPN Network

2.2 Network Management

The network management architecture is the base for both subarea network and APPN network network management implementations. NetView [4] is the implementation for subarea networks. The continuing development of network management is key for the integrated management of the network.

"Network Management" on page 36 provides information about the network management implementation on an AS/400 APPN environment. In "Network Management" on page 50 the network management aspects in a mixed environment are discussed.

2.3 Availability

Network availability is the result of availability of various network components:

- Host or node
- Communications controller
- Link.

In a subarea network paths through the network are predefined. Alternate paths can be selected but also have to be predefined. Planning of alternate paths has to be done carefully to make sure that there is no single point of failure in the defined path (if possible at all). When a path becomes unavailable, the session is interrupted and can be re-established via an alternate path.

[4] trademark of IBM

SSCP failure only harms the session initiating and terminating process. A predefined back up SSCP can take over responsibilities of the failing SSCP without disrupting the session.

If a selected route makes use of multilink TGs, failure of a link (if not the last one!) does not interrupt the session; it only can impact the response time. Another possibility of dynamic link recovery is SNA switched network backup. A dial connection that is transparent for the session is made after a link failure.

As explained earlier, in an APPN network routes are established during session start up time. APPN nodes are automatically informed about unplanned network topology changes such as node and link failure. If an intermediate route node fails, the session is cut off. The end user can reestablish the session; if the COS table definition and network topology enables this, session services will dynamically set up a new session via another route. Today the APPN extensions do not describe multilink TGs as available in subarea networks. So in case of a link failure the session can be reestablished if the network topology allows this.

Though an APPN network has no hierarchical structure, there is a special relationship between an APPN end node and network node. In principle an end node is independent of a network node. However to take advantage of the APPN features a network node provides directory and route selection services to connected end nodes. The network node acts as serving network node for attached end nodes that request those services. If a serving network node or the link between an end node and serving network node fails, APPN recovers dynamically from that situation. If the link or the serving network node fails, the end node automatically can select the next network node with which it has a link to be its server.

2.4 Ease of Use/Installation

When considering the previous discussed differences between the APPN extensions as they are designed and subarea networks as they are implemented today, it is apparent that APPN can eliminate a lot of definition effort (once the traffic patterns through the network can be estimated). Expansion of the network does not result in definition changes. The network itself learns about the changed topology. Especially when planning for availability in a subarea network, it is a complex task to predict what can go wrong and to develop scenarios for the different types of failure.

One has to keep in mind that the dynamic properties of an APPN network only show full advantage after carefully designing the network. The design is based on projected traffic volumes and traffic patterns and is basically the same as the design process for a subarea network.

2.5 Conclusion

Comparing subarea networks with APPN networks today is in fact comparing apples with oranges. The subarea network functions of today, which have been constantly enriched since the introduction of subarea networks, are compared with the APPN extensions in an early stage which are implemented in the AS/400 and the System/36.

Also the APPN extensions have properties which are not available for S/370 systems and workstations at this moment. These properties are needed in a changing networking environment where independent LU-LU sessions will become of increasing importance.

On the other hand today subarea networks offer efficient communication and fast session startup to support a mass of terminals and applications or sessions through a non-terminal backbone network.

When considering the long term it is evident that the APPN extensions combine the flexibility of dynamic adaptation of network topology changes and locating session partners without predefined knowledge of the network configuration, with the possibility to provide fast session startup where needed.

A fast backbone network with a relatively stable topology and the flexibility in the periphery to dynamically adjust to a frequent changing environment is an excellent combination.

When combining the properties of subarea networks and APPN networks, one could say that APPN networks are today most suitable as peripheral networks interconnected by a subarea network infrastructure.

3.0 T2.1 Support in VTAM/NCP

3.1 Introduction

In Chapter 1 we explained that SNA T2.1 nodes can connect to other SNA T2.1 nodes and to subarea networks via the NCP[5] function.

Attachment of T2.1 nodes to subarea networks requires VTAM V3R2 and NCP V4R3/V5R2.

3.2 VTAM/NCP SNA T2.1 Support

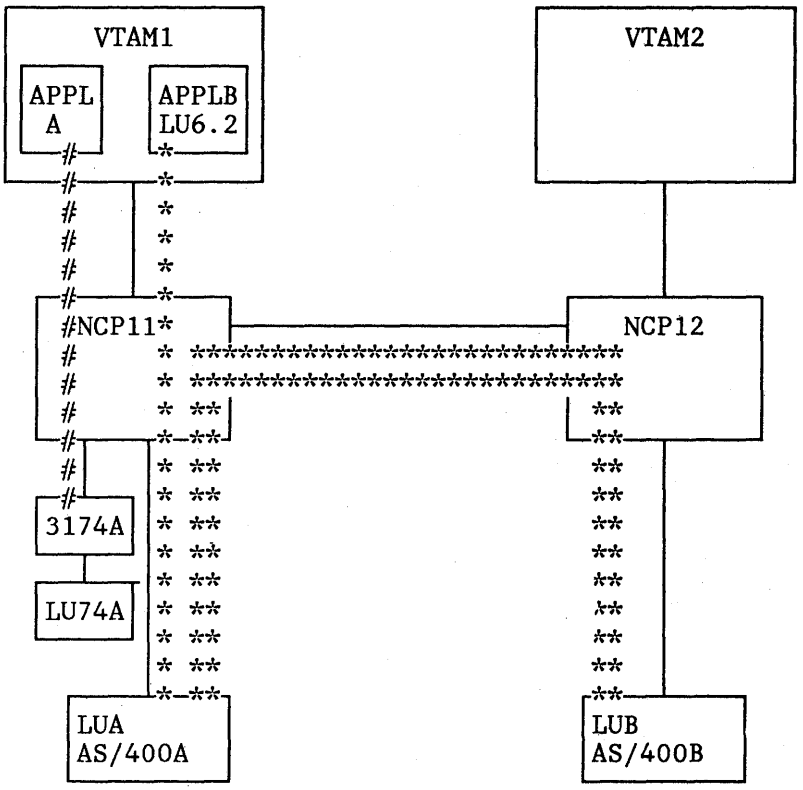
T2.1 node support in VTAM/NCP provides the following functions:

- Attachment of T2.1 node (APPN or LEN) to NCP
- Support of independent LUs
  - Capability to initiate a session as a PLU (sending BIND)
  - Support of many different session partners simultaneously (multiple sessions)
  - Support of many sessions with the same partner (parallel sessions)
  - Session partner can be an LU 6.2 application in the subarea network or another T2.1 node connected to the subarea network (peer-to-peer session)
  - Independent LUs must reside in a T2.1 node
  - Independent LUs cannot initiate sessions as SLUs
- Support of dependent LUs
  - Can only be a SLU (receive BIND)
  - Limited to a single session only
  - Can be within a T2.1 node, a type 2 node, a type 1 node or a type 4 node (NTO, NRF).

Figure 11 on page 22 illustrates this.

---

[5] trademark of IBM



####### dependent LU session
******* independent LU session

Figure 11. Example of VTAM/NCP T2.1 Node Support

The following description refers to the example in Figure 11. To any T2.1 node that attaches to the subarea network, the entire subarea network (including VTAM and NCP) appears to be a peer T2.1 node. In this context, the subarea network (which may consist of a single domain, multiple domains or multiple interconnected networks) is called a "composite T2.1 node".

From the perspective of AS/400A, LU B is located within the VTAM/NCP composite, and from AS/400B's perspective LU A is also located in the VTAM/NCP composite.

As a result of LU A's session initiation request, VTAM performs a search on behalf of the subarea network; it is capable of locating session partner LU B in AS/400B, or session partner APPLB in VTAM1. If LU B is the destination LU, the session request traverses the subarea network. VTAM uses the standard techniques for locating an LU. First it finds out if the destination LU is located in the local domain; if not, VTAM inspects the CRDRSC or ADJSSCP tables to locate the LU.

It is important to realize that VTAM/NCP acts as a T2.1 LEN end node. This means that VTAM/NCP cannot have a control session with connected APPN nodes. So there is no way to exchange directory information between the VTAM/NCP T2.1 node and the attached APPN node. A request from an APPN network to locate a destination LU in the subarea network or in another subarea network-attached APPN network stops at the APPN node adjacent to the NCP. As T2.1 LEN end nodes only support sessions between adjacent nodes, the destination LU has to be defined as being in the subarea network. The APPN or LEN node regards the subarea network as one T2.1 LEN end node; the subarea network in turn regards the attached APPN or LEN network as one T2.1 LEN end node. To accomplish this, VTAM defines an APPN or LEN node as a type 2.0 node with XID=YES, which tells the NCP that there is an T2.1 LEN end node at the other end of the link. All APPN resources must be defined to VTAM and NCP as LUs with LOCADDR=0. Figure 12 on page 25 shows the relationship.

In this figure all LUs are explicitly defined. When connecting several APPN networks with many resources via the subarea network, explicit definition of all resources will be a complex task. Using a wildcard can ease the definition process. The wildcard can be used to route all session requests for resources outside the APPN network to a node to which the network is connected. The AS/400 implementation of the wildcard is discussed in "Generic Location Naming and Generic Routing" on page 32. The naming convention aspects are discussed in "Naming Conventions" on page 47.

3.3 Overview Link Activation

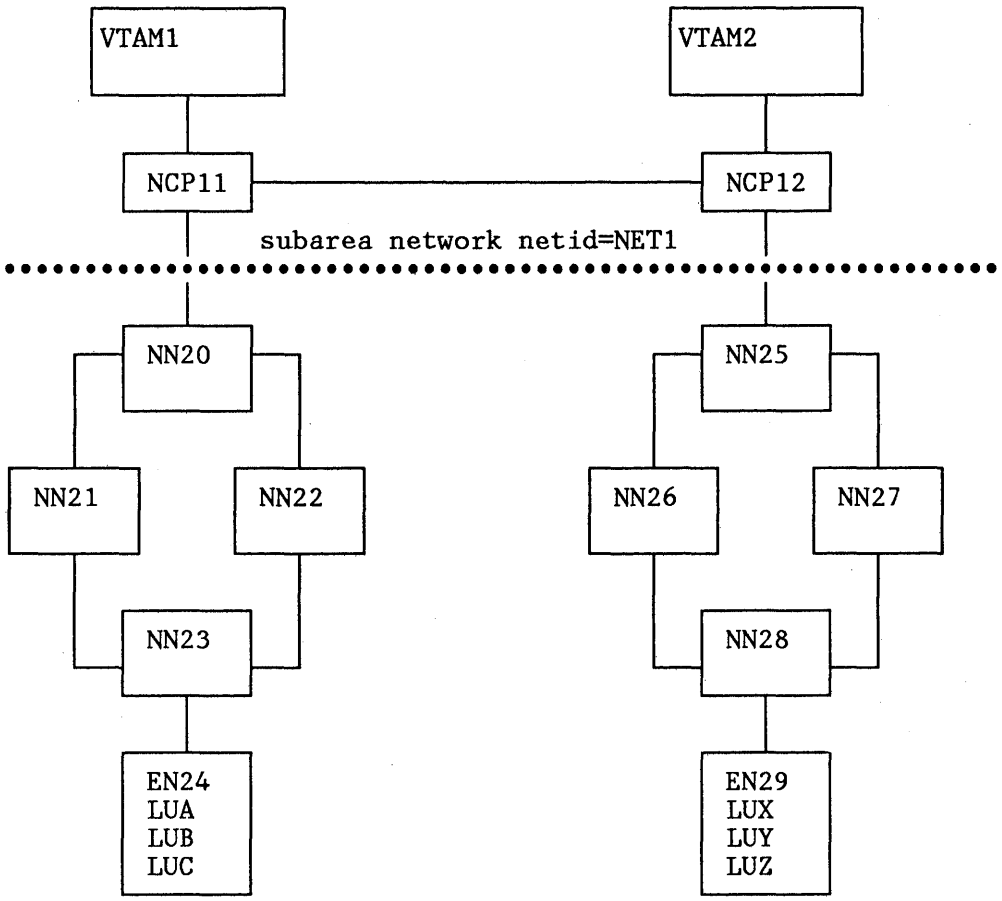
An APPN node is defined to VTAM as an PU with XID=YES. This results in an XID3 exchange during link activation. The link activation process consists of the following steps:

- VTAM activates the link.
- VTAM now starts the activation process of the node.
  - VTAM provides the NCP with the network address of the node to be contacted.
  - NCP sends a null XID command to poll the node.
  - The APPN node responds with an XID3 command specifying its node type as T2.1. Also included in the XID3 is information about the node characteristics, node name/network name, XID type (link activation or non-activation), buffer size, pacing parameters, etc. NCP knows now that it is connected to a T2.1 node.
  - NCP returns an XID3 with the characteristics of VTAM/NCP such as SSCP and NCP name, network name, buffer size, pacing parameters and XID type. The APPN node now also knows that it is connected to a T2.1 LEN end node.
  - NCP sends a mode setting SDLC command (Set Normal Response Mode or Set Asynchronous Balanced Mode)
  - The APPN node answers with UA (Unnumbered Acknowledgement).
  - NCP informs VTAM that the T2.1 node is contacted now.

3.4 APPN Subarea Network Session Initialization Flow

This section illustrates the steps needed to establish a session between LUs in two APPN networks that are interconnected through a subarea network. LU A in EN24 will try to initiate a session with LU Z in EN29. (Refer to Figure 12 on page 25 for the configuration described in this example.)

- LU A in EN24 tries to locate LU Z (LU Z is not in the local directory).
- NN23, as serving network node for EN24 inspects the local domain directory, determines that LU Z is not listed in its local domain and issues a broadcast search.
- NN20 finds LU Z listed in its directory as being located in NCP11.
- NN23 receives a positive response, calculates the route to NN20 and returns the response with the RSCV to EN24.
- EN24 issues the BIND with the RSCV appended to it.
- NN20 forwards the BIND to NCP11.
- NCP11 informs VTAM1.
- The SSCP in VTAM1 uses search techniques to locate LU Z and finds out that LU Z is defined to VTAM2 as being located under NCP12, in NN25.
- The BIND is forwarded from NCP11 via NCP12 to NN25.
- LU Z is not in the local directory of NN25; NN25 uses a broadcast search to locate LU Z.
- NN28 informs NN25 that LU Z is in its directory.
- NN25 calculates the route to NN28 and forwards the BIND with the RSCV.
- LU Z responds to the BIND, and the session is initialized.



Definitions:

NCP11:

```
NN20   PU PUTYPE=2,XID=YES
LUA    LU LOCADDR=0
LUB    LU LOCADDR=0
LUC    LU LOCADDR=0
```

NCP12:

```
NN25   PU PUTYPE=2,XID=YES
LUX    LU LOCADDR=0
LUY    LU LOCADDR=0
LUZ    LU LOCADDR=0
```

NN20 DIRECTORY

Location name	Netid
LUX in NCP11	NET1
LUY in NCP11	NET1
LUZ in NCP11	NET1

NN25 DIRECTORY

Location name	Netid
LUA in NCP12	NET1
LUB in NCP12	NET1
LUC in NCP12	NET1

Figure 12. NCP and APPN/LEN Sample and Node Definitions for T2.1 Nodes

3.5 SSCP Takeover

In a configuration where an NCP is attached to a primary and a backup host (for example in an CMC network situation) NCP informs the control point of the adjacent APPN node if a takeover has taken place. NCP sends a non-activation XID3 with the new SSCP name to the control point.

NCP also informs its VTAM about existing sessions and their partners.

3.6 Configuration Considerations

An APPN network can only have one link to the subarea network. Two APPN networks each connected to the subarea network cannot have an additional link (between network nodes) interconnecting the APPN networks together directly. In this topology APPN end nodes in two APPN networks could be connected but APPN does not perform routing between APPN end nodes.

In "Availability Aspects" on page 48 availability is discussed in more detail.

3.7 NETID Considerations

An LU in an APPN network is identified by the combination of LU name and NETID. This indentifies an LU uniquely over network boundaries. From an APPN point of view there is no restriction in setting up a session between LUs in different APPN networks. However the way NETIDs are treated is implementation dependent.

A session is established by issuing a BIND to negotiate the session characteristics. The NETID is exchanged in the BIND. The implementation of the current VTAM/NCP T2.1 node support requires that the originating LU (PLU) must have the same NETID as the connecting VTAM. The NETID of the destination LU (SLU) must also be the correct NETID corresponding to the VTAM which connects to the SLU. So if a NCP is involved in session set up between APPN nodes or between an APPN node and a host application, the NETIDs should be the same. This means for practical reasons that the NETIDs of all the nodes in an APPN network attached to a subarea network should be the same.

In the case where APPN networks are connected to subarea networks with different NETIDs, the NETID of the APPN network should be identical to the portion of the network to which it is connected. On the other hand, for reasons of network management it is recommended to avoid a large subarea APPN network conglomerate by defining separate logical networks with different NETIDs.

Interconnection of APPN networks with different NETIDs via a subarea network, requires the usage of SNA Networking Interconnect. Figure 13 on page 27 shows a sample confguration.

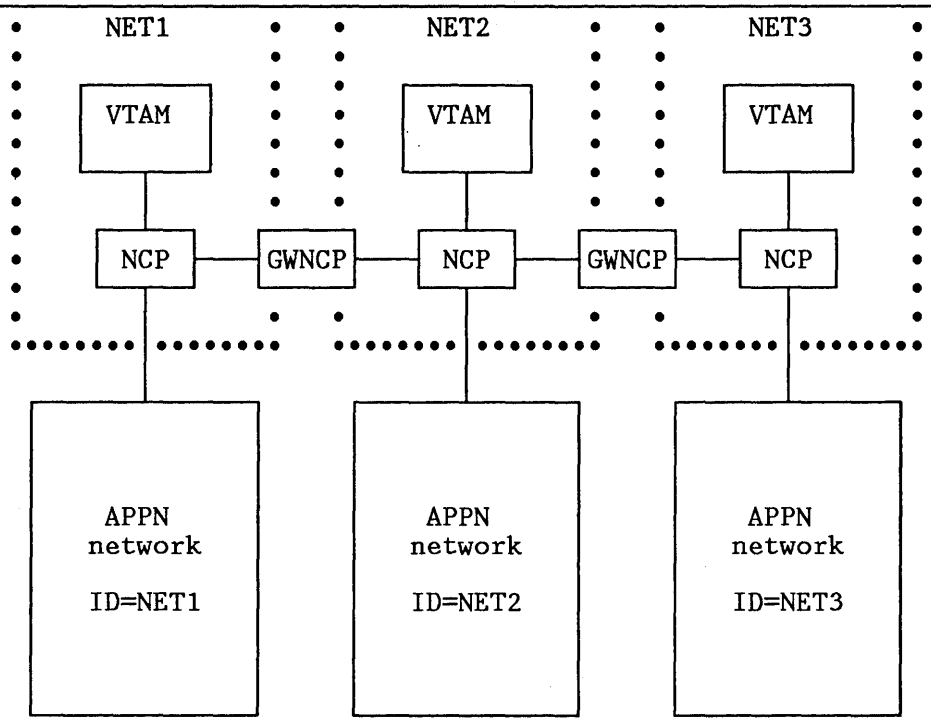


Figure 13. Sample Multi Network APPN/Subarea Network Environment

3.8 LU Name Considerations

The current VTAM/NCP node type 2.1 implementation does not allow for originating and destination LU names to be the same in two APPN networks with different NETIDs if the session path traverses a subarea network.

3.9 Conclusion

The discussion in this chapter about the APPN subarea network connection as it is today shows that the subarea network and the APPN network are "loosely" connected. This kind of connection will in most cases offer an appropriate means to attach APPN nodes to an existing subarea network.

3.9.1 Future Considerations

3.9.1.1 Integration of Subarea and APPN Networks

In the future an APPN network could be a more integrated part of a mixed subarea/APPN network, therefore one could consider the following functions for a "seamless" connection:

- The ability of having control sessions through a subarea network to systems in other APPN networks and to systems in the subarea network. This makes it possible to support topology data bases and directories which contain information about the mixed environment.
- Single definition of all network resources and the ability to locate them across the mixed network allowing the elimination of the definition of network resources at the boundary between APPN and subarea networks.

- Calculation of session routes through the network, based on topology data base information and responses of search requests. This will allow dynamic route selection without the need to predefine paths through the subarea network.

4.0 AS/400 APPN Implementation

4.1 Introduction

In the previous chapters we discussed the APPN extensions from a general point of view. However the APPN extensions are already implemented in the AS/400. The purpose of this chapter is to give an overview of the way APPN is implemented in the AS/400 without going into great detail.

The following topics will be discussed:

- AS/400 networking terminology
- AS/400 APPN support
- Configuration of an APPN node
- Attachment to subarea networks
- Network management.

4.2 Terminology

The AS/400 networking terminology differs from the terminology used in the subarea network and APPN publications. In order to understand the way an AS/400 node is defined and to avoid confusion, an explanation of some AS/400 terms follows.

4.2.1.1 End Node

An end node is used as a synonym for an APPN end node

4.2.1.2 LEN Node

A LEN node is used as a synonym for a LEN end node

4.2.1.3 Location

A location is a logical unit. A local location is an LU defined at the local node as a local resource. The remote location is the local definition of the LU at the remote node.

4.2.1.4 Location List

The location list contains information about the node's configuration. It consists of the local location list and the remote location list and constitutes the directory. The local location list contains the node's local locations (LUs). The remote location list contains the following entries:

1. Locations in the end node for which the network node provides network node server support.
2. Cached locations as a result of a successful directory search operation.

3. Locations in adjacent LEN nodes.
4. Locations in adjacent APPN end nodes without a control-point-to-control-point session.
5. Locations in host systems using VTAM/NCP with T2.1 support.
6. Locations in nodes that are not directly attached and use attached host systems with T2.1 support for intermediate session routing
7. Single session connections between a local location and a remote location, for example 5520 and DisplayWriter sessions. Single sessions can be configured in such a way that the session is established after the connection with the remote system is made.
8. Sessions for which a password is required. As this refers to APPC sessions, one should distinguish between password protection on session and conversation level. Session level security, conversation level security and resource access control is discussed in "Security in a Mixed APPN Subarea Network Environment" on page 53.

The remote location list entries mentioned under 1 are called registered, those mentioned under 2 cached and those under 3 to 8 are called home entries.

4.3 AS/400 APPN Support

4.3.1 AS/400 Node Support

The AS/400 nodes are distinguished from other nodes in the network by a unique name. This name consists of two parts, a network identifier and a control-point name. An AS/400 node can be one of the following:

4.3.1.1 LEN Node

A LEN node is an AS/400 system configured for not using APPN. Such a node may participate in an APPN network by using the services of the adjacent network node server and can only be at the end of the network. However the user of the non-APPN node must system-define all remote locations with which communications can take place as if they existed at the network node server.

4.3.1.2 APPN End Node

As explained in previous chapters, an APPN end node may use the services of an attached network node server. The AS/400 system allows you to define up to five potential servers. The remote locations with which the end node wishes to communicate do not have to be defined in the end node because of the directory services provided by the network node server. In addition, the server does not have to configure the locations residing at the end node because the AS/400 system end nodes are able to send register requests informing the network node of all the location names that are defined in the end node (if a control-point-to-control-point session is activated between the end node and the network node).

The AS/400 system end node can be attached to multiple network nodes, but will have one control-point-to-control-point session active at a time which can be a session with the network node server.

4.3.1.3 APPN Network Node

A network node provides, in addition to the end node functions, the following:

- Intermediate session routing
- Network server functions, performing directory searches and route selection for attached APPN end nodes and LEN nodes.

- Can be defined as the management services focal point.

4.3.2 APPN Functions Provided by AS/400

4.3.2.1 Control Point Services

Control point services as provided by AS/400 APPN systems are described in "APPN Extensions" on page 6 and can be summarized as follows:

- Exchange of identification information (XID3) and start-up of control sessions between the control points of adjacent network nodes. Also the start-up of control sessions between a network node and its adjacent end nodes.
- Exchange of changed network topology information between network node
- Initiation of directory searches from a network node
- Creation and maintenance of the network topology data base.

4.3.2.2 Communication Protocols

The AS/400 system supports the following protocols:

- SDLC leased or switched
- X.25 PVCs and SVCs
- Token-Ring.

4.3.2.3 Parallel Transmission Groups

Between two directly attached systems more than one connection is possible. Such a connection consists of transmission groups (TG), each identified by a unique TG number.

The AS/400 system does not support multilink TGs. Each link is considered to be a unique TG.

4.3.2.4 Automatic Disconnect of Switched Lines

If the TG consists of a switched line, AS/400 offers the possibility of automatically disconnecting the switched connection when there are no sessions currently active. If a control-point-to-control-point session is established over a transmission group, then the number of active sessions using the transmission group will never drop to zero, meaning that automatic disconnect will not take effect.

4.3.2.5 Directory and Network Topology Data Base

Directory and topology information are saved across initial program loads on the AS/400 system. This means that the AS/400 system does not have to rebuild the entire network configuration and directory data bases after initial program loading. When an APPN end node is changed to be a network node, the directory is deleted and recreated with current information for the network node.

The directory data base is built from configuration information contained in the location lists as well as from information obtained dynamically over control-point sessions. The directory services simplify the configuration of the network because there is no need to define every location (LU) in the network with which you want to communicate. The only remote locations that must be configured as directory entries are:

- Locations in adjacent LEN nodes.
- Locations in adjacent APPN end nodes without control-point sessions to any network node (for example in the case of a switched connection).

- Locations in nodes that are not directly attached and use attached host systems with T2.1 support for intermediate session routing
- Single session connections between a local location and a remote location.

4.3.2.6 Generic Location Naming and Generic Routing

The definition of locations of adjacent attached LEN or APPN end nodes without a control-point session can be an extensive task, especially in the case of the attachment of a subarea network. All locations (LUs) in the subarea network and all locations for which the subarea network acts as an intermediate route have to be defined. To minimize this definition effort, it is possible to use generic location names. Generic location naming allows you to define a location name ending with an * (asterisk). This implies that any location name starting with the same characters preceding the * match this entry. For example, if locations RAL1, RAL2 and RAL3 exist in an APPN end node or LEN node with the control-point name of RALEIGH, you only need to configure RAL* as being located in RALEIGH.

Generic naming requires a consistent naming convention for all networks involved. When using name*, there should not be other location names in the network which match the character string defined with name*. A positive directory search response found with a generic name appears the same to the search origin, as compared to a location name that was spelled out completely.

Generic routing or wild card allows you to specify *ANY as a location name. This indicates that when a session is requested for a location that does not match an explicit entry or a generic location name anywhere in the network, that location will be assumed to reside in the node associated with the *ANY entry. In a mixed APPN subarea network environment that node is the NCP attached to the APPN node having the wildcard definition. To ensure that the network operates properly, *ANY should only be defined once in the network.

Every time the node with the *ANY entry receives a search request, it responds positively. However this response is not used when a positive response on a generic or explicit match is found.

When a System/36 is a network node in the network, the usage of *ANY is not allowed. The S/36 does not support the NETID name thus is not able to distinguish between the same locations names in different networks with different NETIDs.

4.3.2.7 Route Selection

Frequently there are multiple paths available over which a session between two locations can be routed. AS/400 APPN route selection support uses information about link and node characteristics, which is defined as a part of the configuration, to determine the best route through the network. The link and node characteristics expressed in "weight factors" are compared with the required route characteristics as defined in the class-of-service description. The combination of nodes and links with the lowest weighting factor is selected out of the combination of nodes and links available to constitute a path through the network.

When route selection calculations results in various routes with the same weight factor, the route with the fewest nodes and links is selected. If also the number of nodes and links are equal, a route is selected at random.

4.3.2.8 Transmission Group and Node Characteristics

The transmission group characteristics that can be configured for each port are:

- Specification of the data rate for the line.
- Security on the line (this specification has no relationship with the system user ID and password security). The following categories are available:
  - Nonsecure, meaning there is no security on the line.

- Packet switched network, so the line is secure in the sense that the data does not always use the same path through the network.
- Underground cable.
- Secured conduit.
- Guarded conduit, meaning the line is protected against tapping.
- Encrypted, meaning that line encryption devices are used. This does not mean that the AS/400 is performing encryption.

- Cost per connect time, a relative value. For example a non-switched line has the lowest relative cost compared with a switched line.
- Cost per byte, also a relative value expressing the cost per byte of sending and receiving data on the line.
- Propagation delay options are:
  - Minimum delay
  - Local area network delay (less than 48 milliseconds)
  - Telephone network delay (48 milliseconds to 49.152 milliseconds)
  - Packet switched network delay (49.152 milliseconds to 245.76 milliseconds)
  - Satellite delay (greater than 245.76 milliseconds)
  - Maximum delay.
- Three user-defined fields.

The node characteristics define the ability of a particular network node to perform intermediate routing. There are two node characteristics, route addition resistance (RAR) and congestion, that are used in route selection.

Route addition resistance is expressed in a value indicating the desirability of each network node to perform intermediate session routing functions as compared with other network nodes in the network.

Congestion is defined as the maximum number of intermediate sessions allowed for a network node. A node is considered congested if 90% of the configured maximum number of intermediate sessions allowed is reached. A node is considered no longer congested when the number of intermediate sessions drops below 80% of the maximum number. Depending on the class of service selected, node congestion may or may not allow additional sessions to be routed through the network node. However it indicates to the rest of the network that alternate routes should be used if possible.

4.3.2.9 Class of Service Description

Each session request is associated with a specific mode that has an attached class of service description (COS). The COS description defines the range of node and transmission group characteristics that are acceptable when determining the route to satisfy the session initiation request. Apart from the node and link characteristics, the transmission priority is also configured in the COS description. The priorities are: high, medium and low.

On each session end point (the local location and remote location) must exist a mode with the same name. On a network node being the network node server for a T2.1 node, a mode description must also exist with the same name as the other session partner's mode.

4.3.2.10 Control of Dataflow

To manage the flow of data over the network, the AS/400 APPN support uses adaptive session pacing, intermediate session routing and transmission priority.

Adaptive Session Pacing
Adaptive session pacing controls the amount of data that is sent or received during normal session operation. It allows the receiving system to control the rate at which it receives data into its buffers. So the data flow is controlled by a receiving system in a route. The system-defined pacing value, indicating the number of message units that can be transferred before receiving an acknowledgement, is used as the minimum pacing value to start with. Depending on the availability of a receiving systems resources, the value can be changed, thus providing an efficient way to use buffers.

Intermediate Session Routing
As discussed before, how many intermediate sessions an intermediate node can handle can be system-defined. Based on the maximum number of intermediate sessions defined for a node, an AS/400 system automatically determines when congestion in the node occurs. In such a case, route selection will try to avoid using the congested node as intermediate node in a route. As shown in Figure 14 intermediate session routing takes place at the path control level. The session is not established above the AS/400 machine interface level, thus minimizing the system overhead.

Transmission Priority
Every AS/400 system node in a session path is aware of the transmission priority assigned to a session. If multiple sessions are crossing an intermediate network node, higher priority traffic (interactive) is transmitted earlier than lower priority traffic.

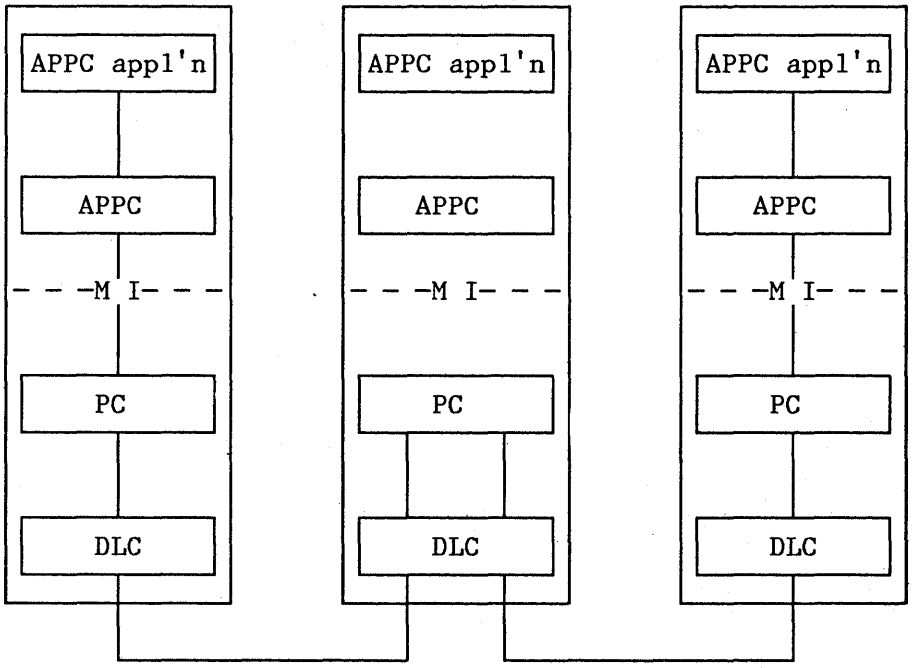


Figure 14. AS/400 APPN Intermediate Session Routing

4.4 Configuring an AS/400 APPN Node

An AS/400 APPN network is configured by describing:

- The characteristics of a node (controller)
- The locations (LUs) in that node
- Remote locations which are in non-APPN nodes with which sessions may be established

- The characteristics of the links to adjacent nodes
- The adjacent nodes (remote controllers).

It is not our intention to discuss in detail all the configuration parameters of an AS/400 APPN network but to give you an idea what information is needed to set up an AS/400 APPN network. It is also important to understand the relationship between some definitions.

A local node is defined by:

- Network ID
- Control point name
- Default local location name, the LU name of the control-point
- APPN node type, end node or network node
- Maximum number of intermediate sessions per node, used to determine when node congestion occurs
- Route addition resistance, which specifies the relative desirability to perform intermediate session routing
- For end nodes the network node service provider list
- Location lists to describe local locations and some remote locations (see "Location List" on page 29).

The characteristics of the links to the adjacent nodes are used for route selection and are discussed in "Transmission Group and Node Characteristics" on page 32.

The adjacent nodes are defined in the controller description as follows:

- Control point name
- APPN capable or not
- Support of control-point-to-control-point session
- In case of a VTAM host connection the SSCP ID
- The network ID of the remote system.

The logical connections between local and remote locations (a session between an originating LU and destination LU) is described in the device description. The device description is created automatically at session initiation by AS/400 APPN support. Only in case of dependent LU sessions to VTAM host applications and sessions to remote locations in non-APPN nodes, the device descriptions has to be predefined.

4.5 Attachment to Subarea Networks

The way an APPN network attaches to a subarea network is shown in "T2.1 Support in VTAM/NCP" on page 21. When connecting an APPN network node with a subarea network the following has to be considered:

- A LU in an AS/400 APPN network is accessible through only one link
- Dependent and independent LUs are supported on the same link
- The NETID of the node of the originating LU and the NETID of VTAM must be the same.

4.6 Network Management

Network management or communications and systems management can be defined as the process of planning, organizing and controlling a communication-oriented information system. Support of the network management process is based on system and network management as defined in the APPN extensions and SNA Management Services (SNA/MS).

Network management relies on a structured flow of network management information through the network and on a hierarchy of systems in which implicitly is defined what action has to be undertaken and where.

AS/400 has implemented the tools to manage an APPN AS/400 data communication network. These tools also interface with network management tools that are implemented in subarea networks (NetView).

4.6.1 Network Management Structure

As discussed in chapter "Management Services (MS)" on page 12 end points monitor their own environment and exchange information with their focal point. Focal points consolidate the information gathered from the end points for which they are responsible and decide which actions to start. AS/400 focal points can manage their own domain and can exchange network management information with a focal point in a subarea network. Figure 15 shows the physical layout of an AS/400 APPN network connected to a subarea network. Figure 16 on page 37 shows the network management structure of the same network. Note that the NN1 focal point in Figure 16 on page 37 is called a nested focal point.

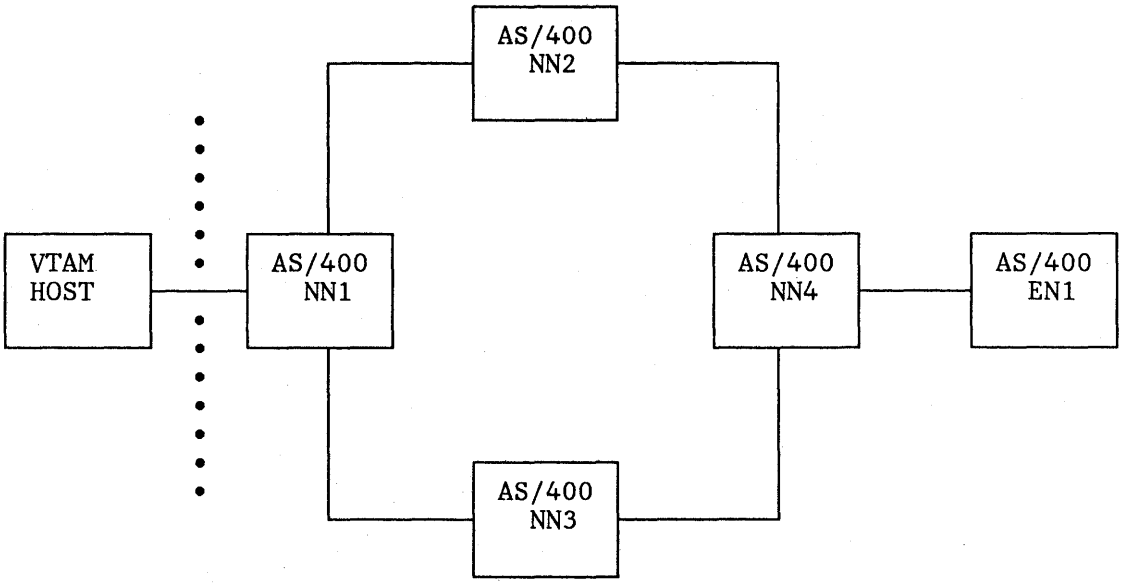


Figure 15. Physical Layout AS/400 APPN and Subarea Network

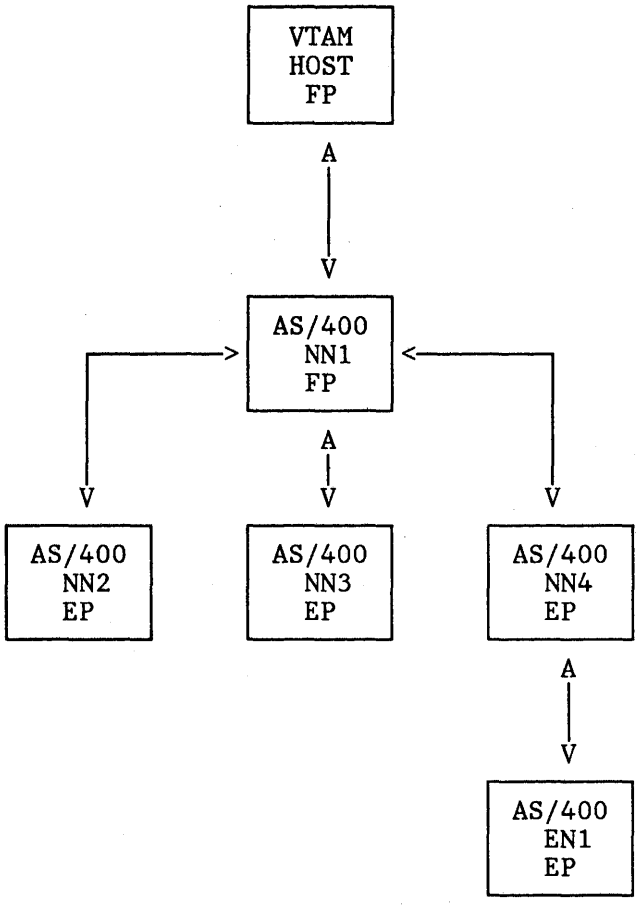


Figure 16. Network Management Structure AS/400 APPN and Subarea Network

4.6.2 AS/400 Network Management Services

AS/400 network management provides the following functions:

- Problem management
- Change management
- Configuration management
- Operator management.

4.6.2.1 Problem Management

When a problem in an AS/400 APPN network occurs, an alert is sent to the operator to give information about the nature of the problem. An AS/400 alert is an architectured SNA management services message. The information it contains summarizes the nature of the problem and can also contain guidance for corrective action. An AS/400 system can send alerts to other AS/400 systems, S/36, S/38 and S/370 host systems. The S/36 and S/38 are only able to forward alerts and can not be a focal point.

The AS/400 alert support makes it possible to start or stop the automatic creation of alerts, to specify which systems send alerts to a focal point and to control which error conditions are able to create alerts. OS/400 alert support provides the following functions:

- Create alerts

  Alerts are created by an AS/400 system to inform the operator about problems. The operator also can report alerts by using operator-generated alerts.

- Sending and receiving of alerts

  Alerts that have been created by the AS/400 system can be sent to a focal point, which may be another AS/400 or an S/370 host with NetView. Alerts that have been created by another system in the network are received by the AS/400 system as a focal point and forwarded to the focal point, if the receiver has a higher level focal point.

- Logging alerts

  Alerts will be logged on the AS/400 in an alert data base. The alerts can originate from the local system and other systems in the network.

- Display alerts

  Alerts logged in the alert data base can be displayed using AS/400 commands.

- Hold alerts

  If an AS/400 system cannot send an alert, the alert is held until it can be sent.

4.6.2.2 AS/400 Focal Point Service

AS/400 provides focal points service when it is part of an APPN network. The focal point is in an APPN network the destination of alerts. AS/400 focal point support allows you to configure several focal points in the network. The sphere of control of a focal point is a collection of network nodes control-points within an APPN network from which the focal point receives alerts. End nodes send their alerts to the network node server. In Figure 16 on page 37 the sphere of control of the focal point in NN1 consists of NN2, NN3 and NN4. An AS/400 system can be configured as:

- A system that is not a focal point but can send and/or forward alerts to another system that is a focal point
- A focal point in a network not attached to a S/370 host system
- A focal point for forwarding alerts to a S/370 host system with NetView from an APPN network.

An AS/400 system can be defined as a primary or default focal point. A primary focal point has explicitly defined all systems which belong to its sphere of control. The default focal point receives all alerts from systems that do not already have a primary focal point. The AS/400 APPN node's role as primary or default focal point is system-defined.

AS/400 systems commands allow you to display the status of the systems in the sphere of control.

4.6.2.3 Change Management

In an environment where NetView Distribution Manager (NetView DM) is the main vehicle for planning, scheduling and controlling the exchange of data between the host system and remote system, OS/400 Distributed Systems Node Executive extends the NetView DM functions into the AS/400 network. NetView DM functions supported by OS/400 DSNX are:

- File and save file support.
  - Retrieve data base files members (data sets) from an AS/400 system
  - Send sequential files that were prepared at the host system to an AS/400 system
  - Send data base file members created on one AS/400 system to another AS/400 system
  - Delete data base file member from an AS/400 system.

- Retrieval of all other objects from an AS/400 system, sent to an AS/400 system or deleted from an AS/400 system.
- Batch job (CLIST) support makes it possible to run batch job streams that were created or stored at the host system on the AS/400. Also batch jobs stored on an AS/400 can be retrieved by NetView DM and and sent to another AS/400 for execution.
- Send messages to the AS/400 system operator.
- Personal computer support.

The AS/400 cannot start a transfer; it can only respond to requests made by the NetView DM host system. DSNX is using SNA/DS as the transport network to transport objects between the NetView DM system and the destination node.

Object Distribution Facility (ODF) provides the same services in an AS/400-only network and also uses SNA/DS as the transport mechanism. Though DSNX and ODF can share the SNA/DS network, they cannot integrate their functions.

4.6.2.4 Configuration Management

Configuration management is the control of information necessary to identify network and system resources. Configuration management assures that this information is updated whenever changes are made and always reflect the current situation. Configuration management in an APPN environment means on one hand that the configuration is kept up-to-date dynamically and on the other hand having access to the configuration information. Configuration changes are registered by the control-point in the directory (addition, deletion or change of resources) and in the topology data base (addition, deletion or changes of links and nodes).

AS/400 provides tools to display information about the APPN network. The following information is available:

- Topology information
  - Characteristics of the nodes and links in the topology data base as system-defined.
  - Status of the links (TG number, active/not active).
  - Status of the node (control-point name, node type, congestion and route addition resistance).
- Directory information providing information about the locations (LUs) that are known by the node.
- Session information about the session end points and the sessions active on a intermediate node.

Configuration management not only provides information about the configuration of the networks and the nodes in the network; it also provides tools to support problem determination and problem diagnosis and to schedule changes.

4.6.2.5 Operator Management

In an AS/400 network it is possible to operate the nodes in the network from one point using the Distributed Host Command Facility (DHCF). Also in a mixed APPN subarea network environment it is possible to operate the AS/400 network from the S/370 host using the Host Command Facility on the S/370 host in conjunction with DHCF on the AS/400 systems. Not only does it offer these advantages of reducing cost of operating an APPN network with distributed systems, it also is extremely useful in problem management. If the distribution of the operator functions matches the focal point/end point hierarchy, it is possible for a focal point operator to connect to the system which generated the alert.

For more detailed information about the AS/400 implementation of communications and systems management in an APPN environment we suggest you read the appropriate documentation listed in the bibliography.

5.0 Interconnection of APPN Networks and Subarea Networks

5.1 Introduction

The previous chapters were mainly dedicated to a functional discussion about APPN; its components, the relationship with subarea networks and the way APPN is implemented in the AS/400. The various parts which together constitute the base for a communication and information system.

In the next chapters we will focus on how one can take advantage of the combination of APPN and subarea networks and how to use the network infrastructure in an environment with an office application requiring any-to-any connections and offering various office functions.

In this chapter we will first elaborate on a simple configuration with a subarea network and two APPN networks. Afterward we will discuss a complex configuration with two layers of subarea networks (back bone and terminal network) connected via SNI and several APPN networks.

5.2 Interconnection Scenarios

The reasons for interconnecting subarea networks and APPN type of networks can be various. In one scenario large customers with subarea networks installed start to distribute processing in their organizations. Desk top automation is gaining ground. This urges the need for bringing the tools to the users. Departmental systems and personal systems are the answer to the challenge of managing personal computing. As discussed before, APPN networks offer the dynamics to support these new type of peripheral networks requiring minimal support and flexible adaptation to the dynamics of the environment.

As the AS/400 is a system that supports a distributed processing environment, one may expect the introduction of AS/400 systems, first stand-alone then rapidly expanding to multiple systems which need to communicate with each other. Also communication is needed with existing applications and data bases in host systems. In this situation, APPN networks will arise and these APPN networks also require attachment to the existing subarea network infrastructure, herewith combining the advantages of subarea networks such as high performance, backbone facilities and extensive network management capabilities with APPN dynamics needed in the periphery of the network.

In another scenario there are a lot of situations where the AS/400 serves as a mainframe and in the case of multiple systems will be connected to an APPN network. These organizations in most cases do not have subarea networks installed nor do they have a subarea network history. However the need to connect to a subarea network can arise for example in the situation where a supplier connects its APPN network to its customer's subarea network. Another example of interconnection is the case of a merger between companies.

In both scenarios the connection techniques are the same but can require different implementations.

So when discussing the sample configurations illustrating how to connect APPN networks with subarea networks, the following issues will get attention:

- Definition of the configuration and naming conventions

- Availability aspects
- Network Management.

5.2.1 Configuration Considerations

5.2.1.1 Division of APPN Networks

Before discussing the interconnection scenarios, it is important to have a closer look at the way APPN networks can be structured. For several reasons it is worthwhile to divide an APPN network into logical coherent units. Separate clusters could be considered for the following reasons:

- ***Performance***

  The change rate, also called dynamics, of an APPN network determines the amount of network control information that is transmitted through the network. Also the number of session initiations and terminations contribute to the amount of control information flowing through the network. This control information consists of topology data base updates, directory updates and search requests. The nodes in the network also are involved in running the network by maintaining the topology data base and directory, calculating routes and performing intermediate session routing.

  It is evident that unbridled growth of a network can cause an unbalance between network control flow and data traffic; also nodes can get congested by performing network control tasks. The mentioned factors determine if and how an APPN network should be divided into separate parts.

- ***Management of an APPN Network***

  In most cases APPN networks, as being implemented in an end user environment, are maintained by a system administrator responsible for her/his department or organizational unit. In this sense system administration is not considered to be a technical job. Though APPN networks are "self learning" and do not need extensive definitions, there is a limit to the size of a network that can be contained by a system administrator. That limit is determined by the number of nodes, dynamics and geographical distribution of the network.

- ***Controlled Access***

  When APPN networks of different companies, for example a manufacturer's network and a supplier and customer network, are connected, the networks should remain independent of each other. Controlled access from one network to another can be achieved by connecting the networks via a backbone network.

  Also within a company it can be a requirement to have independent APPN networks for various business units, for example different product divisions or functions.

When designing APPN networks you have not only to be aware of of the considerations mentioned above but also of the fact that a limited data flow should cross the APPN network boundary. A rule of thumb is that approximately 80% of the total traffic volume should remain within the network. Though there are still a lot of host applications in use today, the 80/20 rule of thumb should only be taken into account for independent LU-LU sessions to other APPN networks. Today applications will be developed for use as close to the user as possible, resulting in a decrease of host applications and an emphasis on departmental and personal systems.

To facilitate the adaptation of the changing environment, consideration of the design options as discussed in this chapter should be part of the basic design of peripheral networks, though the size of these networks today makes it less obvious to do so.

5.2.1.2 Interconnection of APPN Networks

Interconnection of APPN networks requires a gateway function to exchange information between the APPN networks, which have to remain independent of each other for the reasons discussed.

Today subarea networks offer these interconnection functions:

- High speed paths
- Backup routes
- Ability to gather accounting information about dependent and independent LU-LU sessions, thus providing information about the volumes transferred between the APPN networks
- Network independence if required (when using the SNA Interconnect feature)
- Proven ability to handle large amount of traffic efficiently.

5.2.1.3 Dedicated Network Nodes Within APPN Networks

In the case of rapidly growing and very large APPN networks it is worthwhile to implement dedicated network nodes. This concentrates networking functions such as topology data base updates, route selection and directory search providing another way to control the amount of network control traffic. The end nodes are connected to two network nodes from which only one acts as server. Figure 17 is an example of such a configuration. The arrows point to the network nodes with which a link is active without a control session.

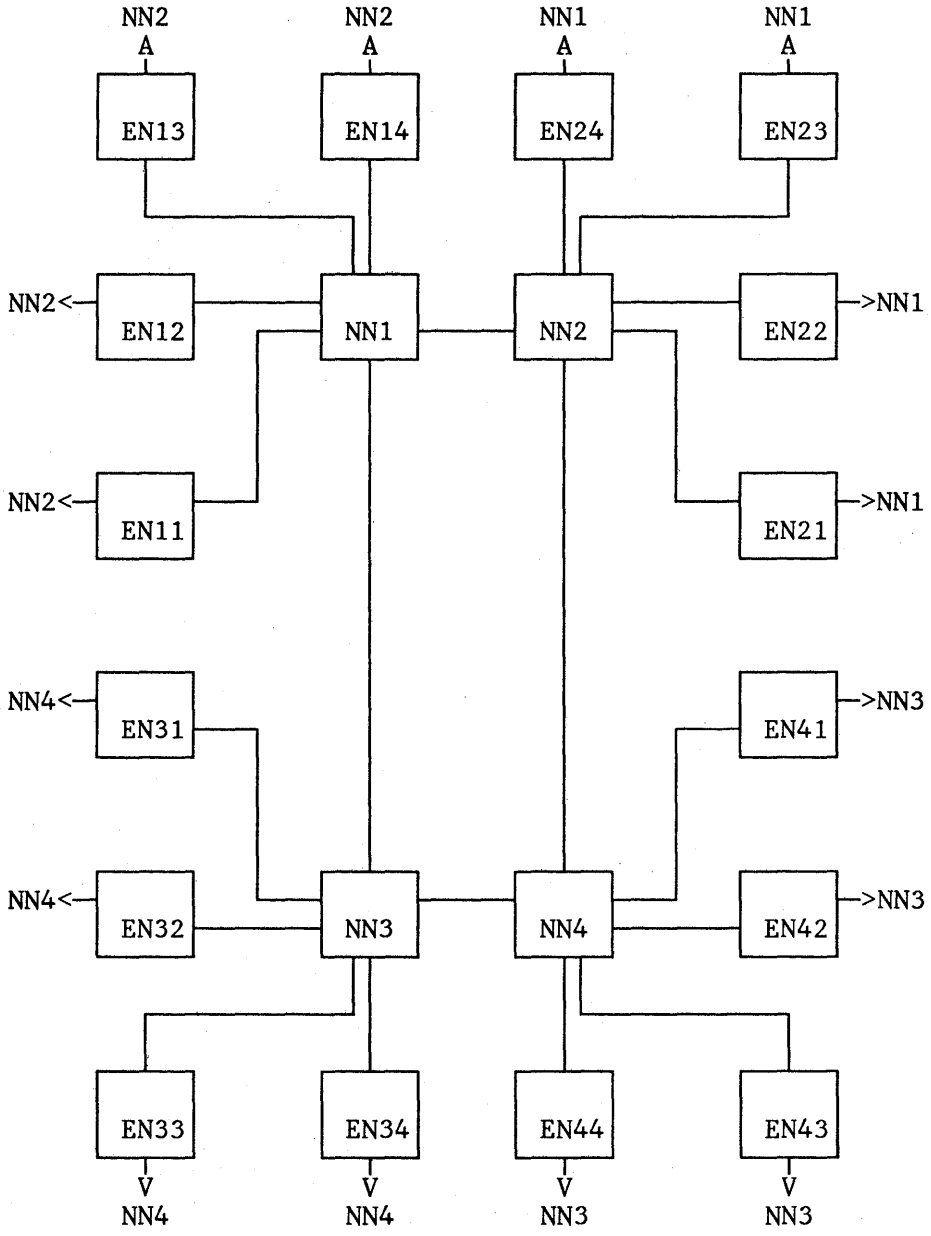


Figure 17. Sample Configuration with Dedicated Network Nodes

5.3 Sample Configuration with a Connection to a Single Subarea Network

5.3.1 Sample Configuration

Figure 19 on page 46 shows a configuration where two APPN networks are connected to a subarea network. This configuration provides access to host applications for dependent LUs, access to APPC applications located in both the host system as in the AS/400 APPN nodes in the other APPN network for independent LUs. In this configuration the subarea network provides the backbone function for both APPN networks.

As mentioned before, you should be aware of the fact that the current T2.1 implementation of VTAM/NCP does not allow you to interconnect the AS/400 network connected to NCP1 with the one connected to NCP2 in in order to get an alternate path to the subarea network.

A session partner located in EN24 only can have a session with its partner in the subarea network via NCP2, a session from EN14 to a session partner in the subarea network only can use the session path via NCP1.

A session from EN14 to EN24 can use a link between the APPN networks directly. (Figure 19 on page 46).

In this sample configuration, the host acts as a SNA/DS node with CICS and DISOSS and also provides other CICS transaction programs and TSO service.

The 3270DE applications in NN10 and NN20 provide 3270 emulation for terminals in the APPN networks which will have sessions with host applications.

Display Station Passthrough (DSPT) is used to give AS/400 terminals access to applications in any node in the AS/400 networks with DSPT installed. DSPT is an APPC application and uses APPN functions to set up sessions between the terminal node and the node where the application resides.

Also in some nodes AS/400 Office is present to show the way SNA/DS sessions are set up. Finally APPL1 in EN14 makes use of DDM to access files in the network.

5.3.1.1 Dependent/Independent LU-LU sessions

Figure 19 on page 46 also shows the difference between independent and dependent LU-LU sessions. In this configuration the 3270DE sessions from NN20 to the host are dependent.

Examples of independent LU-LU sessions are SNA/DS sessions between NN10 and CICS/DISOSS, SNA/DS sessions between the APPN nodes, the DDM session between EN14 and NN24 and the session between a terminal on EN24 with APPL1 on node EN14 using DSPT.

A terminal on EN24 in session with a host application uses both an independent and dependent session. Figure 18 on page 46 illustrates this.

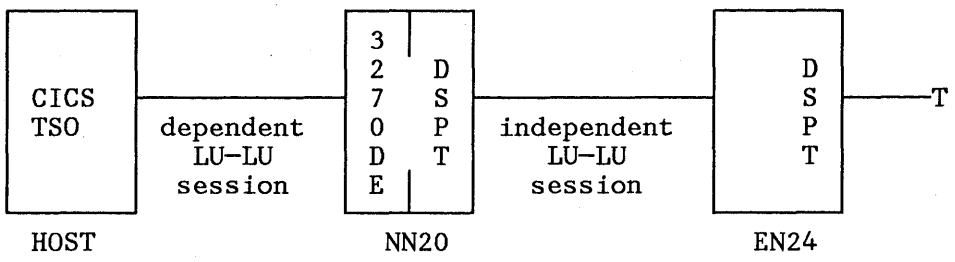


Figure 18. Sample Dependent/Independent LU-LU Session

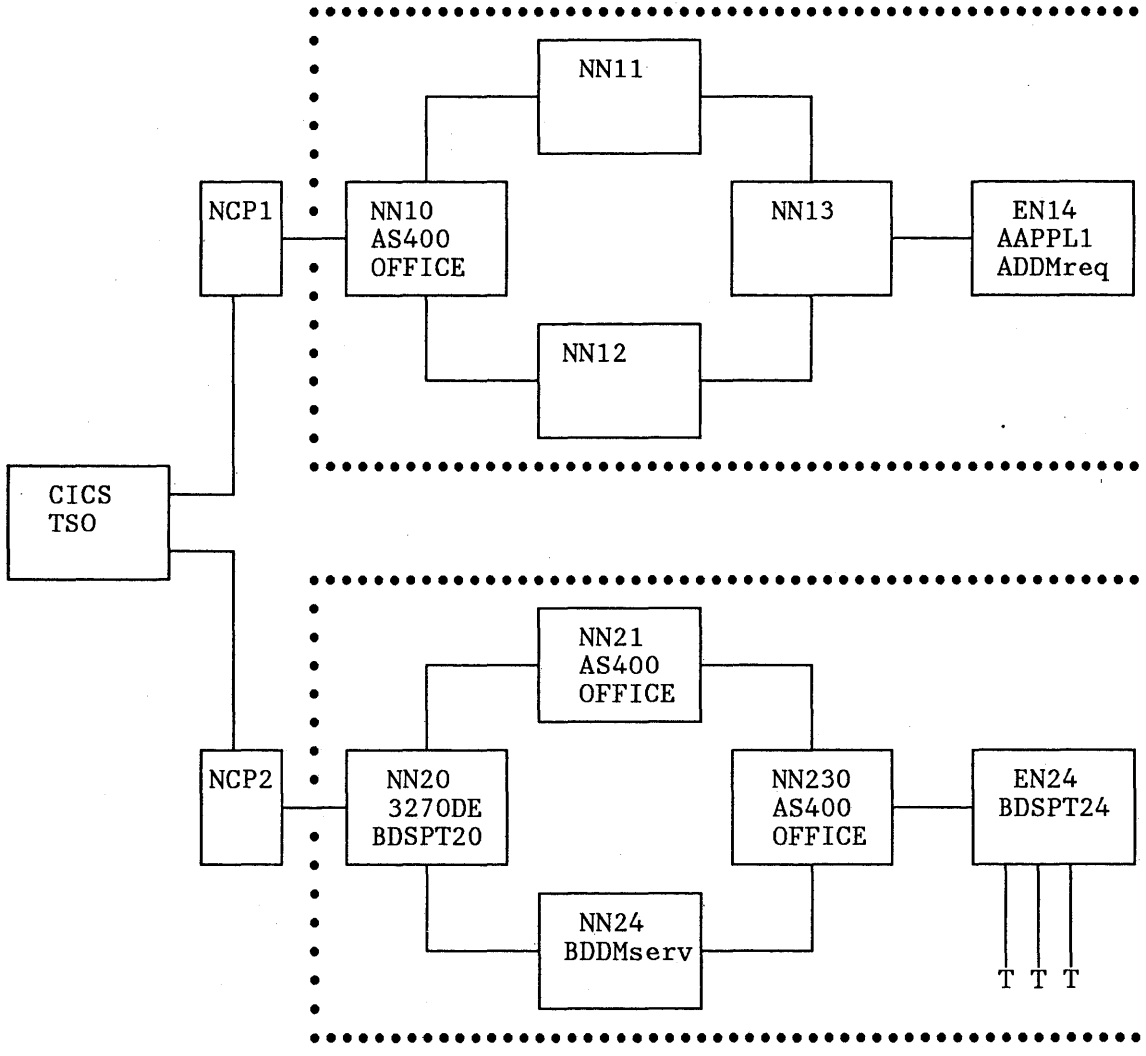


Figure 19. Sample Configuration

5.3.2 Definition of the Resources

Figure 12 on page 25 shows how to define the resources in a mixed APPN subarea network. The following chart summarizes the definition of the various network resources as shown in Figure 19. Note that the option to use generic names and generic routing is used. The local definitions are not shown. The definition *ANY represents generic routing (wildcard). A* and B* are generic location names.

System/Node	Resources	Remote system
HOST1	CICS TSO	
NCP1	dependent LUs 3270DE independent LUs OFFICE AAPL1 ADDMreq	NN10 NN10 NN10 NN10
NCP2	dependent LUs 3270DE independent LUs BDSPT20 BDSPT24 BDDMserv	NN20 NN20 NN20 NN20
NN10	CICS TSO BDSPT BDDMserv -> B* BDSPT24 -> *ANY	HOST1 HOST1 HOST1 HOST1 HOST1
NN20	CICS TSO AOOFICE ADDMreq -> A* AAPPL1 -> *ANY	HOST1 HOST1 HOST1 HOST1 HOST1

Figure 20. Network Definition APPN Subarea Network

5.3.3 Naming Conventions

5.3.3.1 Network Identification

In the current implementation of AS/400 APPN, the various nodes in the network may have different network IDs. The default ID is APPN. However for reasons mentioned in "Division of APPN Networks" on page 42 it is recommended to use a consistent network ID naming convention scheme.

Today it is required that the subarea network and the connected APPN networks have to be the same name.

The following NETID convention could be used:

Byte	Usage
1–2	Country code ISO standard
3–6	Enterprise code
7–8	Suffix

Figure 21. Suggested NETID Naming Convention

The NETID for a company in the Netherlands could look like NLCUST00

5.3.3.2 LU Names

The process of defining the LUs in the AS/400 systems connected to the subarea network can be simplified considerably. The usage of *ANY offers the most simplicity; however you should keep in mind that it is not always possible to use the *ANY definitions. If an S/36 is included in the network, the usage of generic routing is not allowed. Also the node with the *ANY definition reacts on all search requests in the network with a positive response. If another node also responded positively (having the searched LU), the response from the node with the *ANY definition is discarded. Depending on the network load, it could cause some extra load.

When you want to take full advantage of generic names, you could use an LU name convention which can distinguish the various networks. In the configuration of Figure 19 on page 46 an LU name convention is used to address all LUs in the other APPN networks with one definition. There is no need for updating the definitions if LUs are added or changed. The same applies also for applications in the subarea network. However in most cases there are already naming conventions in use in the subarea network environment.

5.3.3.3 Mode and COS Name

As explained before, session set up to a host in a subarea network or to another APPN system via an intermediate subarea network is a staged process. Session set up to a host system requires that the BIND is forwarded by the NCP. Session set up via an intermediate subarea network requires that the BIND has to be forwarded by the NCP and the AS/400 APPN network node attached to the subarea network. The session characteristics as defined in the BIND are used for all session stages. The logmode table of the subarea network is used to get access to the subarea network class-of-service table to determine the VR. The class-of-service table name does not need to be the same.

5.3.4 Availability Aspects

When discussing the availability aspects of the connection from APPN networks with a subarea network, all elements needed to facilitate the session ultimately determine the session availability. However it is beyond the scope of this document to discuss the end-to-end session availability. In this chapter we will focus on the connection between the APPN network and the subarea network.

The current implementation of VTAM/NCP T2.1 support allows only one link between the NCP and AS/400 (illustrated in Figure 22 on page 49).

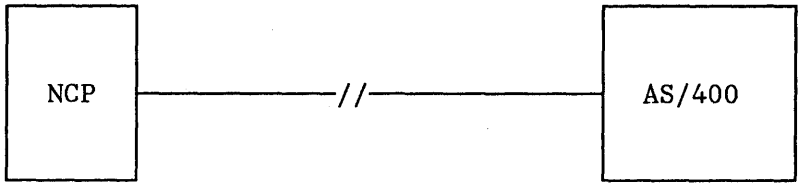


Figure 22. AS/400 NCP Connection

In most cases the communication line turns out to be the most vulnerable link. There are several options to overcome the restriction that only one line is allowed in order to provide backup possibilities.

- SNA switched network backup (SNBU) providing an automatic switched backup connection in case of a line failure.
- If geographically possible, a Token-Ring connection offers a reliable connection
- Usage of X.25 network, providing backup facilities within the X.25 network.
- X.21 connection in those countries where an X.21 service is offered.
- Installation of a backup line to another NCP (illustrated in Figure 23). In this case the APPN network LUs have to be defined in both NCPs. In one NCP the LUs remain inactive. After a line failure, the backup line to the other NCP and the inactive LUs must be activated while the corresponding LUs in the other NCP have to be made inactive. This process can be automated by using NetView CLISTs.

  This suggested procedure is not formally tested.

Depending on the availability requirement of the link between an APPN network and a subarea network a trade off must be made between costs and this requirement. Also a combination of backup options could be considered.

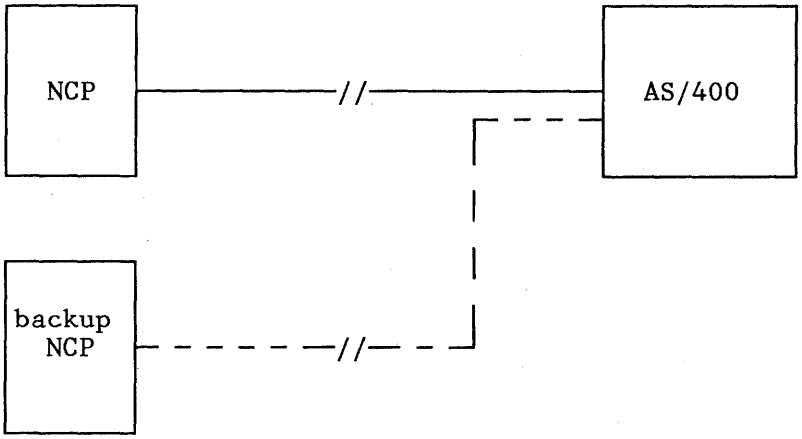


Figure 23. AS/400 NCP Back-up Connection

5.3.5 Network Management

5.3.5.1 Network Accounting and Statistics

NPM provides the possibility to collect session traffic information for both dependent and independent LU-LU sessions. This means that accounting and statistical information can be gathered from traffic to host applications and from traffic that traverses the subarea network, thus offering a central point to collect all information from subarea networks and attached APPN network.

The AS/400 also has the capability to collect network statistics. Traffic volume information can be gathered per link and performance information per communication controller is logged. This information is logged in an AS/400 data base file and is not available for further analysis on an S/370 focal point. It is possible to start the AS/400 system and network monitor function from an S/370 host (for example a focal point) with HCF, DHCF and DSPT on every AS/400 APPN node.

The response time monitor is not supported by the AS/400.

5.3.5.2 Problem Management

In "AS/400 APPN Implementation" on page 29 we discussed which alert facilities are available on the AS/400 and the way the AS/400 can cooperate with NetView to send exchange data to the designated focal point(s). When applying the network management problem management structure to the sample configuration in Figure 19 on page 46 the structure could look as follows:

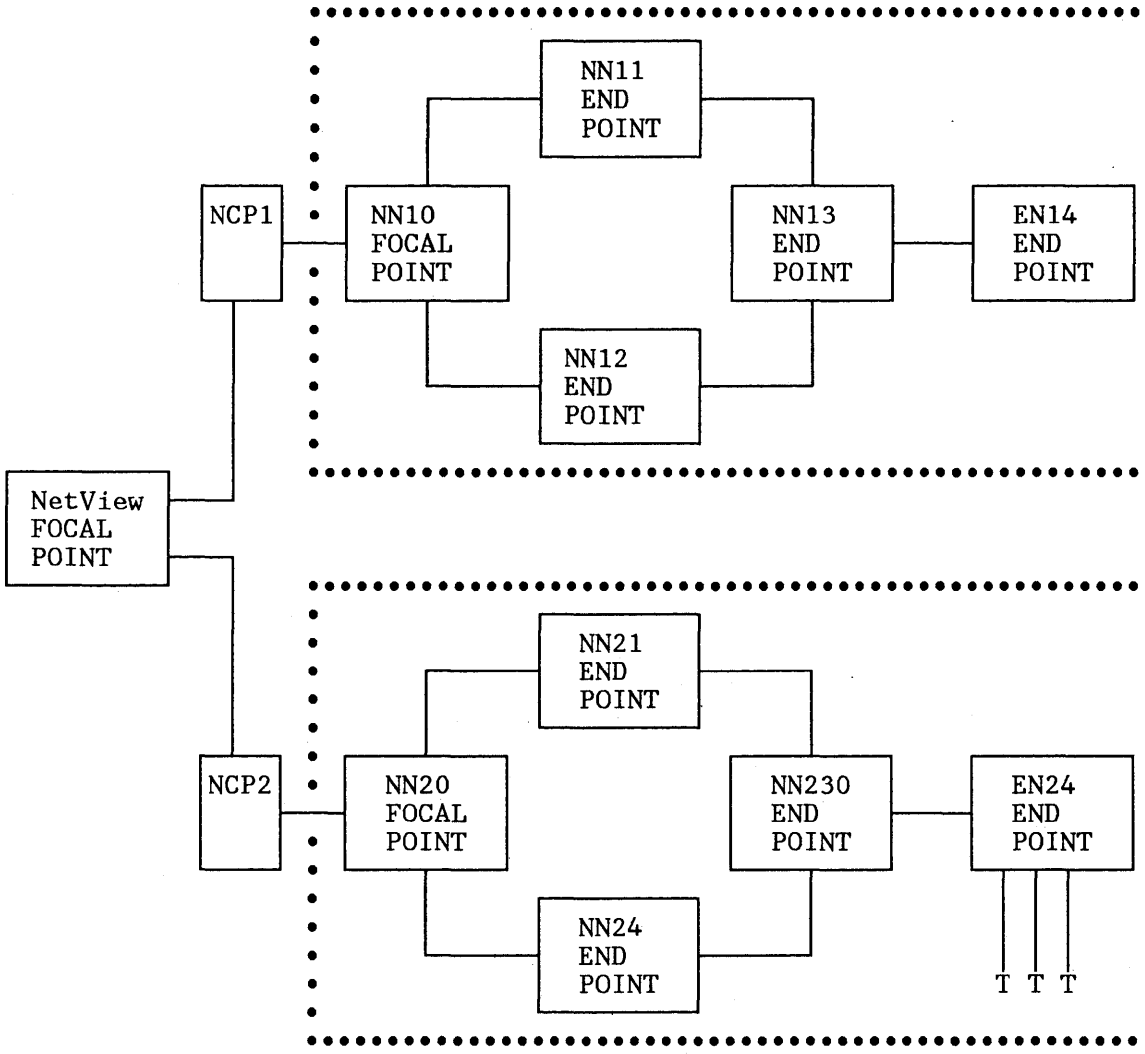


Figure 24. Focal Point/End Point Configuration

In this sample NN10 and NN20 serve as focal point for their respective networks. Local problem management can be handled on the APPN network level but also all problem management data can be sent to the central focal point in the S/370 host. With HCF, DHCF and DSPT direct session to an AS/400 system can be started up to investigate in more detail the cause of the problem, herewith assuming that AS/400 knowledge is available at the central focal point level. Having the AS/400 knowledge on a central point is very effective in terms of usage of scarce skills.

In the case that the subarea network and the APPN networks belong to different organizations or companies, a looser scheme can be implemented. Each focal point is independently serving its own network while only exchanging problem information on an exception level.

5.3.5.3 *Change Management*

As shown before, the network definitions of a subarea network with attached APPN networks require some synchronization. DSNX and NetView DM are the tools to synchronize network definition updates. Synchronization is needed for the definitions facilitating mutual sessions. These are found in NN10, NN20, NCP1, NCP2 and the host. As explained earlier, logmode and the COS table also need to be in sync, though once established the change rate will be rather low. Also in a stabilized network the LU definitions will be rather stable. Addition of new applications require system/network definition

updates; with DSNX and NetView DM these updates can be scheduled to become effective at a predefined time.

5.3.5.4 Configuration Management

In addition to the configuration management functions in the AS/400 as described in "AS/400 APPN Implementation" on page 29 the NetView session monitor can display parts of the configuration of the subarea network. The AS/400 configuration management functions can be activated not only on the AS/400 but also remotely from the NetView host by using HCF, DHCF and DSPT.

5.3.5.5 Operator Management

As mentioned before, HCF, DHCF and DSPT are the tools to operate the AS/400 systems remotely from an S/370 host, provided that the AS/400 operator expertise is available at the host site. The AS/400 also can be initial program loaded remotely by dialing a modem which starts the initial program load procedure.

5.3.5.6 Future Considerations

In the previous paragraphs we discussed the network management tools to support a loosely connected APPN subarea networking environment. Support for a more integrated environment means:

- The ability to manage all resources in a mixed network consistently.
- Functions to support the dynamic properties of an integrated mixed network.

5.3.6 Security

5.3.6.1 Introduction

In general four levels of security can be distinguished:

- Link level security obtained by using special equipment to encrypt/decrypt the data that is transmitted over a link. This equipment can be either modems with encrypt/decrypt facilities or special boxes providing encrypt/decrypt functions.
- Session level security determines if the logical units (locations) may BIND to get in session with each other. This is a way to verify if a system may have access to another system via an LU 6.2 session. Session security uses a session password defined on both systems. During BIND processing the two systems exchange random data, enciphered using the password as input to the Data Encryption Standard (DES) algorithm, to check if they may start a session. In this way the password is not transmitted over the link.
- Conversation level security is used to verify the identity of the end-user partner in an LU-LU session. When a transaction program on the target systems is started, (EVOKE processing) the target system determines if the end-user is acceptable to start the conversation. There are three types of security information that may be sent in the EVOKE request from the source program to the target program. In terms used by the LU 6.2 architecture, conversation level security can be specified as:

  1. None: omit security information on this request.
  2. Same: the user identification from the the request that initiated the source transaction program is verified by the source transaction program and the target transaction program considers the user identification as already verified. The source program may send the already verified indicator (AVI) with the user identification.

3. Program: the source transaction program supplies the target program the user identification information and password. Conversation level security can only be used if session level security is in effect.

- Resource control verifying that the end-user is entitled to access a transaction program, a data base or other resources.

Figure 25 gives an overview of the various levels of security.

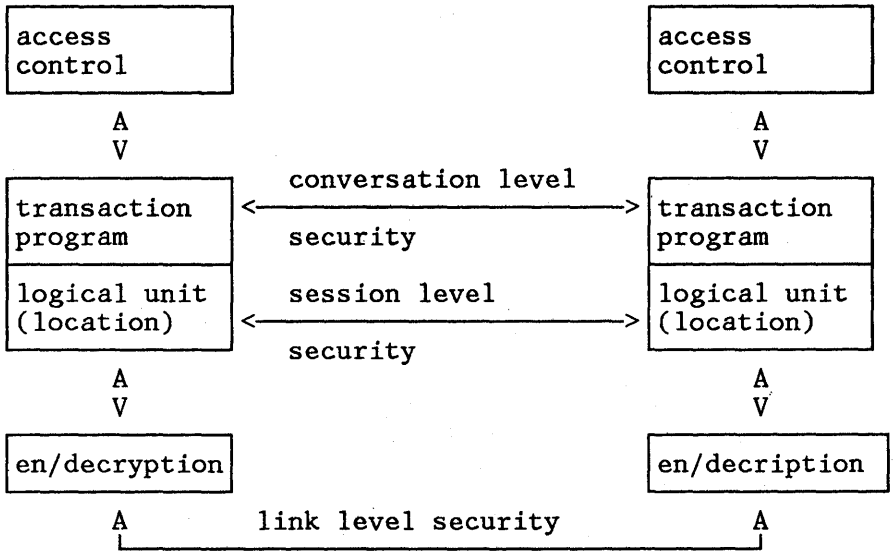


Figure 25. Overview Security Levels

5.3.6.2 *Security in a Mixed APPN Subarea Network Environment*

Link Level Security Link level security is implemented in hardware and independent of the networking environment. A proper definition of the class-of- service tables in the APPN network and the subarea network is needed to establish a secure route though a mixed APPN subarea network.

Session Level Security Both the AS/400 system and CICS (Release 1.7) provide session level security. The AS/400 system requires the appropriate setting of the AS/400 security level. However session level security is not supported in a mixed network environment.

Conversation Level Security Also session level security is provided by the AS/400 system and CICS (Release 1.7), so CICS transaction programs using the LU 6.2 protocol can exchange security information with AS/400 programs.

Resource Control In the S/370 environment RACF is used to verify if an enduser is authorized to access resources such as a transaction program or data bases. In the AS/400 systems resource control is defined in user profiles and authorization lists. Access to a remote data base is transparent for the enduser. Access to the program is checked against user profiles and authorization lists (RACF in the S/370 world). If during processing of the program access to a remote data base is needed, conversation level security ensures that the source program may access the remote data base on behalf of the enduser.

5.4 Sample Configuration with SNI Gateways

5.4.1 Configuration Considerations

This sample configuration shows the connection of APPN networks to various subarea networks which mutually are connected by a backbone subarea network with SNI gateways. In principle the SNI gateway does not basically change the picture as shown in Figure 19 on page 46. The SNI gateway is transparent for both dependent and independent LU-LU sessions.

Using SNA gateways offers the opportunity to connect APPN networks which need to be distinguished by different NETIDs. Figure 26 shows the sample configuration.

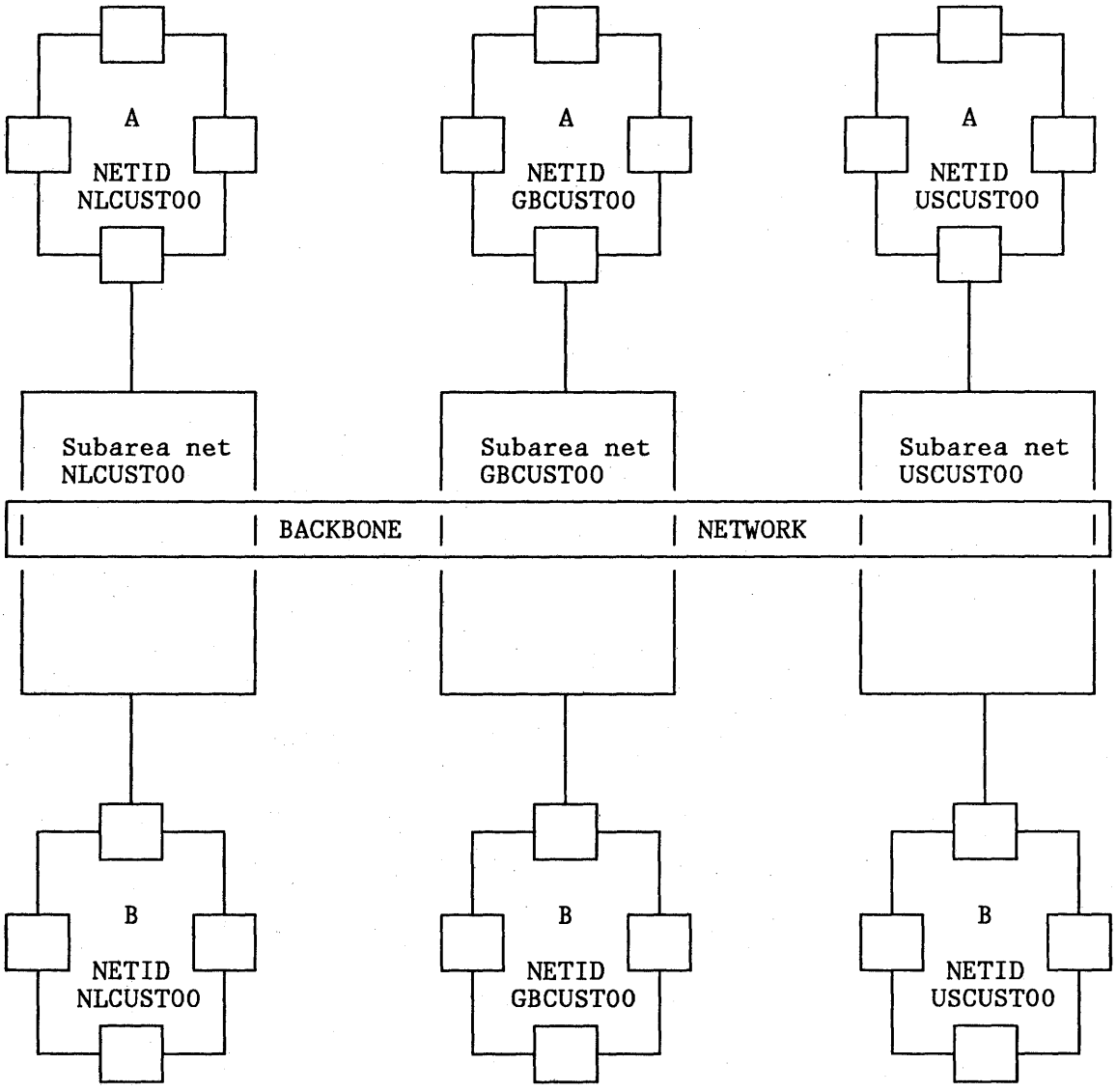


Figure 26. Sample Configuration with SNI

5.4.2 Naming Conventions

5.4.2.1 Network Identification

Figure 26 shows the usage of different NETIDs. The APPN networks with different NETIDs communicate with each other via the SNI gateways and the backbone network.

5.4.2.2 LU Names

When using generic routing, the "gateway" APPN AS/400 nodes propagate all session initiation requests for destination LUs not known in that node to the subarea network. As discussed before the usage of generic routing (*ANY) is not always possible or the best solution.

Generic names can in such a case minimize the definition effort in the APPN AS/400 gateway nodes. The success of minimizing the definition effort depends on the way the LU name structure is built. The LU name convention must make it possible to use generic names for other network IDs and other networks with the same network ID, using the ISO country code and "sub" network code. The generic names in the AS/400 gateway of the APPN network NLCUST00 and network code A could be defined as follows:

NLB*
GB*
US*

This naming convention scheme is effective only in a one-company network environment.

Using generic names in the AS/400 gateway does not prevent you from defining the complete LU names in the NCPs.

5.4.3 Network Management

The network management considerations for the sample network as illustrated in Figure 26 on page 54 are the same as those discussed in "Network Management" on page 50. The combination of one subarea network with the connected APPN networks can be managed independently from the other subarea networks. The backbone network offers the option to centralize parts of the network management function in a backbone focal point, thus distributing network management responsibilities to the appropriate level in the network.

6.0 Applications in a Mixed APPN Subarea Network

6.1 Introduction

In the previous chapter we discussed the various APPN configuration considerations and the ways an APPN network can be attached to a subarea network. Thus focusing on how to design a network infrastructure able to accommodate its users' (applications and end users) needs now and in future. In this chapter we will discuss how the network can be used to provide services to applications and endusers. This will be done by taking two sample applications:

- An office network based on SNA/DS. The relationship between APPN and SNA/DS will be discussed to clarify the way APPN route selection and SNA/DS route selection relate.
- A sample explaining how DDM establishes sessions through the network

6.2 SNA/DS

SNA/DS is an architecture for interchanging data through a subarea or APPN network in a store-and-forward fashion. This means that a user sending information need not be aware of the availability of the system to which he wishes to send that information. A SNA/DS network consists of SNA/DS nodes which exchange information with each other by way of LU 6.2 conversations. If the target node or the link to that node is not available, the information is stored and sent to the next node if the link or node becomes available. Also if the information arrives at the target node and the addressee is not logged on to that node, SNA/DS stores the information and delivers it whenever possible. SNA/DS uses its own routing tables to navigate through the network. However the route to the next SNA/DS node is selected by APPN. In the AS/400 environment SNA/DS is used for:

- Document distribution between AS/400 office nodes
- Exchange of files between AS/400 nodes by Object Distribution Facility (ODF)
- Network management data exchange by DSNX.

In the S/370 environment SNA/DS is used for:

- Document distribution between DISOSS systems.

In a mixed environment DISOSS systems also exchange information with AS/400 nodes using SNA/DS (and vice versa).

The sample SNA/DS network which will be discussed in this chapter is based on an office system network built on top of a mixed network consisting of APPN and subarea nodes.

It is not the objective of this document to discuss SNA/DS in detail; however some insight in the addressing and routing structure is needed when elaborating design options and the sample configuration.

6.2.1 SNA/DS Naming, Addressing and Routing

6.2.1.1 SNA/DS Naming and Addressing

Each node in a SNA/DS network, called a distribution service unit (DSU), has a network unique name called a distribution service unit name (DSUN). The user name in a SNA/DS network is called distribution unit name (DUN). The DUN consists of two parts, the distribution group name (DGN) and the distribution element name (DEN). The DEN is the same as a user identification, and the DGN can be used to identify a group of users, for example a department or a group of users using an office system node. The DEN must be unique within a distribution group; the DGN must be unique within the network. A distribution service unit name consists of a routing element name (REN) and a routing group name (RGN). The REN is the name of an individual DSU and must be unique in one routing group. The RGN can be used to identify a collection of DSUs, for example DSUs placed in the same location. The RGN must be unique in the network. The AS/400 system does not use the RGN, but it may be used by other systems in a network of which an AS/400 system is a part. DISOSS uses the RGN.

Figure 27 gives an overview of the terminology used in DISOSS and the AS/400 systems.

	DEN	DGN	REN	RGN
AS/400	DEN or User ID	DGN or Address	REN or System	not used
DISOSS	Source Address (SA)	Document Distribution Name (DDN)	REN	RGN

Figure 27. Comparison of AS/400 and DISOSS SNA/DS Terminology

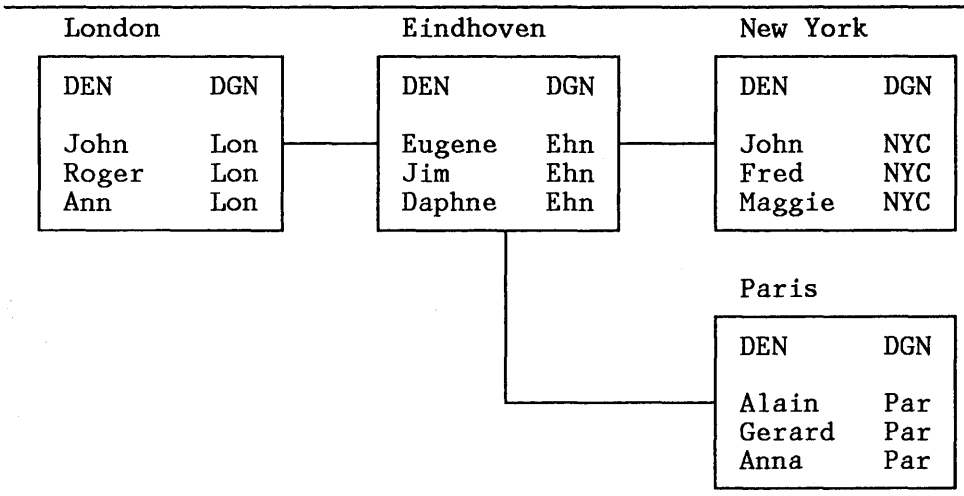
6.2.1.2 SNA/DS Directory

The directory contains information about users of SNA/DS services (in an office environment DISOSS or AS/400 office users) and relates the users to the names of the systems where they can receive distributions. The SNA/DS directory can be set up in such a way that it allows easy updating without maintaining large tables and without a need for central directory management.

The usage of default entries reduces the number of directory entries needed for remote users. Figure 28 on page 59 illustrates this.

6.2.1.3 SNA/DS Routing

SNA/DS routing is based on the relationship between user name and DSUN of the system where the user resides. In the case of a local user SNA/DS delivers the information to that user. In the case of a remote user, routing tables indicate to which SNA/DS node the information is to be sent in order to reach the destination node. Also default entries in the routing table allow easy maintenance of that table. Figure 28 on page 59 shows an example of the relation between the directory and routing tables.



London User Directory

DEN	DGN	REN
John	Lon	Local
Roger	Lon	Local
Ann	Lon	Local
*	Ehn	Eindhoven
*	Par	Paris
*	NYC	New York

Routing Table

REN	Queue
Eindhoven	Eindhoven
Paris	Eindhoven
New York	Eindhoven

Eindhoven User Directory

DEN	DGN	REN
Eugene	Ehn	Local
Daphne	Ehn	Local
Jim	Ehn	Local
*	Lon	London
*	NYC	New York
*	Par	Paris

Routing Table

REN	Queue
London	London
New York	New York
Paris	Paris

New York User Directory

DEN	DGN	REN
John	NYC	Local
Fred	NYC	Local
Maggie	NYC	Local
*	*	Eindhoven

Routing Table

REN	Queue
Eindhoven	Eindhoven

Paris User Directory

DEN	DGN	REN
Alain	Par	Local
Gerard	Par	Local
Anna	Par	Local
*	*	Eindhoven

Routing Table

REN	Queue
Eindhoven	Eindhoven

Figure 28. Sample SNA/DS Network and Directory Structure

6.2.1.4 *Fan Out*

A user may specify that one document has multiple destinations. Only one copy of the document is sent until the DSU where the route to the next DSUs diverge; a DSU sends only one copy along a common route. The process of creating additional copies is known as "fan-out".

6.2.2 SNA/DS and APPN Considerations

SNA/DS and APPN both provide a means to route information through a network. There is however a fundamental difference between SNA/DS and APPN. APPN provides a path through the network across which communication can occur. The path may consist of just one link between adjacent nodes or of a collection of links and nodes. All nodes and links which constitute the path, have to be active to allow the session partners to exchange information. In short, APPN provides connectivity and the possibility for synchronous exchange and is most suitable for interactive traffic. Distribution of data takes place on the communication system level.

SNA/DS allows users (applications using SNA/DS) to communicate with each other without knowing if a route to the destination node(s) is available. As discussed before, SNA/DS stores the information on the receiving node and forwards it to the next node of the route whenever that is possible. The data distribution takes place on the (SNA/DS) application level. APPN provides the path between two SNA/DS nodes. The path can consist of one hop or multiple hops.

SNA/DS considers the next SNA/DS node always as an adjacent node, regardless of how many intermediate APPN nodes are involved in the route

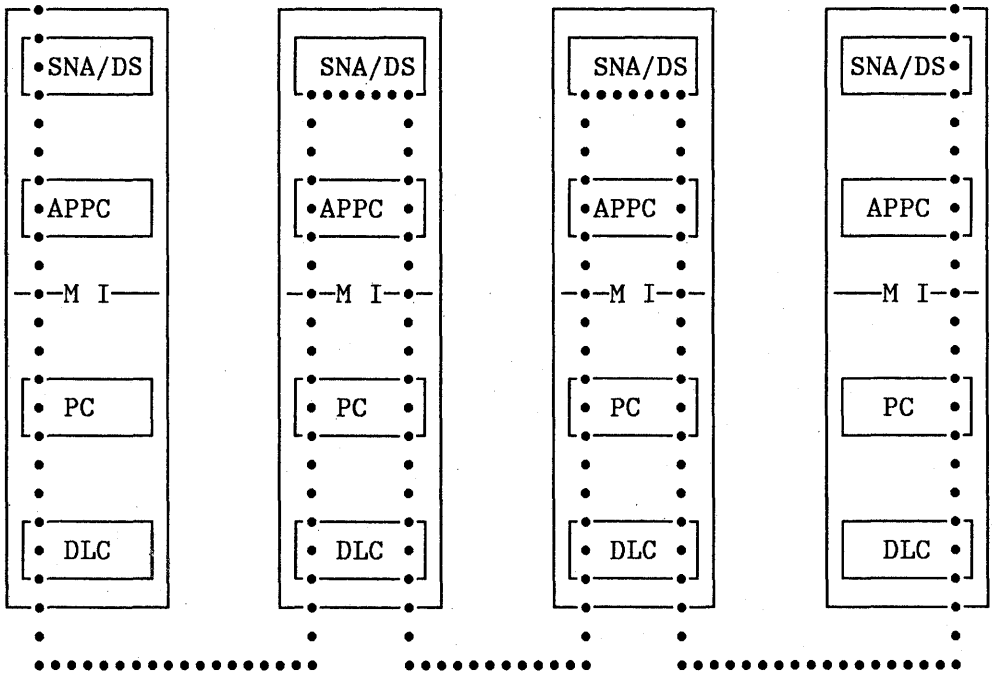


Figure 29. SNA/DS Intermediate Session Routing

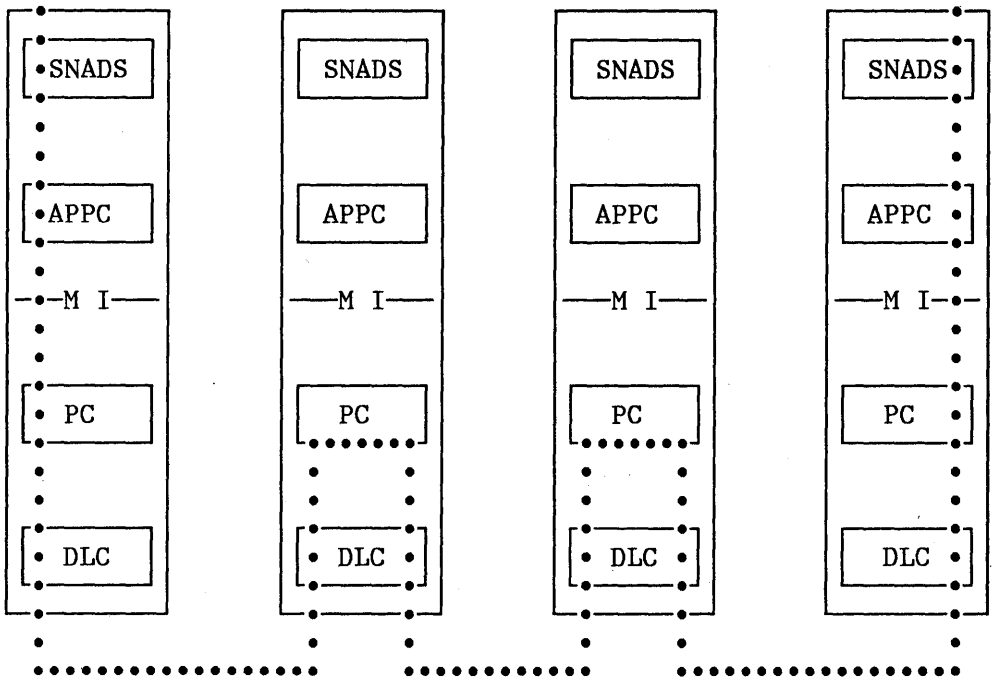


Figure 30. APPN Intermediate Session Routing

6.2.3 Design Considerations

As both APPN and SNA/DS provide routing functions, next design criteria could be considered when setting up a SNA/DS network in an APPN environment or in a mixed APPN subarea network environment.

6.2.3.1 Dynamic Routing

Dynamic routing is the ability of APPN to dynamically select a route through the network. APPN is able to dynamically select a route when alternatives are available. SNA/DS routing tables do not provide the possibility to select a route out of a number of routes available.

6.2.3.2 Intermediate Routing

As discussed before, both SNA/DS or APPN can be used to select a path through the network. When using SNA/DS in such a way that APPN only provides the path to the adjacent SNA/DS node, full advantage can be taken from SNA/DS functions. These are:

- Storing the information if the link to the next SNA/DS node cannot be established
- Fan out of document with multiple addressees.

When intermediate nodes are involved, SNA/DS processing on each node adds processing load to these nodes. Generally speaking APPN is faster than SNA/DS and uses less resources on an intermediate node. Figure 29 on page 60 and Figure 30 on page 61 illustrate this. Intermediate routing processing as performed by APPN requires less resources than SNA/DS intermediate routing processing. Whether or not the increased SNA/DS load is acceptable depends on the characteristics of that node. Depending on size, DASD capacity and application load, adding of SNA/DS processing has to be considered acceptable or not.

6.2.3.3 Deferred Transmitting of SNA/DS Queues

The ability of SNA/DS to queue send requests and transmit these only when a reasonable amount of requests for a destination node are queued. This is also an advantage when using switched connections. The session between the SNA/DS nodes only has to be established when transmitting the queues. Transmission can take place one or more times per day. In a batch file transfer environment such a procedure may be considered.

6.2.3.4 Fan-Out

Depending on the communication patterns, the trade off between APPN or SNA/DS processing on one hand and the sending of multiple documents through the network, the usage of the SNA/DS fan-out function has to be judged.

6.2.3.5 Traffic Patterns

On an average, 80% of the traffic should flow within a cluster of nodes constituting a network.

6.2.3.6 Naming Considerations

In a complex environment it is important to keep the number of definitions, needed to define the APPN and SNA/DS network, as low as possible. For this reason a naming convention for the the distribution group name (DGN) is very important. The DGN could be the node name identifier or a department name made unique for a specific node. Using the same department names (DGNs) on various nodes has the disadvantage that generic routing becomes difficult and makes directories very complex. The DGN is a unique name in the network.

Though the routing group name (RGN) is not used by the AS/400 system, it can be specified for use by other SNA/DS implementations. DISOSS can use the RGN and in Figure 36 on page 68 it is used for default RGN definitions in the DISOSS routing tables. This simplifies the definition of routes through the DISOSS network and allows one definition to route all documents to a specific APPN network. The usage of the RGN is optional, in that case however DISOSS should know all SNA/DS nodes in the entire network.

6.2.4 SNA/DS APPN Routing Structure

Based on the Figure 31 sample configuration, the various design options will be discussed. The sample consists of two APPN networks, each connected to a subarea network with a DISOSS node.

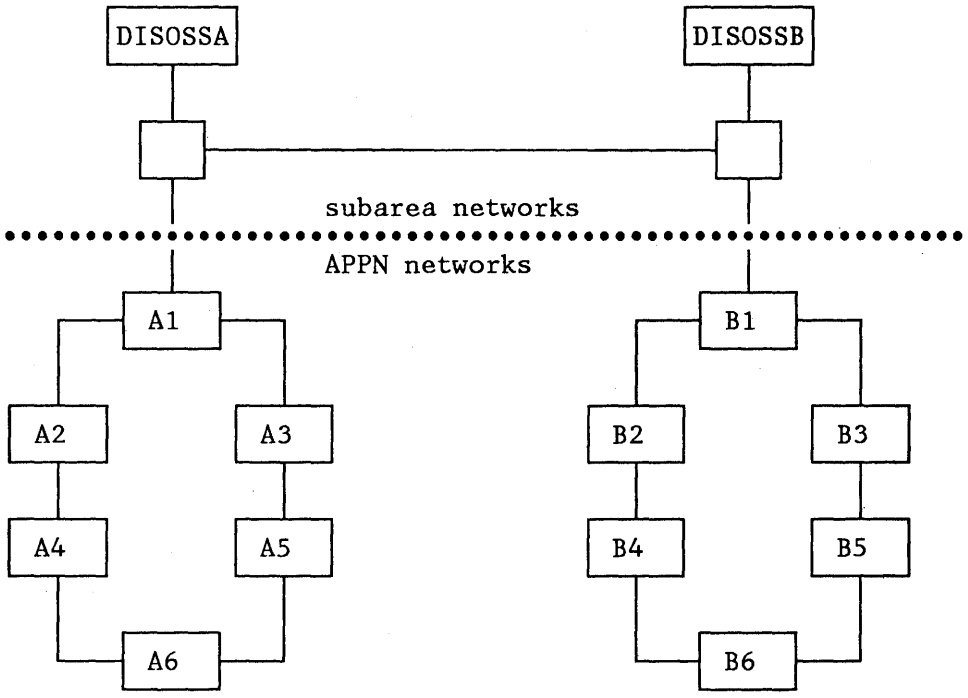


Figure 31. APPN SNA/DS Routing Sample

6.2.4.1 SNA/DS Routing

In the case of SNA/DS taking care of all routing, SNA/DS is responsible for intermediate routing. Assuming that in the case of an office communication system all nodes have SNA/DS activated, each node can be an intermediate SNA/DS node. In contrast with APPN SNA/DS is not able to select dynamically a route through the network if routing alternatives are possible. By setting up the routing tables and distribution queues the decision has to be made which route to select in case of alternatives. In Figure 31 each node is accessible via two routes, node A6 can send documents and files via the nodes A3 and A5 or via the nodes A2 and A4.

Note that when using SNA/DS routing, APPN may select an alternative route for one hop. For example if in node A6 the SNA/DS queue indicates that all non-local messages have to be sent to A5, APPN route selection may select a route via A4, A2, A1 and A3. If such an alternative is unwanted, the class-of-service table can be set up in such a way that such a route is not selected.

In the case of a relatively small network and an evenly distributed traffic load, SNA/DS routing may be an option. However in a larger APPN network environment or in an environment with multiple APPN networks and subarea networks, the number of hops and intermediate SNA/DS routing processing increases.

When using SNA/DS routing, fan-out will have its maximum effect. Files or documents sent to multiple addressees on different nodes will be copied on the node where the route to an addressee diverges.

6.2.4.2 Any-to-Any Routing

In the case of routing from one source SNA/DS node to any other target SNA/DS node, APPN is used to select the route and set up the session between the two end point SNA/DS nodes. The consequence of this option is that every node must know any every other SNA/DS node in the network. This means that any change of the network topology (as far as the logical SNA/DS network is concerned) results in a change of all routing tables and distribution queues. Though full advantage is taken from the APPN dynamic route selection, every topology update has to be defined manually in each node. When extending any-to-any routing to a multiple subarea APPN network environment, this option will turn out to be very hard to manage.

Also fan-out of documents and files has no effect.

6.2.4.3 Central Intermediate SNA/DS Node

The introduction of "central intermediate SNA/DS node" is a way to bring the SNA/DS network definition to a central point in an APPN network. APPN dynamic routing is used to establish a session from the source APPN node to one intermediate node from where documents or files are distributed to the target SNA/DS node. Figure 32 illustrates the logical SNA/DS network where A1 acts as a distribution node for the APPN network consisting of the nodes A1-A6.

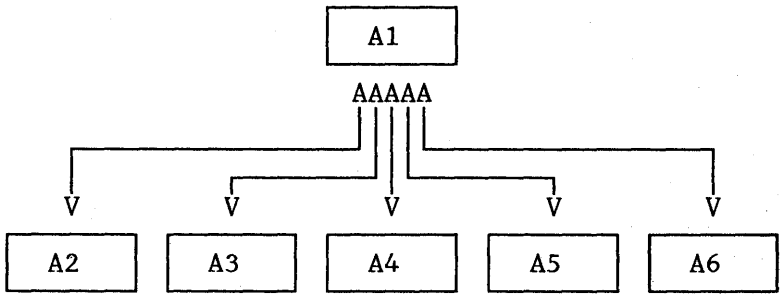


Figure 32. APPN Network with Central Intermediate SNA/DS Node

The routing table and distribution queues of node A1 reflect the SNA/DS network topology. Changes in the configuration only need updates in node A1. In the other nodes the entry in the routing table for non-local distributions points to node A1. As in most APPN networks one node is a network management focal point, the distribution function can be combined with the focal point function. The support function for the network is most likely located near the system which plays a central role.

In the case of mixed subarea/APPN networks, a layered structure as discussed can be extended with another layer. As shown in the sample configuration in Figure 31 on page 63, the subarea network with the SNA/DS nodes DISOSS1 and DISOSS2 constitutes the connection between two APPN networks. The subarea network can play the role of a SNA/DS backbone network. Figure 33 on page 65 shows a combination of subarea and APPN networks.

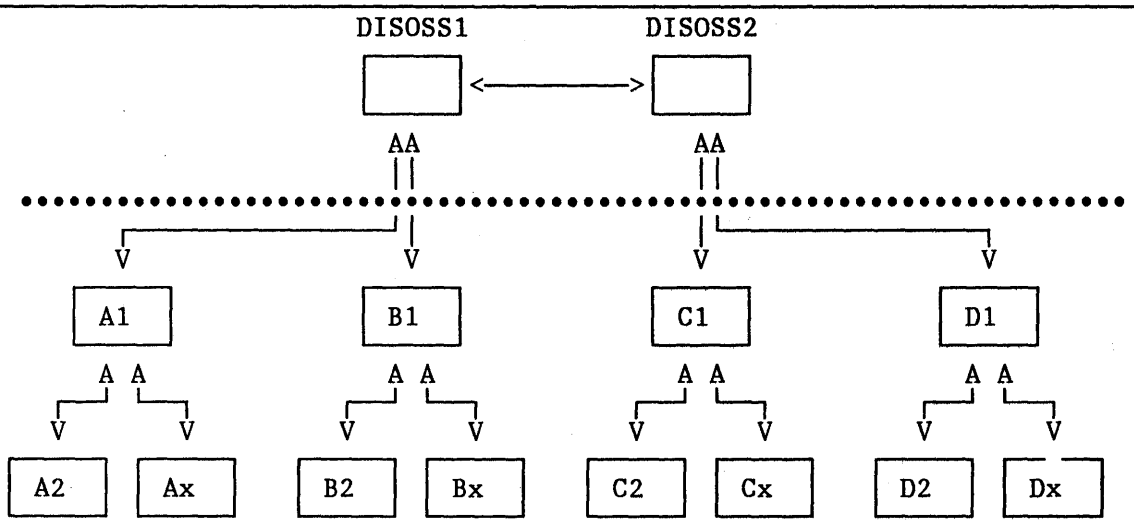


Figure 33. Layered APPN/Subarea SNA/DS Network

In this case the APPN nodes A1, B1, C1 and D1 not only play a central role in the SNA/DS network, they also are the gateway nodes between the subarea network and the APPN network. One could think of dedicated systems performing a central role in network management, routing of all traffic between the subarea network and the APPN network and distribution of SNA/DS traffic.

A disadvantage of this approach could be the availability of the central node. When the central node is not active, SNA/DS is not able to distribute the traffic through the network or to send it via the gateway function to other connected networks. Due to the asynchronous nature of the SNA/DS distribution, the user of the SNA/DS services is not directly affected. On the origin SNA/DS node SNA/DS will store the information and forwards it whenever the central SNA/DS node becomes available. Using a backup central SNA/DS node is a complex process, in case of using a backup node, definitions in all to the central node connected nodes have to be changed.

SNA/DS traffic between APPN nodes A1-A6 and APPN nodes B1-B6 in Figure 31 on page 63 is assumed to be routed via the DISOSS nodes. This is not required. Another possibility could be to use VTAM/NCP T2.1 node support to set up a SNA/DS-to-SNA/DS session between the nodes A1 and B1 via the subarea network without using the DISOSS nodes as intermediate SNA/DS nodes. In such a case the APPN gateway node routes the SNA/DS traffic directly to other APPN gateway nodes. This means that the APPN gateway nodes, constituting a SNA/DS backbone layer, must be defined in each gateway node (see Figure 34 on page 66).

If there are PS/CICS, PS/PC or PROFS [6] users in the subarea network, it is preferable to use the DISOSS systems as intermediate SNA/DS nodes. But also if this is not the case, it is preferable to use DISOSS because it simplifies the definitions at the APPN gateway nodes.

6.2.4.4 Conclusion

There is no standard solution for designing a SNA/DS network based on the infrastructure of an APPN/subarea network. The option to be chosen depends on the organizational environment, traffic patterns between the nodes and existing support structure. However it should be attempted to minimize the definition effort to configure the SNA/DS network and to use the APPN advantages whenever possible.

[6] registered trademark of IBM

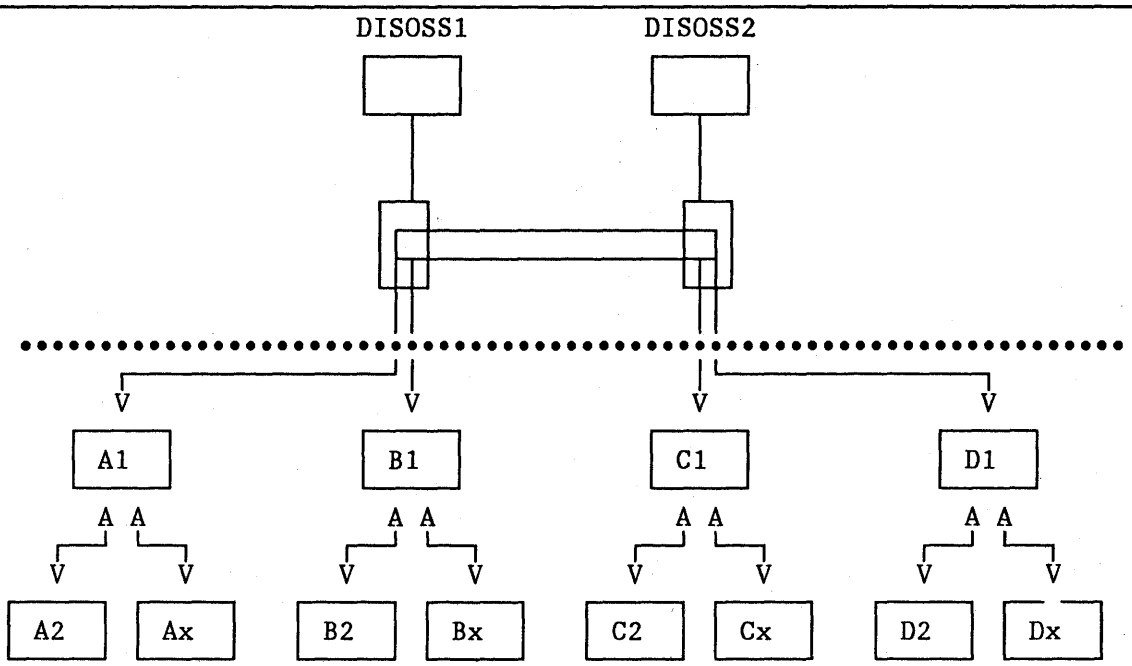


Figure 34. Layered APPN/Subarea SNA/DS Network

6.2.5 Sample Office Network

Based on the considerations discussed before, this chapter shows an office network supporting users in both an APPN and subarea network. The SNA/DS nodes in the subarea network are DISOSS systems. In the APPN network every node has AS/400 office installed and uses SNA/DS to distribute documents to other office system nodes. In this sample a central SNA/DS node is combined with direct distribution of SNA/DS traffic to the "neighbor" SNA/DS nodes. The purpose of this sample is to provide insight into how a SNA/DS network can be configured and what this means in terms of definitions.

In Figure 35 on page 67 two APPN networks are connected to a subarea network with two host systems. Figure 36 on page 68 shows the content of the AS/400 office directories and routing tables; Figure 37 on page 69 shows the DISOSS directory and routing tables.

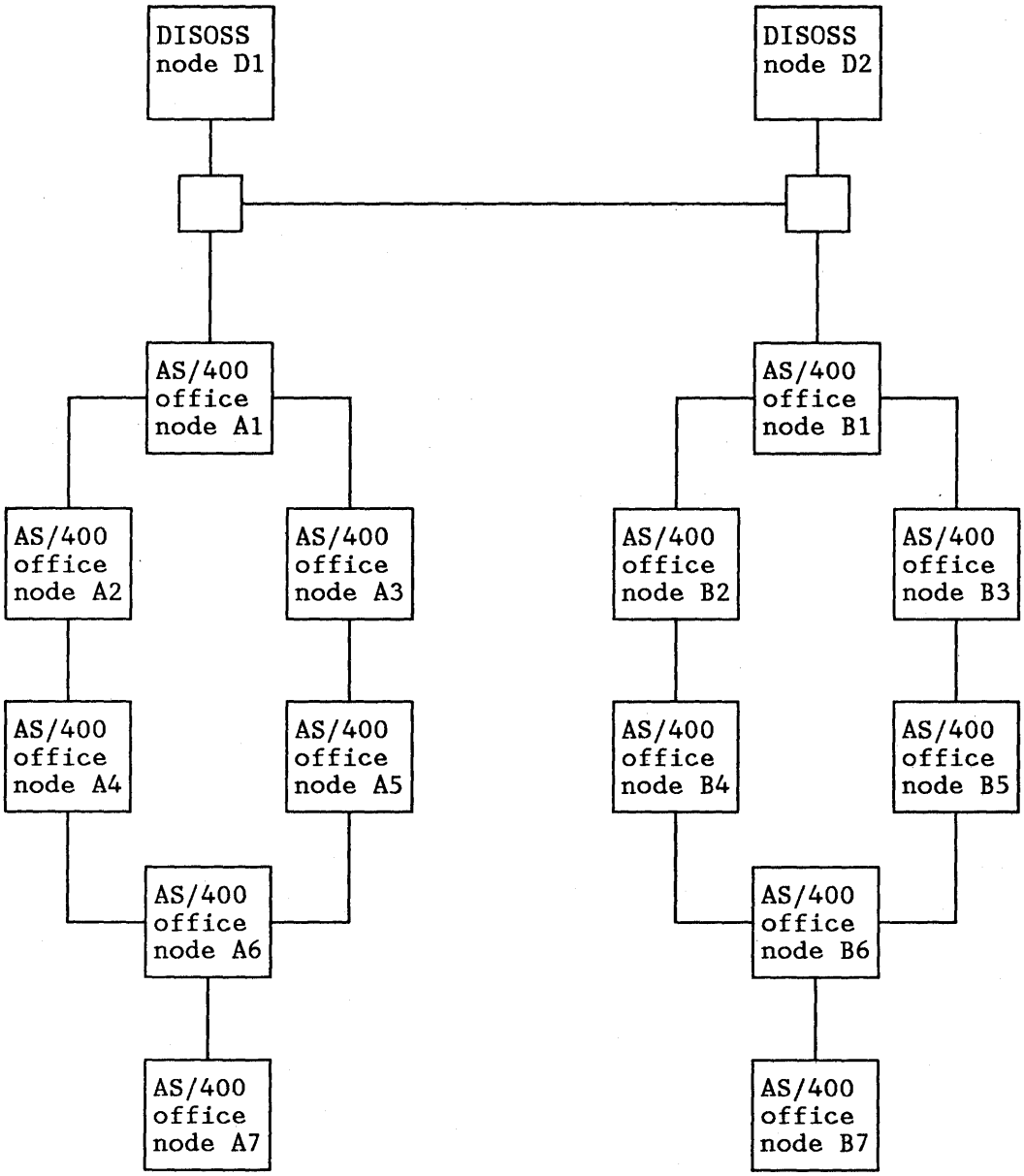


Figure 35. Sample Office Network

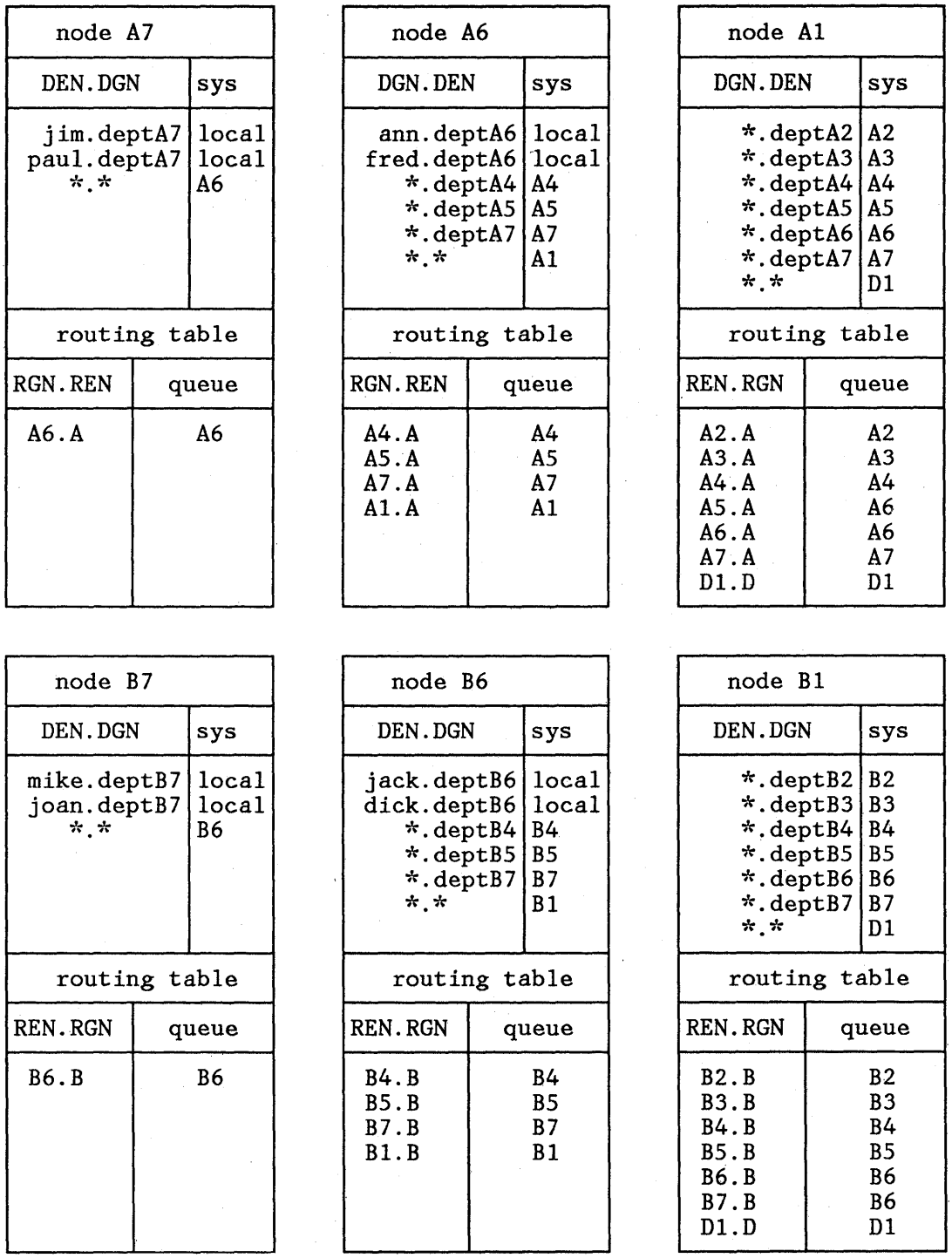


Figure 36. Directory and Routing Table APPN Nodes

system D1	
DEN.DGN	sys
*.deptA1	A1
*.deptA2	A2
*.deptA3	A6
*.deptA4	A4
*.deptA5	A5
*.deptA6	A6
*.deptA7	A7
*.deptB1	B1
*.deptB2	B2
*.deptB3	B6
*.deptB4	B4
*.deptB5	B5
*.deptB6	B6
*.deptB7	B7
.	error

routing table	
REN.RGN	queue
*.A	A1
*.B	D2

system D2	
DEN.DGN	sys
*.deptB1	B1
*.deptB2	B2
*.deptB3	B3
*.deptB4	B4
*.deptB5	B5
*.deptB6	B6
*.deptB7	B7
*.deptA1	A1
*.deptA2	A2
*.deptA3	A3
*.deptA4	A4
*.deptA5	A5
*.deptA6	A6
*.deptA7	A7
.	error

routing table	
REN.RGN	queue
*.B	B1
*.A	D1

Figure 37. Directory and Routing Table DISOSS Nodes

6.2.5.1 SNA/DS Routing Considerations

The complexity of a mixed APPN subarea network determines the way the routing is set up. In this sample the routing through the APPN network is performed by SNA/DS to the adjacent nodes and by APPN to other nodes. The routing to DISOSS users (PS/CICS or PS/PC) or through the DISOSS network to other APPN nodes is performed by SNA/DS. It should also be possible to use APPN functions to route documents from an office system node in APPN network A to a node in APPN network B. If in this sample user Ann.deptA6 sends a document to user Mike.deptB7, the route hops from node A6 to node B7 via node A1, node D1, node D2, node B1, node B6. The routing could also be set up in such a way that SNA/DS sends the document directly from node A1 to node B1. However DGNs in all other APPN SNA/DS nodes have to be defined in each "gateway" APPN node. In a large network this could lead to excessive definitions.

In this sample the network node server also is a SNA/DS node for the attached end nodes. There are other options to set up the SNA/DS routing, it highly depends on the organization of the office environment and the traffic patterns.

6.3 DDM

DDM is an architecture that allows interconnected systems to share data. DDM defines the data transfer between systems regardless of individual data management implementations. If an application requests access to a file that is not on the local system, DDM locates the target file and handles the data interchange between the source and target system using LU 6.2 protocols. The location of the files has to be defined in DDM. In contrast with SNA/DS processing this is a synchronous process. When DDM locates a target system the underlying APPN protocols are used to locate the DDM application on the target system. After route selection and session set up, the session is established to exchange information between the session partners. From an APPN point

of view DDM is an LU 6.2 application as any other LU 6.2 application. Figure 38 on page 70 illustrates this.

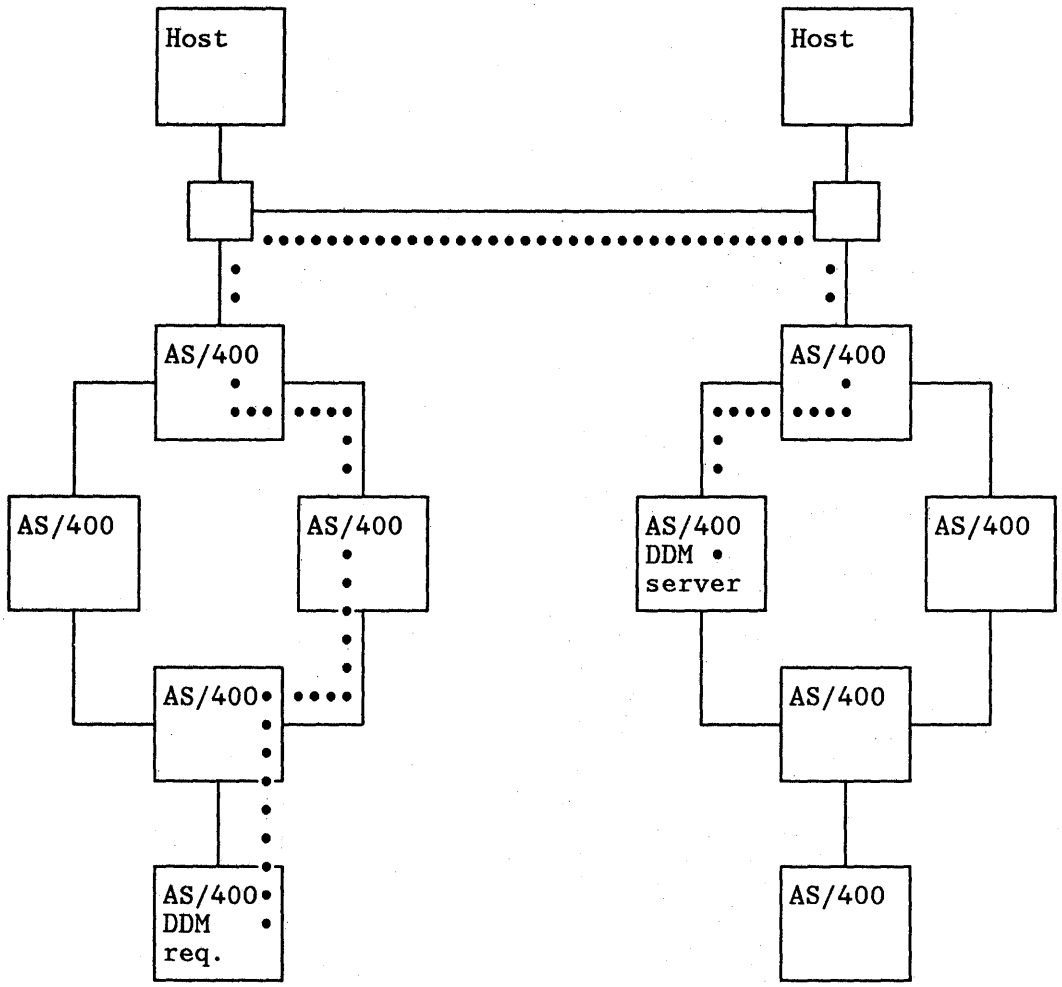


Figure 38. Sample DDM Session

Appendix A. Bibliography

SNA Format and Protocol Architecture Logic Type 2.1 Nodes	SC30-3422
SNA Format and Protocol Architecture Logic for LU Type 6.2	SC30-3269
VTAM V3R2 and NCP V4R3/V5R2 Installation Considerations	GG66-3102-0
VTAM V3R2 and NCP V4R3/V5R2 SNA Type 2.1 Node Support Using the System/36 as an Example	GG66-0299-0
VTAM V3 R2 and NCP V4R3 Planning Guide For New Functions	GG24-3121-0
A Technical Overview: VTAM Version 3 Release 2 NCP Version 4 Release 3 NCP Version 5 Release 2	GG66-0283-0
AS/400 Advanced Peer-to-Peer Networking (APPN)	GG24-3287-0
Management of AS/400 in SNA Subarea Network Using Netview Products	GG24-3289-00
AS/400 Communications: Advanced Program-to-Program Communications and Advanced Peer-to-Peer Networking User's Guide	SC21-9598-0
AS/400 Communications: Communications and Systems Management User's Guide	SC21-9661-0
AS/400 Office: Planning Guide	SC21-9626-0
AS/400 Office in a DIA/SNADS Network	GG24-3268-0
S/36 APPC Security in Network with S/36 S/38 and CICS	GG22-9427-0
Systems Journal Vol.26, No.4, 1987: A Perspective on Advanced Peer-to-Peer Networking	G321-0088-0

Appendix B. List of Abbreviations

APPC Advanced Program-to-Program Communication

APPN Advanced Peer-to-Peer Networking

ASM Address Space Manager

BTU Basic Transmission Unit

COS Class of Service

CP Control Point

CS Configuration Services

DAF Destination Address Field

DDM Distributed Data Manager

DEN Distribution Element Name

DGN Distribution Group Name

DHCF Distributed Host Command Facility

DLC Data Link Control

DSNX Distributed System Node Executive

DSPT Display Station Pass Through

DSU Distribution Service Unit

DSUN Distribution Service Unit Name

EN End Node

EP End Point

FP Focal Point

FQPCID Fully Qualified Procedure Correlation Identifier

HCF Host Command Facility

LEN Low Entry Networking

LFSID Local Form Session Identifier

LU Logical Unit

MI Machine Interface

MS Management Services

NetView DM NetView Distribution Manager

NN	Network Node
NOF	Network Operator Facility
OAF	Origin Address Field
ODAI	OAF-DAF Assignor Indicator
ODF	Object Distribution Facility
PC	Path Control
PIU	Path Information Unit
PLU	Primary Logical Unit
PVC	Private Virtual Circuit
RACF	Resource Access Control Facility
RAR	Route Addition Resistance
REN	Routing Element Name
RGN	Routing Group Name
RSCV	Route Selection Control Vector
SLU	Secondary Logical Unit
SNADS	SNA Distribution Services
SNBU	Switched Network Back Up
SOC	Sphere of Control
SS	Session Services
SSCP	System Services Control Point
SVC	Switched Virual Circuit
TG	Transmission Group
TRS	Topology and Routing Services
XID	Exchange Identidfication

Appendix C. Overview SNA T2.1 and APPN Product Implementations

C.1 SNA T2.1 LEN Implementations

- S/36
- S/38
- PS/2 [7] with OS/2 EE [7]
- RT PC
- AS/400
- VTAM V3R2 in conjunction with NCP V4R3 or NCP V5R2
- S/88.

C.2 SNA T2.1 with APPN Extensions Implementations

- S/36
- AS/400.

---

[7] trademark of IBM

Index

H

I

L

M

N

O

P

R

S

T

V

W

X

APPN / SUBAREA NETWORKING
DESIGN AND INTERCONNECTION
CONSIDERATIONS
GG24-3364-00

READER'S
COMMENT
FORM

You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Your comments will be sent to the author's department for whatever review and action, if any, is deemed appropriate. Comments may be written in your own language; use of English is not required.

Note: *Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.*

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

What is your occupation? _____

Please use pressure sensitive or other gummed tape to seal this form.

Reader's Comment Form

Cut or Fold Along Line

Fold and tape | Please Do Not Staple | Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE:

IBM International Technical Support Center
Department 985A, Building 657
P.O. Box 12195
Research Triangle Park
Raleigh, North Carolina 27709
U.S.A.

Fold and tape | Please Do Not Staple | Fold and tape

IBM®

APPN / SUBAREA NETWORKING DESIGN
AND INTERCONNECTION CONSIDERATIONS
GG24-3364-00

GG24-3364-00

PRINTED IN THE U.S.A.

GG24-3364-00