Manual #WNTSU06504A **Edition: May 1998**

The information in the **FPX Communication Services for Windows NT / Windows 95** document is subject to change without notice and should not be construed as a commitment by Cirel. It assumes no responsibility for any errors that may appear in this document. The information enclosed herein is proprietary to Cirel and as such, no part of this publication may be reproduced, disclosed, stored in a retrieval system or transmitted in any form or by any means, including electronic, mechanical, photographic or magnetic, without the prior written consent of Cirel.

Contents

CHAPTER 1

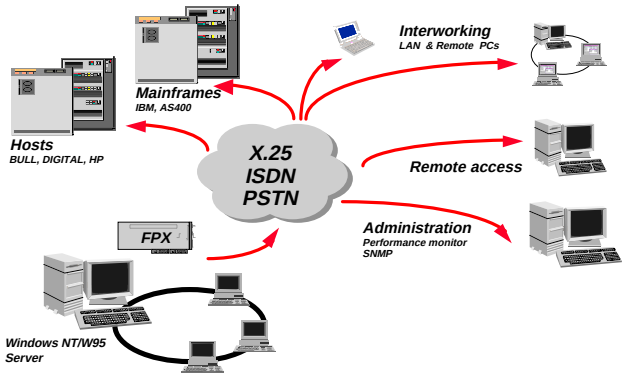
Welcome

1

This chapter introduces the main features of the different components that come with the FPX and its associated softwares.

What is this product for ?

The **FPX Communication Services for Windows NT / Windows 95** product offers a complete range of services to solve connectivity problems with remote hosts. It supports a wide variety of communication media through X.25, PSTN and ISDN networks.



It provides connections to BULL and PAD hosts with DKU/TTU and VT emulations via the X.25, PSTN and ISDN networks.

It provides SDLC and QLLC connections for SNA Servers providing LAN workstations access to remote IBM mainframes and AS/400.

It is used for LAN and remote stand-alone PCs interworking using the Windows NT/W95 TCP/IP stack through the X.25, PSTN, Frame Relay and ISDN networks.

It extends the capabilities of the Microsoft Remote Access Service over X.25, PSTN and ISDN networks.

It includes various administrative tools to manage ISDN and X.25 FPX equipment and to control the behavior and state of each component.

FPX adapters

The **FPX Communication Services for Windows NT / Windows 95** product requires one or more of the following FPX adapters:

- FPX/B X.25 adapter (V28 electrical interface)
- FPX/B-AS X.25 adapter (V28, V11 and V35 electrical interface)
- FPX/S Simultaneous X.25 (V28 interface) and ISDN adapter
- FPX/SL Strict ISDN adapter
- FPX/S-AS Simultaneous X.25 (V28, V11 and V35 electrical interface) and ISDN adapter
- FPX/IM Simultaneous X.25 (V28 interface) and PSTN (V.32 bis modem)
- FPX/I Simultaneous X.25 (V28 interface), ISDN and PSTN (V.32 bis modem)
- FPX/B PCI (Identical to FPX/B-AS) with PCI bus
- FPX/S PCI (Identical to FPX/S-AS) with PCI bus

All FPX adapters operate as communication co-processors providing autonomous communication protocol management. Their multichannel technology is used to make simultaneous connections to different transport networks such as X.25 and ISDN. Multichannel adapters integrate an internal routing mechanism (FIC routing) used by Windows NT/W95 Server applications to select one of the available links according to a call prefix; this enhances application programs independence.

These smart adapters are equipped with surface mounted devices (SMD) including an Intel 80186 microprocessor and are built around an application specific integrated circuit (ASIC) that provides a powerful communication interface.

The adapters with an -AS (Auto Switch) designation have a V28 or V11 or V35 electrical interface while standard adapters feature only a V28 interface.
The main adapters are described below (the FPX/B PCI and FPX/S PCI have the same features as the FPX/B and the FPX/S, but they have a PCI bus):

FPX adapters features	FPX/B-AS	FPX/S-AS	FPX/IM	FPX/I
X.25 Line speed	64 Kbits/s	64 Kbits/s	64 Kbits/s	64 Kbits/s
ISDN Line speed		144 Kbits/s		144 Kbits/s
PSTN Line speed (V32b)			14400 bits/s	14400 bits/s
X.25 virtual circuits	32	32	32	32
Bus	ISA/EISA	ISA/EISA	ISA/EISA	ISA/EISA
RAM / IRQ configuration	Software	Software	Software	Software
I/O address	Jumpers	Jumpers	Jumpers	Jumpers
Electrical interfaces	V28/V11/V35	V28/V11/V35	V28	V28

The product includes the utilities required to manage the FPX adapters:

- X.25, X.29, ISDN, TGTX25, QLLC and SDLC protocol software down-loaded into the FPX adapters
- Configuration programs used to customize X.25, TGTX25 and SDLC parameters
- Loader and initializer programs
- Windows NT/W95 FPX services providing FPX automatic startup

A set of diagnostic tools is provided and accessible via an FPX diagnostic control panel to:

- Execute hardware selftests
- Analyze line behavior
- Detect the electrical interface signal states
- Check the status of an X.25 connection, etc.

FPX/SL II adapter

FPX/SL II is a monochannel adapter with an ISDN plug.
The detection is automatically made after the adapter installation, and the associated features are displayed according to the availabilities of the machine: they can be modified.
This adapter only supports:

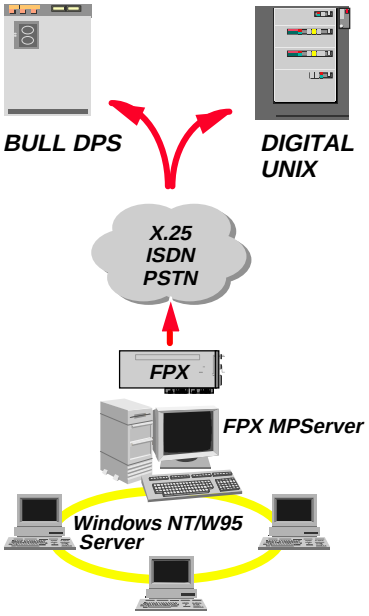
- **FPX PassLan/IP service,**
- **FPX Support RAS service,**
- **FPX Host Access service.**

The product can be ordered with the *FPX Communication Services ISDN for Windows NT / Windows 95* label.

Note: Be careful to use the FPX Diagnostic Tools utility:
The use principle stays identical to the one described in this documentation: only some commands or options have been removed or grayed.
To use the FPX Diagnostic Tools program:

- Start it to activate the traces (all channels are simultaneously activated)
- Select the *View* menu, then click on the *Refresh* command or use the associated shortcut. For more information, refer to the Online Help.

BULL and X.25/X.29 connectivities

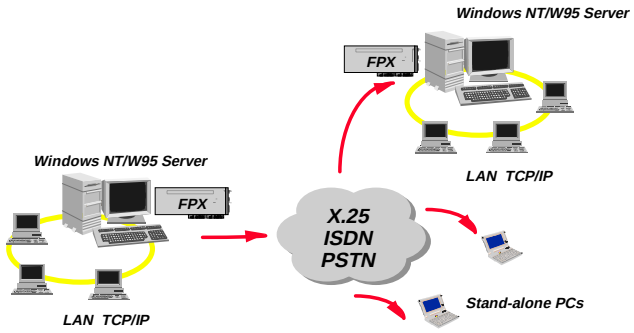


In the DSA environment, FPX MPServer emulates a Bull TCS/TCU controller capable of simultaneoulsy managing 4 remote sites and 32 DKU/TTU sessions. To reach a central DPS host, the workstations can use the FPX WinniSTATION DKU software or one of the three products it supports (WINCOM 7107 from Icom, TALKMAN from Integro or SIVIPW from Sit). As a function of the product used, DKU and TTU emulations, MicroFIT and FTF file transfer support, VTI and UVTI APIs are available for each user.

FPX MPServer also emulates a PAD to dialogue with all the central systems supporting X.25 and X.29 access. Working with the FPX WinniSTATION PAD, or with the X25BAPI interface, it provides users with a complete work environment (VT100 and VT220 terminal emulations).

It supports 32 simultaneous X.25/X.29 sessions.

TCP/IP networks interworking



The product includes the FPX PassLan/IP service for interconnection of LANs and stand-alone PCs.

It extends the capabilities of the Windows NT/W95 TCP/IP stack over X.25, PSTN, frame Relay and ISDN networks.

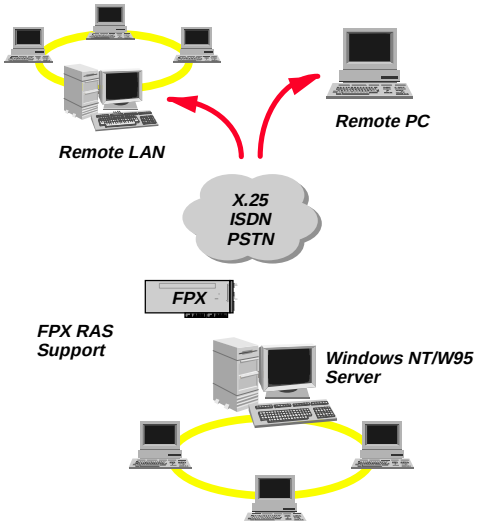
In compliance with the NDIS 3.x specifications, FPX PassLan/IP supports up to 64 simultaneous gateways. For each gateway, a backup mechanism ensures the automatic switching from a primary link to a secondary one.

The advanced features (adaptive routing, bandwidth-on-demand, accreditation on X.25 address or IP address, PPP authentication, inactivity timeout, etc.) improve the security and the reliability of the entire environment.

FPX PassLan/IP implements Request For Comments 877, 1144, 1356, 1490 and 1661 and interoperates with the main routers of the market:

- Cisco
- Retix
- Wellfleet
- Spider
- 3Com

Remote access

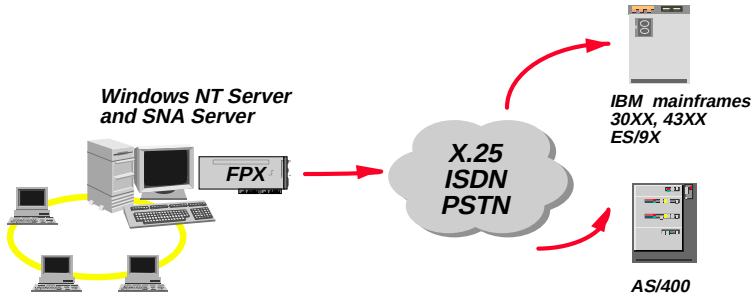


The product includes FPX RAS Support to enhance the capabilities of the Microsoft Remote Access Service over X.25, PSTN and ISDN networks.
It extends the local area network to remote workstations and offers full network access to remote PCs.

Built around the Microsoft WAN TAPI Miniport interface, FPX RAS Support provides a high speed connection pipe between Windows NT/W95 servers over X.25, PSTN and ISDN.
Stand-alone Windows for Workgroups PCs can also use the WAN connection to access the Windows NT/W95 RAS server and share resources on the network.

IBM connectivities

Links services for SNA Server on Windows NT



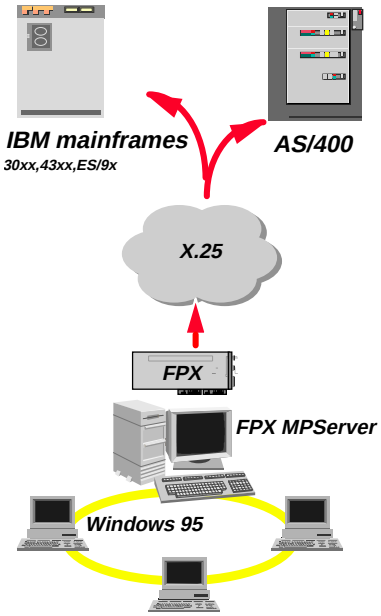
The product includes Link Services which enable a Microsoft SNA Server to communicate with IBM mainframes and AS/400 using the X.25, PSTN and ISDN networks.

These Link Services support all SNA Server functions and are compatible with all other FPX Windows NT services.
They include Microsoft SNA interface specification compliant drivers:

X.25/QLLC driver for X.25 connections
X.25 is the CCITT standard used for communicating over a packet-switched network. It uses the qualified logical link control protocol (QLLC).

SDLC driver for SDLC connections
SDLC uses a standard phone line (leased or switched line) with a modem at each end.

Using FPX MPServer on Windows 95

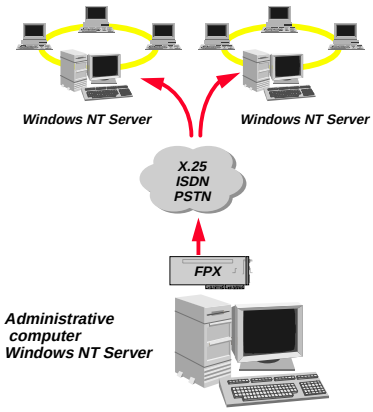


In the SNA environment, FPX MPServer emulates an IBM controller managing one remote site using the X.25 network:

- IBM mainframes : 30xx, 43xx, ES/9x
- AS/400

To reach a central IBM host, the workstations can use the FPX WinniSTATION IBM software or one of the products it supports (TALKMAN from Integro,..).

Administration tools



The product includes FPX MPSupervisor, an object-oriented administrative product.
It fits perfectly with Windows NT standard tools (performance monitor, registry, event viewer, SNMP service, etc.).
It performs the following functions:

- Link level analysis (electrical interface, frame and packet levels)
- Statistics, logs and events
- Event and alert management,...

System Requirements

The details of the system requirements to ensure proper operation of the FPX product are:

- **Hardware:** 32-bit x-86 Intel personal computer equipped with at least one FPX adapter
- **Software:** Windows NT Server 4.0 or Windows 95 and the **FPX Communication Services for Windows NT / Windows 95** product
- **Memory:** 16Mb

Online help

Various components of this product use the Microsoft Windows Help feature.

There are sections that describe parameters and the user can access online help by clicking on the help button.

Technical support

Technical support is available from 9 A.M. to 6 P.M. Monday through Friday by contacting Cirel's Technical Support Department by fax or telephone at the numbers printed on the cover page of this document.

Please inform us of any problems you encounter with this product, or any comments or suggestions about this manual you wish to make. We are eager to hear from you !

Please collect the information listed on the Technical Support Information Form at the back of this guide before calling Technical Support and check the following:

- Is it a communication problem ?
- When does the problem occur ?
- Is it machine-dependent ?
- Make sure all cables are firmly attached.
- Re-boot the Windows NT/W95 Server and try again.
- Try the procedure on another system.

Email address: **techsup@cirel.com**

Common abbreviations

The following is an alphabetical list of common abbreviations used in this document.
For definitions of particular terms, refer to the glossary in the appendix.

Abbreviation	Meaning
ACTPU	ACTivate Physical Unit
API	Application Programming Interface
APPC	Advanced Program-to-Program Communications
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSC	Binary Synchronous Communication
BTU	Basic Transmission Unit
CCITT	International Telegraph and Telephone Consultative Committee
CCN	Cluster Control Node
CD	Carrier Detect
CICS	Customer Information Control System
CPI-C	Common Programming Interface for Communications
CSV	Common Service Verb
CTS	Clear-To-Send
CUCN	CommUnication Controller Node
DACTPU	DeACTivate Physical Unit
DCE	Data Circuit Terminating Equipment
DLC	Data Link Control
DLL	Dynamic Link Library

DNS	Domain Name Systems
DSA	Distributed System Architecture
DSE	Distributed System Environment
DSR	Data-Set-Ready
DTE	Data Terminal Equipment
DTR	Data-Terminal-Ready
EBCDIC	Extended Binary Coded Decimal Interchange Code
EISA	Extended Industry Standard Architecture
FCS	Frame Check Sequence
FEP	Front-End Processor
FTF	File Transfer Facility
FTP	File Transfer Protocol
HDLC	High level Data Link Control
IBM	International Business Machines
IMS	Information Management System
IP	Internet Protocol
IRP	Interrupt Request Packet
IRQ	Interrupt Request Line
ISA	Industry Standard Architecture
ISO	International Standards Organization
LAN	Local Area Network
LAPB	Link Access Protocol Balanced
LAPD	Link Access Protocol for D-channel
LLC	Logical Link Control
LU	Logical Unit
LUA	Logical Unit Application
MAC	Media Access Control
MIB	Management Information Base
MTA	Message Transfer Agent
NAU	Network Addressable Unit
NCP	Network Control Program
NetBIOS	Network Basic Inpout/Output System
NPSI	Network Packet Switched Interface
NRZ	Nonreturn to Zero
NRZI	Nonreturn to Zero Inverted
PABX	Private Automatic Branch Exchange
PLP	Packet Layer Protocol
PSDN	Packet-Switched Data Network
PU	Physical Unit
PVC	Permanent Virtual Circuit
QLLC	Qualified Logical Link Control
RAS	Remote Access Service
RH	Request/Response Header
RPC	Remote Procedure Call
RU	Request/Response Unit
RUI	Request Unit Interface
SAA	Systems Application Architecture
SAP	System Access Point
SDLC	Synchronous Data Link Control
SID	Security IDentifier
SLI	Session Level Interface
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNADIS	SNA Driver Interface Specification
SNMP	Simple Network Protocol Management
SON	Session Outage Notification
SSCP	System Service Control Point
SVC	Switched Virtual Circuit
TCAM	TeleCommunications Access Method
TCP	Transmission Control Protocol

TCP/IP	Transmission Control Protocol / Internet Protocol
TCS	Terminal Control System
TCU	Terminal Control Unit
Telnet	Telecommunications Network Protocol
TH	Transmit Header
TGT	Transpac Clustered Terminal
TP	Transaction Program
TPDU	Transport Protocol Data Unit
TSO	Time Sharing Option
UDP	User Datagram Protocol
UVTI	Unified Virtual Terminal Interface
VM	Virtual Machine
VM/CMS	Virtual Machine/Conversational Monitor System
VTAM	Virtual Telecommunications Access Method
VTI	Virtual Terminal Interface
WAN	Wide Area Network

CHAPTER 2

Overview

2

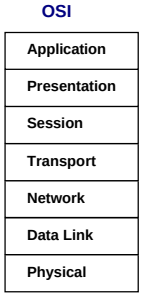
This chapter provides a tutorial introduction to the different theoretical notions that make up the various architectures of the FPX product components.

Basic Concepts

The product is intended to enhance the Windows NT/W95 environment giving it Wide-Area Networking capabilities.
It relies on communication adapters to provide WAN functionality over X.25, PSTN and ISDN networks.

X.25 Network

X.25 is a CCITT international standard for data communications used in almost every country in the world. The X.25 protocol includes the first three levels of the OSI reference model.



The Physical Layer represents the X.21 standard.

The Data Link Layer is a sub-set of the HDLC protocol labeled LAP-B.

The X.25 recommendation defines the interface between a PDN (Public Data Network) and a packet-mode user device (DTE, Data Terminal Equipment). It also defines the services that the user devices can expect from the X.25 PDN including the ability to establish virtual circuits through a PDN to another user device, to exchange data from one user device to another and to clear the virtual circuit when through.

PSTN Network

Local Area Networks (LANs) were designed to interconnect desktop computers within workgroups and departments, allowing people to share information and resources.
The next step in the evolution of this interconnection was to combine it with one of the most basic business tools: the telephone.
The Public Switched Telephone Network is basically designed to handle analog signals used for voice transmission. A modem is therefore required to MOdulate and DEModulate the data from digital to analog (transmission) and from analog to digital (reception).
When accessing the PSTN network, the FPX adapter is linked with an external synchronous modem. In synchronous mode, internal clock pulses are used to synchronize the signals of transmission and reception. When exchanging information, the data frames are encapsulated within a specific set of control characters, describing the exact part of useful data being transmitted in each frame. This mode is used for high transmission speed and provides a good ratio of final useful data to total data transmitted.
The modem can be one of two types:

- Half-duplex, where transmission and reception cannot be done simultaneously
- Full-duplex, where transmission and reception are done simultaneously

ISDN Network

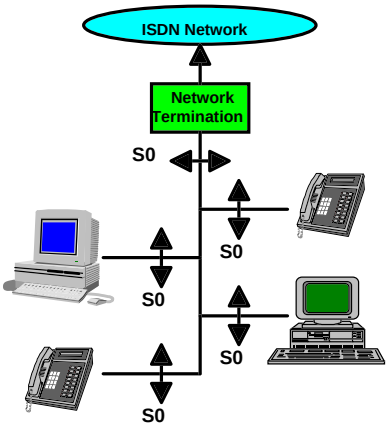
The Integrated Services Digital Network (ISDN) specification is a digital evolution for the analog phone system. It provides end-to-end digital connectivity to support a wide range of services which can be either voice or non-voice services.

An ISDN network requires ISDN lines with the following:

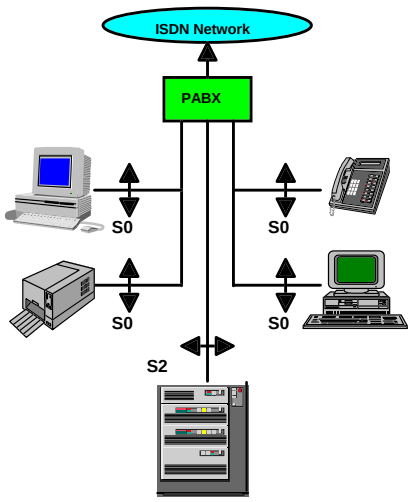
- Two B-channels for voice and data at 64Kbit/second per channel
- One D-channel at 16 Kbits/second for signaling and line control. This channel is used for call setup but it is also possible to transfer data on it. The X.25 protocol is sometimes available over the D-channel (X.31 Case B recommendation).

Two types of ISDN access can be defined:

- Basic Rate Interface (BRI) (S0)
- Primary Rate Interface (PRI) (S2)



BRI uses two B-channels and one D-channel.



The European implementation of PRI uses 30 B-channels.
The United States implementation uses 23 B-channels.
PRI uses different signalization and a type of interface not compatible with BRI.

The different types of connections

The FPX adapters supplied with the FPX package provide a wide variety of connections through X.25, PSTN and ISDN networks. This section does not describe all the possibilities of connections, but proposes the main diagrams currently used.

Public X.25 network.

Private X.25 network through a leased line.

Point to point through a PSTN network using X.25 protocol.

X.25 network through a SDP. (synchronous dial-in port)

ISDN network using X.25 protocol on B or D-channel or PPP protocol on B-channel.

Note: When the FPX adapter is equipped with an external modem, it can be a standard synchronous modem or a smart HDLC synchronous modem with V.25 bis capabilities. This CCITT recommendation provides a way to optimize communication between the modem and the FPX equipment. As it is not possible to execute AT commands in synchronous mode, the V.25 bis mode is used to perform the dialing. It offers the same control as the Hayes commands to determine how the modem will work.

The following modes are available:

- [108/1] Modem stored: the PSTN number is stored in the modem, and the dialing is done when the DTR signal on the modem is set. This connection can be performed using either a standard modem or a V.25 bis modem.

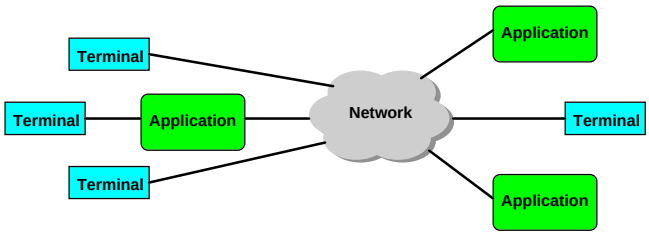
- [108/2] SDP or Point to point: HDLC frames are exchanged between the FPX and the V.25 bis modem. The V.25 bis dialing command puts the PSTN number in one of these frames. When the communication is established, X.25 frames are exchanged transparently between the FPX and the modem. The half or full-duplex transmission type is only used at this level.

Introducing DSA architecture

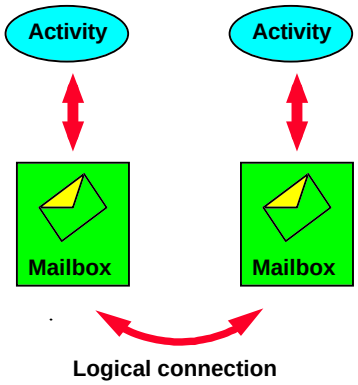
Distributed System Architecture (DSA) is the network architecture developed by Bull for the interconnection of its various systems and products.
It conforms to the reference model for Open Systems Interconnection (the OSI model) as defined by the International Standards Organization (ISO).

Communication between end-users

A DSA end-user is either a person or a device using the network services. It can be an application program dialoguing with the network via a terminal operator or it can be the program itself. Program execution and terminal usage are called activities.



Connection identifier



In order to communicate with an end-user on another system an end-user must be identified. Each resource has its own end-point name represented by a unique address in the system.
These end-points are known as mailboxes.

End-users and sessions

A session must be established between two end-points before communications between the two end-users can begin. Session control services are used to establish this logical connection so that data exchanges between mailboxes can take place. As long as the logical connection is maintained, messages can flow simultaneously in both directions.

A session is a temporary connection between end-users that is used to:

- Transfer data
- Synchronize actions
- Reserve required resources (memory space, cpu time, etc.)

In session control, the data unit is called a letter.

Session execution

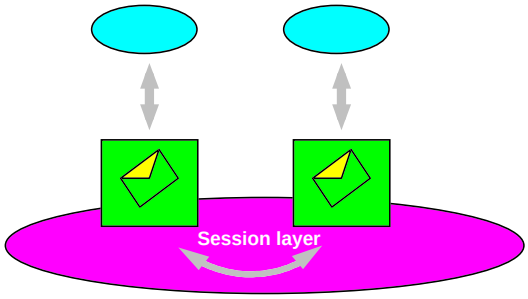
To execute a session, a request that specifies the following is sent:

- The name of the system where the called program is located
- The name used to identify the program in the system i.e., the mailbox name

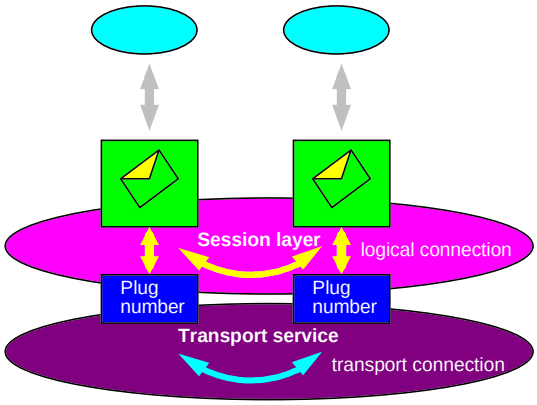
When receiving this request, the session control service checks whether:

- The requested connection is in the same system. In this case, it assigns a number to the logical connection.
- The program is on another system. In this case, it determines the required transport service. Then, the transport service assigns a plug number to identify the access point for the requester mailbox.

The calling transport service identifies the routing service in order to establish a network route between the two systems. The called transport service replies by sending its own plug number. At this point, each transport service identifies the other one by its plug number.

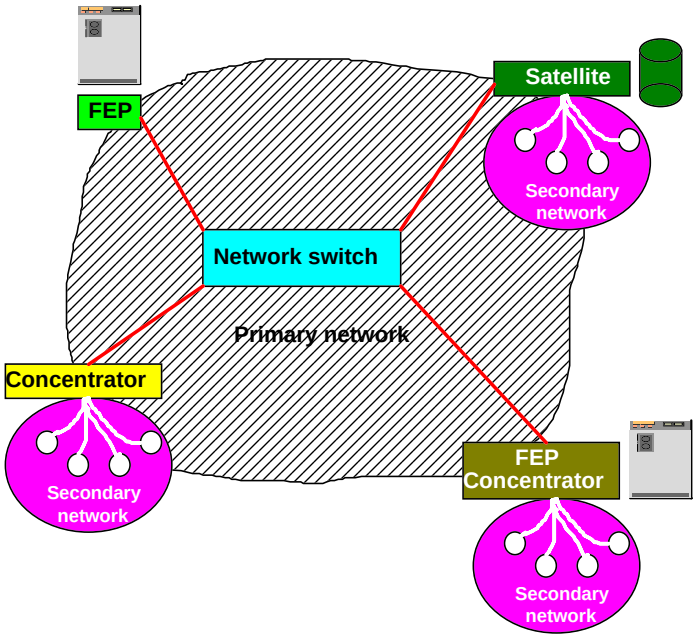


A logical connection is established between two programs of the same system.



A logical connection is established between two programs of two different systems.

DSA network organization



A DSA network includes several components:

- Hosts
- Front-end processors (FEP)
- Concentrators
- Switches
- Satellites
- Terminals, etc.

The primary network complies with all DSA rules and includes all the devices described above.
The devices that do not belong to the primary network are part of the secondary networks.
Each FEP or concentrator or satellite can have its own secondary network.

Front-end processor (FEP)

An FEP is directly linked to the central host (also called information processor). It provides communication control services and terminal management functions. The most representative FEP is a Bull Datanet network processor.

Concentrator

The main function of a concentrator is to manage the terminals connected to it locally or remotely. It can be located anywhere in the network. It receives data from a large number of physical connections and forwards them to a smaller number of connections and vice versa.

Network switch

A switch is used to route data. It manages service data that includes addressing information.

Satellite

A satellite is a minicomputer that provides the same processing and storing capacities as an FEP for what communications are concerned. It is used for applications that are:

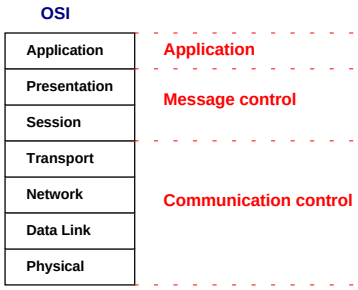
- Locally located
- Connected to the secondary network terminals
- Logically connected to other applications via the primary network

It can be for example a mini6 computer.

Terminal

A terminal represents a device used to communicate with the system. It is generally composed of a screen and a keyboard and optionally, a printer.

DSA functions



As described before, the DSA architecture complies with the OSI model that consists of seven layers.
The function of each layer can be defined as user services.

Application layer

The application layer includes application programs and software sub-systems such as:

- Remote Batch Facility (RBF)
- Transaction Driven Sub-system (TDS)
- File Transfer Facility (FTF)
- User programs

At this level, the data unit is called a message. It can have any format or size.

Presentation layer

The presentation layer provides end-users with a set of services used for data formatting:

- Coding, decoding
- Packing, unpacking
- Encryption, decryption, etc.

The required services are negotiated by the two parties when the logical connection is established. The presentation control protocols include:

- Standard Device Protocol (SDP)
- Transparent Protocol
- Real Device protocol

The protocol to be used may also be negociated during session establishment.

At this level, the data unit is the record.

Session layer

The session layer controls the logical connection establishment between two activities which can be either local or remote:

- Transmission and reception of the connect request
- Multiplexing on the established path
- Option negotiation

At this level, the data unit is the letter.

Transport layer

The main functions of the transport layer are:

- Establishing the route between networks
- Multiplexing logical connections on a route
- Fragmentation and reassembly of fragments into letters
- Flow, sequence and error control when not done at lower level
- Negotiation of the credit and the transport data unit size

At this level, the data unit is the fragment.

Network layer

The network layer is responsible for selecting the network route. Several types of communication are possible:

- Direct connections
- Point-to-point connections (leased lines)
- Public networks (X.25 packet-switched network or X.21 circuit-switched network), etc.

At this level, the data unit is the packet.

Data Link layer

The data link layer manages transmission between two adjacent nodes of the network using the HDLC procedure that ensures:

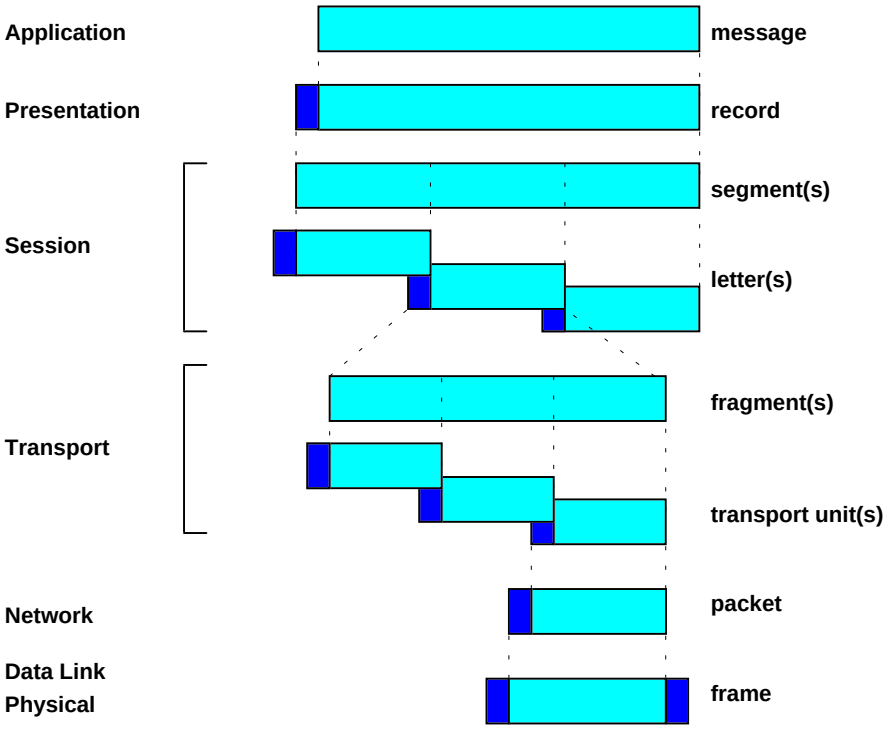
- Data coding independence
- Error control
- Credit mechanism

At this level, the data unit is the frame.

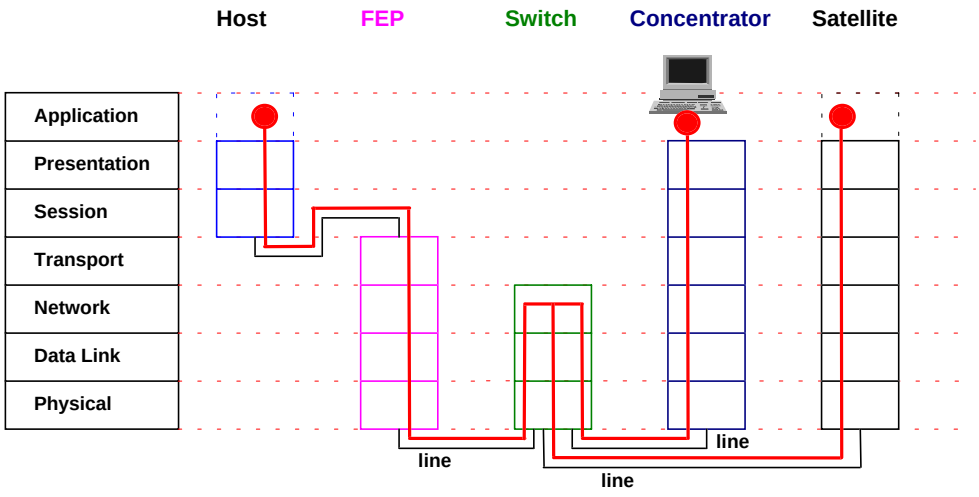
Physical layer

The physical layer provides the electrical transmission means according to the network type and its associated throughput.

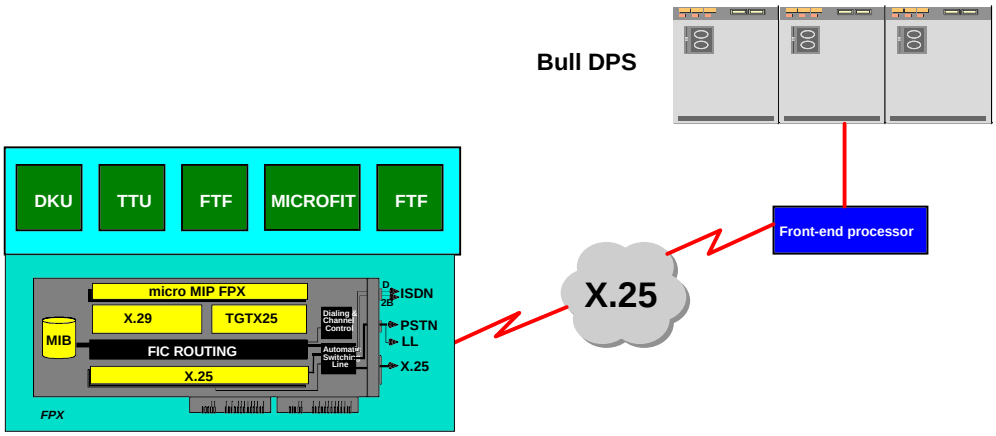
Message transmission



Protocols dispatching



TGTX25 configuration



TCP/IP design principles

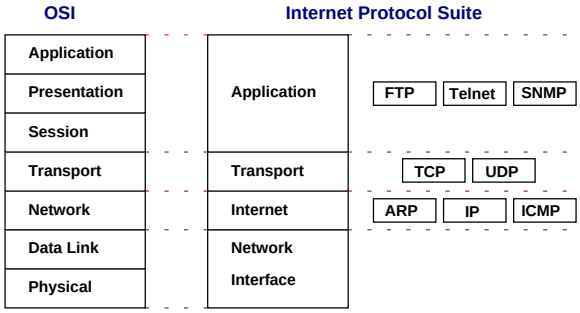
The Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard suite of protocols designed for the interconnection of desktop computers over wide-area network environments. In 1969, the U.S. Department of Defense Advanced Research Projects Agency founded a new project to provide high-speed communication links using packet switched networks and to create a network called ARPANET. This network was used for many successful experiments by 1972 and was at this time basically composed of military sites and research organizations.

The mechanism used to exchange information between researchers was based on technical reports called Requests For Comments (RFC).
The ARPANET network was divided into several networks. The interconnection of all these networks was called Internet.

Although the appropriate term to define this set of protocols is Internet protocols, the term TCP/IP is commonly used in this guide to refer to this family of protocols.

The OSI Model

The TCP/IP protocol suite fits into the seven layers of the OSI model.



The Network Interface layer is responsible for moving frames over the wire.
The Internet layer encapsulates the packet into an Internet datagram.
The Transport layer provides the connection pipes between two hosts.
The Application layer corresponds to applications such as FTP, Telnet, SNMP, etc.

The Internet protocol

The main functions of the IP protocol are:

- Determination of a route, defining how data is transfered throughout the internetwork
- Packet fragmentation or reassembly (datagrams)
- Routing of information from one host to another

It is an unreliable connectionless packet delivery service for all the other protocols of the TCP/IP family. That means that the packet delivery is not guaranteed. A packet might be lost, delivered out of sequence, duplicated, or delayed with no notification to the sender or the receiver. These packets are independent from other packets. No acknowledgement is required when data are received.

The Transmission Control Protocol (TCP)

The TCP protocol provides a reliable, connection-based protocol over or encapsulated within IP. TCP guarantees that the packets arrive at their destination. Data is transmitted into segments. For each segment sent, the receiving host must return an acknowledgement for the bytes received within a specified period.
When the acknowledgement is not received, the data is transmitted again.
If the segment is received damaged, the receiving host will discard it.
The required acknowledgement frequency varies according to the reliability of the data link in order to reduce the impact of the traffic on the performance.

TCP ensures proper sequencing of the data by assigning a sequence number to each byte transmitted, and a checksum to each segment.
The sequence numbers guarantee that all bytes sent were received.
The checksum validates the packet header and its data for accuracy.

The User Datagram Protocol (UDP)

The UDP protocol is the TCP complement and offers an unreliable connectionless datagram service. Neither delivery of the datagram nor the correct sequencing is guaranteed.
It is used by applications that don't require data acknowledgments.

The Internet Control Message Protocol (ICMP)

The ICMP protocol can be considered as a maintenance protocol allowing two hosts on an IP network to share IP status and errors. These data can be exploited by higher-level protocols to recover from transmission or reception problems.
The ping utility is the most representative element of this protocol. It uses the echo request and echo reply packets to determine whether a particular host on the IP network is reachable. This is very helpful in diagnosing IP network failures.

The Address Resolution Protocol (ARP)

Two computers can communicate over an IP network by using their physical address. The ARP protocol is used to obtain the physical address of a TCP/IP host, and map it to the host's logical IP address. TCP/IP uses the IP address to identify a host as part of a TCP/IP internet. The process of obtaining this physical address is called address resolution.
Both IP and physical addresses are stored locally as an entry in the ARP cache for subsequent use. The ARP cache is maintained by the hosts and includes their own IP-physical address mapping.

IP Addressing

IP addressing defines a scheme for identifying TCP/IP hosts, which can be workstations, servers, or routers.
Each host on a TCP/IP network is identified by its unique IP address. This address identifies a node on a network and provides information in an internetwork.

IP address

An IP address is defined by a 32-bit value (four bytes) and is typically represented in dotted decimal notation as follows:

a.b.c.d

It provides two data elements:

- The network identifier: it specifies the network to which a node is linked.
- The host identifier for a node: it specifies the node within its network.

Networks that connect to the public Internet must have an official network identifier given by the Defense Data Network-Network Information Center (DDN-NIC) to guarantee the network ID uniqueness.
When the network identifier has been assigned, the host IDs for computers can then be defined within the network.

The Internet community has defined address classes according to network size.
Each network class is calculated using the first byte of its IP address:

	0-7	8-15	16-23	23-31
Class A	0 Network ID	Host ID		
Class B	1 0	Network ID	Host ID	
Class C	1 0 0	Network ID		Host ID

The following table provides the total number of network and host IDs according to each address class (the IP address being defined as a.b.c.d):

Class	Values	Network ID	Host ID	Number of networks	Number of hosts/network
A	1-126	a	b.c.d	126	16,777,214
B	128-191	a.b	c.d	16,384	65,534
C	192-223	a.b.c	d	2,097,152	254

Class A addresses are used for networks with a very large number of hosts. The high-order bit in a class A address is always set to zero. The next seven bits (first field) represent the network address. The remaining 24 bits (last three fields) represent the host address. This allows for 126 networks and 16,777,214 hosts per network.

Class B addresses are used for medium-sized networks. The high-order bits in a class B address are always set to 1 – 0. The next 14 bits (first two fields) represent the network address. The remaining 24 bits (last two fields) represent the host address. This allows for 16,384 networks and 65,534 hosts per network.

Class C addresses are used for small LANs. The high-order bits in a class C address are always set to 1 – 1 – 0. The next 21 bits (first three fields) represent the network address. The remaining eight bits (last field) represent the host address. This allows for 2,097,152 networks and 254 hosts per network.

Notes:
The network address 127 is reserved for internal loopback functions.
The first field in a network address cannot be zero (all bits set to 0). Zero indicates that the address is a local host and will not be routed.
The first field in a network address cannot be 255 (all bits set to 1). The number 255 acts as a broadcast.
A host address cannot consist of all bits set to 0 or to 1.

Subnet masks

A subnet mask is a 32-bit value that TCP/IP hosts use to distinguish which bits of the 32-bit IP address correspond to the network address and which bits correspond to the host address.
It is also represented in dotted decimal notation.
The subnet mask is applied to the IP address. The bits corresponding to the network address are set to 1. The bits corresponding to the host address are set to 0.
The number of bits used for the subnet mask determines the possible number of subnets and hosts per subnet.
The following table provides the default subnet masks applied to the different address classes:

Class	Subnet Mask (binary notation)	Dotted Decimal Notation
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

IP Routing

IP gateways or routers are used to provide IP datagram delivery between the IP subnets connected to an internet. This functionality is called IP routing. When the datagrams are sent on the local network by a host belonging to the same network, this function is not necessary. When the host wants to communicate with another network, a gateway or a router must be used to forward the datagrams to the appropriate destination network.
Each gateway or router maintains routing tables indicating which direction the datagram should take to reach its destination.

TCP/IP Common application layer protocols

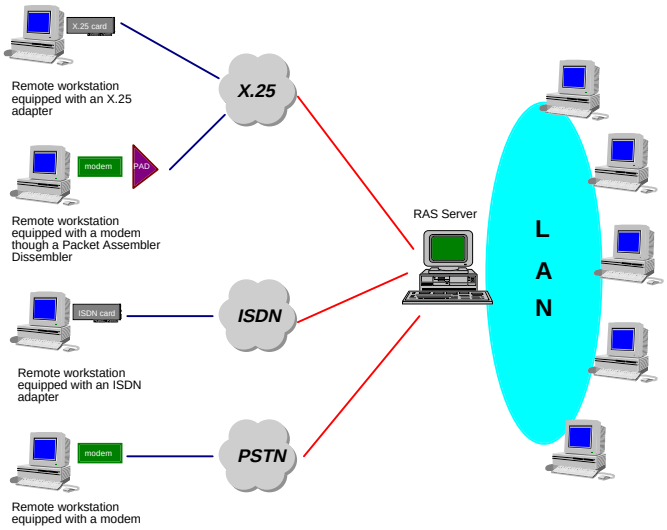
A set of common application protocols supplied with the main TCP/IP systems offers basic services such as file transfer services or terminal emulations.

These applications are for example:

Application	Description
DNS	Distributed database that allows applications to map between computer names and IP addresses.
FTP	Copy files from one Internet machine to another.
SMTP	Govern the exchange of electronic mail between two message transfer agents (MTAs) on the Internet.
SNMP	Define a protocol for remote administration of TCP/IP machines.
Telnet	Offer remote login between hosts running potentially different operating systems.

Remote Access Service

The Microsoft Remote Access Service has been designed to connect mobile or stand-alone workforces to corporate networks. It enables remote workstations to dial in to the Local Area Network in order to transparently access resources on it.



The Remote Access Service for Windows NT/W95 supports the following Wide Area Networks:

- PSTN
- X.25
- ISDN

The Remote Access Service (RAS) connects users over these networks through a remote access server to a Windows NT/W95 network. Once a user has made a connection, these pipes become transparent and the user can access all network resources as if they were at a computer in the office.
The RAS Server acts as a gateway between the remote workstation and the LAN.

RAS Features

The Windows NT/W95 Remote Access Service provides:

- Full network access for remote workstations including files and print resources and client/server applications
- Integrated administration: there is no administrative difference between remote and local users.
- Advanced security: RAS uses Windows NT/W95 security authentication before allowing remote users access to the LAN.

Its main advantages are:

- Down level compatibility: this ensures that old RAS clients can connect to any Windows NT/W95 Server.
- Standard network interfaces: any network application that uses standard network interfaces will work over RAS (NetBIOS, mailslots, named pipes, RPC, etc.).
- Scalability: it provides multiple simultaneous connections and takes full advantage of Windows NT/W95 multiprocessing capabilities.
- Extensive WAN support: it provides X.25, ISDN and PSTN connectivity.
- LAN topology independence: it supports all topologies currently supported by Windows NT/W95 (Ethernet, Token Ring, FDDI, etc.)
- Protocol independence: NetBEUI, TCP/IP and IPX protocols are supported.

RAS Security

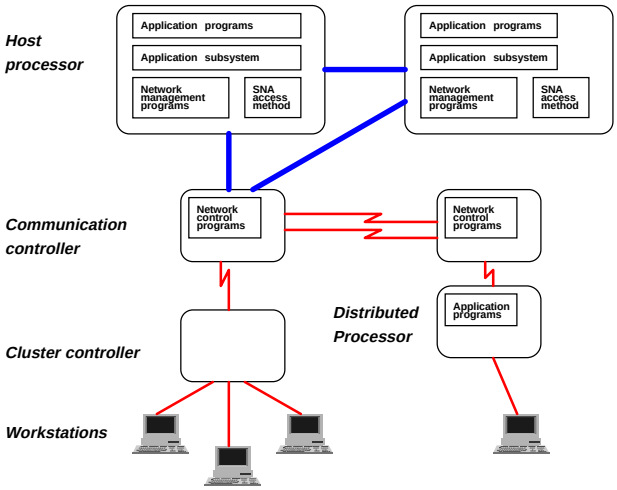
The Remote Access Service provides the following security features:

- Integrated domain security: the RAS Server uses the same account database as the Windows NT/W95 Server.
- Encrypted authentication and logon: the user name, password and logon information are encrypted when transmitted over the WAN.
- Auditing: when it is enabled, RAS will generate audit information on all remote connections, including activities such as authentication, logons, etc.
- Restricted network access: it is used to restrict RAS Clients to the RAS Server only or to access the entire network.
- Callback security: the user can be called back at a user specified number. This provides the best security for the RAS Server. The callback occurs after the user has been authenticated by the RAS service and just before the user is logged in by Windows NT/W95.
- User disconnection: the RAS Admin utility allows the administrator to disconnect an unauthorized user without disrupting other connected users.

Introducing SNA architecture

System Network Architecture was originally an IBM master plan for communications with and between IBM computers, terminals and office systems. It was the company's vehicle for interconnection with other industry-standard networks such as X.25.

SNA contains specifications for the devices or nodes in a network and for the paths between those nodes. Both nodes and paths are organized in hierarchies of seven levels.



SNA network components include:

- Host processors
- Distributed processors
- Communication controllers
- Cluster controllers
- Workstations
- SNA access methods
- Application subsystems
- Application programs
- Network management programs, and network programs

SNA Nodes

Each element in an SNA network controls a specific part of the network. There are different types of nodes:

- Type 5 represents mainframes
- Type 4 represents communication controllers
- Type 2 represents cluster controllers
- Type 1 represents workstations, terminal controllers and minicomputers

Host processor

This node corresponds to the central unit, with one operating system (VM/CMS Virtual Machine/Conversational Monitor System), one or several access methods (VTAM Virtual Telecommunications Access Method, TCAM TeleCommunications Access Method, etc.) and databases. It also includes one or more application programs (TSO Time Sharing Option, IMS Information Management System, CICS Customer Information Control System, etc.).

Host processors are typically IBM 370 machines, IBM 43xx (4381), or IBM 303x, 308x with an SNA method access.

Communication controller

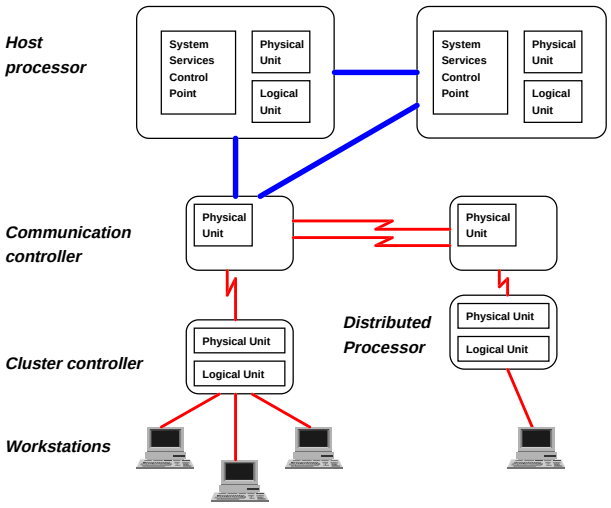
The CommUnication Controller Node (CUCN) is responsible for network management, checking lines (polling/addressing), adding or removing special characters needed to control transmission and line activation and deactivation.
This node is represented by a 3705 or 3725 or 3745 communication controller executing the Network Control Program (NCP). When the X.25 protocol is used, the NCP program includes an associated program called Network Packet Switched Interface (NPSI) that provides translation and simulation functions for terminals using the X.25 network.

Cluster controller

Terminals access applications (for example databases) managed by the host using a Cluster Control Node (CCN).
It is typically represented by a 3274 or 3275 cluster. Terminals linked to the cluster are typically 3278 (monochrome display), 3279 (color display), 3289 (monochrome printer) or 3287 (color printer).

Network Addressable Units

Each device or program that is part of the SNA network represents a network addressable unit (NAU). It uniquely defines a device (terminal or control unit), a line, a program, etc.



There are three general types of NAU:

- System Services Control Point (SSCP)
- Physical Unit (PU)
- Logical Unit (LU)

SSCP

The SSCP corresponds to the communication access method of a mainframe. It contains the network's address tables, the translation table, the routing tables and the instructions that deal with these tables. SSCP establishes connections between nodes in the SNA network.

PU

The PU provides a set of services that the node performs for itself. In an SNA network, each PU operates under the control of the SSCP and provides an entry point between the network and one or several logical units.

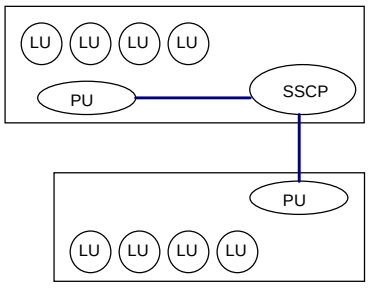
LU

The LU represents an end-user to the network. It can be an operator at a terminal or an application program which can be a data entry task running at a terminal, a database update running in a host or any process that serves as an endpoint to an SNA communication.
The number of LUs residing at a given PU depends on the type and the function of the PU:

- LU 0 Session for a user's specific application
- LU 1 Session between a host application and a remote batch terminal
- LU 2 Session between a host application and a 3270 display terminal
- LU 3 Session between a host application and a printer in the 3270 information display system
- LU 4 Session between a host application and an SNA word processing device or between two terminal devices
- LU 5 Undefined
- LU 6 Session between application programs usually in different hosts
  - LU 6.0 CICS/CICS session
  - LU 6.1 CICS/IMS session
  - LU 6.2 Advanced Program-to-Program Communication (APPC) session. APPC defines a session between an application program in a host computer and an application program in the same host or a different one.
- LU 7 Session between a host application and a 5250 display terminal

SNA Sessions

In an SNA network, all communications occur within sessions between NAUs. A session corresponds to a logical two-way connection between two NAUs over a specific route during a specific period of time. The SSCP controls the beginning of a session (connection), the end of a session (disconnection) and checks status during communications.



There are different types of SNA sessions that can be opened between:

- The SSCP and PUs
- The SSCP and LUs
- A PU and a LU

SSCP-to-PU Session

The SSCP requests status or diagnostic information from a PU within its domain and the PU answers appropriately. The session is established during network startup or by the operator with an ACTivate Physical Unit (ACTPU) request. The session is deactivated by an operator DeACTivate Physical Unit request, (DACTPU) or when the data link is down (Session Outage Notification, SON).

SSCP-to-LU Session

The SSCP requests status or diagnostic information from a LU and the LU answers appropriately. The SSCP-to-PU session must be established before the SSCP-to-LU session.
The SSCP-to-LU session must be established before any LU-to-LU session.
The session is established during network startup or by the operator with an ACTivate Logical Unit (ACTLU) request. The session is deactivated by an operator DeACTivate Logical Unit request, (DACTLU) or when the SSCP-to-PU session is down. The session can be also disconnected using a Session Outage Notification (SON).

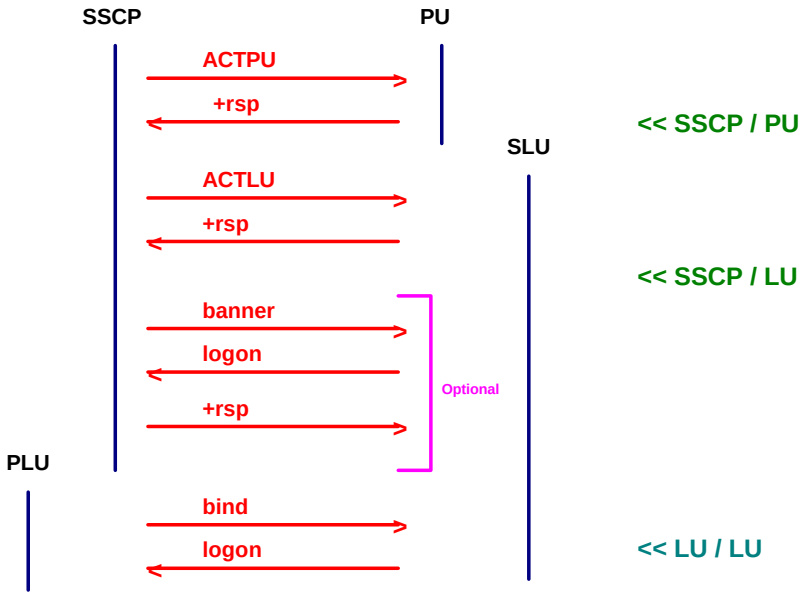
SSCP-to-SSCP Session

Two SSCPs in the same or different domains use this session to exchange information.
The SSCPs can reside in different access methods within the same host. The main goal of this type of session is to help establish LU-to-LU sessions between LUs in domains controlled by different SSCPs.

LU-to-LU Session

This session is used to exchange information between two LUs. All end-user communications in an SNA network take place in LU-to-LU sessions. This session is established using the BIND request.

Establishing an SNA session



Describing SNA layers

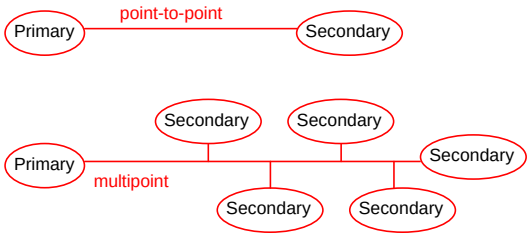
The SNA network has a layered architecture which can be compared to the ISO's Open Systems Interconnection reference model. Both the OSI model and the SNA have seven functional layers.

SNA	OSI
Transaction Services	Application
Presentation Services	Presentation
Data Flow Control	Session
Transmission Control	Transport
Path Control	Network
Data Link Control	Data Link
Physical Control	Physical

The Physical Control layer connects adjacent nodes at physical and electrical levels.
The Data Link Control layer transmits data between adjacent nodes.
The Path Control layer routes data and controls traffic.
The Transmission Control layer paces data exchanges.
The Data Flow Control layer synchronizes data flow.
The Presentation Services layer formats data.
The Transaction Services layer represents distributed databases, document interchange, etc.

The SDLC data link layer

The Synchronous Data Link Layer (SDLC) is a protocol for managing synchronous, code-transparent, serial-bit data transfer between adjacent nodes. Data can be sent simultaneously in both directions or alternately in one direction at a time. SDLC is defined as a subset of the CCITT High Level Data Link Control (HDLC) protocol.



The link connection may have a point-to-point, or multipoint, or loop configuration. A point-to-point link can be switched or non-switched.

SDLC frame format

The basic unit of an SDLC transmission is a frame composed of a string of bits with addressing and control information at the beginning, data from the higher levels in the middle and error control information at the end.

F	Flag (0x7E hexadecimal)
A	Address field
C	Control field
FCS	Frame Check Sequence

SDLC frame types

Format	Usage
Unnumbered format (U)	Link establishment and disconnection, Errors report, Data transfer
Supervisory format (S)	Frame acknowledgement Frame numbering errors report
Information format (I)	Information transfer

The X.25/QLLC data link layer

The SNA network architecture for packet-switched data networks relies on Logical Link Control (LLC) protocols to provide services and to enhance the quality of those services.
These protocols are known as QLLC because they use Qualified data packets to transfer information between nodes.
In this type of environment, established virtual circuits (generally referred as switched VCs or SVCs) are viewed by the higher layer of SNA as switched lines while permanent virtual circuits appear as dedicated (leased) lines.

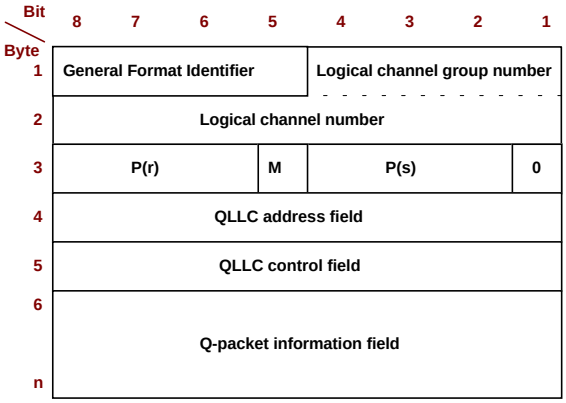
QLLC protocol is dedicated to SNA nodes connected through X.25-based PSDNs. It uses the Qualifier bit set equal to 1 (Q-packets) to transfer HDLC-like commands and responses.

Q-Packet format

The QLLC protocol uses the Q-packet as the basic element of the transmission.

F	Flag (0x7E hexadecimal)
A	Address field
C	Control field
FCS	Frame Check Sequence

The Q-packet is composed as follows:



The address field is one byte long and contains the hexadecimal value FF for commands and any value other than FF for responses.
The control field is one byte long and contains the command/response transmitted by the peer.
The information field consists of a variable number of bytes and is used to carry QXID, QTEST or QFRMR data.

QLLC frame types

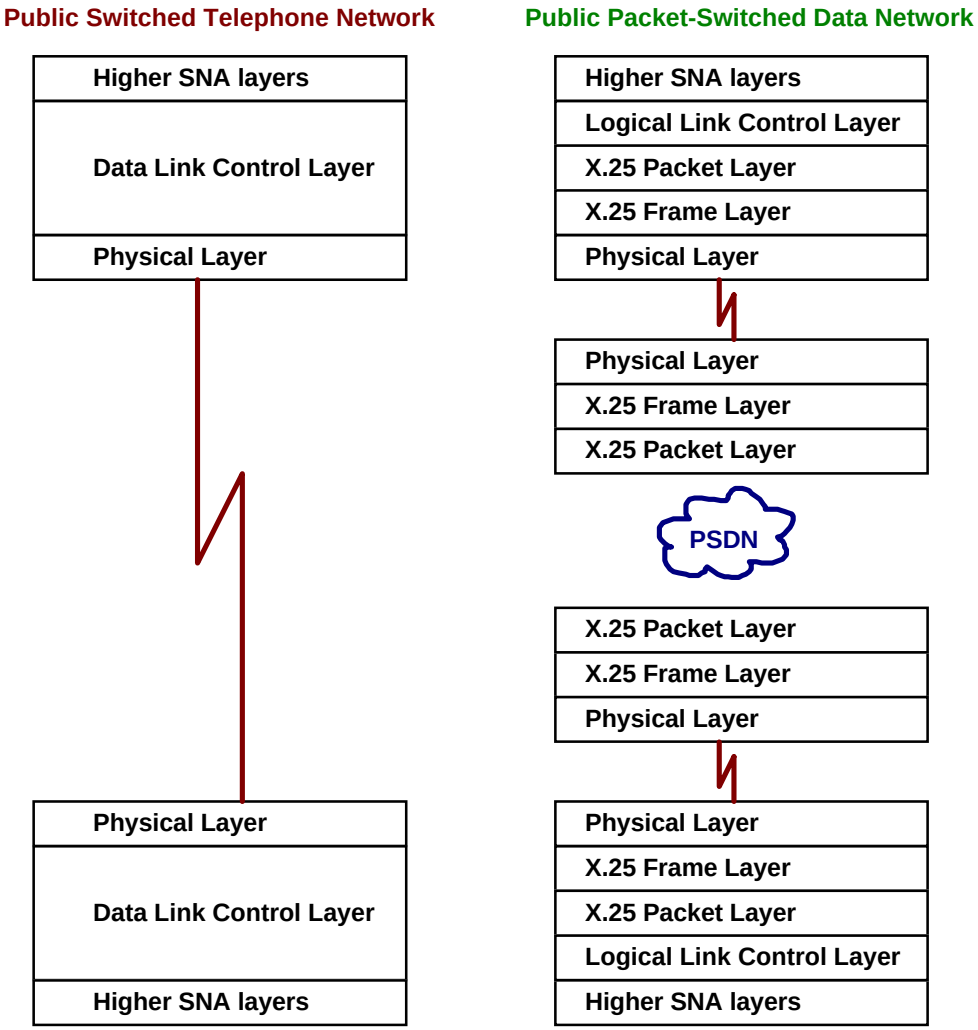
QLLC uses HDLC unnumbered frames, supervisory commands and answers identical to their SDLC counterparts, carried as user data in Q-packets. QLLC commands and responses are initiated by the same higher level events that initiate their SDLC counterparts. As in SDLC, all QLLC commands should have associated timeout processing.

SDLC versus QLLC

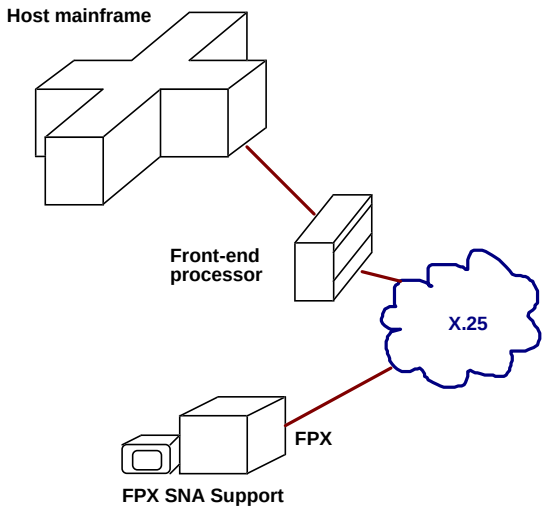
SDLC function	QLLC function
Info	UDP
SNRM/SABM	QSM
DISC	QDISC
XID	QXID
TEST	QTEST
UA	QUA
RD	QRD
RR	QRR
RNR	--
REJ	--
DM	QDM
FRMR	QFRMR

Recapitulative table showing the correlation between SDLC and QLLC functions.

Connecting to an SNA host



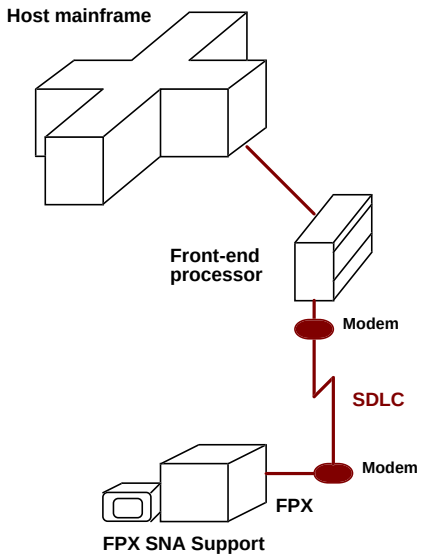
Through the X.25 network



In this example, the FPX adapter associated with the FPX SNA Support program for SNA Server goes through the X.25 line to a 37xx front-end processor and a 3174 communication controller.

Another solution could be represented on the opposite: FPX MPServer should replace FPX SNA Support, when using Windows 95.

Through the switched telephone network



In this example, the FPX adapter associated with the FPX SNA Support program for SNA Server goes through a modem to a 37xx front-end processor and a 3174 communication controller.

General administration guidelines

Windows NT is an operating system combining the safety, the reliability and the power of large systems with user-friendliness and flexibility.
With these assets, Windows NT is an ideal solution for client-server applications.

Windows NT includes sophisticated administration tools fully run by the FPX product, such as:

- Performance Monitor
- Event Viewer
- Registry
- SNMP Service

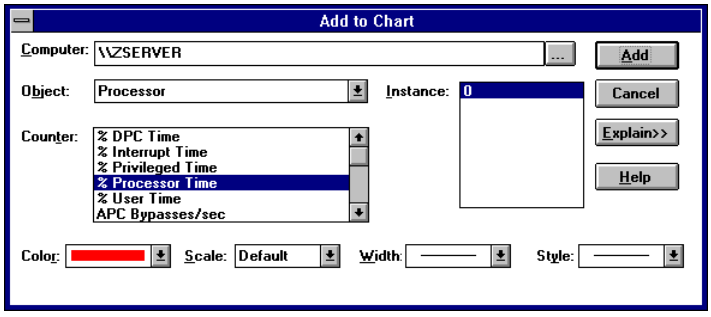
Performance Monitor

This monitoring tool measures computer performances. It is used to carry out the first diagnostic and optimization operations for the computer and workstations linked to the network.

For the performance monitor, the computer is a set of components, including the following:

- Processor
- Memory
- Logical and physical disks
- Network resources, etc.

Each component is an object and its behavior can be viewed by the Performance Monitor.
Windows NT provides a mechanism to add objects and performance counters. The Performance Monitor uses these objects to gather performance information.
Some objects can be provided with multiple instances. For example, a computer may be provided with two physical disks. All instances of the same object have the same counters.

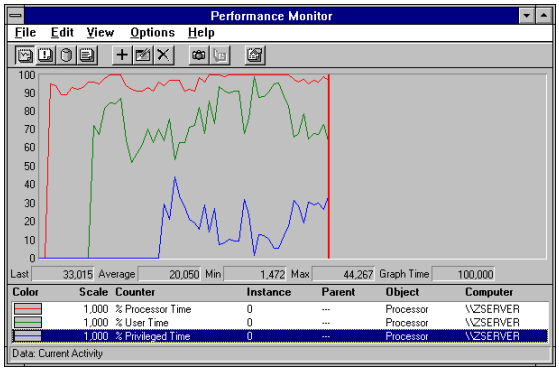


Performance data can be displayed in four different views,

- The chart
- The report
- The alert
- The log

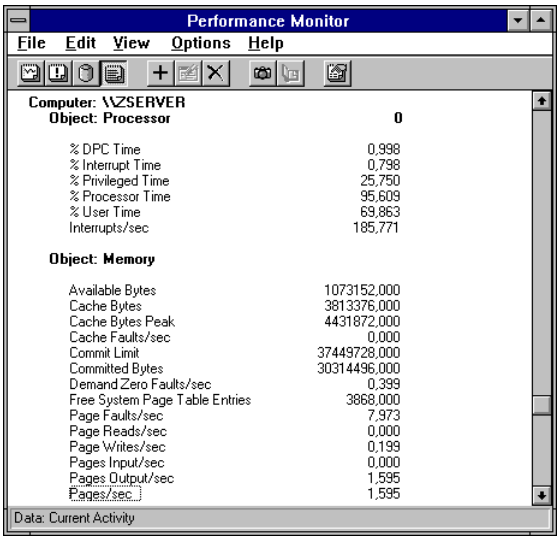
operating independently and concurrently.
Only one can be viewed at a given time.

The chart view



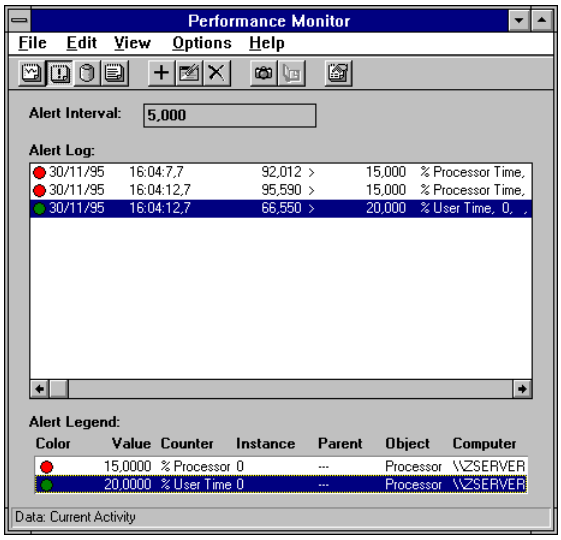
System counters can be viewed responding in real time. Two basic modes are available (graph and histogram).
Graphs are useful for looking at a counter value over time.
Histograms lose historical perspective but are useful when viewing simultaneously many counters.

The report view



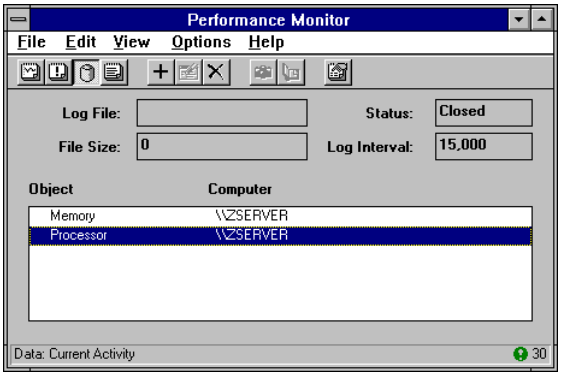
Many counters can be observed at the same time. It is helpful in deciding which counters to place on a chart.

The alert view



A large number of counters can be monitored with minimal overhead.
A threshold value must be defined for each counter that the user wants an alert for. When an alert is triggered, it creates a line in the alert log describing the cause of the alert.
A program can be run either the first time or every time an alert is triggered.

The log view



It is used to save performance information in a log. This log is always available and can be used to avoid displaying complete analysis of the data on the screen.

The Event Viewer

In Windows NT, an event is any significant occurrence in the system or in an application that users should be made aware of.
For some critical events, message boxes may be displayed on the screen. For many other events that do not require immediate attention, Windows NT adds data to an event log file.
The event viewer is used to view and manage event logs. It contains the description of the incidents. The log is updated with no interruption of the work in process. It can be saved to be viewed later or to generate reports.
This event logging service starts up automatically when Windows NT is started.

The event viewer is used to monitor different kinds of events. Windows NT records events in three kinds of logs:

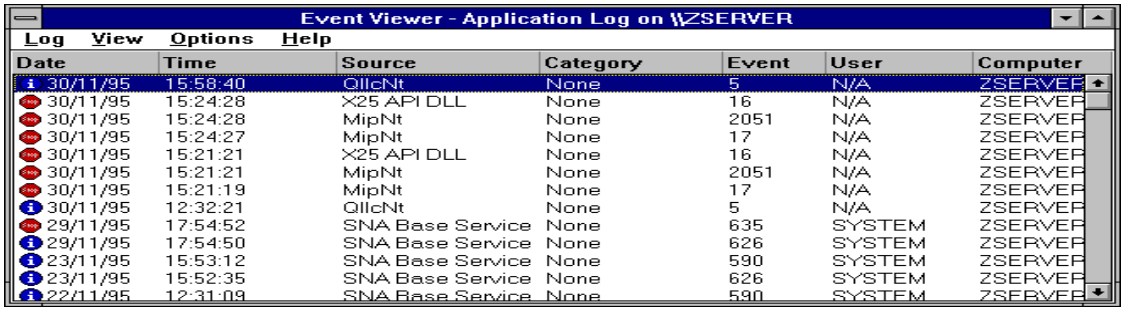
- ***System***
- ***Application***
- ***Security***

The ***system*** log records events logged by the Windows NT system components (for example, the failure of a driver or other system component to load during startup).

The ***application*** log records events logged by applications (for example, the failure of a network service).

The ***security*** log records security events This helps track changes to the security system and identify any possible security breaches.

After selecting a log to be displayed, the user can view, sort, filter and search for details concerning events.
Each line in the log contains data related to one event including the date, time, source, event type, category, Event ID, user account and computer name.



Date	Time	Source	Category	Event	User	Computer
30/11/95	15:58:40	QllcNt	None	5	N/A	ZSERVER
30/11/95	15:24:28	X25 API DLL	None	16	N/A	ZSERVER
30/11/95	15:24:28	MipNt	None	2051	N/A	ZSERVER
30/11/95	15:24:27	MipNt	None	17	N/A	ZSERVER
30/11/95	15:21:21	X25 API DLL	None	16	N/A	ZSERVER
30/11/95	15:21:21	MipNt	None	2051	N/A	ZSERVER
30/11/95	15:21:19	MipNt	None	17	N/A	ZSERVER
30/11/95	12:32:21	QllcNt	None	5	N/A	ZSERVER
29/11/95	17:54:52	SNA Base Service	None	635	SYSTEM	ZSERVER
29/11/95	17:54:50	SNA Base Service	None	626	SYSTEM	ZSERVER
23/11/95	15:53:12	SNA Base Service	None	590	SYSTEM	ZSERVER
23/11/95	15:52:35	SNA Base Service	None	626	SYSTEM	ZSERVER
22/11/95	12:31:09	SNA Base Service	None	590	SYSTEM	ZSERVER

Source specifies the software application that logged the event. This can be either an application name or a system component, such as a driver name.

Category classifies the event according to its source.

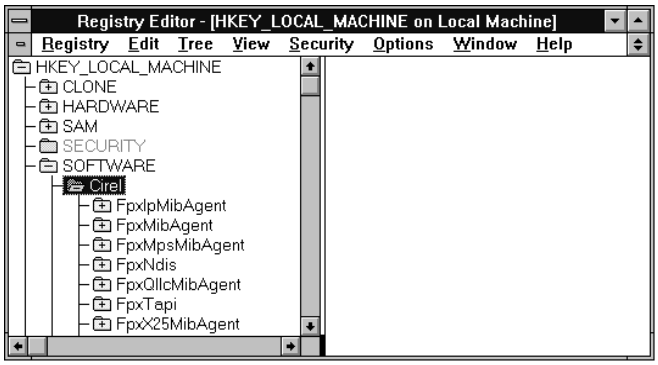
Event is a unique number for each source to identify the event.

User identifies the name of the user who was logged on and working when the event occurred.
Computer specifies the computer name of the computer where the event occurred.

The icon on the left side describes the classification of the event by Windows NT such as error, warning or information.

The Registry

The Windows NT registry is a reliable and consistent database containing all configuration information in a hierarchical form. The administrator uses this structure to access local or remote tools as previously described.



It is accessed from the ***Start*** icon, by selecting **Programs, Administrative tools,** and **Windows NT Diagnostics**.

From the *Windows NT Diagnostics* main screen, click on the *File* menu, then on the *Run* menu to display the dialog box, and double-click on the ***Registry Editor.***

The SNMP Service

When implementing a network component, be it software services or a hardware device, sooner or later it will be necessary to determine how the user will manage the component. Inevitably the user is faced with the question of whether or not it should be remotely managed and, if so, what network protocol should be used.
Network administrators eventually began to demand that all these proprietary management schemes work together. To have these schemes working together enables an administrator to manage any network device, regardless of the manufacturer, from a single management console. Several management schemes have been developed to address this need, with SNMP now being the most widely accepted.

The advantages of using SNMP as the management protocol for the network component are the following:

- SNMP is a well understood and proven technology
- It is not necessary to develop management UI if the user is not interested in tool development
- SNMP is easily integrated with other networking tools
- It can be easily incorporated into larger management frameworks

Because SNMP provides a mechanism for management consoles to learn dynamically about new components, consoles that were written years ago are capable of managing components developed today.

In the SNMP model there is a software component residing on the network device that gathers the related information about that device into a well-defined structure. This software component is referred to as the ***agent***. The agent is responsible for responding to queries and carrying out requests to the network device. The counterpart of the agent is the software component that issues requests. Typically, the results of requests are passed on to some sort of user interface that administrators use to view data concerning the queried device. This component is referred to as the ***manager*** or ***management console***. Typically the agent software and the manager software are running on different network components and are communicating via the network and a common protocol.

The data instrument used by the SNMP agent is organized into collective units that are termed ***management information bases*** or ***MIBs*** for short. MIBS are described via a precise definition language called Abstract Syntax Notation. It makes it possible to define data types and structures and arrays of structures of information on the managed device.

Fundamentally, MIBs define the following for every entity in the agent:

- Association between a device's data entity and a name (object identifier)
- A definition of the data type for that entity
- A textual description of the entity
- How the entity is indexed if the entity is a member of a complex data type
- Access allowed for that entity

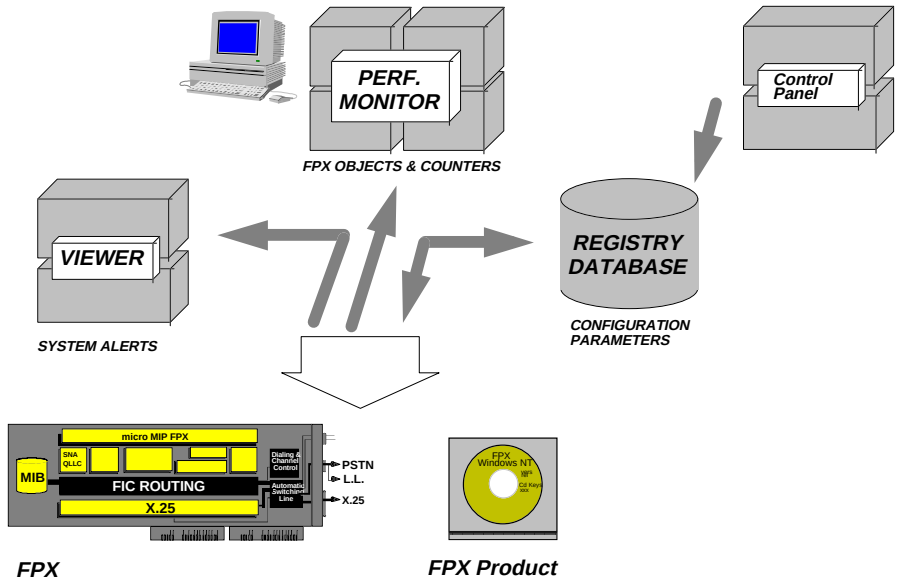
The manager component of SNMP uses MIBs to indicate the structure of the agent data to the SNMP user. Simply put, an SNMP manager console can describe the data on the SNMP agent because it uses the MIB that defines that data to describe it to the user. It is because of this relationship between agents, MIBs and managers that agents created today can work with management consoles that were written years ago.

The Windows NT SNMP service (snmp.exe) is an extendible SNMP agent that developers use to add DLLs to additional service MIBs. The agent itself does not contain instrumentation for any MIBs; instead it is responsible for retrieving SNMP requests for the Windows NT Workstation or Server and passing these requests on to the appropriate DLL for resolution. The response data is then returned to the agent, who is responsible for returning the request to the management station that made it. By default, four extension agent DLLs are shipped with the SNMP service. These DLLs service the MIB-II, LanMan2, DHCP and WINS MIBs.
The extendible agent is also capable of issuing traps on behalf of any of the agent DLLs.

Integration into the System

FPX adapters, servers, and routers are fully integrated in the following Windows NT system management tools:

- The Control Panel
- The Registry
- The Performance Monitor
- The Event Viewer



There are two separate types of management:

- Static management (adapter, software)
- Dynamic management and communication protocols

The FPX software components are interfaced in the system as follows:

- All DLLs, drivers and applications error messages are logged in the Event Viewer in the application and system logs.
- The X.25/QLLC or SDLC link service is installed as a service. It can be stopped or started through the SNA administration program provided by Microsoft or through the ***Services*** icon in the Control Panel.
- The FPX MPServer is installed as a service. It can be stopped or started through the ***Services*** icon in the Control Panel.
- The FPX PassLan/IP, the FPX RAS Support drivers are installed as networks drivers and accessible through the ***Network*** icon in the Control Panel.
- The FPX utilities (automatic adapter loading, services loader) are installed as services accessible through the ***Services*** icon in the Control Panel.

Implementation in the Registry

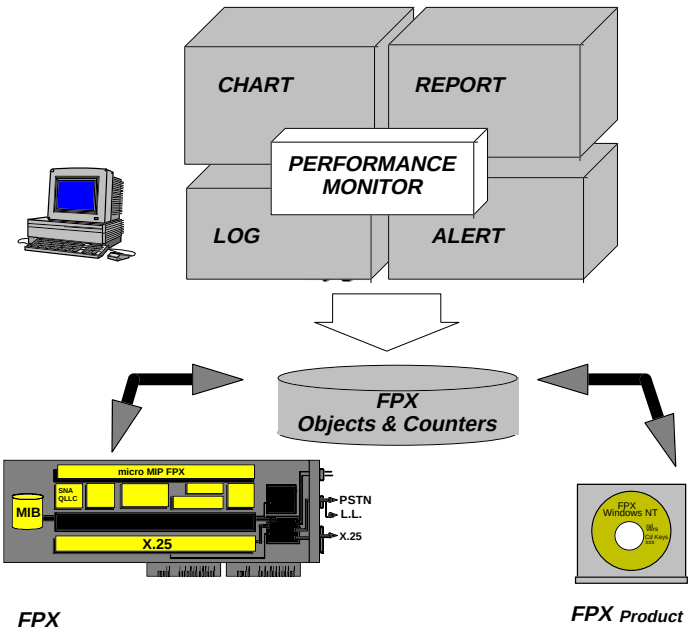
The software components are implemented in the Registry under HKEY_LOCAL_MACHINE in the following main sections:

- HARDWARE\RESOURCEMAP
- HARDWARE\DEVICEMAP
- SOFTWARE\CIREL
- SYSTEM\CurrentControlSet\Services

Integration into the Performance Monitor

Windows NT provides a mechanism to add objects and performance counters. These objects and counters provide the performance monitor with performance data.

Then, it is necessary to create extended objects that will be called when the PERFMON program collects data.



FPX ***FPX Product***

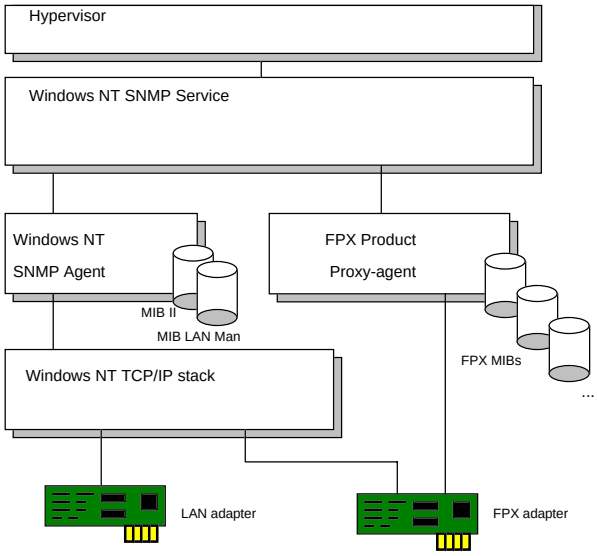
Extended objects for the FPX product are:

- FPX adapter(s)
- FPX MPServer
- The link service for SNA Server
- FPX PassLan/IP
- FPX RAS Support

The SNMP extension DLLs

SNMP administration for the FPX product is integrated into the Windows NT SNMP service functions. There are extensions to the SNMP service that are used for the administration of objects specific to FPX hardware and software components.

SNMP service for Windows NT includes an SNMP agent that administrates the objects in the MIB II INTERNET and in the MIB II Lan Manager. The FPX product provides a proxy agent directly interfaced with the Windows NT SNMP service.



The FPX product includes the following MIBs:

- **FPXADM** MIB: Administration of the FPX adapters and services installed on the computer.
- **FPXX25** MIB: Administration and statistics of the X.25 protocol down-loaded into the FPX adapter.
- **FPXMPS** MIB: Administration and statistics of the FPX MPServer product, BULL, PAD and X.25 multiprotocol server.
- **FPXIP** MIB: Administration and statistics for the FPX Passlan/IP router.
- **FPXQLLC** MIB: QLLC statistics for the FPX SNA Support product.
- **FPXPROXY** MIB: Administration and statistics of FPX remote adapters.

The SNMP manager console must know these MIBs. Please refer to the associated files on the CD-ROM labeled FPX Communication Services for Windows NT.

These MIBs must be compiled with an MIB compiler (usually supplied with the administration console).

The FPX MIBS are integrated in the following tree:

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) .
. fpxadm (1)
. fpxmps (2)
. fpxip (3)
. fpxqllc (4)
. fpxx25 (5)
. fpxproxy(6)

The FPX BackUp features

It is a tool delivered with FPX SNA Support and/or FPX MPServer components.

The FPX BackUp on Windows NT offers backup functions that are used, in case of unavailability or of a problem with the network, to automatically switch from one X.25 or ISDN number to another.

These functions are used for:

- QLLC (FPX SNA Support) connections
- X.25 (FPX MPServer) connections
- BULL (FPX MPServer) connections

The FPX BackUp configuration program is integrated as a **Service**, and associates a backup X.25/ISDN number to a main X.25/ISDN number.

From a main network address, backup parameters can be defined associated with:

- *Backup Criteria* (backup made on defined or undefined clears)
- *Recovery criteria* (no recovery, recovery on idle period, or recovery on timeout)

This allows, if a problem occurs on the *Primary* link to work on the *Secondary* link.

To go back to the initial link, 2 modes can be used:

- one option to avoid important communication costs (once the link is active again, the return is immediate)
- one option showing the service quality: the return is dynamically made for the new connection requests but the active connections on the Secondary link stay on this link.

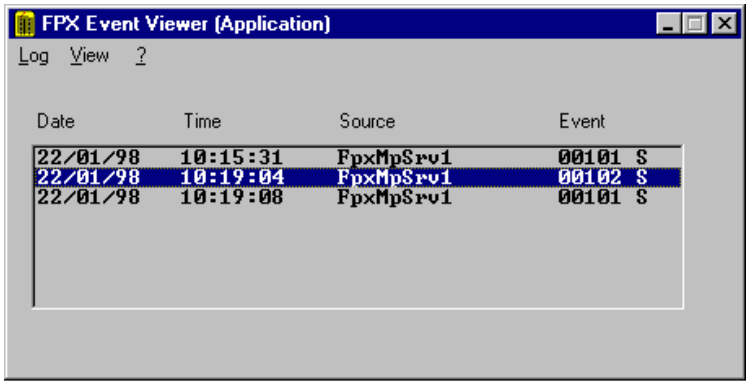
Windows 95 tools

Windows 95 has an architecture that supports preemptive multitasking, multithread execution, protected address space, and 32-bit Windows programs while maintaining backward compatibility with Windows 3.1.

Windows 95 has an increased number of System Management options available for administrators to use for great flexibility and control of the corporate Windows 95 networking environment such as Registry,...

The *FPX Event Viewer* Cirel tool can be used to view and manage event logs. It is added to the **Start Menu Programs** in the **FPX Communication Services** task.

The main screen is represented below, and the use principle is identical to the one described in the Event Viewer NT section.



Each line in the log contains data related to one event including date, time, source, event type,...

- Click on a selected line to obtain the *Event detail* screen with information related to the event. (Be careful : the date displayed is the reading date).

CHAPTER 3

Setting up FPX adapters

3

This chapter describes how to start the FPX hardware components.

Installing the hardware

The FPX Product includes one FPX adapter in a Windows 95 machine or several FPX adapters that must be installed in a Windows NT Server machine.

Checklist

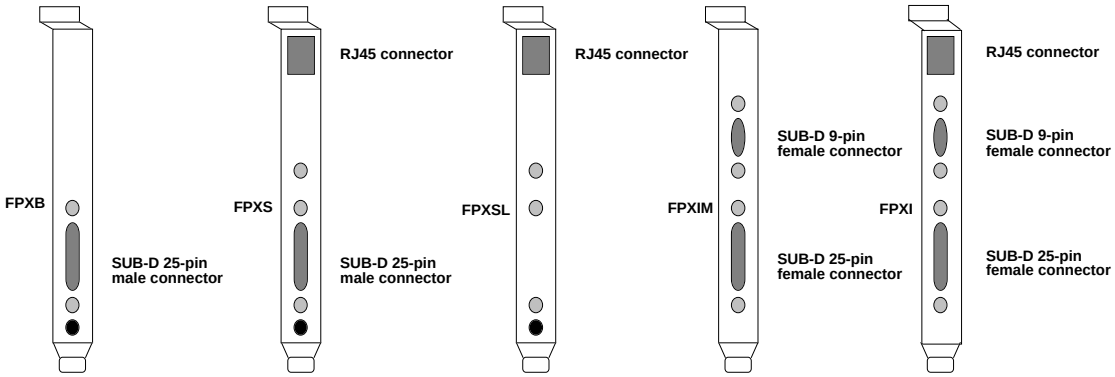
FPX type	Cable
FPX/B	3-meter cable / V28 electrical interface male/female
FPX/B-AS (ISA or PCI)	3-meter cable / V28 electrical interface male/female One adapter male/male SUB-D 26-pin high density / SUB-D 25-pin
FPX/I (only for France)	Interface line and one adapter male/male SUB-D 26-pin high density / SUB-D 25-pin. The other cables are delivered on option.
FPX/IM (only for France)	Interface line and one adapter male/male SUB-D 26-pin high density / SUB-D 25-pin. The other cables are delivered on option.
FPX/S	3-meter cable / V28 electrical interface male/female 5-meter ISDN cable
FPX/SL	5-meter ISDN cable
FPX/S-AS (ISA or PCI)	3-meter cable / V28 electrical interface male/female One adapter male/male SUB-D 26-pin high density / SUB-D 25-pin 5-meter ISDN cable

Since the FPX/B-AS and the FPX/S-AS adapters can also operate with V11, V28 or V35 electrical interfaces, the appropriate cables can be supplied optionaly.

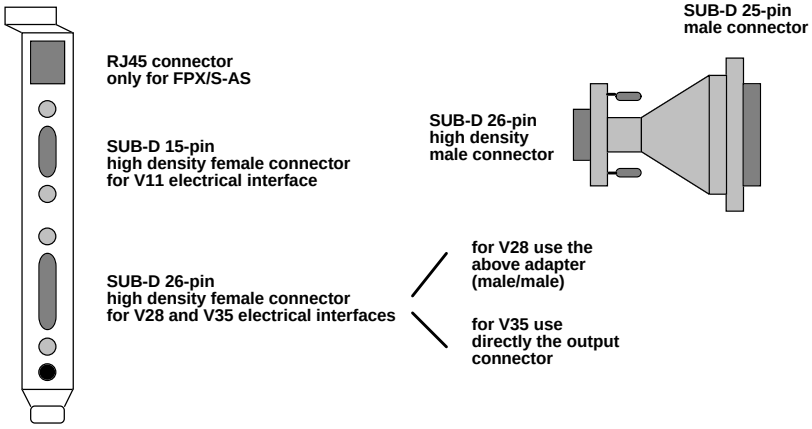
Notes: The FPX/B-AS and the FPX/S-AS are referenced as FPX/B and FPX/S further in this guide since the only difference consists in the electrical interface. The FPX/SL is also referenced as FPX/S further in this guide (this adapter is a strict ISDN adapter).

The following figures show the various FPX brackets.

FPX/B & FPX/S & FPX/SL & FPX/IM & FPX/I



FPX/B-AS & FPX/S-AS



Configuring FPX hardware

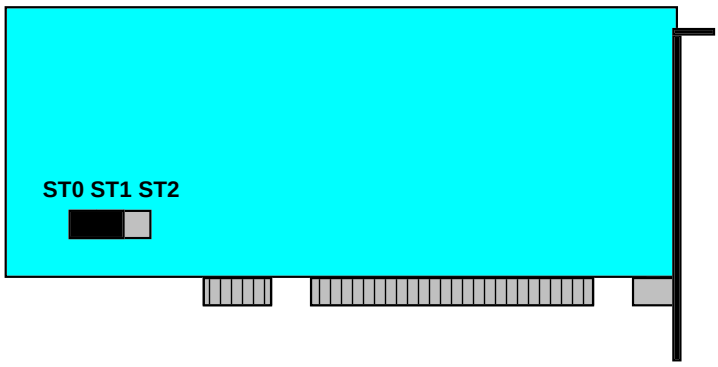
The only parameter that can be physically set on the FPX adapter is the Input/Output port address, but if the adapter is a PCI adapter, there is no hardware configuration.
Jumpers must be set as follows:

I/O Port Address	Jumper Settings		
	ST0	ST1	ST2
300H	■	■	■
310H		■	■
320H	■		■
330H			■
340H	■	■	
350H		■	
360H	■		
370H			

■ signals the presence of a jumper

Shipped with address: **340H**

If the user works on Windows 95, there is no selection for I/O Port Address, IRQ... with a PCI adapter.



Multi-adapter installation

The FPX Communication Services for Windows NT supports up to four FPX adapters providing for different types of connections. The adapters must be installed in the PC, as explained previously.
The user must check the IRQ, I/O address and memory segment addresses to avoid conflicts (refer to the Windows NT Diagnostic application in the Administrative tools for help in determining the available features).

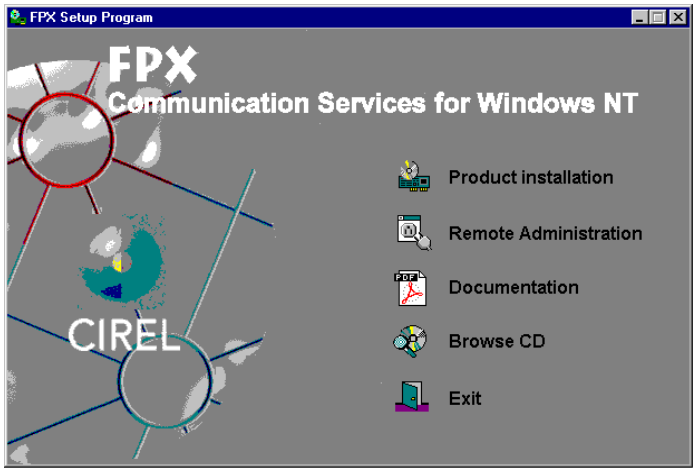
Automatic installation

This product includes an Autorun setup software, guiding the user when installing the different components.

Follow these steps to install the FPX Communication Services correctly:

- Insert the delivered CD-ROM into the appropriate drive to display the main screen installation, or execute the **FPXSETUP.EXE** program.
- Click on the 

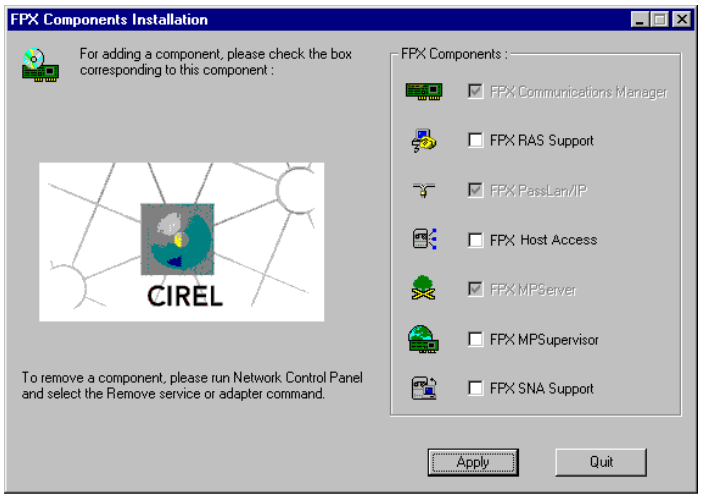
to continue the automatic process.



The other buttons are respectively used to administrate a remote configuration, execute the documentation help and scan the physical support.

- Check the box corresponding to the component to install, then validate by clicking on 

.



Note:
On Windows 95

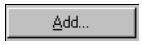
- The PCI adapters are detected when the system is started.
- The installation principle stays identical to this one described above, but only some of the components are included.
- Be careful: Reboot the PC at the end of the installation.

Software installation

This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.

The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM in the appropriate drive.
- Most tasks can be launched from the *Startup* menu. Clicking on the 

button lets the user access a list of function keys.
- From *Settings*, run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Adapters* tab, then click on 

to display the *Select Network Adapter* dialog box.
- Click on 

then enter the following path: "%**unit**%**\I386\card**". Validate by clicking on 

to continue the automatic process.
- When the setup is complete, the **FPX Communication Services** task and the associated utilities are added to the **Start Menu Programs.**

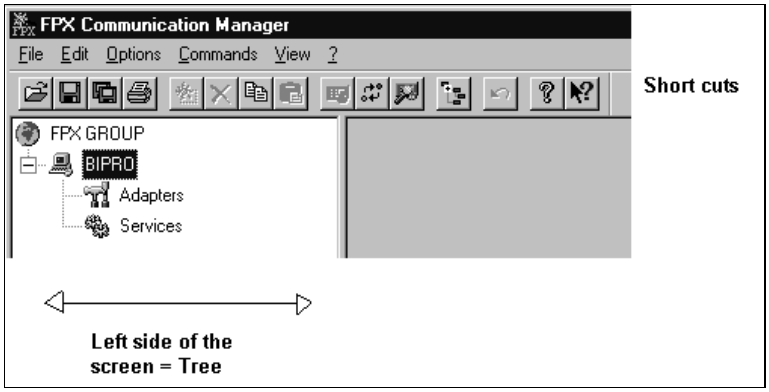
Some differences exist on Windows 95.
An *Install/Desinstall* entry is added on Windows 95.

- Select **FPX Communication Manager,** first to define the Adapters settings.

Configuration process

Overview

- From the *FPX Communication Services* task, double-click on **FPX Communication Manager** to go to the main screen.



The application screen can be divided in several parts as showed on the diagram.

This example represents the *BIPRO* machine, on which the software installation has been successfully made.
The *Adapters* settings are described in the following sections.
The *Services* settings are described in independent chapters, according to the selected services.

Menus description

The menus and their associated commands, described in the following table, are accessible by clicking on them. Some of these commands can be used by directly clicking on the shortcuts.

Menus/commands	Capabilities
File	
Open...	Recover the remote machine configuration
Save	Save the selected machine
Save All	Save the configuration (adapters, services, machines)
Backup*	Backup a local or a remote configuration
Restore*	Restore a local or a remote configuration
Print...	Print the sub-tree, from the selected object
Print Setup	Select a printer and the connection settings
Fonts...	Select the style and size of the font, used to print
Exit	Quit the program
Edit	
Cancel	Clear the screen as if using the Esc key
New object	Add a new object
Cut	Remove an object
Copy	Copy the selected data to the clipboard
Paste	Paste the data contained in the clipboard
Options	
Read report	When checked, report viewing on the FPX adapter loading and initializing
Trace window	When checked, view on the exchanges between the local or remote machine
Read IP configuration	IP configuration recovery (local or remote)
Read MPServer configuration	MPServer configuration recovery (local or remote)
Read BackUp configuration	BackUp configuration recovery (local or remote)
Commands	
Immediate loading	Launch the loading of one or more configured adapters
Report	Report the last loading
Diagnostic refresh	Refresh the information (equivalent to F5)
Diagnostic tool	Load the FPX Diag program
Dynamic IP driver	Update a new IP configuration dynamically (local or remote)
Dynamic RAS driver	Update a RAS configuration dynamically (local or remote)
Dynamic X25Passport	Update a new X25Passport configuration dynamically (local or remote)
Start the MPServer service	Start the service MPServer
Stop the MPServer service	Stop the Service MPServer
View	
Toolbar	Display/hide the Toolbar
Status bar	Display/hide the Status bar
Split window	Give the screen the correct proportion (vertical direction)
Expand tree	Display the tree, according to a selected object
? (Help)	
Help Contents	Provide online information about commands and fields
About FpxNT40...	Display the version information

* The *Backup/Restore* commands can be manually or automatically executed. Refer to the last section in this *Chapter*, for more information.

Toolbar

The toolbar is displayed above the application window, under the Menu bar. The various buttons are used to rapidly access to the different objects in the application, by clicking on the selected icon.
To display or not the toolbar, select the *View* menu, then the *Toolbar* command.

Open an existing configuration (remote or local connection).
The command *FPXNT40.exe -NAME netbios name or ipad* can be also used.

Save the selected object (adapter, service, machine).

Save all parameters (adapter, service...).

Print the active document.

Insert a new object only on Windows NT (it is automatically added on Windows 95).

Delete selected data.

Copy selected data in the clipboard.

Paste the data contained in the clipboard.

Load the selected adapter.

Diagnostic refresh.

Diagnostic tool.

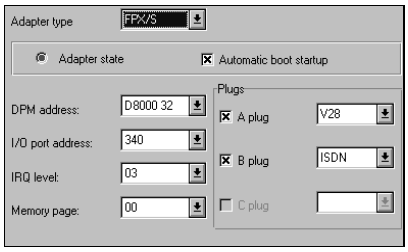
Display all the tree.

Undo the last action.

The adapters

Creating an FPX adapter

- From the *FPX Communication Manager* screen, select *Adapters* then click on the  icon, to define the settings for one FPX telecommunication adapter (FPX01).



The screen is used to modify settings pertaining to hardware, and to display some information.
The values must be filled in according to **hardware configuration** determined by the type of adapter installed in the computer. If multiple adapters have been installed, be careful to configure each adapter properly in order to avoid hardware conflicts.

This window is used to set applicable parameters in the adapter configuration software component:

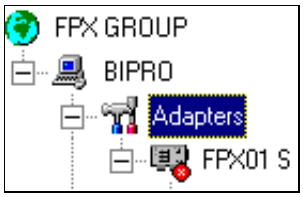
- To select a parameter, click on  .
- A scroll down list shows possible values according to the system NT RAM, I/O, IRQ resources... Click on the value to be selected.

- Some elements are automatically displayed and grayed, when the adapter is a PCI adapter on Windows NT, or a PCI or ISA adapter on Windows 95.

Describing the parameters

Parameter	Meaning
Adapter type	FPX/B, FPX/B-AS, FPX/I, FPX/IM, FPX/S, FPX/S-AS, FPX/SL.
Automatic boot startup	When checked, the adapter is automatically loaded on a restart machine.
DPM address	Dual Port Memory Address
I/O port address	Input/Output port address used to communicate with the adapter
IRQ level	Interrupt level to access the adapter, detected by the System if the adapter is a PCI adapter (the value is automatically assigned).
Memory page	This parameter can be used to set the FPX dual port memory in another megabyte address segment in the computer. Page 00 corresponds to the first mega, page 01 to the second one and so on up to sixteen. Default value = 00 (use cautiously)
A plug	Electrical interface on the A-channel (depends on the FPX used)
B plug	Electrical interface on the B-channel (depends on the FPX used)
C plug	Electrical interface on FPX/I and FPX/IM only
Slot number	Only detected on PCI adapter.

- When all parameters have been filled in, click on the  icon, to save them.



When an FPX adapter is created, the tree is modified.

This example represents the BIPRO machine, on which the first adapter (by default FPX01) has been created and defined by the user as an FPX/S adapter.

Note: The electrical interfaces are displayed on the left side of the screen (tree), under the name adapter according to the type of adapter installed. The user have to configure the line protocols for the different channels supported by the adapter.

Modifying an FPX adapter

- Click on the sigle + in front of the 

icon to see all the created adapters, (4 maximum on Windows NT) displayed under the *Adapters*.
- Select the adapter by clicking on its name to make change(s) if necessary, then click on the  icon to save the new configuration.

Adding a new FPX adapter

- From the *Adapters* label, on the left side of the screen (tree), click on the  icon to add a new adapter, define the settings, then click on the  icon to save the new configuration - on Windows NT only -.

Removing an FPX adapter

- Select an adapter by clicking on its name, then click on the  icon, and click on the  icon to save the new configuration -on Windows NT only-.

The links

Different links are available according to the FPX adapter type and the plug configuration. Most FPX adapters include an Integrated Switching Function for the user to select, by means of a switching prefix, the physical output on the adapter. It is then the application's responsibility to choose the communication network to establish a communication pipe with a stand-alone computer or a remote server.
For the FPX/S, FPX/S-AS, FPX/S-AS PCI, FPX/I and FPX/IM, the X.25, PSTN or ISDN calling number must be preceeded by the *switching prefix* configured for each type of network access.

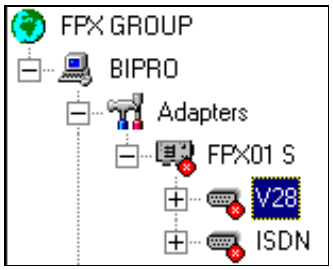
Switching prefix examples: X.25 number = 133010203

- V28, V11, V35 access **1**133010203
- X.25 on D **4**133010203
- ISDN/X.25 **0**133010203
- X.25 on B **33**133010203
- Transparent on B **30**133010203
- X.32 Modem **20**133010203
- P to P Modem **21**133010203

Note: The FPX/B adapter uses a switching prefix only with the V.25bis mode.

Configuring the V28 plug for an FPX/S

- From the *V28* label, on the left side of the screen (tree) configure the line protocols.



- Click on 

.

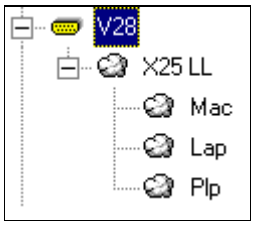
Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. The X.25 number of the remote address must include this prefix at the heading (default value = 1).
X25/X32	Checked: selection of the access type. • Leased line up to 64Kb/s on V11 interface • V27 ter (half duplex) • V32 (full duplex) Leased line: used when the FPX is directly linked to a public or private X.25 network. V27 ter: CCITT recommendation relative to 4800/2400bps standard modem for the Public Switched Telephone Network. The basic speed to access the French X.25 public network (Transpac) is 2400bps in semi-duplex mode. V32: CCITT recommendation relative to the standardized modem up to 9600bps. To access the French X.25 public network (Transpac), the speed is 9600bps in duplex mode. In case of a poor transmission quality, the modem will negotiate an automatic speed decrease to 4800bps in duplex mode.
Frame relay	HDLC synchronous protocol used to take advantage of the flow rate.

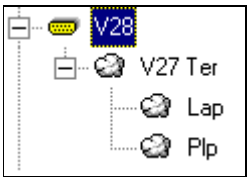
Note:
X.32 is an extension used to access the X.25 packet switched data network through the switched telephone network.

Depending on the previous selection (**X25/X32**), the result of the trees is different but whatever the choice made by the user is, settings divided into three levels must be configured:

- **M**edia **A**ccess **C**ontrol level
- **L**ink **A**ccess **P**rotocol level
- **P**acket **L**ayer **P**rotocol level

For more information, refer to the X.25 Public Network subscription or to the private subscription features.





- If the option **Leased line** has been checked, click on 

then on 

then on 

.

Parameter	Meaning
Speed	Line speed transmission set in units of bits per second. It allows the gauging of the X.25 timeout and the potential supplying of a clock. Available choices: 300, 600, 1200, 2400, 4800, 9600, 19200, 48000 or 64000
Clock	Clocking origin External: supplied by the network Internal: supplied by the FPX adapter
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
Equipment	Equipment operating mode DTE: Data Terminal Equipment DCE: Data Circuit Terminating Equipment
T1 timer	This is the maximum time (in milliseconds) between a frame transmission and the reception of its acknowledgement. When this time has elapsed, the frame is transmitted again. It depends on the transmission speed and the frame length. Available choices: 100, 200, 400, 800, 1600 or 2550
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Restart mode	Function allocated to the data link. Available choices: None, Responder, Initiator, Negotiator
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Incoming: first incoming logical channel Outgoing: first outgoing logical channel Both: first two-way logical channel
Last number of VC	Incoming: last incoming logical channel Outgoing: last outgoing logical channel Both: last two-way logical channel

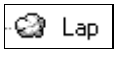
Parameter	Meaning
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in packet window, packet size and throughput class. If a negotiation for "window size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

- When all parameters have been filled in, click on the  icon to save the settings.

- If the option **V27Ter** has been checked, click on  then on  .

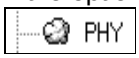
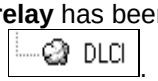
Parameter	Meaning
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
XID identification	When checked, fill in ID and SIG parameters, assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields.
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128 or 256
First number of VC	Incoming: first incoming logical channel Outgoing: first outgoing logical channel Both: first two-way logical channel
Last number of VC	Incoming: last incoming logical channel Outgoing: last outgoing logical channel Both: last two-way logical channel

- When all parameters have been filled in, click on the  icon to save the settings.

- If the option **V32** has been checked, click on  then on  .

Parameter	Meaning
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
XID identification	When checked, fill in ID and SIG parameters assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields.
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128 or 256
First number of VC	Incoming: first incoming logical channel Outgoing: first outgoing logical channel Both: first two-way logical channel
Last number of VC	Incoming: last incoming logical channel Outgoing: last outgoing logical channel Both: last two-way logical channel

- When all parameters have been filled in, click on the  icon to save the settings.

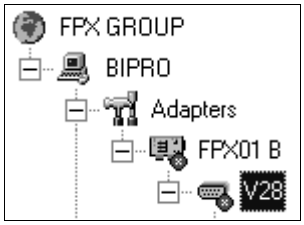
- If the option **Frame relay** has been checked, click on  then click on  then on  .

Parameter	Meaning
LMI protocol	Local Management Interface. Permanent Virtual Circuit signalization protocol. Default value = LMI Available values: None, ITU, ANSI or LMI
Full status polling state (N391/N1)	Request cycle for global state. Default value = 6 Value from 1 to 255
Error threshold (N392/N2)	Counter from 1 to 10 Default value = 3
Monitored events count (N393/N3)	Events number displayed from 1 to 10 Default value = 4
Link integrity verification timer (T393/T1)	Timeout checking the link. Value from 5 to 30 secondes, multiple of 5. Default value = 10
PHY	• Speed: 64000 • Clock: Clocking origin External or Internal.
DLCI	Data Link Connection Identifier For each DLCI, enter the *DLCI* and the *Throughput* parameters: • DLCI: Numeric value from 16 to 1007 • Throughput: numeric value from 4 to 64 for 1Kbit/s to 64 Kbits. • Services: FPX PassLan/IP or FPX Host Access.

- When all parameters have been filled in, click on the  icon to save the settings.

Configuring the V28 plug for an FPX/B

- From the *V28* label, on the left side of the screen (tree) configure the line protocols.



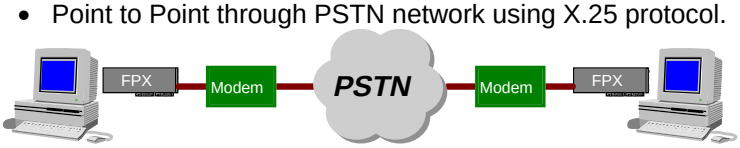
- Click on 

  Select the **X25/X32** option.

Parameter	Meaning
X25/X32	Checked: selection of the access type. • Leased line • V25bis 108/1 • V25bis 108/2 (PABX prefix and PSTN number) Leased line: Used when the FPX is directly linked to a public or private X.25 network. V25bis 108/1 or V25bis 108/2: This configuration must be used when the FPX/B card is directly equipped with an external modem that can be either a standard synchronous modem or a smart HDLC synchronous modem with V.25 bis capabilities. V25bis 108/1: The number is stored in the modem. V25bis 108/2: The application manages the number.
SDLC	The Synchronous Data Link Control is used with the FpxSDLC link service for Microsoft SNA Server.
Transparent mode	Transparent mode is very useful for forwarding data when using Point-to-Point protocol to interconnect with third party equipment.
Frame relay	HDLC synchronous protocol used to take advantage of the flow rate.

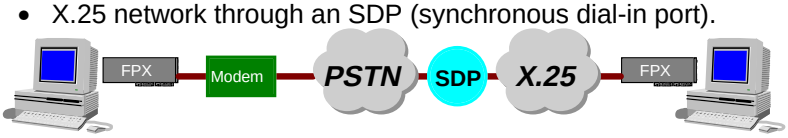
Note:

- Point to Point through PSTN network using X.25 protocol.



or

- X.25 network through an SDP (synchronous dial-in port).

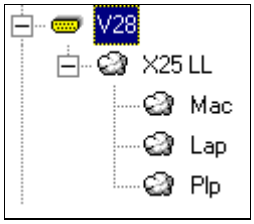


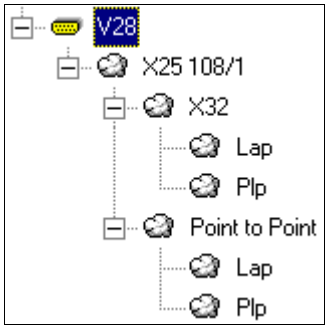
The remote site can be called using the following modes:

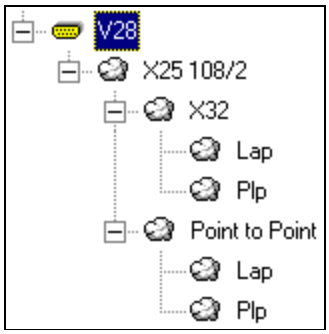
[108/1] Modem stored:
The PSTN number is stored in the modem, and is dialed when the DTR signal is set on the modem. The connection can be performed using either a standard modem or a V.25 bis modem.

[108/2] SDP or Point to Point:
HDLC frames are exchanged between the FPX and the V.25 bis modem. The V.25 bis dialing command puts the PSTN number in one of these frames. When the connection is established, X.25 frames are exchanged transparently between the FPX and the modem. The half or full-duplex transmission type is only used at this level.

Depending on the previous selection (**X25/X32**), the result of the trees is different but whatever the choice made by the user is, settings must be configured, as described below:







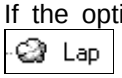
- If the option **Leased line** has been checked, click on 

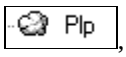
then on 

then on 
.

Parameter	Meaning
Speed	Line speed transmission set in units of bits per second. It allows the gauging of the X.25 timeout and the potential supplying of a clock. Available choices: 300, 600, 1200, 2400, 4800, 9600, 19200, 48000 or 64000
Clock	Clocking origin External: supplied by the network Internal: supplied by the FPX card
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement. Value from 1 to 7
Equipment	Equipment operating mode DTE: Data Terminal Equipment DCE: Data Circuit Terminating Equipment
T1 timer	This is the maximum time (in milliseconds) between a frame transmission and the reception of its acknowledgement. When this time has elapsed, the frame is transmitted again. It depends on the transmission speed and the frame length. Available choices: 100, 200, 400, 800, 1600 or 2550
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement. Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Restart mode	Function allocated to the data link. Available choices: None, Responder, Initiator and Negotiation.
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Permanent: first permanent logical channel Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel
Last number of VC	Permanent: last permanent logical channel Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*

Parameter	Meaning
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

- If the option **X25 108/1** has been checked, define the **X32** settings by clicking on 

and on 

, then define the **Point to Point** settings.

Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 1 if X32, and default value = 2 if Point to Point.
Mode	Operating mode to be selected between Half Duplex and Full Duplex. Half: Transmission and reception cannot occur simultaneously. Full: Transmission and reception can occur simultaneously. This option is only used when V.25 bis commands have been exchanged between the card and the modem, i.e. during the X.25 data transfer.
Using default prefix for incoming call	When checked, the default switching for incoming calls is used.
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement. Value from 1 to 7
Equipment	Equipment operating mode DTE: Data Terminal Equipment DCE: Data Circuit Terminating Equipment
T1 timer	This is the maximum time (in milliseconds) between a frame transmission and the reception of its acknowledgement. When this time has elapsed, the frame is transmitted again. It depends on the transmission speed and the frame length. Available choices: 100, 200, 400, 800, 1600 or 2550
XID identification	When checked, fill in ID and SIG parameters, identifiers consisting of 32 hexadecimal characters, assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields (only if X32).
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel
Last number of VC	Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel

Parameter	Meaning
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

- If the option **X25 108/2** has been checked, enter the PABX prefix and the PSTN number, then define the **X32** settings by clicking on 

and on 

, then define the **Point to Point** settings.

Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 1 if X32, and default value = 2 if Point to Point.
Mode	Operating mode to be selected between Half Duplex and Full Duplex. Half: Transmission and reception cannot occur simultaneously. Full: Transmission and reception can occur simultaneously. This option is only used when V.25 bis commands have been exchanged between the card and the modem, i.e. during the X.25 data transfer.
Network type	Configuration depending on the telephone installation PSTN/DTMF or PSTN/Pulse. To determine the network type used, press a key on the phone: PSTN/DTMF: If a musical note is heard, it is DTMF (multifrequency). PSTN/Pulse: If a clicking is heard, as on old telephones, then select Pulse. Selecting one of these two network types determines the type of V.25 bis command that will be used when dialing (CRN command)
Using default prefix for incoming call	When checked, the default switching for incoming calls is used.
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement. Value from 1 to 7
Equipment	Equipment operating mode DTE: Data Terminal Equipment DCE: Data Circuit Terminating Equipment
T1 timer	This is the maximum time (in milliseconds) between a frame transmission and the reception of its acknowledgement. When this time has elapsed, the frame is transmitted again. It depends on the transmission speed and the frame length. Available choices: 100, 200, 400, 800, 1600 or 2550

Parameter	Meaning
XID identification	When checked, fill in ID and SIG parameters, identifiers consisting of 32 hexadecimal characters, assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields (only if X32).
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel
Last number of VC	Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

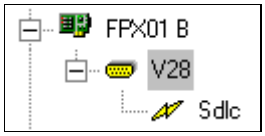
- When all parameters have been filled in, click on the  icon to save the settings.

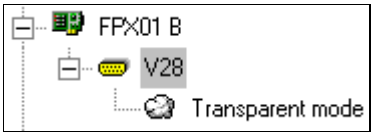
Notes:

- From the *V28* label, the line protocols selection can be also **SDLC**, **Transparent** or **Frame relay**. For the two first selections, parameters are set transparently. The user does not need to define the configuration. For **Frame relay** selection, it is necessary to describe parameters as noted in the next page.

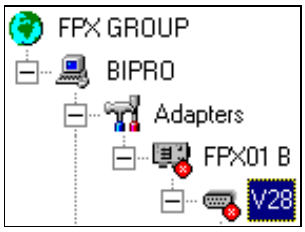
- The only product that can take place with this option SDLC is the FpxSDLC link service for SNA Server.

- In the two cases **SDLC** and **Transparent**, the update (on the left side of the screen) is immediate and represented as below:





- From the *V28* label, on the left side of the screen (tree) configure the line protocols.



- Click on 

.

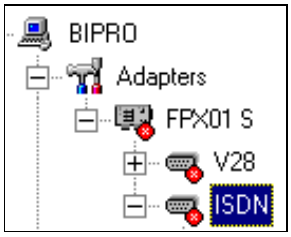
  Select the **Frame relay** option.

Parameter	Meaning
LMI protocol	Local Management Interface. Permanent Virtual Circuit signalization protocol. Default value = LMI Available values: None, ITU, ANSI or LMI
Full status polling state (N391/N1)	Request cycle for global state. Default value = 6 Value from 1 to 255
Error threshold (N392/N2)	Counter from 1 to 10 Default value = 3
Monitored events count (N393/N3)	Events number displayed from 1 to 10 Default value = 4
Link integrity verification timer (T393/T1)	Timeout checking the link. Value from 5 to 30 secondes, multiple of 5. Default value = 10
PHY	• Speed: 64000 • Clock: Clocking origin External or Internal.
DLCI	Data Link Connection Identifier For each DLCI, enter the *DLCI* and the *Throughput* parameters: • DLCI: Numeric value from 16 to 1007 • Throughput: numeric value from 4 to 64 for 1Kbit/s to 64 Kbits. • Services: FPX PassLan/IP or FPX Host Access

- When all parameters have been filled in, click on the  icon to save the settings.

Configuring the ISDN plug

- From the *ISDN* label, on the left side of the screen (tree) configure the line protocols.

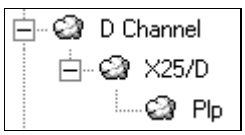


- Click on 

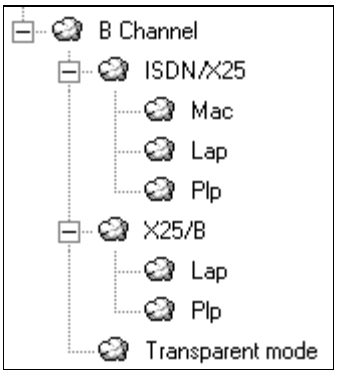
.

The **I**ntegrated **S**ervice **D**ata **N**etwork plug is used to establish:

- X.25 communication on the D-channel
- ISDN/X.25 (SDP), X.25 or Transparent protocol on the B-channel



The **D-channel** is used for connections up to 9600 bps.
X25/D is a specific service that may be provided on the ISDN network (for example, on the French ISDN network, Numeris is available from France Telecom).



The **B-channel** authorizes all digital links at 64 Kbits from ISDN allowing transmission and reception of phone information or data.

ISDN/X25 is used to interconnect to X.25 networks via ISDN networks. It acts as an interworking gateway.

X25/B allows data forwarding on X.25 mode.

Transparent mode is useful for forwarding data when using Point-to-Point protocol to interconnect with third party equipment.

- In the two cases, enter the *Local ISDN address* to identify the calling address (incoming call through a PABX), then according to the D or B-channel selection, fill in the following parameters.

D-channel

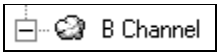
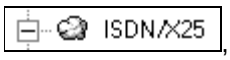
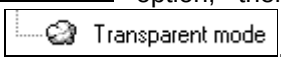
- Select the D Channel option, then click on X25/D, then on Plp.

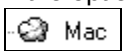
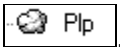
Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 4.
TEI number	Network subscription number for the use of X.25 on D-channel (Terminal Equipment Identifier). Default value = 1. Available values: from 1 to 63 for a non-automatic user equipment.
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128 or 256
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 10
First number of VC	Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel
Last number of VC	Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.

Parameter	Meaning
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

- When all parameters have been filled in, click on the  icon to save the settings.

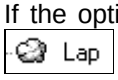
B-channel

- Select the  option, then click on  , or on  or on  .

- If the option **ISDN/X25** has been checked, fill in the following parameters, then click on  then on  then on  .

Parameter	Meaning
DDI	Check the Direct Dialing in Use option, if the selection is direct on arrival. In this case the Local ISDN address is grayed.
Local ISDN address	Main address to be filled in, if the previous option is not checked.
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 0.
Local ISDN address	Main address, common to all different profiles.
Local ISDN sub-address	Switching prefix needed for incoming calls, by default fitting the prefix value. If the area is blank, no filtering is done: the first profile is used.
ISDN/X25	• Address: SDP number. • Sub-address: Calling ISDN sub-address for incoming calls. (Access to the Public Switched Data Network using the B-channel: it refers to the X.31 case A recommendation).
Speed	Line speed transmission set in units of bits per second. It allows the gauging of the X.25 timeout and the potential supplying of a clock. Available choices: 300, 600, 1200, 2400, 4800, 9600, 19200, 48000 or 64000
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement. Value from 1 to 7
XID identification	When checked, fill in ID and SIG parameters, identifiers consisting of 32 hexadecimal characters, assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields.
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement. Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel

Parameter	Meaning
Last number of VC	Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

- If the option **X25/B** has been checked, fill in the following parameters, then click on 

then on 

.

Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 33.
Local ISDN address	Main address, common to all different profiles.
Local ISDN sub-address	Switching prefix needed for incoming calls, by default fitting the prefix value. If the area is blank, no filtering is done: the first profile is used.
Incoming call identification with ISDN address	When checked, the calling address provided by the card is the ISDN network calling address. If not, it is the local address.
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128, 256, 512, or 1024
Throughput class	Statement relative to the maximum throughput for the DTE Available choices: 5 to 13 corresponding to 300 to 64000 bits per second
First number of VC	Incoming: first incoming logical channel Both: first two-way logical channel Outgoing: first outgoing logical channel
Last number of VC	Incoming: last incoming logical channel Both: last two-way logical channel Outgoing: last outgoing logical channel

Parameter	Meaning
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*
Reverse charging acceptance	For the case of an incoming call, if reverse charging is set, the call packet will be accepted.
Fast select acceptance	This function is used to increase the user data in the call and clear packets and is reserved for packets greater than or equal to 256.
Negotiation acceptance	This function applies only to switched virtual circuits. If the option is checked, the following negotiable values can be filled in: packet window, packet size and throughput class. If a negotiation for "window, size or throughput class" is requested for the packet when the connection is being established, negotiations will be accepted only if negotiated values are lower or equal to the maximum values.
Packet window	Negotiated parameter
Packet size	Negotiated parameter
Throughput class	Negotiated parameter

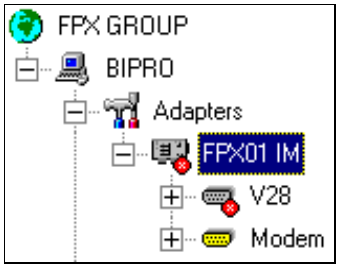
- If the option **Transparent mode** has been checked, fill in the following parameters.

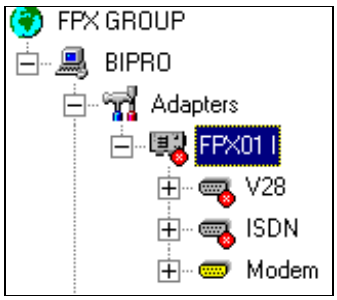
Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 30.
Local ISDN address	Main address, common to all different profiles.
Local ISDN sub-address	Switching prefix needed for incoming calls, by default fitting the prefix value. Specify the sub-address for each service (IP and RAS) installed.

- When all parameters have been filled in, click on the  icon to save the settings.

Configuring the Modem plug for an FPX/IM and FPX/I

- If the user has selected an **FPX/IM** or an **FPX/I** card configuration and checked the C plug, the option **Modem** must be displayed on the left side of the screen (tree).



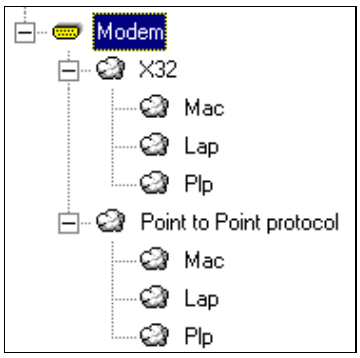


- Click on 

.

The **Modem** plug is used to establish communications using X.25 through internal modem:

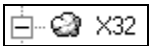
- via an Synchronous Dial-in Port access
- via Point to Point access

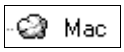


- **X32**

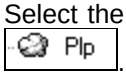
- **Point to Point**

X32

- Select the 

option, then click on 

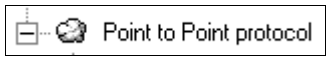
then on 

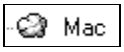
then on 

.

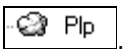
Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 20 if X32.
Network type	Configuration depending on the telephone installation PSTN/DTMF or PSTN pulse. To determine the network type used, press a key on the phone: PSTN/DTMF: If a musical note is heard, it is DTMF (multifrequency). PSTN/Pulse: If a clicking is heard, as on old telephones, then select Pulse. If the card is an FPX/I, 2 additional options are displayed: ISDN (in this case, plug a RJ45-RJ45 cable) and Leased line (on request).
SDP number	Access to the remote site through PSTN using a synchronous dial-in port (In France for example, 3602 or 3603 according to the card and the wanted speed). If the modem is connected through a PABX, enter its prefix just before the SDP number.
Speed	Line speed transmission set in units of bits per second. It allows the gauging of the X.25 timeout and the potential supplying of a clock. Available choices: 2400, 4800, 9600, 12000 or 14400
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
XID identification	When checked, fill in ID and SIG parameters, identifiers consisting of 32 hexadecimal characters, assigned by the X.25 network administrator or Transpac. CRC1 and CRC2 are checksum parameters applied to the previous fields (only if X32).
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128 or 256
First number of VC	Input: first incoming logical channel Both: first two-way logical channel Output: first outgoing logical channel
Last number of VC	Input: last incoming logical channel Both: last two-way logical channel Output: last outgoing logical channel

Point to Point protocol

- Select the 

option, then click on 

then on 

then on 

.

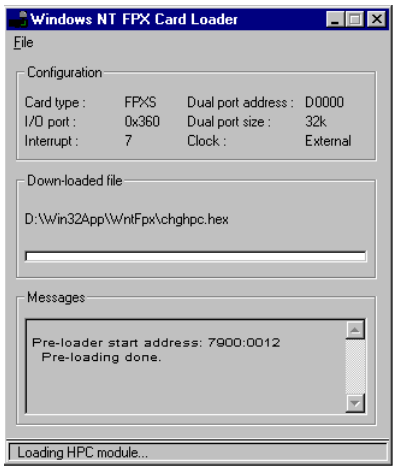
Parameter	Meaning
Switching prefix	Numeric parameter used to route the call on the physical link. Default value = 21 if Point to Point.
Network type	Configuration depending on the telephone installation PSTN/DTMF or PSTN pulse. To determine the network type used, press a key on the phone: PSTN/DTMF: If a musical note is heard, it is DTMF (multifrequency). PSTN/Pulse: If a clicking is heard, as on old telephones, then select Pulse. If the card is an FPX/I, 2 additional options are displayed: ISDN (in this case, plug a RJ45-RJ45 cable) and Leased line (on request).
Speed	Line speed transmission set in units of bits per second. It allows the gauging of the X.25 timeout and the potential supplying of a clock. Available choices: 2400, 4800, 9600, 12000 or 14400
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet window	Maximum number of packets that can be sent before waiting for an acknowledgement Value from 1 to 7
Packet size	Maximum size of the basic X.25 message unit, in bytes Available choices: 128 or 256
First number of VC	Input: first incoming logical channel Both: first two-way logical channel Output: first outgoing logical channel
Last number of VC	Input: last incoming logical channel Both: last two-way logical channel Output: last outgoing logical channel
Full addressing	Checked: during transmission of a calling packet through equipment connected to the network, the calling address includes the local address, possibly with the sub-address: the calling address identifies the sending application in the calling equipment. Unchecked: during reception of an incoming call from the network, the called address includes the local address of the called equipment, possibly with the sub-address; the call packet is routed to the receiving application. *When the X.25 network adds the calling address, do not check this option (for example, for Transpac, the French X.25 public network).*

- When all parameters have been filled in, click on the  icon to save the settings.

Getting started

Manual loading

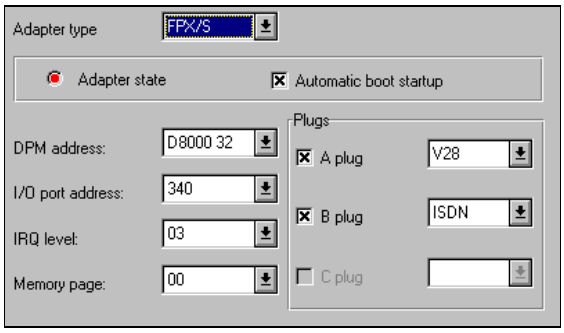
- From the *FPX Communication Manager* screen, select the card to be loaded on the left side of the screen.
- Select the *Commands* menu, then click on the *Immediate loading* command.



The user can follow, during the card loading, the different steps relating to the telecommunication layers to be down-loaded into the card.
The **Initialization ended successfully** message must be displayed, when finished.

It is recommended to check the *Report* command in the *Commands* menu to have a report, in which the loaded and initialized information are stored.

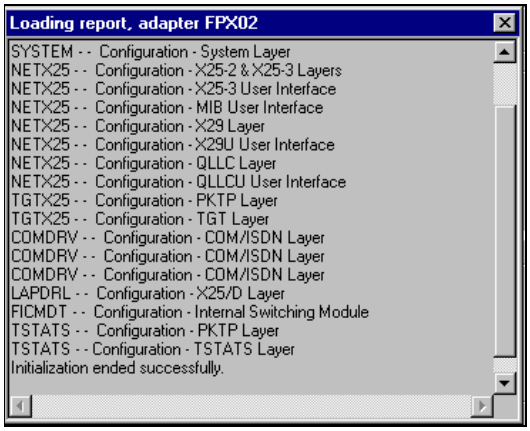
Automatic loading



- When creating an FPX adapter, check the *Automatic boot startup.*
- After a shutdown and a restart machine, the FPX will automatically be loaded.

Loading reports

After the adapter(s) have been loaded and initialized, the user can examine a report, if the *Report* command has been selected.



The windows includes all the data provided by the FPX operation.

The appendices include a list of loading errors. Moreover, for each adapter, the loading and the initialization results are saved in the Event Viewer.
(Source = InitFpx)

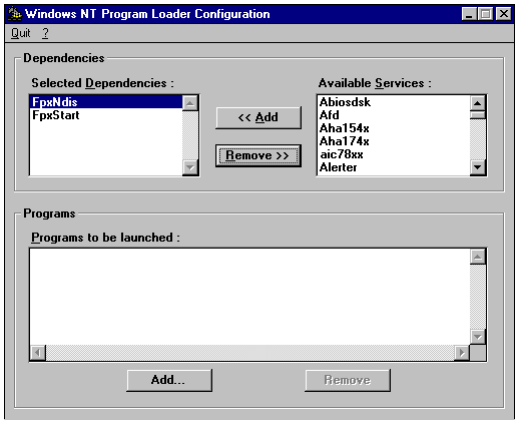
Note:
If the *Read report* command has been checked in the *Options* menu, the report is automatically displayed at the end of the adapter loading.

Program loader on Windows NT

- When the setup is complete, the **FPX Communication Services (Common)** task and the associated utilities are added to the **Start Menu Programs.**

- Select **FPX Config Loader** to launch a set of applications after a shutdown.

- From the *FPX Communications Services (Common)* task, double-click on **FPX Config Loader** to go to the *Program Loader Configuration* screen.



According to the dependency criteria, these applications can be launched only when drivers are loaded into memory or when specific services have been started.

The program loader is very useful when combined with, for example, the Fpx PassLan/IP service to automatically add static routes to the Windows NT TCP/IP stack using the "**ROUTE ADD**" command.

This command can be executed only when:

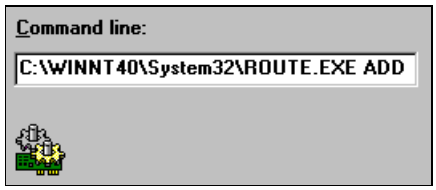
- the FPX PassLan/IP driver is loaded into memory (FpxNdis driver dependency)
- the FPX adapter is initialized (FpxStart utility dependency).

- Select a service from the *Available Services* list box.
- Click on 

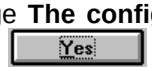
to display the service in the *Selected Dependencies* list box, or
- Click on 

to cancel the operation.
- Click on 

to go to the *Add Program* screen and define the application which will be executed automatically.



can be used to make a search without entering data on the command line. In the case command line parameters are necessary, then enter them after the path name.

- Select the *Quit* menu to exit from program.
- When the message **The configuration has changed. Do you want to save it?** is displayed, click on 

to confirm.

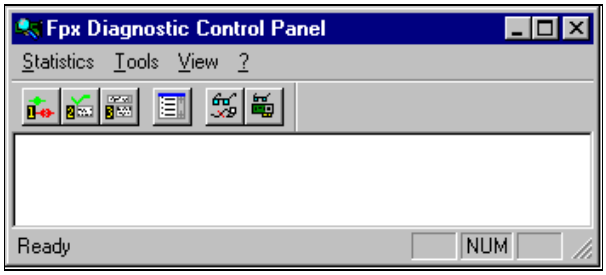
Diagnostic tools

FPX Diag

- When the setup is complete, the **FPX Communication Services (Common)** task and the associated utilities are added to the **Start Menu Programs.**

- Select **FPX Diagnostic Tools** containing various diagnostic tools to analyze the problem.

- From the *FPX Communication Services* (Common) task, double-click on **FPX Diagnostic Tools** to go to the *Fpx Diagnostic Control Panel* screen.



The menus are accessible from the main window:

- Statistics
- Tools
- View
- ?

Each of them contain commands. Only one can be viewed at a time.

Statistics:

- Display the state of the three OSI levels (physical, frame and packet) of the X.25 protocol.

Tools:

- Trace the X.25 or ISDN events.
- Explain X.25 cause and diagnostic in clear packets.
- Execute hardware selftests.

View:

- Display the Toolbar and Status bar (by default): the user can change the display by checking the options.

?:

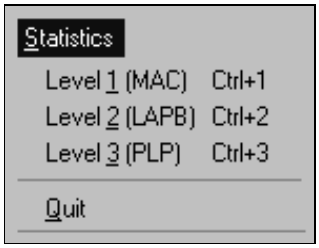
- Access to help information.

The various buttons in the Toolbar correspond to commands used in the *Statistics* and *Tools* menus.

To run a particular utility, select the corresponding command or click on the associated button.

Menus description

Statistics



This menu provides information concerning X.25 protocol streaming. General and specific statistics are displayed and are useful to examine FPX behavior.

The following levels are available:

- MAC (Media Access Control) level
- LAPB (Link Access Protocol Balanced) level
- PLP (Packet Layer Protocol) level

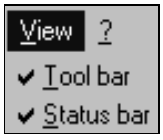
The information provided for each layer is used to determine the state of the physical level (cable plugged in or not), the frame level (SABM/UA received and transmitted indicating that level 2 has been established) and the packet level (Restart packet/Confirmation received and transmitted indicating that level 3 has been established). These data are refreshed every five seconds.

Tools menu

This menu gives access to the following commands:

- *Traces:* gathering traces (ISDN and X.25).
- An *X.25 Clears* displays the cause and diagnostic (in decimal or hexadecimal) with their associated explanations (Refer to Appendix C).
- A *Card Selftests* is used to run hardware tests on various FPX adapter components.

View menu



It is used to:

- Click on the buttons without opening the menu to see the various commands: it is a shortcut for the end-user.
- See the messages in the status bar.

? menu

The *Help* menu gives access to the different types of online help.
The *About Admin...* command displays version information for the FPX Control Panel utility.

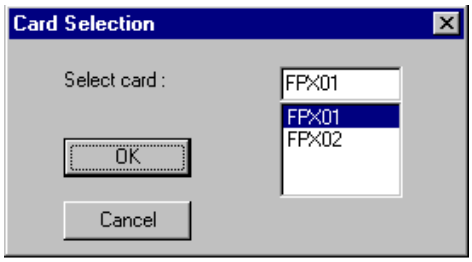
Checking connections

The product FPX associated to its services supports up to four adapters in order to provide different types of connections. The state of the connections and the data transiting through the X.25 protocol can be viewed using the commands in the *Statistics* menu.

MAC Level

To access the information provided by this command, choose the *MAC Level* command from the *Statistics* menu or click on the button in the toolbar:

The message **Gathering information about MAC Level** is displayed in the status bar if this option has previously been checked.



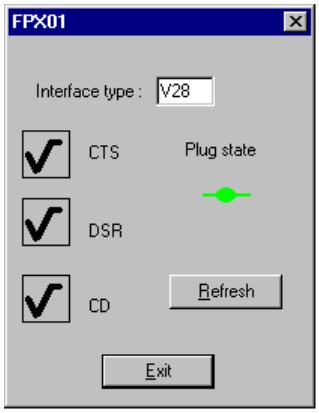
The *Adapter Selection* dialog box appears, and the user can specify the adapter to be managed.

In the following example, the FPX01 adapter is an FPX/B.

The following actions can be performed:

- Click on Cancel to return to the main screen, and select another button if necessary
  or
- Click on OK to move to the next screen that displays MAC Level information

The electrical interface and control signals can be controlled through this panel. These signals regulate the data flow and ensure that the connection is made.



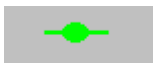
CTS: Clear to Send:
activated by the modem as a reply to a request of sending, when the link is ready to transmit data.

DSR: Data Terminal Ready:
activated by the terminal (DTE) when it is ready to communicate (terminal on).

CD: Carrier Detect:
activated by the modem (DCE) when it has established communications with the remote modem. The modem usually detects the carrier before activating data set ready.
The plug icon varies according to the plug state.
Red indicates that the connection has not been established.
Green indicates that the connection has been established.

Plug state Not OK

Plug state OK



- Click on Refresh to see another step
  or
- Click on Exit to return to the main screen, and select another button if necessary.

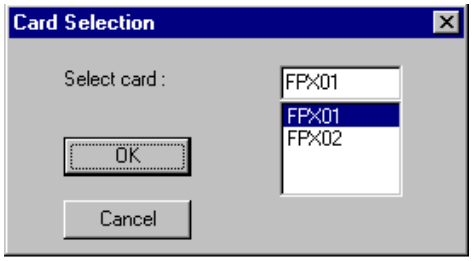
An automatic refresh is made every 5 seconds.

Refer to Online help for detailed information.

LAPB Level

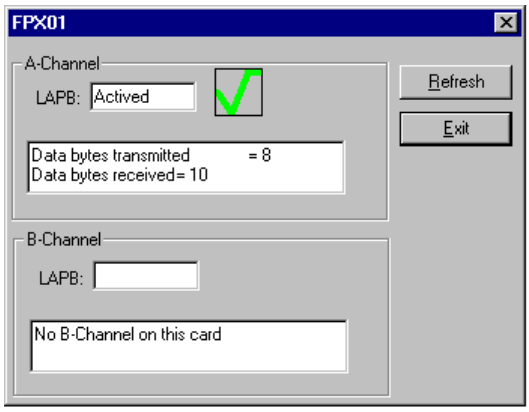
To access the information provided by this command, choose the *LAPB Level* command from the *Statistics* menu or click on the button in the toolbar:

The message **Gathering information about LAPB Level** is displayed in the status bar if this option has previously been selected.



The *Adapter Selection* dialog box is displayed, and the user can specify the adapter to be managed.

Once the adapter has been selected, the data concerning the LAPB level are displayed:



- Frame level established (green icon) or not: level 2
- Data bytes transmitted/received at frame level, etc.

In this example, the FPX01 adapter is an FPX/B: so there is no B-channel.

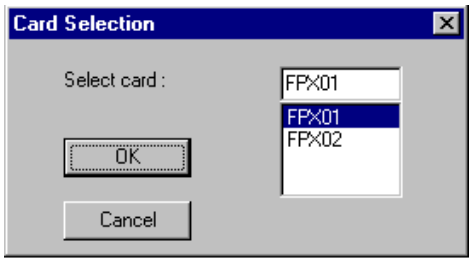
An automatic refresh is made every 5 seconds.

Refer to Online help for detailed information.

PLP Level

To access the information provided by this command, select the *PLP Level* command from the *Statistics* menu or click on the button in the toolbar:

The message **Gathering information about PLP Level** is displayed in the status bar if this option has previously been selected.



The *Adapter Selection* dialog box appears, and the user can specify the adapter to be managed.

Once the adapter has been selected, the data concerning the PLP level of this adapter are displayed:

- The *Remote Address* combo box indicates the remote X.25 number.

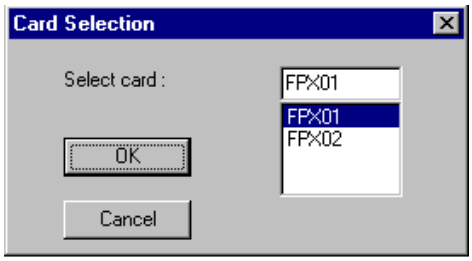
- The edit box displays various statistics such as the number of data bytes transmitted or received at packet level, the number of established virtual circuits, the number of local or remote clears, the number of call failures, the latest clear cause and diagnostic, etc.

Refer to Online help for detailed information.

Traces

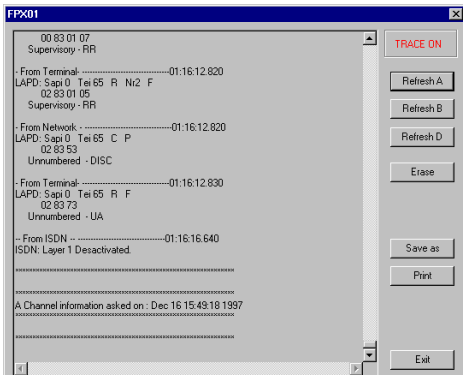
To access the information provided by this command, choose the *Traces* command from the *Tools* menu or click on the button in the toolbar:

The message **Gathering information about LAPD Level** is displayed in the status bar if this option has previously been selected.



The *Adapter Selection* dialog box is displayed, and the user can specify the adapter to be managed.

Once the adapter has been selected, a new dialog box is displayed containing all the information relative to the ISDN channels:



- ISDN level 1 established or not
- etc.

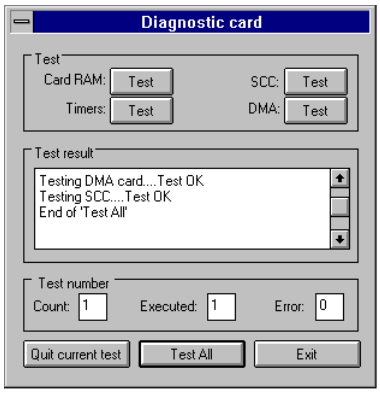
- Click on 

button to update information.

In this example, the FPX01 adapter is an FPX/S but the adapter is to connected to the network with the cable.

Refer to Online help for detailed information.

Caution: These tests can be run at any time, but we recommend to run them after installing the adapter into the PC to be sure that the adapter is working correctly. When exiting the selftest utility, the adapter will be reloaded automatically by the FPX Diagnostic Control Panel.



To run these tests, select the *Card Selftests* command from the *Tools* menu or click on  .

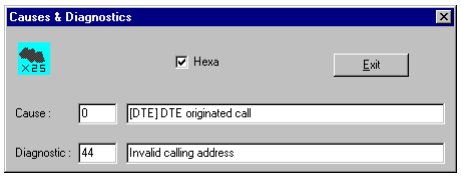
- When the warning is displayed, click on  to confirm, then select the adapter(s) and validate by clicking on  .

The program searchs for the loader, then displays the *Diagnostic card* screen.

- Click on  to check the hardware.

Interpreting X.25 clears

- To run the X.25 Clears utility, select the corresponding command from the *Tools* menu or click on  .



This utility displays the cause and diagnostic of any X.25 clear packet received or transmitted by the FPX adapter.
The *Causes & Diagnostics* dialog box is displayed.

Testing the hardware

The product includes utilities used to run diagnostic tests on the FPX adapter. These tests ensure that the FPX components work properly. Each main component can be tested individually or tested in a sequence of tests.

These tests check the following components:

- The dual-port memory and RAM memory
- The 80186 Intel microprocessor and its interrupt controller
- The two channels of the serial communication controller
- The PC's input/output interface, etc...

Backup/Restore command

These commands can be used to **save a configuration** or to **update a new version** (migration) -*automatically* or *manually* in the installation directory of the Product.

Automatically

- Click on the *File* menu, then click on the *Backup* command to activate this operation. A FPXBACK directory is created at the level of FPX softwares installation path (where the products have been previously installed): all the elements are saved.
- Then, use the *Restore* command to restore them.

Manually

- **FPXSAVE - BACKUP - BATCH - SECRET**
- **FPXSAVE - RESTORE - BATCH - SECRET**
  Batch: path automation

Secret: mode avoiding the display of the dialog boxes

Note: *Be careful, before a desinstallation*:
To save a configuration, before a new version update, it is mandatory to use the Fpxsave program, delivered on the last CD-ROM received, so that the migration of the parameters and keys will be Ok.
It is recommended to reboot the machine, after a restore.

CHAPTER 4

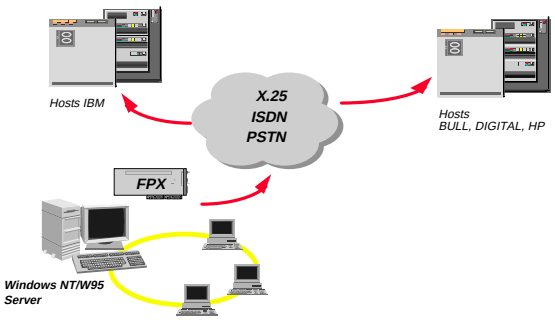
FPX MPServer

Windows NT / Windows 95

4

This chapter describes how to install and use the FPX MPServer component Service included in FPX product.

About this component



FPX MPServer is a multiprotocol server for LAN workstations to connect :

- to BULL and PAD hosts with DKU/TTU and VT emulations via X.25, ISDN and PSTN networks.
- to IBM with 327x emulations via X.25, only on Windows 95.

Based on a client/server architecture, it communicates with its client workstations across the local network via NetBIOS.

It provides a user-friendly configuration environment to select the type of FPX adapters used, the connection mode, the X.25 addresses and characteristics of remote sites.
In the DSA environment, FPX MPServer emulates a BULL TCS/TCU cluster controller capable of simultaneoulsy managing 4 remote sites and 32 DKU/TTU sessions.
It also emulates a PAD to dialogue with all the central systems supporting X.25 and X.29 access and supports 32 simultaneous X.25/X.29 sessions.
A Server machine can support up to 4 FPX MPServers, each one using its own FPX adapter.
In the SNA environment, and only on Windows 95, FPX MPServer emulates an IBM controller, managing one remote site.

Software installation

Before setting up the FPX MPServer component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

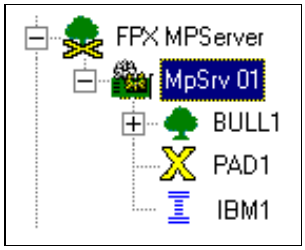
This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.
The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM into the appropriate drive.
- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Services* tab, then click on [Add...] to display the *Select Network Service* dialog box.
- Click on [Have Disk...] then enter the following path: "%**unit**%**\I386\mps**". Validate by clicking on [OK] to continue the automatic process.

- When the setup is complete, the tree is modified. FPX MPServer is added under *Services*.

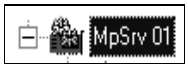
Configuring the Service

- Select *FPX MPServer* then click on  icon to define the various settings of the **first server.**



The settings can be classified in two categories:
- *global* (MpSrv 01)
- *specific* to a server type
(BULL1, PAD1 or IBM1).
IBM only on Windows 95

Global parameters

- Click on  and fill in the following parameters.

Parameter	Meaning
FPX adapter	Adapter previously configured (for example FPX01, FPX02,...)
Message length	Message size that can be routed on the server. It is recommended not to modify this value (used for OEM Kits using FPX X.25 32-bit API or FPX X.25 16-bit API).
Trace file	Trace file name and associated path (default value = c:\fpxmps.trs)
Max sessions	Numeric value of maximum sessions on each server type (32 by default). Example: 32 sessions for each server: 32 DKU/TTU and 32 X.25/X.29.
Network routes	List of the NetBIOS network routes used on the machine, according to the network settings (when installing). Check at least one box. Note: TCP/IP Winsock 2 is added for TCP route: if checked, the port TCP is accessible with a default port number, that can be changed.
Startup setting	Check the exclusive option to activate or not a server. • Automatic: loaded on a start machine • Manual: activated by a user action (Menu or Services) • Disabled: not accessible

Configuring the BULL Routing Service

The component is necessary to define the features of the routing service.
LAN workstations can be connected to the multiprotocol server when it is correctly configured.
The BULL routing service is characterized by the FPX adapter. Before using any workstation emulator, it is mandatory to configure the different sites for access to the BULL hosts.

Creating the BULL Routing Service

- Click on  , then on  and fill in the following parameters.

Parameter	Meaning
Server Name	Identification name (8 alphanumeric characters)
State	Check the exclusive option. • Active: the BULL Routing Service can be active and allow the workstations to connect to the server. • Idle: the BULL Routing Service is inactive and avoid the workstations to connect to the server. • Trace: as "active" and log some traces for further analysis.
Port TCP	Enter the value, if the network route checked is TCP/IP.
Local form processing	Depending on the settings of the host. Used to store predeined DKU screens (form) on the machine and manage local dialog with workstation to process these screens.
X25 n°	X.25 remote site (host) address. It consists of 1 to 15 hexadecimal digits. At this level, enter the public or private X.25 number or the ISDN number of the called remote site (to use an FPX adapter in an ISDN environment, please refer to chapter 3 (Setting up FPX adapters, switching prefix).
Site name	Optional symbolic name associated with the X.25 address. It can be used on workstation to hide the X.25 number, and is highly recommanded to simplify the X.25 numbers management on the server.
Connection	Type of connection: • Normal: the X.25 n° is sent on the X.25 network to establish the connection with the remote site. In this case the calling n° is grayed because it is completly managed by the X.25 network itself. • Direct DNS: (local connection using a cross-cable). The X.25 n° is used only as a configuration reference by the multiprotocol server. The calling n° is used by the Front-end processor (datanet) to establish the connection. • Caller handling: the X.25 n° and the calling n° are both used by the multiprotocol server to build the call packet in order to establish the remote connection.
Calling number	Calling address is waited by the remote site according to the option previously selected.
Reverse charging	When checked, the outgoing call packet includes a facility specifying a reverse charging request. The called party can refuse the request, then the connection is rejected. If not checked, charges are attributed to the calling party.
CUG	Closed user group 00: in general, common group From 1 to 99: private group Empty: no CUG or unique group (Refer to the note).
Facilities	Facility field of call packet
Workstation rights	The panel represents the 32 terminal addresses which can be connected to a cluster (from 00 to 31). In front of each address, select the access right, according to the Front-End processor configuration. The available values are: • Forbidden: this address is not allowed in this terminal cluster. • Dedicated: this address has a privileged access. Only a terminal asking for this number will be able to use it, if the address is free. This workstation is never dynamically allocated. • Free: this address can be used by any terminal that uses dynamic addressing or specifies a particular address. Buttons are added at the bottom of the screen allowing the user, if he wants the same rights to quickly select all the workstation rights. In this case, click on *All Forbidden*, *All Dedicated* or *All free.*

Notes:
If the *Reverse charging* option has been checked, the correspondent code must not be entered in the *Facilities* field (0101). Caution: if option is checked and code entered in the field, no control is made on the *Facilities* field: it is the same for the *CUG*.
Dynamic addressing: LAN workstations can launch emulators without stating a special terminal address. In this case, the server is scanning the list of the non-dedicated addresses and dynamically allocates an address to the requesting station (within addresses of this type available at a given time).

- When all parameters have been filled in, click on the  icon to save the settings.

Modifying a site

- Click on 

to make change(s) if necessary, then click on the  icon to update the modifications, and save the new configuration.
All parameters can be changed.

Adding a site

A maximum of 10 sites is allowed for a same server. 4 sites maximum are simultaneously accessible.

- Select the server by clicking on its name, on the left side of the screen (tree), click on the  icon to add a new site, define the settings, then click on the  icon to save the new configuration.

Removing a site

- Select a site by clicking on its name, then click on the  icon, and click on the  icon to save the new configuration.

Configuring the PAD Routing Service

The component is necessary to define the features of the routing service.
LAN workstations can be connected to the multiprotocol server when it is correctly configured. The PAD routing service is characterized by the FPX adapter. Before using any workstation emulator, it is highly recommended to configure the number of X.25/X.29 MPS sessions dedicated to X.25 and/or X.29.

Creating the PAD Routing Service

- Click on 

and fill in the following parameters.

Parameter	Meaning
Server name	Identification name (8 alphanumeric characters)
State	Check the exclusive option. • Active: the PAD Routing Service can be active and allow the workstations to connect to the server • Idle: the PAD Routing Service is inactive and avoid the workstations to connect to the server • Trace: as "active" and log some traces for further analysis.
Port TCP	Enter the value, if the network route checked is TCP/IP.
Number of sessions dedicated to X25	Enter the value of number of sessions exclusively reserved to an X.25 access.

Parameter	Meaning
Number of sessions dedicated to X29	Enter the value of number of sessions exclusively dedicated to an X.29 access.
Number of non dedicated sessions	Enter the value of number of available sessions to X.25 or X.29 according to their needs and to the server availability.

- When all parameters have been filled in, click on the  icon to save the settings.

Note: The total of these three numbers, in the PAD Routing Service cannot exceed the maximum number of sessions.
Example 1: (without non-dedicated sessions):
Number of X.25 sessions = 5
Number of X.29 sessions = 3
Number of non-dedicated sessions = 0
The number of X.25 sessions is limited to a maximum of 5 and the number of X.29 sessions is limited to a maximum of 3, with no other possible connections.
Example 2: (with non-dedicated sessions):
Number of X.25 sessions = 5
Number of X.29 sessions = 3
Number of non-dedicated sessions = 10
5 sessions are dedicated to X.25 and cannot be used by X.29, 3 sessions are dedicated to X.29 and cannot be used by X.25. There are 10 other possible connections, either for X.25 or X.29 depending on availability.

Reminder

In the *Global Parameters* section, the number of maximum sessions means the following:
- the number of DKU/TTU sessions on the BULL server
- and the number of X.25/X.29 sessions on the X.25/X.29 server

It is relative to the maximum number of sessions allowed for each type of server (BULL, X.25/X.29) i.e., 32 DKU (with or without their TTU sessions) + 32 X.25 or X.29 sessions.

Updating the Service

- Click on 

to make change(s) if necessary, then click on the  icon to save the new configuration.

Configuring the IBM Routing Service

The component is necessary to define the features of the routing service.
LAN workstations can be connected to the multiprotocol server when it is correctly configured. The IBM routing service is characterized by the FPX adapter. Before using any workstation emulator, it is mandatory to configure the site for access to the IBM host.

Creating the IBM Routing Service

- Click on 

and fill in the *Server name* and *State* parameters

Parameter	Meaning
Server Name	Identification name (8 alphanumeric characters)
State	Check the exclusive option. • Active: the IBM Routing Service can be active and allow the workstations to connect to the server. • Idle: the IBM Routing Service is inactive and avoid the workstations to connect to the server. • Trace: as "active" and log some traces for further analysis.

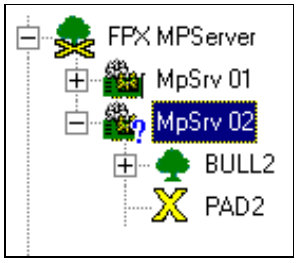
X25 n°	X.25 remote site (host) address. It consists of 1 to 15 hexadecimal digits. At this level, enter the public or private X.25 number or the ISDN number of the called remote site (to use an FPX adapter in an ISDN environment, please refer to chapter 3 (Setting up FPX adapters, switching prefix).
Cluster identifier	Number (8 hexadecimal digits) which identifies the local system. • IDBLK: block number on the first three digits. • IDNUM: node number on the last five digits.
Reverse charging	When checked, the outgoing call packet includes a facility specifying a reverse charging request. The called party can refuse the request, then the connection is rejected. If not checked, charges are attributed to the calling party.
CUG	Closed user group 00: in general, common group From 1 to 99: private group Empty: no CUG or unique group (Refer to the note).
Facilities	Facility field of call packet
Data	User data. Enter the hexadecimal values of the EBCDIC codes, on 20 digits maximum, with an even length.
Workstation rights	The panel represents the 32 terminal addresses which can be connected to a cluster (from 02 to 33). In front of each address, select the access right, according to the Front-End processor configuration. The available values are: • Forbidden: this address is not allowed in this terminal cluster. • Dedicated: this address has a privileged access. Only a terminal asking for this number will be able to use it, if the address is free. This workstation is never dynamically allocated. • Free: this address can be used by any terminal that uses dynamic addressing or specifies a particular address. Buttons are added at the bottom of the screen allowing the user, if he wants the same rights to quickly select all the workstation rights. In this case, click on *All Forbidden*, *All Dedicated* or *All free.*

Notes:
If the *Reverse charging* option has been checked, the correspondent code must not be entered in the *Facilities* field (0101). Caution: if option is checked and code entered in the field, no control is made on the *Facilities* field: it is the same for the *CUG*.
Dynamic addressing: LAN workstations can launch emulators without stating a special terminal address. In this case, the server is scanning the list of the non-dedicated addresses and dynamically allocates an address to the requesting station (within addresses of this type available at a given time).

- When all parameters have been filled in, click on the  icon to save the settings.

Creating another server

- Select *FPX MPServer* then click on  icon to create a new server (**4 maximum)**.



- Select an adapter, according to the Adapter configuration (Refer to the previous chapter for more information). The adapter must be different from the one selected, for the first server. Then define the settings, as described for the first server.

- Do not forget to save the new informations.

A Windows NT Server machine can support up to 4 FPX MPServers, each one using its own FPX adapter.

Starting and stopping the Service on NT

- Select the server by clicking on its name: for example 

- Click on the *Commands* menu, then double-click on the *Start the FPX MPServer service* command.
- To stop it, click on the *Commands* menu, then double-click on the *Stop the FPX MPServer service* command.

Notes:
The *FPX MPServer* is in fact installed as a service in the ***Control Panel*.**

- Run the *Control Panel*, then click on the ***Services*** icon to go to the *Services* screen to see the different services, their status and the startup types (automatic or manual), depending on the startup setting option, when installing the server.
  For more information, refer to the *Global parameters* section: any change is possible.
- If the *FPX MPServer FPXxx* fails to start, refer to the Windows NT event viewer to read the error messages that have been recorded in the System and Application logs.

Starting and stopping the Service on W95

- Select the server by clicking on its name: for example 

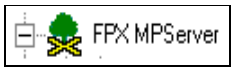
- Click on the *Commands* menu, then double-click on the *Start the FPX MPServer service* command.
- To stop it, click on the *Commands* menu, then double-click on the *Stop the FPX MPServer service* command.

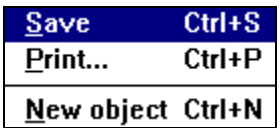
Note :
In the Tasks Bar on the right of the screen, an FPX MPServer icon is added.

- Click on it to obtain statistics information : server names, number of activated sessions,...

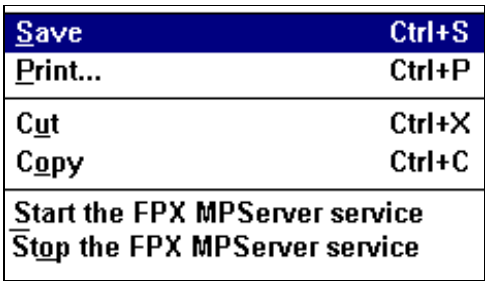
Using the mouse right button

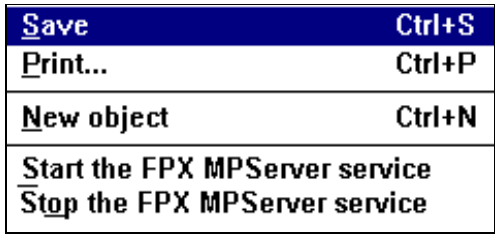
This function is used as a command shortcut, depending on the mouse pointer location.



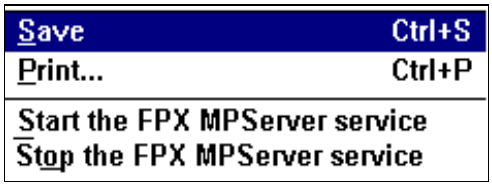


and 





and



For more information about the different commands, refer to *Chapter 3: Setting up FPX adapters*.

CHAPTER 5

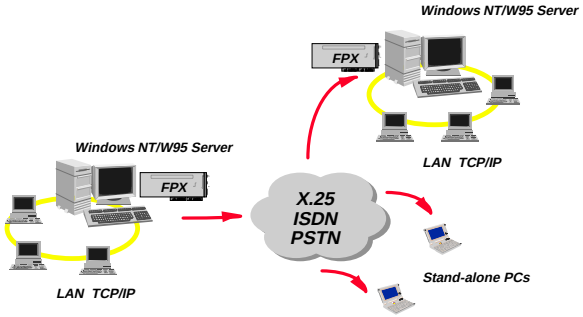
FPX PassLan/IP

Windows NT / Windows 95

5

This chapter describes how to install and use the FPX PassLan/IP component Service included in FPX product.

About this component



FPX product integrates the FPX PassLan/IP component used for LANs and stand-alone PCs interconnection.
It extends the capabilities of the Windows NT/W95 TCP/IP stack over X.25, PSTN, Frame Relay and ISDN networks.

In compliance with the NDIS 3.x specifications, it supports up to 64 simultaneous gateways. For each gateway, a backup mechanism ensures the automatic switching from a primary link to a secondary one.
The advanced features (adaptive routing, bandwidth-on-demand, accreditation on X.25 address or IP address, PPP authentication, inactivity timeout, etc.) improve the security and the reliability of the entire environment.

FPX PassLan/IP implements Request For Comments 877, 1144, 1356, 1490 and 1661 and interoperates with the main routers of the market:

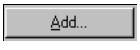
- Cisco, Retix, Wellfleet, Spider, 3Com,...

Note:
FPX PassLan/IP requires that Microsoft's TCP/IP stack be previously set on the computer, before setting up this component.

Software installation

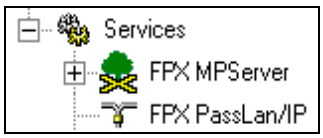
Before setting up the FPX PassLan/IP component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.
The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM into the appropriate drive.
- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Adapters* tab, then click on 

to display the *Select Network Adapter* dialog box.

- Click on Have Disk... then enter the following path: "%**unit**%**\I386\ip**". Validate by clicking on OK to continue the automatic process.



- When the setup is complete, the tree is modified. FPX PassLan/IP is added under *Services*. In this example FPX MPServer has already been installed.

- **Don't reboot the PC immediatly. First configure the FPX PassLan/IP Service.**

Configuring the Service

- Select *FPX PassLan/IP* then define the FpxNdis driver global parameters to ensure that it works properly.

Global parameters

Parameter	Meaning
Local IP address	During installation, the address has been entered in Network settings: TCP/IP config. An Internet address, also called IP is defined by *Network-Identifier/Host-Identifier,* where the first component identifies the network and where the second identifies the host in the network. It is defined by a 32-bits value (4 bytes) and represented in dotted decimal notation as *aaa.aaa.aaa.aaa*
Subnet mask	Subnet mask associated to the local IP address.
Default gateway	Default address of the gateway.
Use	Select one option: Basic use or Advanced use • Basic: To keep *only one connection* on the gateway (no backup). • Advanced: To use *several connections* on a gateway (adaptative routing, flow control, backup,...). *Advanced use is not accessible on Windows 95, if FPX/SL II is selected.*
Level traces	Traces pertaining to communication between driver and adapter: • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*
IP level traces	Select the trace None or Addresses option. • None: No trace • Addresses: When connecting, trace is executed for all IP addresses exchanged.
Bandwith limitation	When checked, fill in the *VC level* and *Trafic level* fields to detect other cv(s) used by a strange application different from PassLan/IP.

Configuring the gateway

Creating a gateway

- When all the global parameters have been selected, click on  icon to insert a new **gateway** or click on the right button of the mouse to add a **dynamic gateway** (only accessible on Windows NT: refer to the corresponding section, in this chapter).

- Then the *Gateway* parameters have to be defined.

- According to the previous selection *Basic use* or *Advanced use*, the *Gateway* screen is different.

Parameter	Meaning
Gateway name	Gateway identification
IP/Wan address	IP address defined on TCP/IP remote configuration.
Allowed gateway	When checked, this access is allowed.
Retry timeout	Delay between attempts (second).
Protocol	Select one X25, PPP or Frame relay option to define the protocol used for the gateway. • X25: Into ISDN B-channel, D-channel or into the V24/V11/V35 pipe. • PPP: Into ISDN B-channel (FpxB, FpxI or FpxS) • Frame relay: Into the V24/V11/V35 (FpxB or FpxS)
Adaptative routing	When checked, the IP flow is routed according to its TCP/UDP port on a specified identified gateway connection. This option can only be used with several connections.
Access control	Access type that can be used for the gateway • Both: Incoming and outgoing calls are authorized. • Inbound: Only incoming calls are authorized. • Outbound: Only outgoing calls are authorized.
Flow control	Two options are available: Bandwith or Overflow backup • By default, the *Bandwith* option is displayed because it is used in most cases. The *Authorized bandwith* parameter (with the value = 100) means the flow control can use up to the maximum value of the bandwith : it can be changed. • If the *Overflow backup* option is selected, the IP flow is routed depending on TCP/UDP port on a specified gateway connection when the currently used connection is saturated. Two parameters must be configured: *Line-up at:* The entered value is the threshold used to determine at what percentage of the bandwith the driver will open another connection. *Line-down at:* The entered value is the threshold used to determine at what percentage of the bandwith the driver will disconnect the new connection. It is strongly recommended that the line-up threshold should be the highest (minimum acceptable value: 70%) and that the line-down threshold should be the lowest (maximum acceptable value: 30%) to avoid opening and closing connections too frequently. If the line-up threshold is 100%, no overflow will be activated.
Permit addresses	Select the *All IP addresses* or *Some IP* addresses option (exclusive choice). • All IP addresses: the driver authorizes all IP Lan addresses included in IP frames to be exchanged between the gateway and the workstation. • Some IP addresses: the driver only authorizes the IP Lan addresses identified as *Workstations, Range* or *Network (subnet)*. *Workstations:* A single IP address *Range:* An IP address range (start and end) *Network:* Network address and subnet mask.

- When the *Gateway* parameters have been filled in, configure the connection(s).

Modifying a gateway

- Click on 

to make change(s) if necessary, then click on the  icon to update the modifications, and save the new configuration.
All parameters can be changed.

Adding a gateway

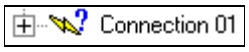
- Select *FPX PassLan/IP*, on the left side of the screen (tree), click on the  icon to add a new gateway, define the settings, click on the  icon.

Removing a gateway

- Select a gateway by clicking on its name, then click on the  icon, and click on the  icon.

Configuring the connection

Creating a connection

- Click on 

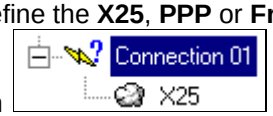
and fill in the *Connection* parameters.
- According to the previous selection *Basic use* or *Advanced use*, the *Connection* screen is different.
If the *Basic use* option has been selected, only one link is possible.
If the *Advanced use* has been selected, a *main link* and a *backup link* can be defined, and the *TCP/UDP ports* parameter is added. Other connections could be added, on the gateway by using the  icon.

Parameter	Meaning
Link	Used to select the output profile and the FPX adapter. The contents of the list box consists of adapters previously configured.
Dlci	Data link connection identifier, number from 16 to 1007 entered previously in the *Adapters* configuration if Frame relay is checked.
Network address [outgoing]	Outgoing address of the remote gateway. It consists of 1 to 15 digits. *This address must not include the switching prefix that may have been defined when configuring FPX adapters. The FPX PassLan/IP program displays for information, then adds this prefix, when required, according to the selected profile and the adapter configuration.*
Network sub-address [outgoing]	Outgoing sub-address of the remote gateway.
Network address [incoming]	It consists of 1 to 15 digits corresponding to the incoming address received by the FPX during an incoming call. If the character * is entered, all incoming addresses are accepted.
Tries number	Number of connection tries to a non-responding remote gateway (default value = 1).
Timeout	Minimal inactivity delay before disconnecting (default value = 90s). The value 0 means an endless timeout.
TCP/UDP ports	List of ports that are accepted (*Authorized*) or refused (*Forbidden)* by the FpxNdis driver. Four ports can be configured: the separator is a space or a comma.

Note:
For each connection, when the *Avanced use* option has been checked, the driver can use two different accesses:

- Main access
- Backup access: it is used only if the main access could not be established after x number of connection tries.

Click on the *Main* tab to fill in the fields, then click on the *Backup* tab to define the parameters as described in the creating section.

- Then define the **X25**, **PPP** or **Frame relay** parameters.
- Click on 

if the X25 protocol has been checked in the *Gateway* screen, or
- Click on 

if the PPP protocol has been checked,or
- Click on 

if the frame relay protocol has been checked.

X25 parameters

Parameter	Meaning
Reverse charging acceptance	When checked, the driver accepts an incoming call with a facility specifying a reverse charging request. The called party can accept to avoid a connection rejected.
Reverse charging request	When checked, the outgoing call packet includes a facility specifying a reverse charging request. The called party can refuse the request and the connection is then rejected.
Closed user group	Complementary service with potential values: • 00: in general, common group. • 1 to 99: private group • blank: no CUG or single group.
Facilities	Facility field of a call packet.
PID included	Protocol identifier. Check this option to transmit the TCP/IP identifier (0xCC) in the X.25 call packet. In general, all routers use this identifier.
Local X25 address	X.25 local address (calling) to be completed, when the X.25 network does not use calling address.
Stac compression	Check this option to use compression algorithm from Stac Company. A licence is necessary. *For more information, refer to the NOTE at the end of this chapter*.

- Click on the  icon to save the parameters entered.

PPP parameters

Point to Point protocol is a set of industry standard framing and authentication protocols. It provides a method for transmitting datagrams over serial point-to-point links.

Parameter	Meaning
Local authentication	Type of authentication: • None: No authentication • PAP: Password Authentication Protocol • CHAP: Challenge-Handsshake Authentication Protocol. By default, authentication is not mandatory: no security is provided. *For more information, refer to the note hereafter.*
Remote user name [Local PAP]	When the *Local authentication* is selected with *PAP*, enter the remote user name: alphanumeric value up to 31 characters maximum.
Password [Local PAP]	When the *Local authentication* is selected with *PAP*, define the password field associated to the remote user name: alphanumeric value up to 31 characters maximum.
Remote authentication	Type of authentication: • None: No authentication • PAP: Password Authentication Protocol • CHAP: Challenge-Handsshake Authentication Protocol. By default, authentication is not mandatory, then no security is provided. *For more information, refer to the note below.*
Local user name [Remote PAP]	When the *Remote authentication* is selected with *PAP*, enter the local user name: alphanumeric value up to 31 characters maximum.
Password [Remote PAP]	When the *Remote authentication* is selected with *PAP*, define the password field associated to the local user name: alphanumeric value up to 31 characters maximum.
CHAP Password	Secret word known by the two peers to perform the authentication.
CHAP Local user	Local user identifier: alphanumeric value up to 31 characters maximum.
CHAP Remote user	Remote user identifier: alphanumeric value up to 31 characters maximum.

- Click on the  icon to save the entered parameters.

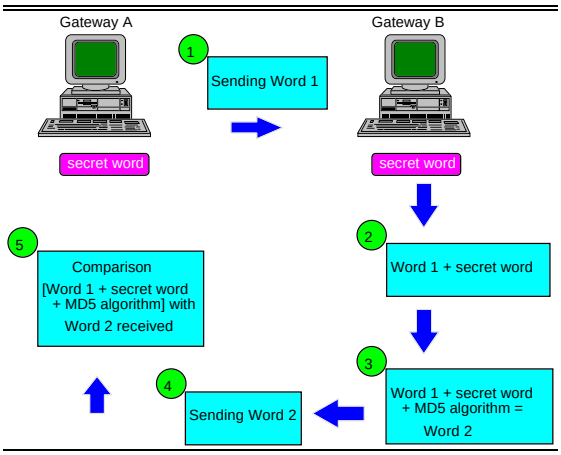
Frame relay parameters

Frame relay protocol, HDLC synchronous protocol (with the frame length = 1600) is used to take advantage of the flow rate.

Parameter	Meaning
Encapsulation	Type of encapsulation, necessary to ensure a good running: • None: No encapsulation • IETF: Internet Engineering Task Force • Other: the user can parameter a specific encapsulation. These options are in compliance with the 1490 R.F.C.

- Click on the  icon to save the entered parameters.

Note:
Password **A**uthentication **P**rotocol (**PAP**) is based on mutual authentication of the two remote peers. PAP uses clear text passwords and is the least sophisticated authentication protocol. It is typically negotiated if the remote gateway (third party router for example) cannot negotiate a more secure form of validation.
Challenge-**H**andshake **A**uthentication **P**rotocol (**CHAP**) uses a challenge response with a one-way encryption on the response; it is the most secure form of encrypted authentication available.



The authenticator sends an identification message (word 1) towards the remote entity. The remote entity uses this message (word 1) by concatenating a secret word known by the two peers (secret word configured for PPP-CHAP gateway) and by applying an encryption algorithm well known by the remote peer.

Then the remote peer sends back a response (word 2) to the authenticator. Upon reception, it applies the same mechanism on the initially transmitted word 1 (secret mode + encryption algorithm) and compares the result with the received response.
Authentication is accepted if the comparison is successful.
The password is never transmitted over the line.
The FpxNdis driver uses the MD5-CHAP encryption algorithm.

Modifying a connection

- Click on 

to make change(s) if necessary, then click on the  icon to update the modifications, and save the new configuration.
All parameters can be changed.

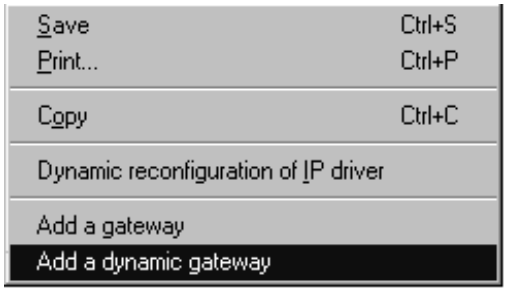
Removing a connection

- Select a connection by clicking on its name, then click on the  icon, and click on the  icon to save the new configuration.

Configuring a dynamic gateway

Creating a dynamic gateway

- This option only exists with **Windows NT.**
- Select *FPX PassLan/IP*, then click on the mouse right button to access to the *Add a dynamic gateway* command, and validate to display the *Gateway* screen.



- When adding a **dynamic** gateway, the protocol used can be only X.25.

Parameter	Meaning
Gateway name	Gateway identification
Maximum number of correspondents	Enter the maximum number of sites to reach simultaneously: in this case, the driver automatically allocates a gateway to each different number.
Allowed gateway	When checked, this access is allowed.
Retry timeout	Delay between attempts (second).
Access control	Access type that can be used for the gateway • Both: Incoming and outgoing calls are authorized. • Inbound: Only incoming calls are authorized. • Outbound: Only outgoing calls are authorized.
IP addresses conversion	Table containing the addresses which form exceptions to the conversion algorithm.
IP	IP address represented in doted decimal notation aaa.aaa.aaa.aaa to add in the table IP addresses conversion (by using the button - the other button is used to delete an IP address).
X25	X.25 number associated to the IP address filled previously.
Permit addresses	Select the *All IP addresses* or *Some IP* addresses option (exclusive choice). • All IP addresses: the driver authorizes all IP Lan addresses included in IP frames to be exchanged between the gateway and the workstation. • Some IP addresses: the driver only authorizes the IP Lan addresses identified as *Workstations, Range* or *Network (subnet)*. *Workstations:* A single IP address *Range:* An IP address range (start and end) *Network:* Network address and subnet mask.

- When all parameters have been filled in, click on the icon to save the entered parameters.

- To configure the connection and the X.25 protocol, refer to the *Configuring the connection* section. The principle stays identical to the one described previously.

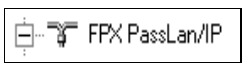
Getting started

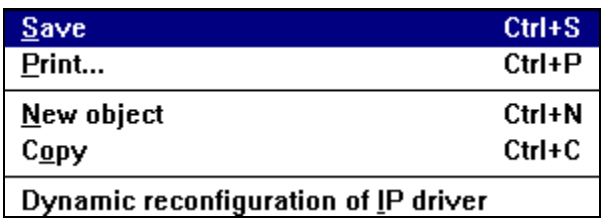
Once the gateways have been defined, the FPX *adapter* must be loaded.

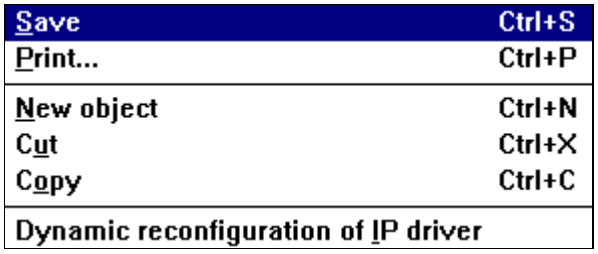
- First select the *adapter* to be loaded, click on the *Commands* menu, then click on the *Immediate loading* command.
- Use the *Dynamic reconfiguration of IP driver* command so that the driver takes into account all the changes made to the gateway(s).

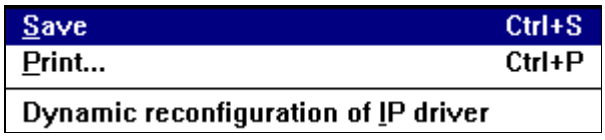
Using the mouse right button

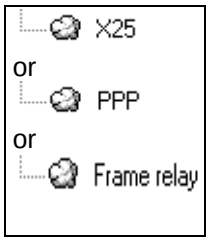
This function is used as a command shortcut, depending on the mouse pointer location.

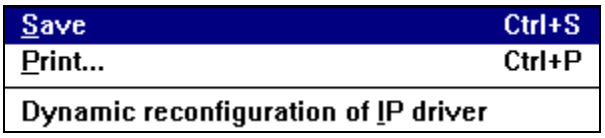






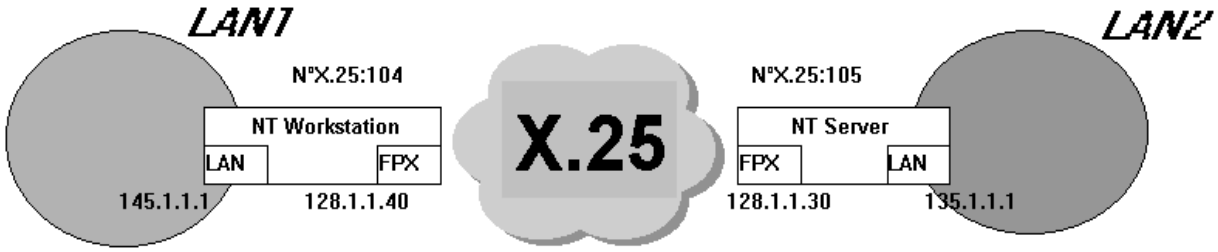






For more information about the different commands, refer to *Chapter 3: Setting up FPX adapters*.

Sample configuration



The X.25 network used in this configuration is a private X.25 network that does not manage insertion of the calling address in the call packet. The computers are NT machines, but could be W95 machines.

NT Workstation

- Define the TCP/IP addresses:
  FPX adapter 128.1.1.40
  LAN adapter 145.1.1.1

- Configure the V28 plug of the FPX *adapter* with X.25 protocol, then check the *Full Addressing* parameter (PLP - Additionnal Options in ***FPX configuration***).

- Configure the local X.25 address = 104 (***FPX PassLan/IP*** Services).

- Define a gateway labeled NT Server with :
  IP address 128.1.1.30
  Link V28 X25 LL
  Remote X.25 address 105

- In the \%system_root%\system32\drivers\etc implement the LMHOSTS file to resolve the NetBIOS names with the following IP addresses:

  128.1.1.40 NTWORKSTATION #PRE
  128.1.1.30 NTSERVER #PRE

Notes:
- NTWORKSTATION and NTSERVER are the computer names and not the user names.
- LMHOSTS file is a local text file that maps the TCP/IP addresses with the NetBIOS names of the Windows NT/W95 computers.

NT Server

- Define the TCP/IP addresses:
  FPX adapter 128.1.1.30
  LAN adapter 135.1.1.1

- Configure the V28 plug of the FPX adapter with X.25 protocol, then check the *Full Addressing* parameter (PLP - additionnal options in ***FPX configuration***).

- Configure the local X.25 address for this profile = 105 (***FPX PassLan/IP*** service).

- Define a gateway labeled WNTWORKSTATION with :
  IP address 128.1.1.40
  Link V28 X25 LL
  Remote X.25 address 104

- In the Windows NT directory \%system_root%\system32\drivers\etc, implement LMHOSTS file to resolve the NetBIOS names with the following IP addresses:

  128.1.1.40 WNTWORKSTATION #PRE
  128.1.1.30 NTSERVER #PRE

Testing TCP/IP operation

The Microsoft TCP/IP stack includes a PING utility used to determine whether a TCP/IP host can be reached. LMHOSTS is a file resolving the NetBIOS names with the following IP addresses:

- To reach the NT Server gateway from the NT Workstation gateway type the command:
  PING 128.1.1.30
  The system should reply immediately.

- To reach the NT Workstation gateway from the NT Server gateway type the command:
  PING 128.1.1.40
  The system should reply immediately.

Notes :
- The user can examine the Windows NT event viewer (system log) if the command fails.
- The IPCONFIG utility provided with TCP/IP stack is used to check the TCP/IP configuration on each computer.

- To reach the IP address of the remote NT Server LAN adapter from the NT Workstation gateway, type the command:
  ROUTE ADD 135.1.1.1 128.1.1.30

- And then from the NT Workstation gateway, type:
  PING 135.1.1.1
  The system should reply immediately.

- To access routing capabilities, check the *Enable IP routing* option when configuring the TCP/IP protocol (Properties).

NetBIOS usage with TCP/IP

The LMHOSTS file is looked-up by the Windows NT/W95, TCP/IP stack to identify the IP gateway to reach.

- On the NT Workstation, type the command:
  NET USE K: \\NTSERVER\C$

Notes :
- On the NT Server side, check the shared name C$.
- Verify also whether the *Enable LMHOSTS Lookup* option is checked (TCP/IP Protocols-Properties).

FTP usage

FTP is a file transfer utility on TCP/IP.

- On NT Server, check that the FTP server is started (***Services*** icon, in the Control Panel).

- On NT Workstation, use ***FTP*** command, then:

  FTP>OPEN NTSERVER or
  FTP>OPEN 128.1.1.30
  FTP>? to get all the available commands, etc.

NOTE about the Stac compression

To use the Stac compression with the FPX PassLan/IP service, and interoperate with the routers (settings: with or without compression), it is necessary:
- to create a gateway with the **same called X.25 address** for the *Main* connection and for the *Backup* connection.
- to check the Stac compression option -only one of the two connections- (for example: the Main connection)

First case: **outgoing** calls
To connect to a router, the first attempt is to establish the connection in compression mode. If the router refuses the call, then the gateway directly switches over to the Backup connection without compression.
Second case: **incoming** calls
To receive a connection from a router (compression mode or not), the NDIS driver first verifies the calling address received, then checks the compression request, and actives or not this compression.

CHAPTER 6

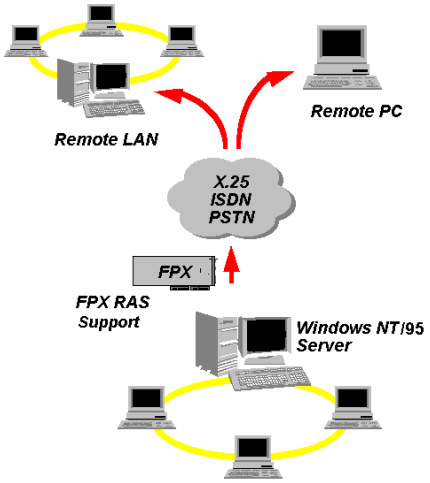
FPX RAS Support

Windows NT / Windows 95

6

This chapter describes how to install and use the FPX RAS Support component included in the FPX product.

About this component



FPX product includes the FPX RAS Support component to enhance the capabilities of the Microsoft Remote Access Service over X.25, PSTN and ISDN networks.
It extends the local area network to remote workstations and offers full network access to remote PCs.

Built around the Microsoft WAN TAPI Miniport interface, it provides a high speed connection pipe between Windows NT/95 servers over X.25, PSTN and ISDN networks.

Stand-alone Windows for Workgroups or Windows 95 PCs can also use the WAN connection to access the RAS server and share resources on the network.

Notes:

- **Windows NT:** FPX RAS Support requires that Microsoft's Remote Access Service be already set on the computer, and a port COM be selected, before setting up this component.
- **Windows 95 :** Microsoft's Dial Up Networking and ISDN Accelerator Pack 1.x have to be already set on the computer.

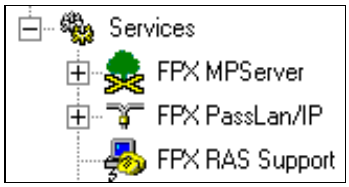
Software installation

Before setting up the FPX RAS Support component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.
The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM into the appropriate drive.
- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Adapters* tab, then click on Add... to display the *Select Network Adapter* dialog box.

- Click on Have Disk... then enter the following path: "%**unit**%**\I386\ras351**" or "%**unit**%**\I386\ras40**" depending on the operating system version. Validate by clicking on OK to continue the automatic process.



- When the setup is complete, the tree is modified. FPX RAS Support is added under *Services*.
  In this example FPX MPServer and FPX PassLan/IP have already been installed.

Configuring the Service

- Select *FPX RAS Support* then define the following features.

Parameter	Meaning
Configured adapters	The contents of the list box consists of adapters previously configured. Select one of them, then click on the >> button to display it into the *Selected adapters* list box.
Selected adapters	Name of one or several adapters that the FpxTapi driver will use to establish a connection towards a remote computer. When the driver is configured to operate with several adapters, the driver attempts to open a connection on the first adapter, then on the second one if the first one failed, etc. It corresponds to a pool of ISDN ports available on several FPX adapters.
FPX RAS Support with FPX PassLan/IP compatibility	If the 2 components FPX RAS Support and FPX PassLan/IP must live together, check this option. Specify a sub-address for each one. • When X.25 connections are selected, the PID sent is 01000000. • When the PPP mode is selected, refer to the transparent mode screen. • Check also this option to accept incoming calls from an X.25/PAD with PID 01000000
Number of retries	Number of times the driver will attempt to establish a connection towards a not responding remote computer (default value = 1).
Timeout	Inactivity delay elapsed before disconnecting (default value = 90 seconds). Value = 0 means an undless timeout.
SYS level	Traces pertaining to communication between the FpxTapi driver and potential driver administration programs. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*
MAC level	Traces pertaining to communication between the protocol stack and the FpxTapi driver. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*

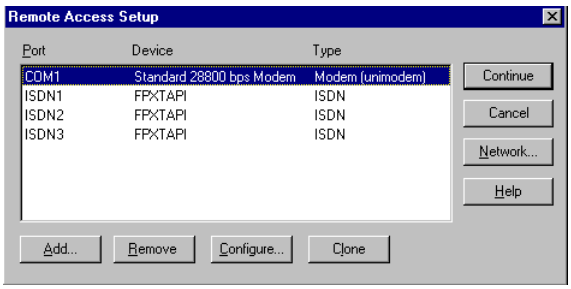
Parameter	Meaning
X25 level	Traces pertaining to communication between the FpxTapi driver and the FPX adapter. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*

- When the parameters have been filled in, click on the  icon to save them.
- Before configuring the **R**emote **A**ccess **S**ervice, reboot the PC configuration.

Note:
It is recommended to check the Microsoft's **R**emote **A**ccess **S**ervice configuration, before getting this Service started.

Configuring Remote Access Service on Windows NT

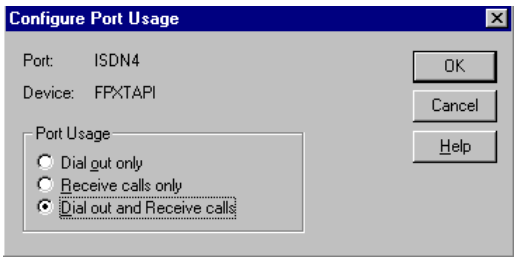
- Run the Control Panel, then double-click on the ***Network*** icon.
- From the main screen, select the *Services* tab, then double-click on *Remote Access Service* to display the *Remote Access Setup* screen.



The Remote Access Setup program lets the user:

- Select and configure network protocols
- Select ports for RAS to use
- Select how each port will be used: *Dialing out, Receiving call,* or *Both*.

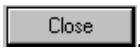
- Select one port then click on  to define the selected port usage.

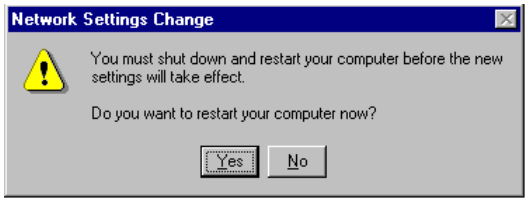


Configure the specified port to be used:

- As a client (*Dial out only*)
- As a server (*Receive calls only*)
- Both (*Dial out and Receive calls*)

- Validate by clicking on  .

- When all steps of settings have been verified, click on  .



Click on  to restart the computer so that the driver takes into account all the changes.

Note:

- It is recommended to refer to Microsoft's **R**emote **A**ccess **S**ervice **Help** for more information on the *Remote Access Setup* program.

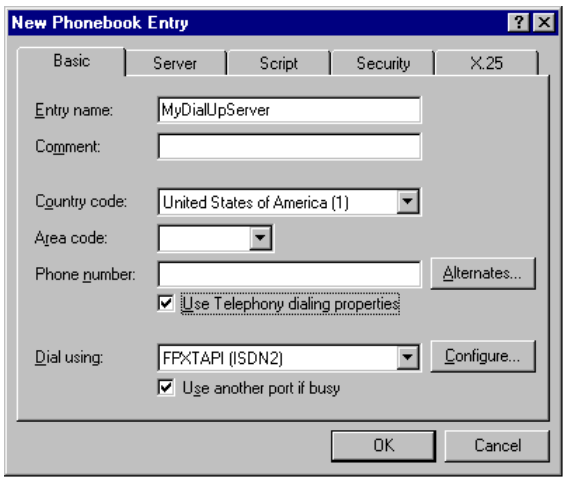
Getting started

Once the RAS Service has been defined, the FPX adapter must be loaded.

- First select the adapter to be loaded, click on the *Commands* menu, then click on the *Immediate loading* command.
- Use the *Dynamic reconfiguration of RAS driver* command so that the driver takes into account all the changes made, without restarting the machine.

Adding an entry in the Phonebook

- From the Desktop, double-click on ***My Computer,*** then double-click on the ***Dial-Up Networking*** icon to display the main screen.
- Click on the New... button to display the *New Phonebook Entry* screen, and create an entry, by giving all information to ensure a valid connection.



- Fill in the different fields, and use the Microsoft's Online Help for more explanation.
- Click on Configure... to define the *Dial using.*
- In the *Phone number* field, don't forget the switching prefixe (refer to the FPX adapter configuration).
- Confirm by OK.

Note about the **Phone Number** syntax**:**

- The parameters enclosed between [ ] are optional.

NetworkAddress [**-***NetworkSubAddress*][**/***Speed*][*****Facilities*][**#**][**M** or **m**]

with

NetworkAddress	Outgoing network address, either X.25, PSTN or ISDN (16 characters maximum)
-*NetworkSubAddress*	Outgoing network sub-address, either X.25, PSTN or ISDN (10 characters maximum)
/Speed	Speed in bits per second, range from 2400 to 64000
*****Facilities*	Facilities field corresponding to additional options
#	Add a PAD protocol identifier to the outgoing call (PID = 01 00 00 00, hexadecimal values)
M or **m**	Send and receive asynchronous frames for an outgoing connection

- For example: 1133010203-02/9600

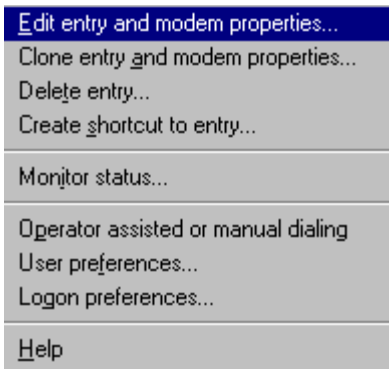
Remainder

When receiving an incoming call that includes a PAD protocol identifier, the FpxTapi driver automatically detects this PID and adapts its behavior accordingly.
The basic operating mode of the FpxTapi driver is to work with synchronous frames since it is designed for ISDN networks.
However, when it receives incoming frames with an asynchronous protocol (from a PAD for example), the FpxTapi driver automatically detects this type of frame and uses asynchronous frames to reply.

Updating an entry in the Phonebook

- From the *Dial-Up Networking* screen, double-click on 

to display the update commands.

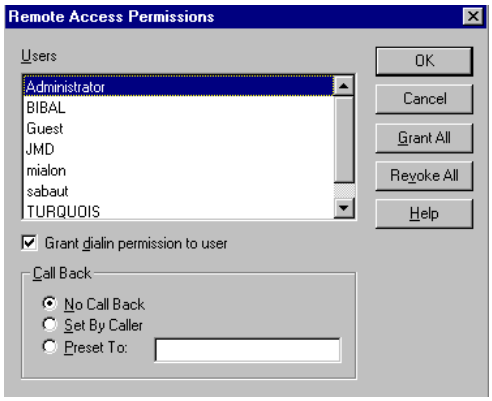


- Use the Microsoft's Online Help for more explanation.

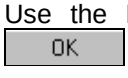
Checking permissions on the Remote Access Server

The user's permissions must be checked on the remote server.

- From the *Program* task, select the *Administrative Tools,* then double-click on the **Remote Access Admin** to go to the *Remote Access Admin on* *ServerName* dialog box. The *ServerName* is the computer name defined during Windows NT installation.



- Select the *Users* menu, then click on the *Permissions...* command and verify the user's rights.
- Check the *Grant dialin permission to user* option to grant permission to the selected user.
- Select one *Call Back* option.

- *No Call back:* to disable call back for a user account.
- *Set By Caller:* to prompt the user for a number.
- *Preset to:* to call the user at fixed number (entered in the opposite field).
- Use the Microsoft's Online Help for more explanation. Validate by clicking on 

Connecting to the Remote Access Server

- From the *Dial-Up Networking* screen, select the Phonebook entry previously prepared then click on Dial to connect to the remote site.
- Verify the fields: Username, Password, Domain, then validate by clicking on OK.

- While the connection is being established, a window is opened and shows various steps:
  - Dialing, ...

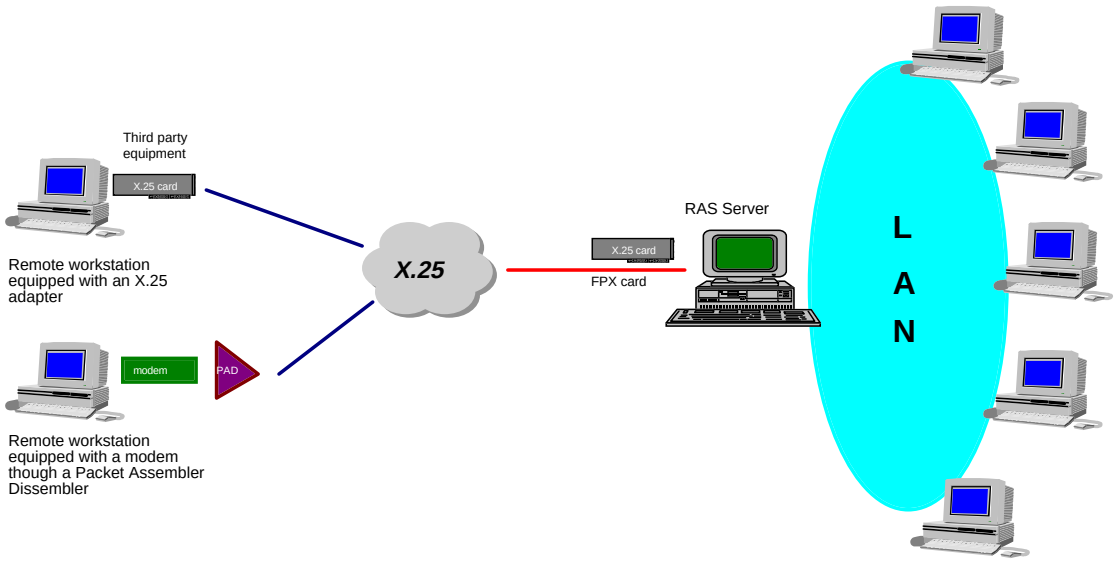
The *Dial-Up Networking Monitor* screen shows the different status: CD is green, TX and RX are blinking if OK.

- Use the Microsoft's Online Help for more explanation.

Accepting asynchronous connections

The FpxTapi driver has been designed to work on ISDN networks, and consequently to use synchronous protocols. However, it can also accept asynchronous connections incoming from a PAD or from another X.25 third party device.

To do this, select the FPX RAS Support with FPX PassLan/IP compatibility option.



As described before, various separators can be used to set up an outgoing connection to manage the PAD protocol identifier or asynchronous frames.

When the connection is an incoming connection, the FpxTapi driver automatically detects the frame format and/or the PID, and adapts its behavior to respond correctly.

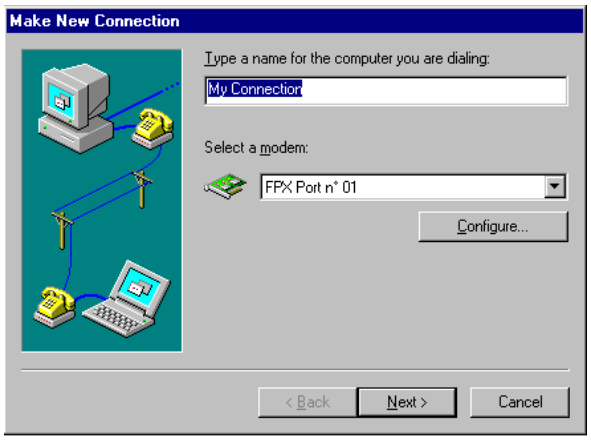
When receiving an incoming call with a PAD PID, the driver sends a PAD profile via a SET parameter command. A default profile is provided in the registry and is used only if PID management is necessary (either by using the # separator in an outgoing call or, when receiving an incoming call, with the PAD protocol identifier).

Note: It is recommended not to modify the default values of parameters that have been defined in the registry for the PAD profile. The user can refer to appendix D to change them when necessary.

Configuring Remote Access Service on Windows 95

- Run the **Dial-Up Networking** task.

- Double-click on the **Make New Connection** icon to display the *Make New Connection* screen.



The program lets the user:

- Define its connection
- Select port for RAS to use,..

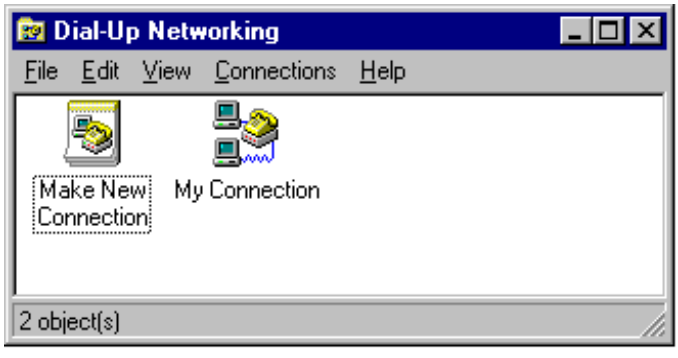
Then by clicking on 

, define other parameters as:

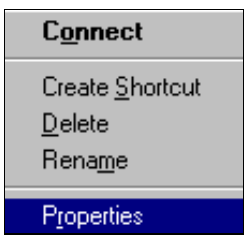
- *Phone number* for the computer to call,... (don't forget the switching prefix: refer to the FPX adapter configuration).

- Click on 

to terminate the configuration and display the following screen.



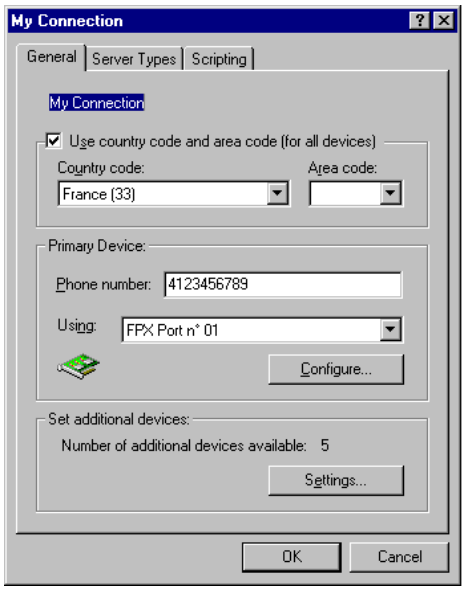
- From the *Dial-Up Networking* screen, select **My connection** and click on the mouse right button to display the short-cut menu below.



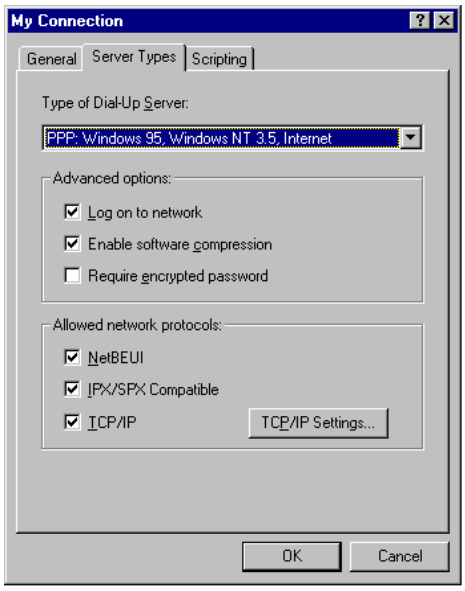
- Click on *Properties* command.

This *Properties* command is used to configure the parameters by using the different tabs to ensure a valid connection:

- *General,*
- *Server Types,*
- *Scripting.*



- Fill in the different fields, and use the Microsoft's Online Help for more explanation.
- In the *Phone number* field, don't forget the switching prefixe (refer to the FPX adapter configuration: in this example, 4 is the prefix).
- Click on Configure... to define the *Dial using.*
- Confirm by OK.



- Select the *Type of Dial-Up Server* in the list box, then check options in *Advanced options* and select the *Allowed Network protocols,* according to the configuration which can be used by the micro-computer.
- Click on TCP/IP Settings... to check the TCP/IP parameters, and change them if necessary.
- Confirm by OK.

Notes:

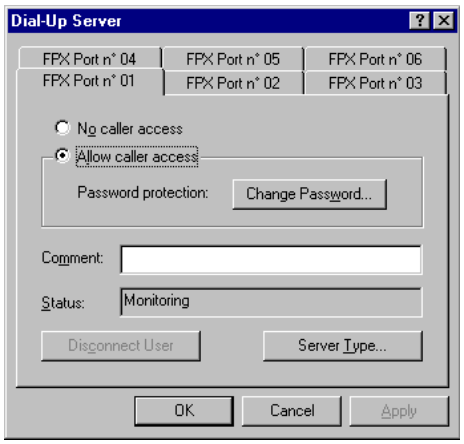
- The **Getting started** step is noted in the NT section and the principle stays identical.
- **Connecting to the Remote Access Server** is done by double-clicking on the connection previously prepared (**My connection**). While the connection is being established, a window is opened and shows various steps: dialing,...

Setting up the Dial-Up Server

- From the *Dial-Up Networking* screen, select the *Connections* menu.

- Click on *Dial-Up Server...* command.

The user's permissions must be checked on the remote server.



- Configure the specified port(s) to be used (01 in this example), check the *Allow caller access* option to determine the selected port usage.
- In this case, the receive calls are authorized and the micro-computer runs as "a server".

It is recommended to control the *Server Type* before the validation by OK.

- Use the Microsoft's Online Help for more explanation.

CHAPTER 7

7

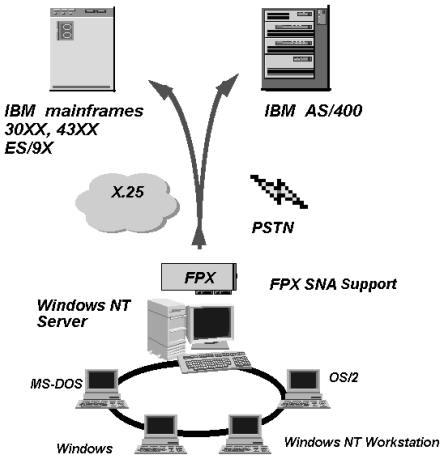
FPX SNA Support

Windows NT

This chapter describes how to start the FPX SNA Support component included in the FPX product Services.

About this component

The FPX SNA Support runs on the FPX adapters and provides the Windows NT SNA Server with the capability of connecting to SNA hosts across packet-switched data networks (X.25) and switched or leased line networks (SDLC).



It uses Microsoft SNA Server client/server architecture to link desktop personal computers to IBM mainframes accessible via the SNA protocols.
A client machine can run Windows NT, Windows 95, Windows, MS-DOS, OS/2 or Macintosh operating systems and can use standard local area network protocols to connect to the server.

Software installation

Before setting up the FPX SNA Support component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

SNA Server Version 2.11 and FPX Links

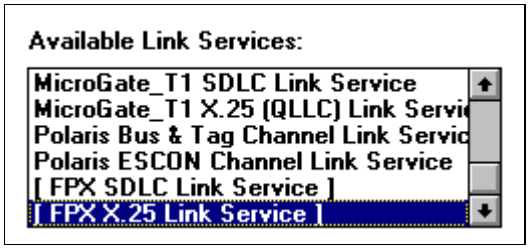
The SNA Server must be installed on the Windows NT server before installing the FPX SDLC or X.25/QLLC link.

The SNA Server is supplied on a CD-ROM. Please refer to the Microsoft SNA Server Installation Guide for installation instructions.

The instructions below provide a quick implementation of a primary SNA Server, from the **BACK OFFICE**. These instructions apply to CD-ROM SNA Server installation. Follow these steps to install SNA correctly.

Follow these steps to correctly install the product:

- Insert the SNA Server CD-ROM into the CD-ROM drive, then execute SETUP.EXE.
- With the BACK OFFICE install program, select **SNA Server installation,** then validate to display the *Welcome to Microsoft SNA Server Setup* dialog box.
- Click on Continue to go to the *Choose Licensing Mode* dialog box.
- Select the appropriate mode and click on Continue.
- Fill in the user name, the company name and the product identifier, then click on Continue.
- From the *Select Client/Server Protocols* dialog box, select one or several or all the check boxes and click on Continue..
- Enter the path in the *Installation Path* dialog box and click on Continue.
- Specify the Network Domain Name and click on Continue.
- Select a **Primary Configuration Server** and click on Continue.
- The *Review Settings* screen appears. The program is ready to copy files.
- Check the Install Online documentation option if desired and click on Continue if no modification is necessary. *Copying files*... is displayed.
- If the help has been previously checked, enter a directory path for the help files.
- Confirm by clicking on Continue to display different messages as *Creating Services...,* then the *Link Service Installation* screen and to install the **Link**.
- Remove the SNA Server CD-ROM and insert the CD-ROM labeled FPX Windows NT into the appropriate drive, click on Other... then enter the following path: "%**unit**%**\I386\us\sna21**" and validate by clicking on Continue to continue the automatic process, and make the *Link Service Installation* screen appear.



At this point, the FPX links have to appear at the end of the list, in the *Available Link Services* sub-window.

- Use the button to see the 2 FPX links.

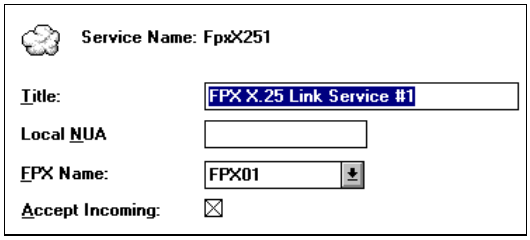
Note:

X.25/QLLC driver for X.25 connections

SDLC driver for SDLC connections

Installing the FPX X25 Link

- Select **FPX X25 Link Service**, click on Install.

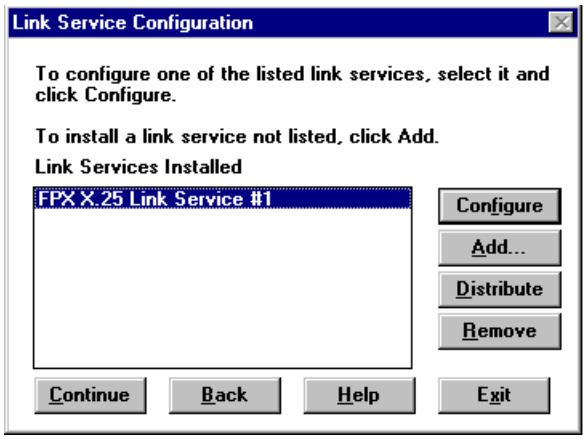


- The *FPX X25 Link Service Setup* is displayed.
- Fill in the different fields.

The *Service Name* defines the name of the Link service and the cloud indicates that the link is an X.25 link.

Parameter	Meaning
Title	Link designation
Local NUA	X.25 local address (15 characters). The *Full addressing* option, in the *Adapters* configuration have to be checked.
FPX Name	Name of the FPX used for this particular link.
Accept incoming	When checked, the incoming calls can be received.

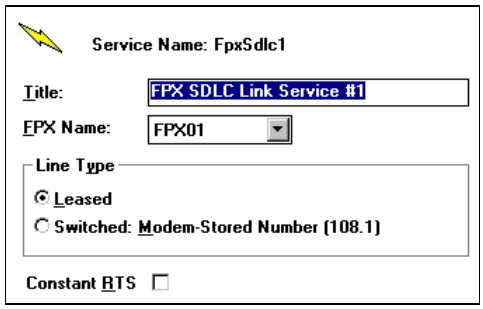
- Validate by clicking on Continue. The link has been successfully installed. It is listed in the *Link Services Installed* list box, in the *Link Service Configuration* screen.



- Click on Exit to exit the SNA setup program.

Installing the FPX SDLC Link

- Select **FPX SDLC Link Service**, click on Install.



- The *FPX SDLC Link Service Setup* is displayed.
- Fill in the different fields.

The *Service Name* defines the name of the Link service and the spark indicates that the link is an SDLC link.

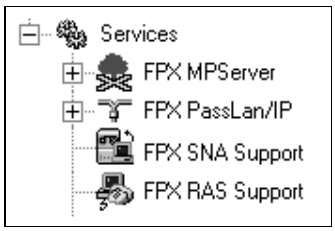
Parameter	Meaning
Title	Link designation
FPX Name	Name of the FPX used for this particular link.
Line type	Select a phone line: *Leased* or *Switched* • Leased: private • Switched: number stored in the modem, dialing when the DTR signal on the modem is set (refer to V.25bis modem)
Constant RTS	Check this option, if the used line is full duplex.

- Validate by clicking on Continue. The link has been successfully installed. It is listed in the *Link Services Installed* list box, in the *Link Service Configuration* screen (as described in the previous section, for the FPX X25 Link).

- Click on Exit to exit the SNA setup program.

Verifying the installation

- When the setup is complete, select **FPX Configuration.**



- The tree is modified, FPX SNA Support is added under Services.

On the right side of the screen, the message **Please use the SNA configuration tool to set the FPX Link service** is displayed.

SNA Server Admin Interface

Overview

Once the SNA Server and the FPX Link Service have been installed, use the ***SNA Server Admin*** program: the graphical interface allows the user to configure connections between Pc and remote computers - IBM mainframes, AS/400s or other PCs - within an IBM SNA network. It is structured around three windows that appear inside the main window. The windows can be shrunk to icons, and then restored to windows.

- Configure servers, connections, and logical units (LUs).
- Start and stop servers and connections.
- Reset LUs.

- Configure LU pools.

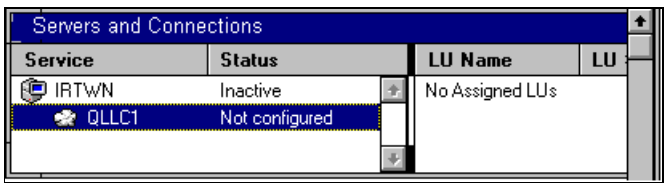
- Assign items for users: LUs, LU pools and properties.

Sample configuration

This example is intended to show a quick set up of SNA Server and a specific FPX link service. For more information, please refer to the SNA Server Administration Help.

- The Microsoft **SNA Server (Common)** task and the associated utilities are added to the **Start Menu Programs**.
- Select **SNA Server Admin** to display the *SNA Server Admin* main window.

QLLC connection



In this example, the FPX QLLC link service was installed previously with SNA Server.

The QLLC1 Connection must be configured in order to ensure proper operation of the link service.

- To configure it, double-click on 

.

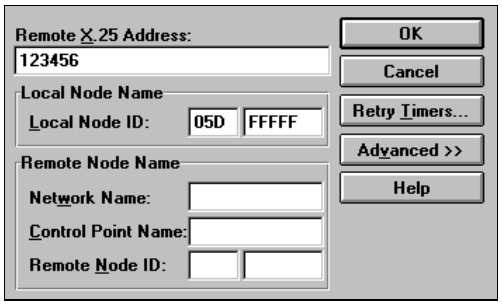
Initial QLLC Connection Properties

- When the *Connection Properties* screen is displayed, configure the different fields.

Parameter	Meaning
Connection Name	The QLLC1 name is the default name assigned by SNA Server during installation of the link service. The name can be from one through eight characters long, and can contain alphanumeric characters as well as special characters £, # and @.. Lowercase letters are converted to uppercase.
Comment	A comment up to 25 characters long
Link Service	Represents the corresponding FPX Link Service. It enables the connection with the FPX communication adapter.
Remote End	Defines the type of remote system for this connection: • Host system • Peer system • Downstream system
Activation	Indicates the activation settings: • On Server Startup • On Demand • By Administrator
Allowed Directions	Defines the allowed call directions: • Outgoing Calls • Incoming Calls
Virtual Circuit Type	Indicates the type of virtual circuit used by this connection: • Switched (SVC) • Permanent (PVC)

Basic X.25 settings

Once the initial X.25 connection properties have been defined, the basic X.25 settings must be configured.



- To do this, click on 

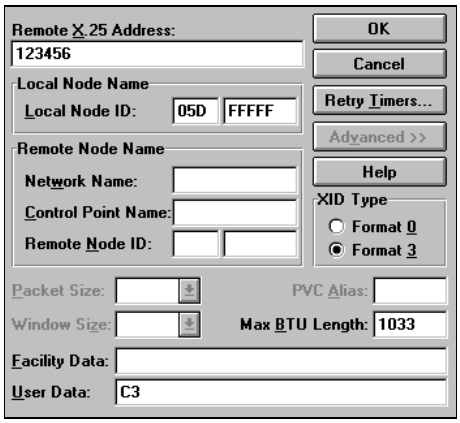
. The *X.25 Setup* dialog box is displayed.

Parameter	Meaning
Remote X.25 address	X.25 remote system address. It consists of 1 to 15 hexadecimal digits.
Local Node ID	Eight digit hexadecimal number which identifies the local system. The first three digits are the block number, the last five are the node number.
Network Name	SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @.

Parameter	Meaning
Control Point Name	Control point name associated with the SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @.
Remote Node ID	Eight digit hexadecimal number which identifies the remote system. The first three digits are the block number, the last five are the node number.

Advanced X.25 settings

After configuring the basic X.25 settings, the advanced X.25 parameters can be defined.



- Click on Advanced >>.

Parameter	Meaning
XID Type	Defines the type of identifying information for SNA Server to send: • Format 0 (only sends the Node ID) • Format 3 (sends up to 100 bytes of identifying information)
Max. BTU Length	Specifies the maximum length for the Basic Transmission Unit. It represents the number of bytes transmittable in a single data-link information frame.
Facility Data	Specifies the codes for any facility data required by the network provider or by the administrator of the remote system (63 hexadecimal bytes maximum).
User Data	Specifies the codes for any user data required by the network provider (even number of hexadecimal characters up to 32 characters). It is a coded string of information indicating items such as the communication protocol identifier used by the PSDN network. For SNA, since this protocol is QLLC this field is C3.

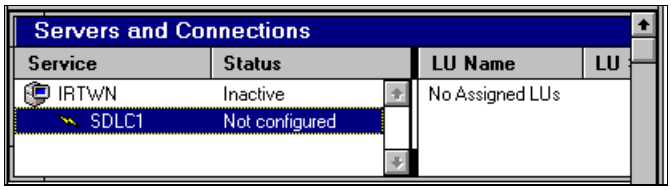
Retry timers

The connection activation limits can be configured from the *X.25 Setup* dialog box by clicking on Retry Timers.... Fill in the following fields.

Parameter	Meaning
Maximum number of attempts	Number of SNA Server attempts (in the list box) to make when trying to establish the connection.
Delay after failed attempts	Length of time for SNA Server (in the list box) to wait between attempts, to establish the connection.

- Confirm all the settings by clicking on OK.

SDLC connection



In this example, the FPX SLLC link service was installed previously with SNA Server.

The SDLC1 Connection must be configured in order to ensure proper operation of the link service.

- To configure it, double-click on 

.

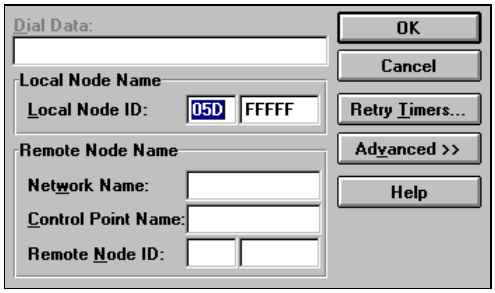
Initial SDLC Connection Properties

- When the *Connection Properties* screen is displayed, configure the different fields.

Parameter	Meaning
Connection Name	The SDLC1 name is the default name assigned by SNA Server during installation of the link service. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @. Lowercase letters are converted to uppercase.
Comment	A comment up to 25 characters long
Link Service	Represents the corresponding FPX Link Service. It enables the connection with the FPX communication adapter.
Remote End	Defines the type of remote system for this connection: • Host system • Peer system • Downstream system
Activation	Indicates the activation settings: • On Server Startup • On Demand • By Administrator

Basic SDLC settings

Once the initial SDLC connection properties have been defined, the basic SDLC settings must be configured.



- To do this, click on 

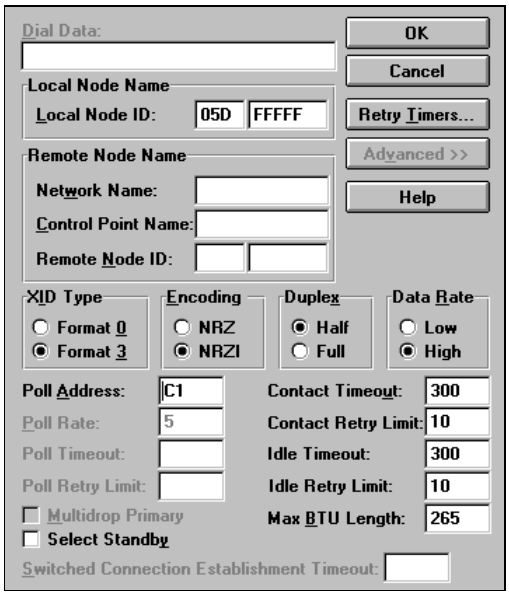
. The *SDLC Setup* dialog box is displayed.

Depending on the type of line selected during the link service installation (leased or switched modem-stored number), some parameters may not be available.
They are grayed in the dialog box.

Parameter	Meaning
Dial Data	When connections are made on a switched line, this defines the data used for dialing (from 1 through 40 characters).
Local Node ID	Eight digit hexadecimal number which identifies the local system. The first three digits are the block number, the last five are the node number.
Network Name	SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @.
Control Point Name	Control point name associated with the SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @.
Remote Node ID	Eight digit hexadecimal number which identifies the remote system. The first three digits are the block number, the last five are the node number.

Advanced SDLC settings

After configuring the basic SDLC settings, the advanced SDLC parameters can be defined.



- Click on Advanced >>.

Depending on the type of line selected during the link service installation (leased or switched modem-stored number), some parameters may not be available. They are grayed in the dialog box.

Parameter	Meaning
XID Type	Defines the type of identifying information for SNA Server to send: • Format 0 (sends only the Node ID) • Format 3 (sends up to 100 bytes of identifying information)
Encoding	Identifies the encoding scheme used by the modem: • NRZ (Non return to zero) • NRZI (Non return to zero inverted)
Duplex	Represents settings that match the modem type: • Half for a half-duplex modem • Full for a full-duplex modem For the multipoint, the *Full Duplex* option must be checked and *Constant RTS* option must absolutely not be checked.
Data Rate	Represents settings that match data transmission rate between the modem and the FPX adapter: • Low results in more reliable transmissions and prevents errors sometimes caused by poor-quality lines at the high rate. • High results in faster transmissions.

Parameter	Meaning
Poll Address	Corresponds to the two-digit hexadecimal number that defines the poll address. If the remote system is a host, the poll address should match the VTAM PU definition for the ADDR=parameter. If the remote system is a peer, the poll value can be any value except 00 and FF.
Poll Rate	Specifies the poll rate from 1 through 50 polls per second for a peer or a downstream system.
Poll Timeout	Specifies the length of time, in tenths of second, for the local system to wait for a response to a poll before trying again. The range is from 1 through 300 (30 seconds). This is only for a peer or downstream connection.
Poll Retry Limit	Specifies the number of times for the local system to poll the remote system if there is no response. The range is from 1 through 255. This is only for a peer or downstream connection.
Contact Timeout	Specifies the length of time, in tenths of second, which the local system should wait between attempts to make a connection with a remote system. The range is from 5 through 300 (30 seconds). This parameter is ignored for incoming calls.
Contact Retry Limit	Specifies the maximum number of times the local system should attempt to make a given connection. The range is from 1 through 20.
Idle Timeout	Specifies the length of time, in tenths of second, for the local system to wait for a response to a transmission before trying again. The range is from 1 through 300 (30 seconds). This is only for a host or peer connection.
Idle Retry Limit	Specifies the number of times for the local system to try to send data to the remote system if there is no response. The range is from 1 through 255. This is only for a host or peer connection.
Max. BTU Length	Specifies the maximum length for the Basic Transmission Unit. It represents the number of bytes that can be transmitted in a single data-link information frame.
Multidrop Primary	Indicates that the server will be the primary station for a multidrop connection if the line used is an SDLC leased line to a downstream system.
Select Standby	Specifies whether the modem requires the standby line setting.
Switched Connection Establishment Timeout	If the connection uses a switched SDLC line (standard telephone line), this specifies the number of seconds given to the user or modem to dial the remote computer's number.

Retry timers

The connection activation limits can be configured from the *SDLC Setup* dialog box by clicking on 

.

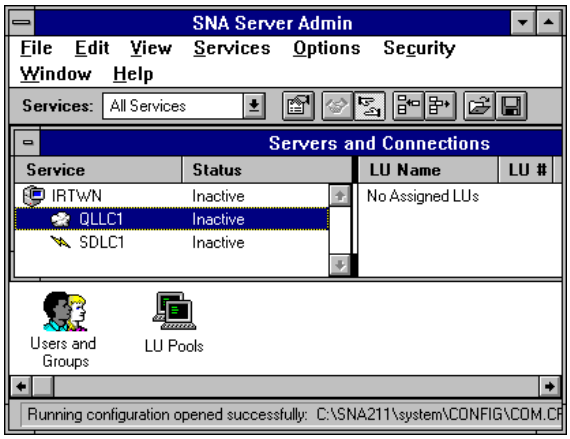
Parameter	Meaning
Maximum number of attempts	Number of attempts for SNA Server (in the list box) to make when trying to establish a connection.
Delay after failed attempts	Length of time for SNA Server (in the list box) to wait between attempts to establish a connection.

- Confirm all the settings by clicking on 

.

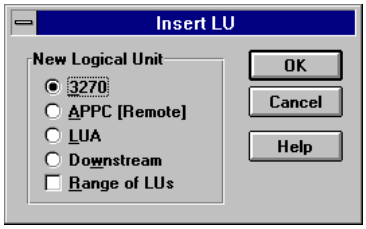
LU configuration

This section of the manual describes the steps required to configure an LU for 3270 emulation. This is only an example and the user should refer to the SNA Administration Guide for detailed information.

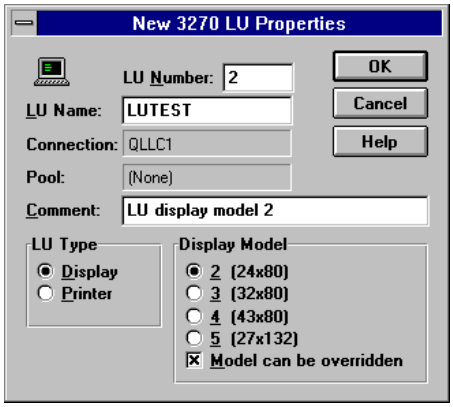


The connection (QLLC or SDLC) has been configured, and the Inactive state indicates that the node is not started and that the connection has not been established.

The *No Assigned LUs* statement in the right column indicates that the 3270 LU that will access the host system must be configured.



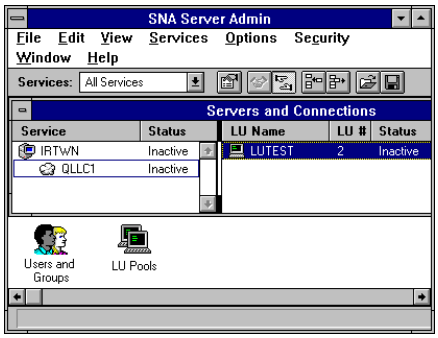
- From the *SNA Server Admin* program, select the *Services* menu, then the *Assign LUs* command.
- Click on 3270 then click on OK.



LU Number field identifies the LU on the connection.
LU Name field identifies the LU.
Connection specifies the connection used by this LU.

The 3270 LU can be used for display or printing. For a display LU, the display model can be specified to control the display size.

- When all parameters are set, click on OK to go back to the *Servers and Connections* window.



The new LU that has been created is defined as Inactive in the right column.

Setting Up User and Group Access

In order for users to be recognized by SNA Server, they must have accounts on the LAN (Local Area Network). Once these accounts have been created, users can be added to the list used by SNA Server.

- To add a new user, double-click on the ***Users and Groups*** icon in the *SNA Server Admin* main window.

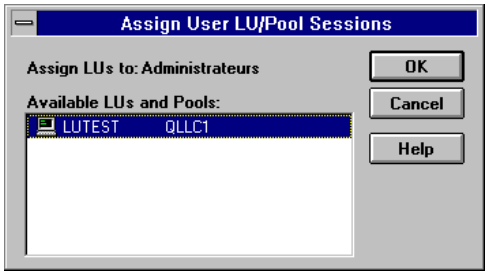
The *Users and Groups* dialog box is now displayed. To add a new user, follow the instructions below:

- Select the *Users* menu then the *New User...* command.
- In the *List Names From* box, select the domain from which to list users (or groups) who have accounts or select the name of the local server.
- In the *Names* box, from the list of users and groups who have accounts, select the one to add.
- Click on Add, then validate by clicking on OK.
- From the *File* menu, click on *Save Configuration* (the configuration is defined as [Out Of Date] in the Users and Groups title: Users and Groups - [Out of Date]).

Giving the new user access to the 3270 LU

The new user can access the host using the 3270 LU only if this LU is assigned to the user account. This can be done by executing the following steps:

- Go to the *Users and Groups* window, select the *View* menu from the *SNA Server Admin* program and click on the *Configured Users* command.
- Select the user to which the LU will be assigned.
- From the *Users* menu, click on the *Assigned LUs* command.



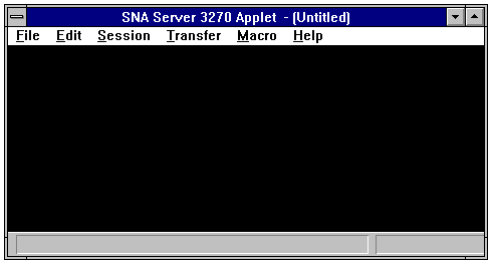
The *Assign User LU/Pool Sessions* dialog box is displayed.

- Select the LU and click on OK.
- From the *File* menu, click on *Save Configuration* (the configuration is defined as [Out Of Date] in the Users and Groups title: Users and Groups - [Out of Date])

Starting a 3270 session

- From the *SNA Server Admin* screen, select the **node**, then the *Services* menu and the *Start Services* command.
- Activate the QLLC1 connection in the same way.
- When the connection is active, go to the **SNA Server (Common)** task.
- Select the ***3270 Applet***.

- The 3270 Applet screen is displayed:



- Select the *Session* menu, then the *Session configuration* command.

- Select the LU. Define the page code and click on OK.
- Select the *Session* menu, then the *Connect* command. The remote host banner is displayed on the screen.
- Continue the session using the host identification commands.

SNA Server Version 3.0 and FPX Links

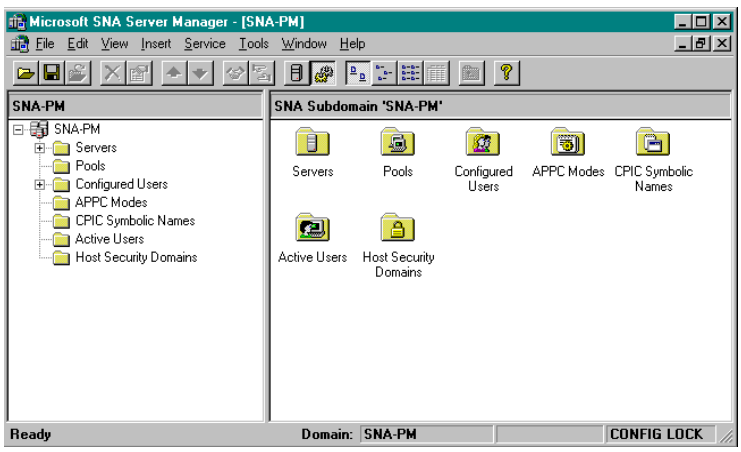
The SNA Server 3.0 must be installed on the Windows NT server before installing the FPX SDLC or X.25/QLLC link.

This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.
The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM into the appropriate drive, and validate by clicking on Continue to continue the automatic process.
- Run the **FPX Link Services Setup** program from the SNA 3.0 directory of the FPX Windows NT CD-ROM :
  "%**unit**%**\I386\us\sna30**"
- The FPX Link Services components are copied into the SNA Server directory and the registry is upgraded. The FPX Link Services are added to the available links.

- When the message **Setup Succeeded** is displayed, click on Run SNA Manager to continue and configure the link or click on Exit Setup to quit the **Setup program** (the Link can subsequently be configured).

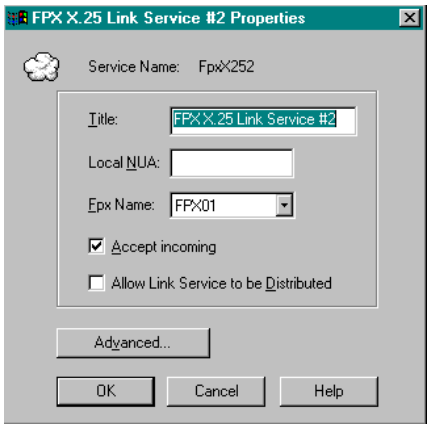
- The SNA Server Administration program, now named *SNA Server Manager*, has been redesigned to display a tree with a hierarchy of all SNA Server resources.



- Click on a branch of the tree in the left panel to display resources linked to that branch in the right panel.

Installing the FPX X25 Link

- From *the Microsoft SNA Server Manager* screen, click on the *Insert* menu.
- Click on the *Link Service...* command to display the *Insert Link Service* screen, containing all available Link Services.
- Select **FPX X25 Link Service**, click on Add...



- The *FPX X25 Link Service Properties* is displayed.
- Fill in the different fields.

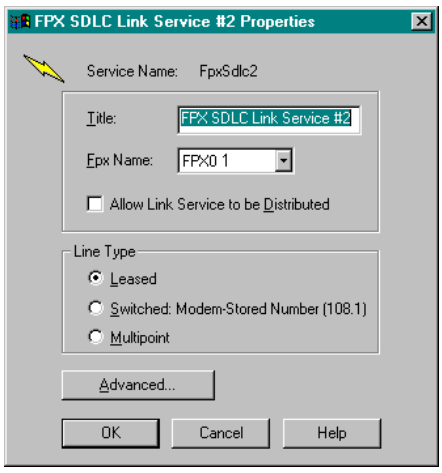
The *Service Name* defines the name of the Link service and the cloud indicates that the link is an X.25 link.

Parameter	Meaning
Title	Link designation
Local NUA	X.25 local address
FPX Name	Name of the FPX used for this particular link.
Accept incoming	When checked, the incoming calls can be received.
Allow Link service to be Distributed	When checked, make the Link to be accessible by the Remote Link Service on other SNA Server.

- Click on Advanced... if the user wants to change FPX parameters.
- Validate by clicking on OK. The link has been successfully installed..

Installing the FPX SDLC Link

- From *the Microsoft SNA Server Manager* screen, click on the *Insert* menu.
- Click on the *Link Service...* command to display the *Insert Link Service* screen, containing all available Link Services.
- Select **FPX SDLC Link Service**, click on Add...



- The *FPX SDLC Link Service Properties* is displayed.
- Fill in the different fields.

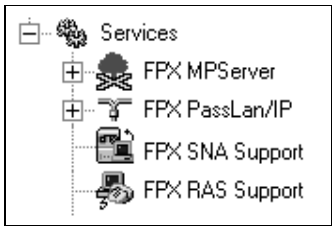
The *Service Name* defines the name of the Link service and the spark indicates that the link is an SDLC link.

Parameter	Meaning
Title	Link designation
FPX Name	Name of the FPX used for this particular link.
Allow Link service to be Distributed	When checked, make the Link to be accessible by the Remote Link Service on other SNA Server.
Line type	Select a standard phone line: *Leased* or *Switched* • Leased: dedicated telecommunication line used for SDLC point to point connection. • Switched: number stored in the modem, dialing when the DTR signal on the modem is set (refer to V.25bis modem) : standard dial-up telephone line used for SDLC connections. • Multipoint : dedicated telecommunication line used by multiple secondary SDLC stations. *For Multipoint Line type, set the Duplex parameter of the SNA Server connection to Full.*

- Click on Advanced... if the user wants to change FPX parameters.
- Validate by clicking on OK. The link has been successfully installed.

Verifying the installation

- When the setup is complete, select **FPX Configuration.**



- The tree is modified, FPX SNA Support is added under Services.

On the right side of the screen, the message **Please use the SNA configuration tool to set the FPX Link service** is displayed.

SNA Server Manager Interface

Overview

Once the SNA Server and the FPX Link Service have been installed, use the ***SNA Server Manager*** program: the graphical interface allows the user to configure connections between Pc and remote computers - IBM mainframes, AS/400s or other PCs - within an IBM SNA network.
It is structured around two parts: a tree on the left panel, and the resources linked to a branch on the right panel. The resources can be shown in a *Services* view or a *Servers* view.

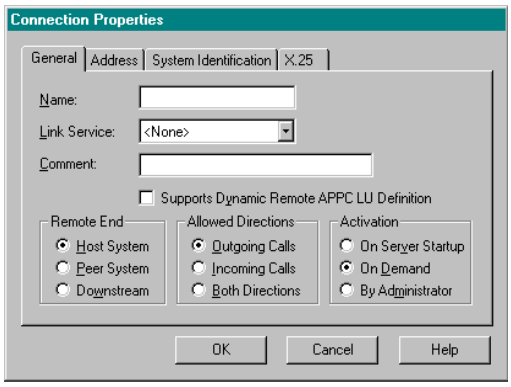
Sample configuration

This example is intended to show a quick set up of SNA Server and a specific FPX link service. For more information, please refer to the SNA Server Manager Help.

- The Microsoft **SNA Server (Common)** task and the associated utilities are added to the **Start Menu Programs**.
- Select **SNA Server Manager** to display the Microsoft *SNA Server Manager* main window.

QLLC connection

- From the Microsoft SNA Server Manager program, click on the *Insert* menu, then select the *Connection* command.
- Click on *X25* to display the *Connection properties* screen and configure the QLLC1 connection in order to ensure proper operation of the link service.



- From the *General* tab, fill in the different fields, then select :
  Address tab,
  System identification tab,
  X.25 tab.

General settings

Parameter	Meaning
Name	Connection name, from one through eight characters long, which can contain alphanumeric characters as well as special characters £, # and @.. Lowercase letters are converted to uppercase.
Link Service	Represents the corresponding FPX Link Service. It enables the connection with the FPX communication adapter.
Comment	A comment up to 25 characters long
Supports Dynamic Remote APPC LU	When checked, dynamic remote APPC LU can be used, even if the remote LU has not been configured in SNA Server Manager.
Remote End	Defines the type of remote system for this connection: • Host system • Peer system • Downstream system
Allowed Directions	Defines the allowed call directions: • Outgoing Calls • Incoming Calls • Both Directions
Activation	Indicates the activation settings: • On Server Startup • On Demand • By Administrator

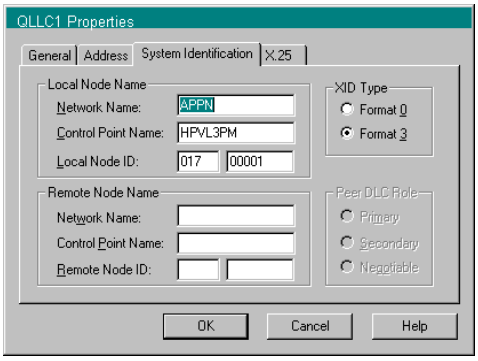
Address settings

- Click on the *Address* tab, then fill in the following fields to indicate the type of virtual circuit used by the connection.

Parameter	Meaning
Switched Virtual Circuit Address	X.25 remote system address, consists of 1 to 15 hexadecimal digits.
Permanent Virtual Circuit Alias	Permanent Virtual Circuit Alias of the host: number identifying the channel (1 for the first channel, 2 for the second...).

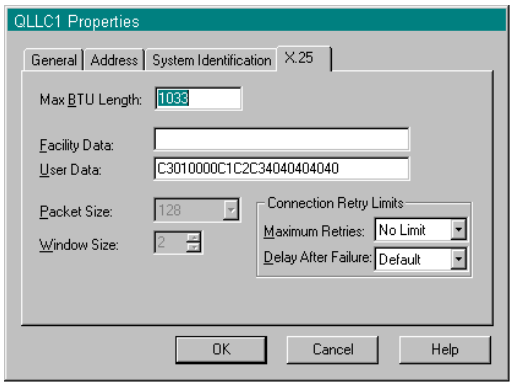
System identification settings

- Once the initial X.25 connection properties have been defined, click on the *System identification* tab, then click on *X25* tab.



Parameter	Meaning
Local Network Name	SNA network name of the local system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @. *The Network Name works with the Control Point Name to identify a system*.
Local Control Point Name	Control point name associated with the SNA network name of the local system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @. *The Control Point Name works with the Network Name to identify a system*.
Local Node ID	Eight digit hexadecimal number which identifies the local system. The first three digits are the block number, the last five are the node number. Values 000 and FFF for the first three digits are reserved.
Remote Network Name	SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @. *The Network Name works with the Control Point Name to identify a system*.
Remote Control Point Name	Control point name associated with the SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @. *The Control Point Name works with the Network Name to identify a system*.
Remote Node ID	Eight digit hexadecimal number which identifies the remote system. The first three digits are the block number, the last five are the node number. Values 000 and FFF for the first three digits are reserved.
XID Type	Defines the type of identifying information for SNA Server to send: • Format 0 (only sends the Node ID) • Format 3 (sends up to 100 bytes of identifying information) If the user wants independent APPC LUs on its connection, he has to use format 3.
Peer DLC Role	Select the Peer DLC Role for Peer to Peer communications. • Primary: The SNA Server will assume the Primary DLC role. It should be selected if the remote system does not support negotiable DLC roles (i.e. the remote is configured as a secondary DLC station). • Secondary: The SNA Server will assume the Secondary DLC role. It should be selected if the remote system does not support negotiable DLC roles (i.e. the remote is configured as a primary DLC station). • Negotiable: The SNA Server and the remote system will negotiate their respective role during connection startup.

X.25 settings



- Click on *X25* tab, then fill in the X.25 specific fields.

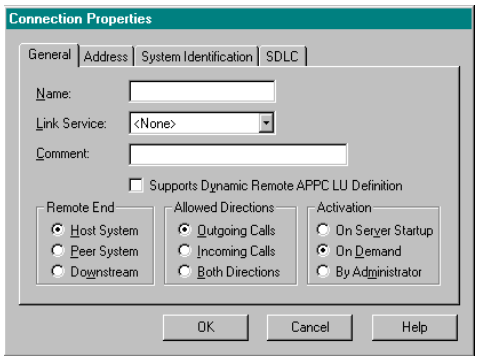
Parameter	Meaning
Max. BTU Length	Specifies the maximum length for the Basic Transmission Unit. It represents the number of bytes transmittable in a single data-link information frame.
Facility Data	For an SVC, specifies the codes for any facility data required by the network provider or by the administrator of the remote system (63 hexadecimal bytes maximum).
User Data	For an SVC, specifies the codes for any user data required by the network provider (even number of hexadecimal characters up to 32 characters). It is a coded string of information indicating items such as the communication protocol identifier used by the PSDN network. For SNA, since this protocol is QLLC this field is C3.
Packet Size	For a PVC only, select the maximum number of data bytes to be sent in a frame. Contact the administrator for more information.
Window Size	For a PVC only, select the maximum number of frames that the local system can send without receiving a response from the remote.
Maximum Retries	Number of SNA Server attempts (in the list box) to make when trying to establish the connection. Default = no limit.
Delay After Failure	Length of time for SNA Server (in the list box) to wait between attempts, to establish the connection. Default = 10s.

- Confirm all the settings by clicking on 

.

SDLC connection

- From the Microsoft SNA Server Manager program, click on the *Insert* menu, then select the *Connection* command.
- Click on *SDLC* to display the *Connection properties* screen and configure the connection in order to ensure proper operation of the link service.



- From the *General* tab, fill in the different fields, then select :
  Address tab,
  System identification tab,
  SDLC tab.

General settings

Parameter	Meaning
Name	Connection name, from one through eight characters long, which can contain alphanumeric characters as well as special characters £, # and @.. Lowercase letters are converted to uppercase.
Link Service	Represents the corresponding FPX Link Service. It enables the connection with the FPX communication adapter.
Comment	A comment up to 25 characters long
Supports Dynamic Remote APPC LU	When checked, dynamic remote APPC LU can be used, even if the remote LU has not been configured in SNA Server Manager.
Remote End	Defines the type of remote system for this connection: • Host system • Peer system • Downstream system
Allowed Directions	Defines the allowed call directions: • Outgoing Calls • Incoming Calls • Both Directions
Activation	Indicates the activation settings: • On Server Startup • On Demand • By Administrator

Address settings

- Click on the *Address* tab, and fill in the following fields.

Parameter	Meaning
Dial Data	When connections are made on a switched line, this field defines the data used for dialing (from 1 through 40 characters).
Pool Address	Corresponds to the two-digit hexadecimal number that defines the poll address. If the remote system is a host, the poll address should match the VTAM PU definition for the ADDR=parameter. If the remote system is a peer, the poll value can be any value except 00 and FF.
Encoding	Identifies the encoding scheme used by the modem: • NRZ (Non return to zero) • NRZI (Non return to zero inverted)

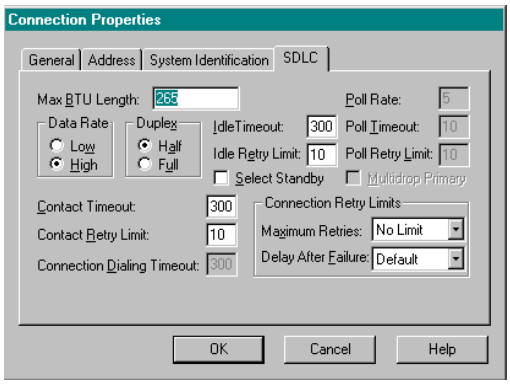
System identification settings

- Once the initial SDLC connection properties have been defined, click on the *System identification* tab, then click on *SDLC* to configure the settings below.

Parameter	Meaning
Local Network Name	SNA network name of the local system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @. *The Network Name works with the Control Point Name to identify a system*.
Local Control Point Name	Control point name associated with the SNA network name of the local system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @.*The Control Point Name works with the Network Name to identify a system*.

Parameter	Meaning
Local Node ID	Eight digit hexadecimal number which identifies the local system. The first three digits are the block number, the last five are the node number. Values 000 and FFF for the first three digits are reserved.
Remote Network Name	SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and special characters £, # and @. *The Network Name works with the Control Point Name to identify a system.*
Remote Control Point Name	Control point name associated with the SNA network name of the remote system. The name can be one through eight characters long, and can contain alphanumeric characters and the special characters £, # and @. *The Control Point Name works with the Network Name to identify a system.*
Remote Node ID	Eight digit hexadecimal number which identifies the remote system. The first three digits are the block number, the last five are the node number. Values 000 and FFF for the first three digits are reserved
XID Type	Defines the type of identifying information for SNA Server to send: • Format 0 (only sends the Node ID) • Format 3 (sends up to 100 bytes of identifying information) If the user wants independent APPC LUs on its connection, he has to use format 3.
Peer DLC Role	Select the Peer DLC Role for Peer to Peer communications. • Primary: The SNA Server will assume the Primary DLC role. It should be selected if the remote system does not support negotiable DLC roles (i.e. the remote is configured as a secondary DLC station). • Secondary: The SNA Server will assume the Secondary DLC role. It should be selected if the remote system does not support negotiable DLC roles (i.e. the remote is configured as a primary DLC station). • Negotiable: The SNA Server and the remote system will negotiate their respective role during connection startup.

SDLC settings



- Click on the *SDLC* tab, and fill in the SDLC specifc fields.

Parameter	Meaning
Max. BTU Length	Specifies the maximum length for the Basic Transmission Unit. It represents the number of bytes that can be transmitted in a single data-link information frame.
Data Rate	Represents settings that match the data transmission rate between the modem and the FPX adapter: • Low results in more reliable transmissions and prevents errors sometimes caused by poor-quality lines at the high rate. • High results in faster transmissions.

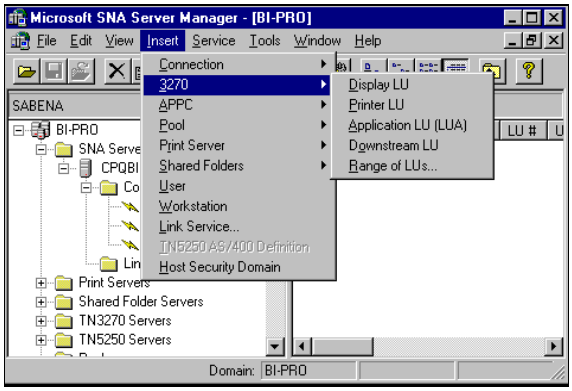
Parameter	Meaning
Duplex	Represents settings that match the modem type: • Half for a half-duplex modem • Full for a full-duplex modem *For Multipoint Line type, set the Duplex parameter of the SNA Server connection to Full*.
Idle Timeout	Specifies the length of time, in tenths of second, for the local system to wait for a response to a transmission before trying again. The range is from 1 through 300 (30 seconds). This is only for a host or peer connection.
Idle Retry Limit	Specifies the number of times for the local system to try to send data to the remote system if there is no response. The range is from 1 through 255. This is only for a host or peer connection.
Poll Rate	Specifies the poll rate from 1 through 50 polls per second for a peer or a downstream system.
Poll Timeout	Specifies the length of time, in tenths of second, for the local system to wait for a response to a poll before trying again. The range is from 1 through 300 (30 seconds). This is only for a peer or downstream connection.
Poll Retry Limit	Specifies the number of times for the local system to poll the remote system if there is no response. The range is from 1 through 255. This is only for a peer or downstream connection.
Select Standby	Specifies whether the modem requires the standby line setting.
Multidrop Primary	Indicates that the server will be the primary station for a multidrop connection if the line used is an SDLC leased line to a downstream system.
Contact Timeout	Specifies the length of time, in tenths of second, which the local system should wait between attempts to make a connection with a remote system. The range is from 5 through 300 (30 seconds). This parameter is ignored for incoming calls.
Contact Retry Limit	Specifies the maximum number of times the local system should attempt to make a given connection. The range is from 1 through 20.
Maximum retries	Number of attempts for SNA Server (in the list box) to make when trying to establish a connection.
Delay After Failure	Length of time for SNA Server (in the list box) to wait between attempts to establish a connection.

- Confirm all the settings by clicking on 

.

LU configuration

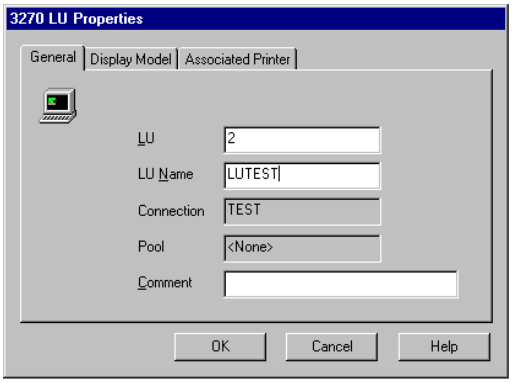
For the first time, it is recommended to use the 3270 Wizard or 5250 Wizard (*Tools* menu), giving some explanation to the user.
This section of the manual describes the steps required to configure an LU for 3270 emulation. This is only an example and the user should refer to the SNA On Line Help for detailed information.



The connection (QLLC or SDLC) has been configured, and appears on the left side of the screen (in this example, the spark indicates that the created connections are SDLC connections).

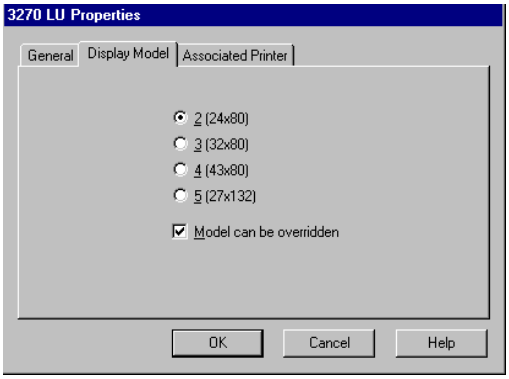
The node is not started and the SDLC connection has not been established.

- From the *SNA Server Manager* program, select the *Insert* menu, then click on the *3270* command, and click on the *Display LU* command to define the LU properties.



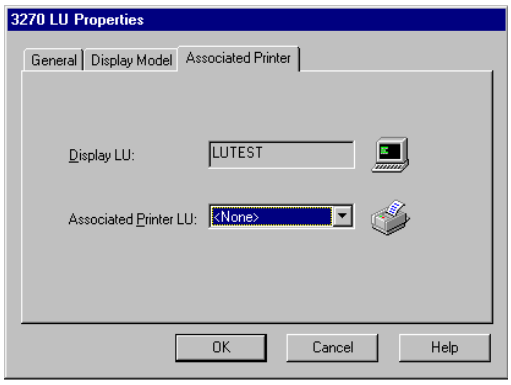
- Fill in the different fields in the *General* screen, then click on the *Display Model* tab, and on the *Associated Printer* tab if necessary.

LU field identifies the LU number on the connection.
LU Name field identifies the LU.
Connection specifies the connection used by this LU.



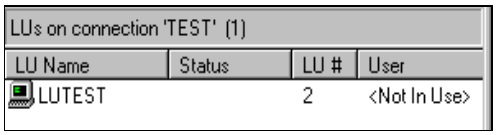
- Click on the *Display Model* tab, and check the type to specify the control of the display size.

Note: When an LU is assigned to a pool, the display model for a pool overwrites the setting of the LU.



- Click on the *Associated Printer* tab.
- Click on the down arrow icon to display the list of available printer LUs on connection, then select one of them in the list box, to associate with the display LU.

- When all parameters are set, click on OK to go back to the main screen. The new LU that has been created is defined as <Not In Use> on the right side of the screen as shown below.

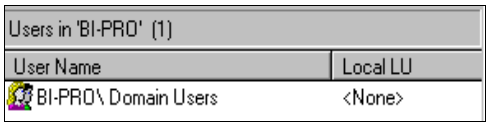


Setting Up User and Group Access

In order for users to be recognized by SNA Server, they must have accounts on the LAN (Local Area Network). Once these accounts have been created, users can be added to the list used by SNA Server.

- To add a new user, select the *Insert* menu then click on the *User* command in the *SNA Server Manager* main window.
- The Add *Users and Groups* dialog box is now displayed. Follow the instructions below.
- In the *List Names From* box, select the domain from which to list users (or groups) who have accounts or select the name of the local server.
- In the *Names* box, from the list of users and groups who have accounts, select the one to add.
- Click on Add, then validate by clicking on OK.

- From the *File* menu, click on *Save* (the Configured Users labeled is defined on the right side on the screen) to save the configuration.



- On the left side, under the **Configured Users**, the *User Name* update is done.

Giving the new user access to the 3270 LU

The new user can access the host using the 3270 LU only if this LU is assigned to the user account. This can be done by different ways.

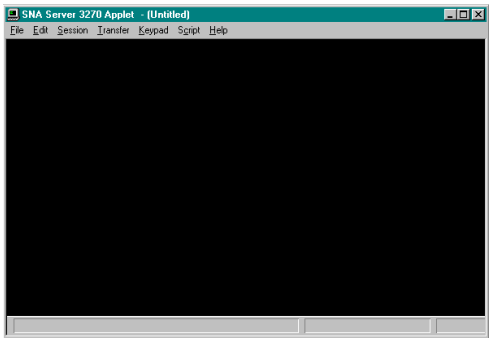
- From the previous diagram, click on the right button of the mouse to display the *Assign* menu.
- Click on the *Assign To* menu, then select *User* and the user to which the LU will be assigned (in this example: Domain Users).

- The LU number 2 is assigned to «Domain Users».
- From the *File* menu, confirm by clicking on *Save.*

Starting a 3270 session

- From the *SNA Server Admin* screen, select the **node**, then the *Service* menu and the *Start* command.
- Activate the connection (example TEST) in the same way.
- When the connection is active, go to the **SNA Server (Common)** task.
- Select the ***3270 Applet***.

- The 3270 Applet screen is displayed:



- Select the *Session* menu, then the *Session Configuration...* command.

- Select the LU. Define the page code and click on OK.
- Select the *Session* menu, then the *Connect* command. The remote host banner is displayed on the screen.
- Continue the session using the host identification commands.

CHAPTER 8

FPX BackUp

Windows NT

8

This chapter describes the component FPX BackUp. Once the FPX MPServer Service and/or the FPX SNA Support Service have been installed, the tree architecture is modified: a new service BackUp is added under Services.

About this component

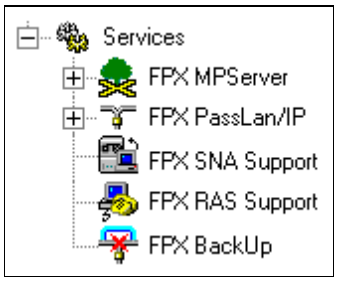
The FPX Product includes an FPX BackUp mechanism for the FPX MPServer and the FPX SNA Support Services.

From a main network address, backup parameters can be defined associated with Backup Criteria (backup made on defined or undefined clears) and Recovery criteria (no recovery, recovery on idle period, or recovery on timeout). This allows, if a problem occurs on the *Primary* link to work on the *Secondary* link.

To go back to the initial link, 2 modes can be used:

- one option to avoid important communication costs (once the link is active again, the return is immediate.
- one option showing the service quality: the return is dynamically made for the new connection requests but the active connections on the *Secondary* link stay on this link.

Configuring the Service



- Select FPX BackUp, then define the following features.

Parameter	Meaning
Selected Services	Check FPX SNA Server and/or FPX MPServer to allow the FPX BackUp service.
Cause	First part of an X.25 liberation code written as CC DD, represented as CC where: • CC = X.25 causes • DD = X.25 diagnostics. Define the cause by entering the code which will be the criterias to use the backup link. Then click on the Add >> button to display it in the *Liberation diagnostic* list box, when the CC and DD are entered. Use the << Remove button to delete it from the list box.

Parameter	Meaning
Diag	Second part of an X.25 liberation code written as CC DD, represented as DD where: • CC = X.25 causes • DD = X.25 diagnostics Define the diag by entering the code which will be the criterias to use the backup link. Then click on the Add >> button to display it in the *Liberation diagnostic* list box, when CC and DD are entered. Use the << Remove button to delete it from the list box.
Hexadecimal display	When checked, the code is displayed in *hexadecimal*. Otherwise, it is displayed in *decimal.*

Note: A clear can occurs when connecting, working or disconnecting. For more information, it is recommended to refer to the X.25 Specifications of the Network.

Configuring the BackUp link

- From the *FPX BackUp* label, on the left side of the screen (tree), click on the  icon to configure the Backup link, then click on the  icon to save the new configuration.

Parameter	Meaning
Main network address	Main link address of the remote, consisting of 1 to 15 characters.
Network address	Outgoing backup address of the remote (on the same adapter).
Facilities	Complementary service according to the subscription (63 hexadecimal bytes maximum)
User data	Complementary service according to the subscription. Even number of hexadecimal characters up to 32 characters.
Use first backup parameters	Check the option to first make the link change mandatory. In this case, the *Backup criteria* and *Recovery criteria* options are grayed.
Use backup	Check this option to allow the access from the main link to the backup link, if a problem occurs.
Backup made on defined clears	When checked, the backup link will only be used if a network clear, amongst the codes previously entered into the *Liberation diagnostic* dialog box, occurs.
Backup made on undefined clears	When checked, the backup link will only be used if a network clear, different from the codes previously entered into the *Liberation diagnostic* dialog box, occurs.
Retry number before backup	Number of connections retries to a non-response before a connection on the backup link. Default value = 1.
No recovery	When checked, the connection stays on the backup link.
Recovery on idle period	Check the option to disconnect when the inactivity timer is exceeded. This timer must be entered in the *Recovery lead time* field. *The return to the main link is not automatic.*
Recovery on timeout	Check the option to disconnect when the timeout is exceeded. This timer must be entered in the *Recovery lead time* field. *The return to the main link is not automatic.*
Recovery lead time	Time in seconds before disconnecting.

- When the configuration has been saved, the tree is updated.

In this example, the *Main network address* previously entered is 133010203.

CHAPTER 9

FPX Host Access

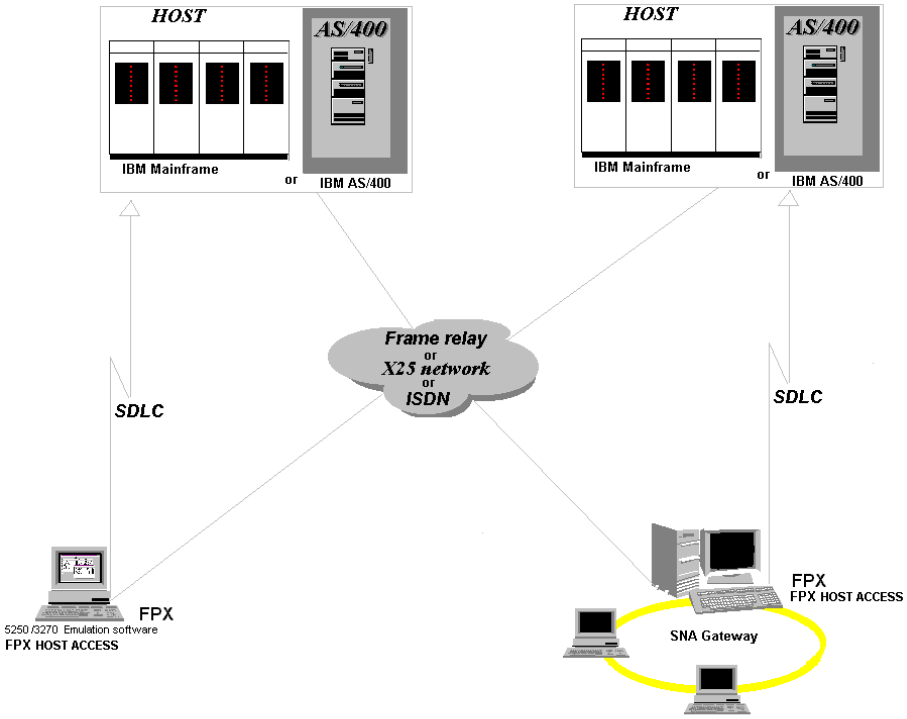
Windows NT

9

This chapter describes the component and its main features.

About this component

FPX Host Access is a component designed to add multiprotocol Wan connectivities (X.25 or ISDN/X.25 or Frame relay or SDLC) to stand-alone or Lan micro-computers with IBM Mainframe or IBM AS/400. It supports most of 5250/3270 emulation and SNA gateway softwares.



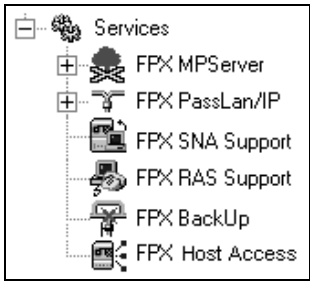
Software installation

It is recommended to **use the Autorun setup** software, guiding the user when installing (Refer to the *Setting up FPX adapter* chapter 3).
Before setting up the FPX Host Access component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

Follow these steps to manually install the component correctly.

- Insert the CD-ROM labeled FPX windows NT into the appropriate drive.
- Run the *Control Panel* then double-click on the ***Network*** icon.

- From the main screen, select the *Adapters* tab, then click on Add... to display the *Select Network Adapter* dialog box.
- Click on Have Disk... then enter the following path: "%**unit**%**\I386\X25pass** then validate by clicking on OK to continue the automatic process.



- **FPX Host Access Logical Adapter** must be displayed.
- When the setup is complete, the tree is modified. FPX Host Access is added under *Services*. In this example, other services have already been installed.
- Then, it is recommended to install the Network Protocol (DLC or LLC2) on Logical Adapter.

- Refer to the *Installing the Network Protocol driver* section, in this chapter.

Remainder

Several modules have to be installed and configured:

- FPX adapter and its software
- FPX Host Access software
- Network Protocol driver: Microsoft DLC or IBM LLC2 (SNA Gateway or terminal emulations).

Configuring the Service

- Select *FPX host Access*, then define the global following features.

Parameter	Meaning
Sys level	Traces pertaining to communication between the FPX Host Access driver and potential driver administration programs. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*
Llc level	Traces pertaining to communications between the protocol stack and the FPX Host Access driver. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*
MAC level	Traces pertaining to communications between the FPX Host Access driver and the FPX adapter. • None: No trace • Errors: Trace is executed only when an error occurs. • Data: Trace is executed for significant events that include useful information. • All: Trace is executed for all events. *The traces are registred through the Event Viewer in the System log.*

- When the parameters have been filled in, click on the icon to save them.

Configuring the site

Creating a site

- When the global parameters have been entered, click on *Site* to fill in the *Site* parameters and create the **first site**, then define the associated protocol.

- Then the *Site* parameters have to be defined.

It is necessary to enter a configuration for each site to be connected. Check the *Allowed* option to activate the site, then fill in the following fields. They have to be in accordance with those defined in the SNA software.

Parameter	Meaning
Site name	Alphanumeric identifier to identify the site (can be modified).
MAC address	Host identifier address in the 802.2 (12 characters)
MAC ad. Format	Check the format type: *TokenRing* (default) or *Ethernet.*
Local SAP	Hexadecimal value from 0x04 to 0xFc, used for incoming calls when the selected protocol is X.25 or SDLC.
Remote SAP	Grayed value displayed according to the value of SAP local.

Two different accesses can be defined: **Main Access** and **Backup Access.**

- Define the *Main access* to define the connection features, then click on the *Backup* tab to do the same operation type, as defined on the previous access.

Note: The *Backup* Access is only used when the *Main* Access could not be established after x number or connection retries.

Parameter	Meaning
Protocol	Protocol type: *X25* or *Frame Relay* or *Sdlc*. The protocol parameters are different and displayed according to this protocol selection.
Link	Adapter and associated profile, displayed in the list, according to the adapters configuration when installing. *The Prefix is displayed according to the selection.*
Inactivity timer	When checked, fill in the minimum inactivity delay before disconnecting. Values from 1 to 360 seconds. Default value = 90.
Tries number	Number of connection tries to a non-responding remote gateway. Default value = 1.

X.25 Protocol

Parameter	Meaning
Network Address [outgoing]	Address used to reach the remote host consisting of 1 to 15 hexadecimal digits. *This address must not include the switching prefix that may have been defined when configuring FPX adapters. The configurator adds the prefix, according to the link selected.*
Network sub-address	Sub-address added to the called number (option).
Network Address [incoming]	It consists of 1 to 15 digits corresponding to the incoming address received by the FPX during an incoming call. If the character * is entered, all incoming addresses are accepted.
Network password	Password used in option to access to the host.

Parameter	Meaning
Reverse charging request	When checked, the outgoing called packet includes a facility specifying a reverse charging request. The called party can refuse the request, and the connection is then rejected.
Closed user group	Complementary service with potential values. • 00: in general, common group • 1 to 99: private group • blank: no Closed user group or single group
Facilities	Facility field of a call packet
X25 local address	X25 local address (calling) to be completed, when the X.25 network does not use calling address.

Frame Relay Protocol

Parameter	Meaning
Network Address [outgoing]	Address used to reach the remote host consisting of 1 to 15 hexadecimal digits. *This address must not include the switching prefix that may have been defined when configuring FPX adapters. The configurator adds the prefix, according to the link selected*.
Network sub-address	Sub-address added to the called number (option).
Network Address [incoming]	It consists of 1 to 15 digits corresponding to the incoming address received by the FPX during an incoming call. If the character * is entered, all incoming addresses are accepted.
Dlci	Data Link Connection Identifier Decimal number on four digits length, displayed in the list, according to the adapters configuration for FPX Host Access, when setting up.
Encapsulation	Encapsulation option to be selected when activating the connection, among *Bridged Token-Ring* (default value), *Bridged Ethernet*, *Routed Peripheral Node*, *Routed APPN Peripheral*, *Routed HPR level2*, *Others*. The corresponding hexadecimal value is displayed in the *hexadecimal value* field.

SDLC Protocol

Parameter	Meaning
Network Address [outgoing]	Address used to reach the remote host consisting of 1 to 15 hexadecimal digits. *This address must not include the switching prefix that may have been defined when configuring FPX adapters. The configurator adds the prefix, according to the link selected*.
Network sub-address	Sub-address added to the called number (option).
Network Address [incoming]	It consists of 1 to 15 digits corresponding to the incoming address received by the FPX during an incoming call. If the character * is entered, all incoming addresses are accepted.
Polling address	Address hexadecimal number. Default value: 0xC1.
Frame window	Maximum number of frames that can be sent before waiting for an acknowledgement. Value from 1 to 7.
Mode	Represents settings of SDLC protocol level *Full-duplex* or *Half-duplex*. Default value: Full-duplex.
Coding	Represents settings of SDLC line level *NRZ* or *NRZI.* Default value: NRZ • NRZ (Non return to zero) • NRZI (Non return to zero inverted)

Parameter	Meaning
Line type	Select one of theses options*: LS* or *Switched* or *Multipoint*. • Leased SDLC line: a dedicated telecommunications line for SDLC point to point connections. • Switched SDLC line: standard dial-up telephone line used for SDLC connections. • Multipoint SDLC line: a dedicated telecommunications line used by multiple secondary SDLC stations.
Accept incoming call	Check the option to accept incoming call.

- When the *Site* and the *Protocol* parameters have been filled in, click on the  icon to save the settings.

Modifying a site

- Click on 

to make change(s) if necessary, then click on the  icon to update the modifications, and save the new configuration.
All parameters can be changed.

Adding a site

- Select *FPX Host Access*, on the left side of the screen (tree), click on the  icon to add a new site, define the settings, then click on the  icon to save the new configuration.

Removing a site

- Select a site by clicking on its name, then click on the  icon, and click on the  icon to save the new configuration.

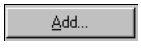
Note:
After each saving the *Dynamic reconfiguration of the Services* windows is displayed. A modification has been detected among the services, select the service then validate to dynamically reconfigure the driver.

Installing the Network Protocol driver (DLC/LLC2)

To run with FPX Host Access, the SNA Pc-to-host communication product needs to be installed, then configured for a LAN 802.2 connectivity.
Most of Pc-to-host communication products use the DLC Network Protocol, provided with Windows NT system. For IBM products, install the LLC2 driver.

DLC

Follow the steps below to install it correctly:

- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Protocol*s tab, then click on 

to display the *Select Network Protocol* dialog box.
- Select the *DLC Protocol*, validate by clicking on 

to continue the process.
- The *DLC Protocol* will automatically bind with the FPX Host Access driver (**FPX Host Access Logical Adapter**) previously installed.

LLC2

Follow the steps below to install it correctly:

- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Protocol*s tab, then click on Add... to display the *Select Network Protocol* dialog box.
- Select the *IBM LLC2 Protocol*, validate by clicking on OK to continue the process.
- The *IBM LLC2 Protocol* will automatically bind with the FPX Host Access driver (**FPX Host Access Logical Adapter**) previously installed.

Note:
If the user does not use the DLC Protocol with other LAN adapters, physically installed in the machine, deactivate the DLC bindings with them.

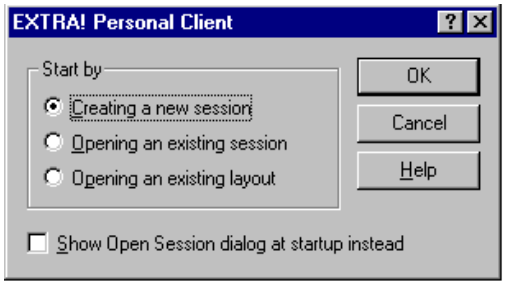
Installing the SNA Pc-to-host communication

To run with FPX Host Access, the SNA Pc-to-host communication product needs to be installed, then configured for a LAN 802.2 connectivity.

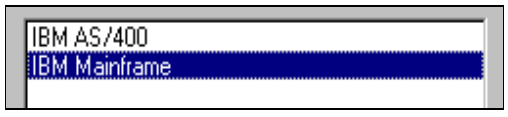
- Install the SNA Pc-to-host communication product, by using the provided **Setup** program.
- Two examples are described in this chapter:
  - Attachmate E!PC product
  - IBM Personal Communications

Configuring the Attachmate E!PC product

- Run the E!PC product. It is recommended to create a session by using the **New session Wizard.**

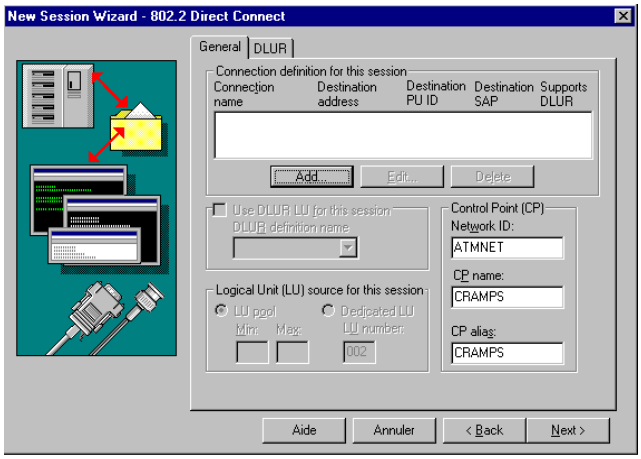


- Check the *Creating a new session* option.
- Validate by clicking on OK to display the *New session Wizard* screen and define the host type the user would like to connect to.

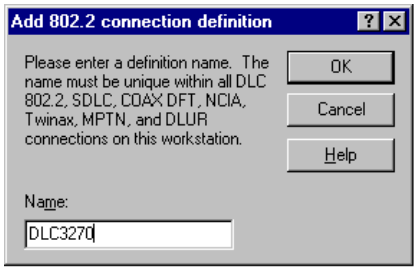


- For example, select **IBM Mainframe**, then click on Next >.

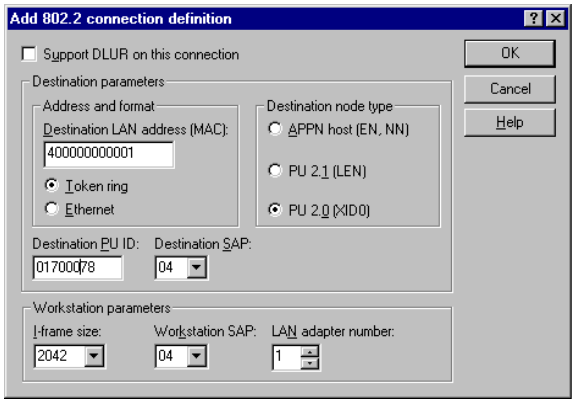
- Define the session type among **3270 Display** or **3270 Printer** by selecting one of them, click on Next >.
- Select mandatory **802.2 Direct Connect** connection type, and click on Next >.



- Click on Add... then define an unique definition name.



- Validate by clicking on OK to display the **Add 802.2 connection definition** screen and define the parameters of this session.



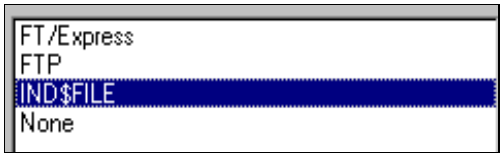
- Fill in the different fields, and use the Online Help for more explanation.
- When the fields have been filled in, confirm by OK.

Be careful:
The *Destination LAN address (MAC)* field must be the same as described in the FPX Host Access configuration.

Notes:

- If another LAN adapter exits on the machine, verify that the *LAN adapter number* corresponds to the FPX Host Access driver (Logical Adapter).
- To simultaneously use several connections in a configuration with multi-sites, be careful to define a different *Destination LAN address (MAC)* and a different *Workstation SAP* for each one.

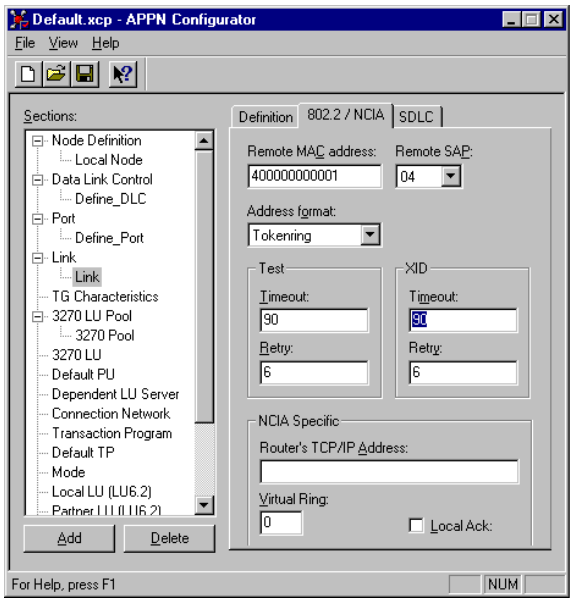
- Define a file transfer type if necessary, by selecting one of them, click on Next >.



- Terminate the IBM Mainframe configuration by clicking on Finish.

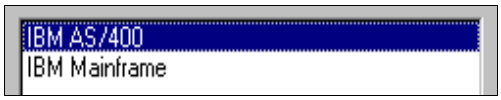
Note:
To use X.32 PSTN connections, it is necessary to increase the *XID Timeout*, so that the modem can establish the X.25 connection.

- Execute the **APPN Configurator**, select the *File* menu, then click on the *Open active* command, select 802.2 NCIA and check the *Timeout* values.



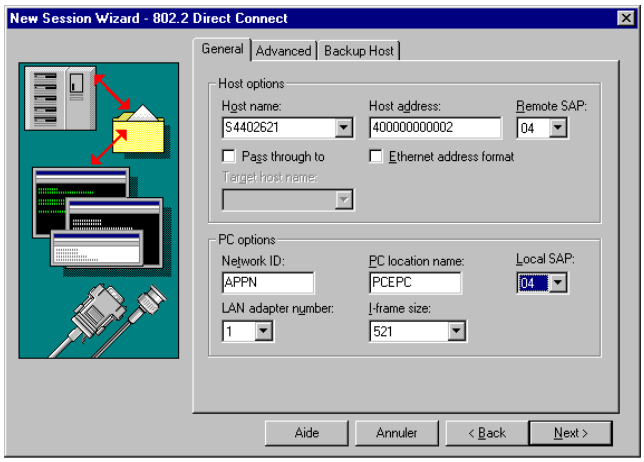
- Enter the value 90 in the *Test Timeout* and in the *XID Timeout* fields.
- Confirm by clicking on the icon to save these modifications.

- As the Mainframe has been previously defined, the user can prepare an AS/400 session.



- In this case, select **IBM AS/400**, then click on Next >.

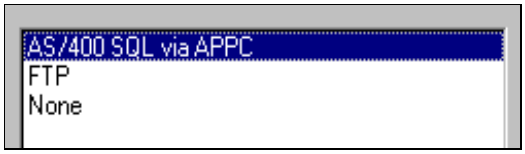
- Define the session type among **5250 Display** or **5250 Printer** by selecting one of them, click on Next >.
- Select mandatory **802.2 Direct Connect** connection type, and click on Next >.



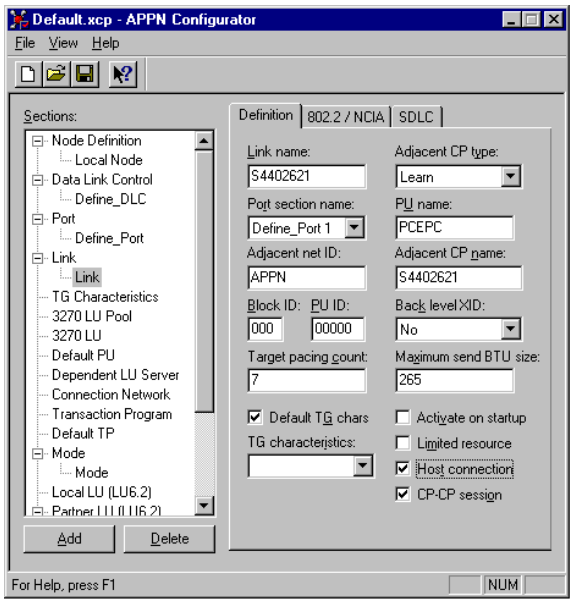
- Fill in the different fields, and use the Online Help for more explanation.
- When the fields have been filled in, confirm by OK.

Be careful: The *Host address* field must be the same as described in FPX Host Access configuration.

- Define a file transfer type if necessary, by selecting one of them, click on Next >.



- Terminate the IBM AS/400 configuration by clicking on Finish.



- Execute the **APPN Configurator**, select the *File* menu, then click on the *Open active* command, enter a *PU name* and check the *Host connection* option.
- Click on the *802.2 NCIA* tab to check the *Timeout* values, and refer to the previously note for more information.
- Confirm by clicking on the  icon to save these modifications.

Once the installing and configuring steps of the E!PC product have succeeded, a connection with E!PC can be activated.

Activating a connection with E!PC

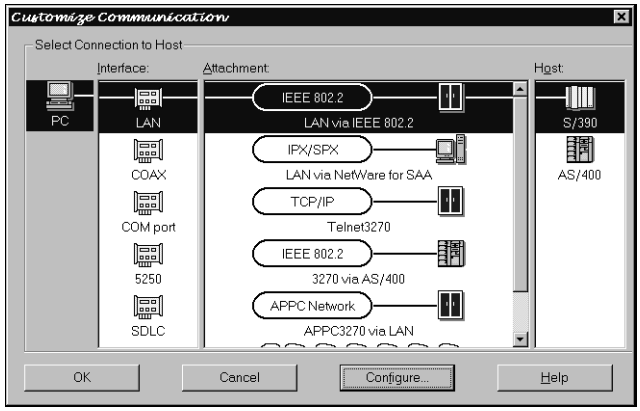
- First, load the selected *adapter* (manual or automatic loading).
  For more information refer to the Chapter 3: *Setting up FPX adapters.*
- Run Attachmate Extra! Personal Client 32-bit software, then open one of the sessions, previously defined. The FPX Host Access driver will be activated, trying to connect to the remote site associated to this session.

Notes:

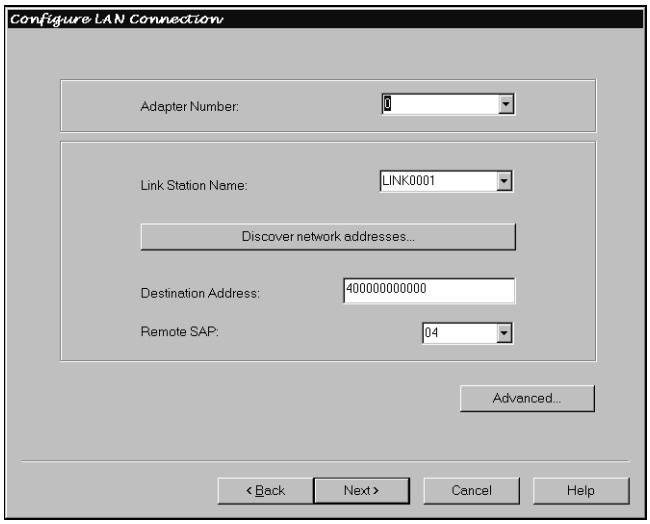
- To diagnose connection failure, refer to The *Event Viewer* in the System log or use the **FPX Diag** utility. Refer to the next section for some explanation.
- The **E!PC status** program can also help the user in solving configuration problems.

Configuring the IBM Personal Communications product

- Run the *Start or Configure Session* program to define a new session. Follow the necessary steps to define a connection to S/390 or AS/400 hosts. Use a IEEE 802.2 Attachment to Host.



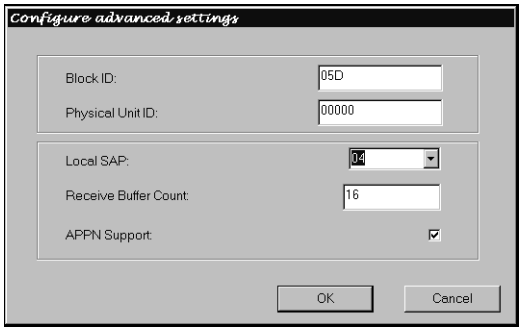
- Click on  to define the link parameters.
- Set the Local System parameters, and create a new *SNA Node Configuration* file.



- Enter the same *Destination Address* as specified for this site in the FPX Host Access configuration (driver).

Be careful: to use several connections simultaneously in a multi-sites configuration, be careful to define a different Destination Address for each LAN Connection.

- Click on  to define advanced settings.



- Enter the PUID needed by the remote host in this section.

Be careful: To use simultaneously several connections in a multi-sites configuration, be careful to define a different Local SAP for each LAN Connection.

Notes:

- The adapter number must be the same number associated with the Cirel FPX Host Access Adapter. Windows NT defines this number during installation of Network Adapters. The first is number zero.
- The user will problably need to complete the configuration of the new connection using the SNA Node Configuration. More parameters are accessible using this utility program.

Activating a connection with IBM Personnal Communications

- First, load the selected *adapter* (manual or automatic loading).
- For more information refer to the Chapter 3: *Setting up FPX adapters.*
- Run ***Start*** in the IBM Personnal Communications group.
- Open one of the sessions, previously defined, by selecting the *Connect* item in the *Communication* menu. The FPX Host Access driver will be activated, trying to connect to the remote site associated to this session.

Troubleshooting

Windows NT Event Viewer

This utility is provided with Windows NT to help the user in identifying the reason of a connection failure.
It is logged via the FPX Host Access driver, connection and disconnection events.

- Press the F5 key to update the event list box.
- Select an event, then double-click on it to display the complete information.

See the list of LlcX25 available system events:

- X25 CON_REQ : a connect request was sent by the driver.
- X25 CON_CON : a connect confirmation was received.
- X25 DIS_REQ : a disconnect request was sent by the driver.
- X25 DIS_IND : a disconnect indication was received.

The message displays the cause-diagnostic codes. Run the **FPX Diag** program to get the meaning of these codes.

Notes:

- If no events are logged in the *Event Viewer*, when activating a connection, it is recommended to verify if another LAN adapter exists on the machine. In this case, check the *LAN adapter number* in the *802.2 connection definition* screen: this parameter must correspond to the FPX Host Access driver.
- To be sure to select the good adapter, deactivate the DLC bind with other Lan adapters, then keep the DLC protocol binded with only the Logical Adapter so that the number to select in the *802.2 connection definition* screen will be the number 0.
- More events can be displayed by modifying the traces levels in the FPX Host Access Service.

FPX Diag

This utility has been added in the FPX Communication Services (Common) task at the end of the FPX software installation. It helps the user by giving the meaning of codes (cause-diagnostic).

For more information refer to the Chapter 3: *Setting up FPX adapters.*

Warnings

- To connect simultaneously to several hosts, it is necessary to enter a different *Destination LAN address (MAC)* and a different *Workstation SAP* number for each one (check in the *FPX Host Access configuration* screen and check in the *802.2 connection definition* screen).

- Closing a session will not necessary clear the Wan connection. With the E!PC product, it is cleared when the APPN Node is unloaded : to automatically close the APPN Node, check the *Limited Resource* parameter in the Link definition of the session. However, the Wan connection can be cleared by using the *Inactivity timer* in the *FPX Host Access configuration* screen.

CHAPTER 10

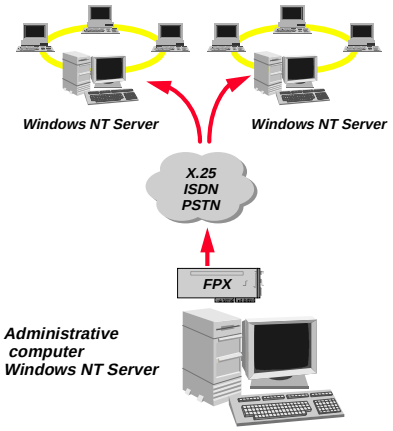
Services Administration

Windows NT

10

This chapter describes how to use the performance objects via the **Performance Monitor** standard tool delivered with Windows NT.

About this tool



It provides a mechanism to add objects and performance counters.

The extended objects for the FPX product are:

- The FPX adapter(s)
- The FPX MPServer
- The link service for SNA Server
- The FPX PassLan/IP
- The FPX RAS support

Note:
The FPX adapters and the different services must have been installed and configured on the computer. Follow the steps described in the previous chapters to install them correctly.

Running the Performance Monitor

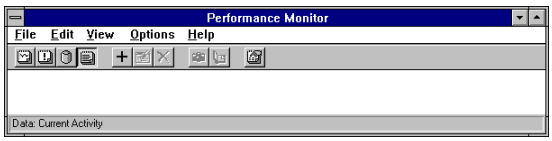
Starting the Performance Monitor

- From the **Start Menu Programs**, select the **Administrative Tools (Common)** task: the **Performance Monitor** is a Windows NT standard tool integrated.
- Click on it to display the *main* menu and select a view among the four available views.

Selecting a view

Four views can be selected from the *main* menu:

- Chart
- Report
- Alert
- Log



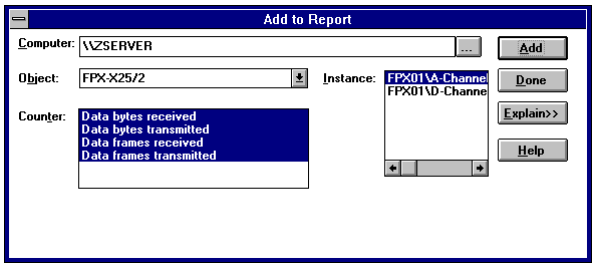
- From the tool bar click on  or select the *Report* command (for example).

The *Report* view is designed to show the value of accumulated counters such as the total number of exchanged bytes, or of state counters with a 0 or 1 value.

The *Chart* view is intended to monitor changes in counter values. It is used for counters displaying throughputs, such as the number of bytes transmitted per second.

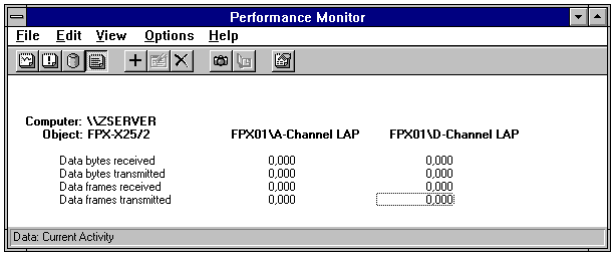
Adding an object

From the tool bar, click on  or select the *Edit* menu and then click on the *Add to Report...* command to display the associated screen.



- Select an object using the  button, and then a relevant instance in the *Instance* list box.

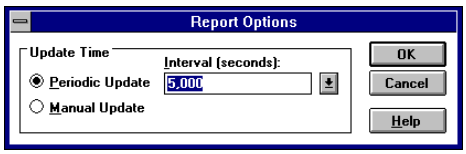
- Select the counters the user wants to display and click on  to insert all the counters selected for this instance.
- Click on  to go back to the previous screen.



The selected counters and instances are displayed in the report view.

Changing the periodic update

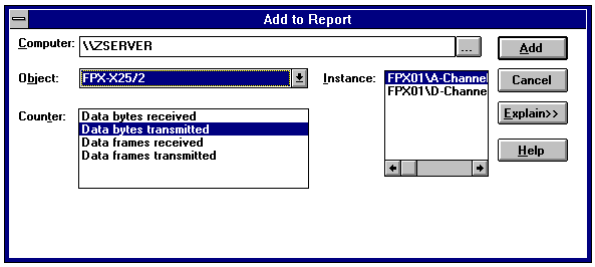
- From the tool bar, click on  , or select the *Options* menu, then click on the *Report...* command (or one of the other commands depending on the previous selected view) then change the periodic update interval.



In order not to degrade computer and FPX adapter performance, it is advisable not to select a value that is less than 5 seconds.

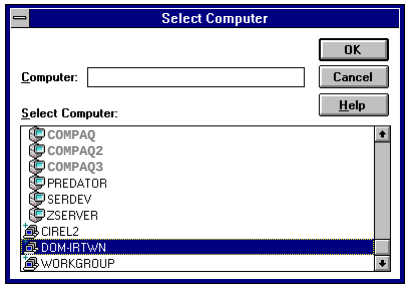
Administrating a remote computer

Performance data coming from another Windows NT computer on the local network can be obtained via the Performance Monitor program.



- From the tool bar, click on  , then modify the computer name in the dialog box.

- Select another computer by clicking on  : the *Select Computer* dialog box is displayed:



The Performance Monitor controls only the computers located on the local network.

The administrator can control a remote computer by connecting through RAS (Remote Access Service), using the FPX RAS Support Service, between the computer to administrate and the computer running the Performance Monitor.

Note:
For more information, refer to the Microsoft's OnLine Help.

Supervising with the Performance Monitor

Introducing the FPX Product Objects

FPX features

FPX objects are dedicated to a particular FPX adapter and have 3 levels:

- MAC level (physical link): the object is called FPX-X25/1
- LAP level (frame): the object is called FPX-X25/2
- PLP level (packet): the object is called FPX-X25/3

They can each simultaneously control the configured and loaded FPX adapters.

FPX-X25/1

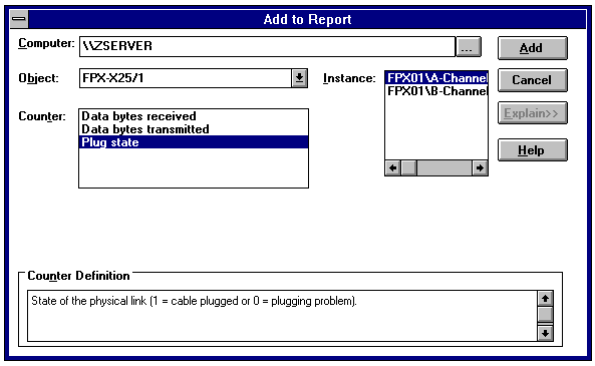
This object corresponds to the physical interface of an FPX adapter. An instance of this object is defined for each physical interface of the FPX adapter. A maximum of two instances may be available per adapter, depending on the FPX adapter type and its configuration.

X.25 interface for FPX adapter:

- It corresponds to the A-channel of an FPX/B adapter or the A-channel of the FPX/S, FPX/I and FPX/IM adapters configured for an X.25 network.
  The name of the instance shows the type of interface used and the name of the managed FPX.
  For example: FPX01\A-Channel (V28)

ISDN interface for FPX adapter:

- It corresponds to the B-channel of the FPX/S and FPX/I adapters configured with one ISDN channel or corresponds to the A-channel and B-channel of the FPX/S and FPX/I adapters configured with two ISDN channels.
  For example: FPX01\B-Channel (ISDN)



For these instances, three counters have been defined:

- Data bytes received
- Data bytes transmitted
- Plug state

The meaning of a counter is given by clicking on Explain>>.

Counter	Description	Possible Values
Data bytes received	Number of data bytes received at MAC level (media access control)	From 0 to 4,294,967,295
Data bytes transmitted	Number of data bytes transmitted at MAC level (media access control)	From 0 to 4,294,967,295
Plug state	Indicates whether the outgoing cable is connected correctly	value 1 = plugged value 0 = not plugged (Non-connected cable, modem off, etc.)

FPX-X25/2

This object defines the frame level of an FPX adapter.
An instance of this object is defined for each frame level set up on the FPX adapter. A maximum of three instances is available per adapter.

Frame level of the A-channel for FPX adapter:

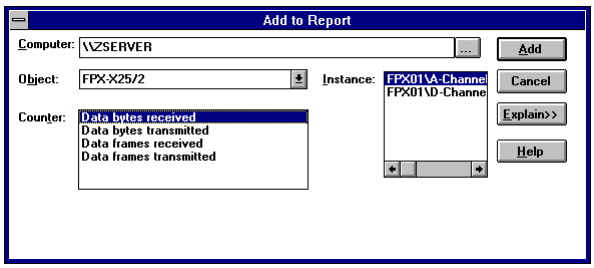
- For an FPX/B, FPX/S, FPX/IM or FPX/I adapter, whose A-channel is configured to use X.25 protocol, the frame level corresponds to a LAP instance using the X.25 electrical interface (V28, V11 or V35 interface).
- For an FPX/S or FPX/I adapter configured with two ISDN channels, the frame level of the A-channel corresponds to a LAP instance using the ISDN interface through one of the two B-channel.
  For example: FPX01\A-Channel LAP

Frame level of the B-channel for FPX adapter:

- It corresponds to a LAP instance using the ISDN interface of an FPX/S or FPX/I configured with one or two ISDN channels through one of the two B-channels.
  For example: FPX01\A-Channel LAP

Frame level of the D-channel on the FPX/S and FPX/I adapters:

- It corresponds to the LAP instance of the D-channel of the ISDN interface.
  For example: FPX01\D-Channel LAP



For these instances, three counters have been defined:

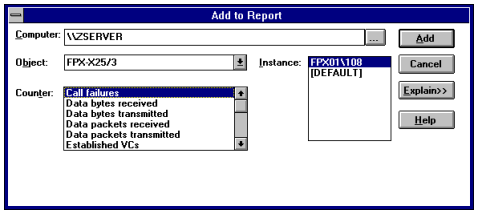
- Data bytes received
- Data bytes transmitted
- Data frames received
- Data frames transmitted

The meaning of a counter is given by clicking on Explain>>.

Counter	Description	Possible Values
Data bytes received	Number of data bytes received at LAP level (link access control)	From 0 to 4,294,967,295
Data bytes transmitted	Number of data bytes transmitted at LAP level (link access control)	From 0 to 4,294,967,295
Data frames received	Number of data frames received at LAP level (link access control)	From 0 to 4,294,967,295
Data frames transmitted	Number of data frames transmitted at LAP level (link access control)	From 0 to 4,294,967,295

FPX-X25/3

This object represents the packet level of an FPX adapter. For this object, there are as many instances defined as there are calls and/or called remote sites.



Each instance is identified by the X.25 number of the called site and the name of the FPX adapter used.

For example: FPX01\108

For these instances, several counters have been defined:

- Call failures
- Data bytes received
- Data bytes transmitted
- Data packets received
- Data packets transmitted
- Established incoming Vcs
- Established outgoing Vcs
- Established VCs
- Latest clear diagnostic
- Latest clear cause
- Local clears
- Remote clears
- Troughput bytes/sec.

The meaning of a counter is given by clicking on Explain>>.

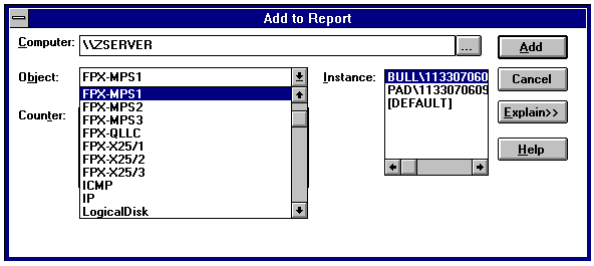
Counter	Description	Possible Values
Call failures	Number of attempts of failed connections	From 0 to 4,294,967,295
Data bytes received	Number of bytes received on a virtual circuit at packet level	From 0 to 4,294,967,295
Data bytes transmitted	Number of bytes transmitted on a virtual circuit at packet level	From 0 to 4,294,967,295
Data packets received	Number of messages received on a virtual circuit at packet level	From 0 to 4,294,967,295
Data packets transmitted	Number of messages transmitted on a virtual circuit at packet level	From 0 to 4,294,967,295
Established incoming VCs	Number of established incoming VCs	From 0 to 4,294,967,295
Established outgoing VCs	Number of established outgoing VCs	From 0 to 4,294,967,295
Established VCs	Number of established VCs	From 0 to 4,294,967,295
Latest clear diagnostic	Latest clear diagnostic on a virtual circuit	From 0 to 255
Latest clear cause	Latest clear cause on a virtual circuit	From 0 to 255
Local clears	Number of local clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
Remote clears	Number of remote clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
Throughput bytes/sec.	Total number of bytes per second	From 0 to 4,294,967,295

FPX MPServer features

There are four FPX MPServer objects, each of them corresponding to a BULL/PAD/X25 multiprotocol server on an FPX adapter:

- FPX-MPS1
- FPX-MPS2
- FPX-MPS3
- FPX-MPS4

The only objects to be displayed in Windows NT™ Performance Monitor are those corresponding to the multiprotocol servers which have been configured.

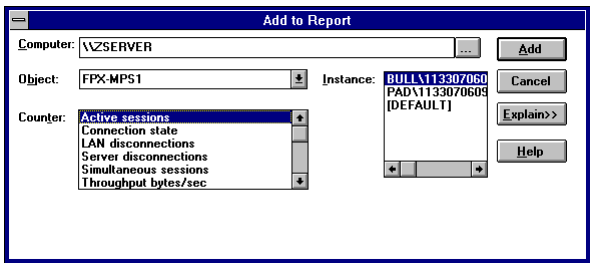


In this example, a Bull Server and a Pad Server have been defined, when configuring the associated Routing Services.

FPX-MPSn

In this paragraph, "n" index can be valued between 1 and 4. All written counters for each FPX-MpSn objects are identical, whatever the "n" value is. For this object, several instances are defined, corresponding to the BULL, PAD or X25 sites which are connected:

- BULL\xxxx where xxxx is the called X25 or ISDN number of the BULL site.
- PAD\xxxx where xxxx is the called X25 or ISDN number of the PAD site.
- X25\xxxx where xxxx is the called X25 or ISDN number of the X25 site.



For each instance, the following counters have been defined:

- Active sessions
- Connection state
- LAN disconnections
- Server disconnections
- Simultaneous sessions
- Throughput bytes/sec
- Throughput messages/sec
- WAN disconnections

The meaning of each counter is detailed in the description obtained by clicking on Explain>>.

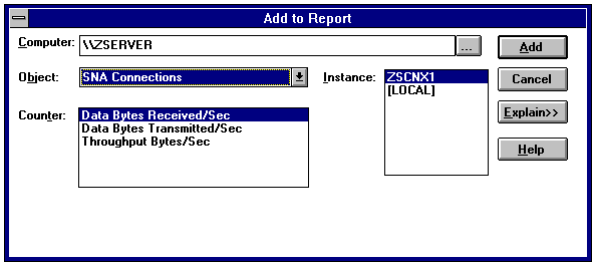
Counter	Description	Possible Values
Active sessions	Number of active sessions on the host through emulators For example BULL site : 4 DKU + 2 TTU = 6 active sessions	From 0 to 64 for a Bull site From 0 to 32 for a Pad or an X25 site
Connection state	State of the host connection	value 1 = host connected value 0 = host disconnected
LAN disconnection	Number of clears detected on LAN's side following a LAN error	From 0 to 4,294,967,295
Server disconnections	Number of clears detected on server's side following a server error or a host connection reject	From 0 to 4,294,967,295
Simultaneous Sessions	Maximum number of simultaneous sessions on this site since the starting of the FpxMpSrvn service	From 0 to 64 for a Bull site From 0 to 32 for a Pad or X25 site
Throughput bytes/sec	Total number of bytes per second flowing through the server connection	From 0 to 4,294,967,295
Throughput messages/sec	Total number of messages per second flowing through the server connection	From 0 to 4,294,967,295
WAN disconnections	Number of clears detected on WAN's side following an FPX or WAN error or a host connection reject	From 0 to 4,294,967,295

FPX SNADIS features

There are two types of objects for SNA Server and one object for the QLLC level of the FPX adapter:

- SNA connections
- SNA Logical Unit Sessions
- FPX-QLLC

SNA Connections



An instance, defined for each SNA Server connection contains the list of counters:

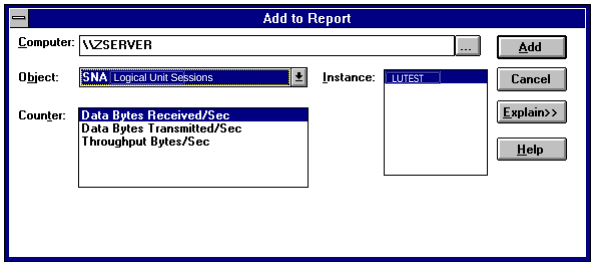
- Data bytes received/sec
- Data bytes transmitted/sec
- Throughput bytes/sec

The meaning of a counter is given by clicking on Explain>>.

Counter	Description	Possible Values
Data bytes received/sec	Number of data bytes received per second	From 0 to 4,294,967,295
Data bytes transmitted/sec	Number of data bytes transmitted per second	From 0 to 4,294,967,295
Throughput bytes/sec	Total number of bytes flowing through the SNA server. This number includes incoming and outgoing bytes and is a good indicator of how heavily the SNA Server is loaded.	From 0 to 4,294,967,295

SNA Sessions Logical Unit

This object defines an instance for each session of active emulation on the SNA Server.



Each instance includes the following counters:

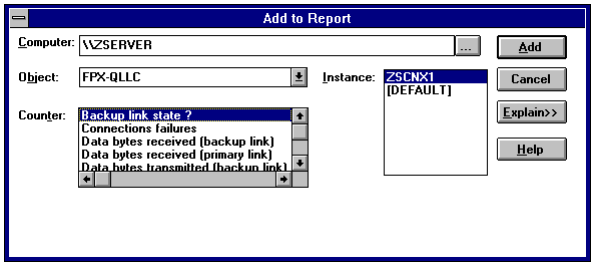
- Data bytes received/sec
- Data bytes transmitted/sec
- Throughput bytes/sec

The meaning of a counter is given by clicking on Explain>>.

Counter	Description	Possible Values
Data bytes received/sec	Number of data bytes received per second	From 0 to 4,294,967,295
Data bytes transmitted/sec	Number of data bytes transmitted per second	From 0 to 4,294,967,295
Throughput bytes/sec	Total number of bytes flowing through the SNA server. This number includes incoming and outgoing bytes and is a good indicator of how heavily the SNA Server is loaded.	From 0 to 4,294,967,295

FPX-QLLC

This object defines an instance for each active QLLC connection.



Each instance includes the following counters:

- Connections failures
- Data bytes received (primary or backup link)
- Data bytes transmitted (primary or backup link)
- Data frames received (primary or backup link)
- Data frames transmitted (primary or backup link)
- Primary or backup link state
- Successful connections (primary or backup link)
- Throughput bytes/sec
- Throughput frames/sec

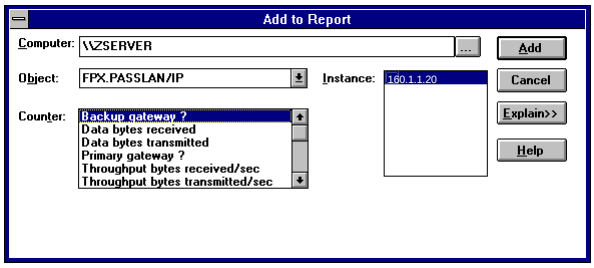
The meaning of a counter is given by clicking on Explain>>.

Counter	Description	Possible Values
Connections failures	Number of connections failed on both primary and backup links	From 0 to 4,294,967,295
Data bytes received (backup link)	Number of data bytes received on the backup link	From 0 to 4,294,967,295
Data bytes received (primary link)	Number of data bytes received on the primary link.	From 0 to 4,294,967,295
Data bytes transmitted (backup link)	Number of data bytes transmitted on the backup link	From 0 to 4,294,967,295
Data bytes transmitted (primary link)	Number of data bytes transmitted on the primary link	From 0 to 4,294,967,295
Data frames received (backup link)	Number of data frames received on the backup link	From 0 to 4,294,967,295
Data frames received (primary link)	Number of data frames received on the primary link	From 0 to 4,294,967,295
Data frames transmitted (backup link)	Number of data frames transmitted on the backup link	From 0 to 4,294,967,295
Data frames transmitted (primary link)	Number of data frames transmitted on the primary link	From 0 to 4,294,967,295
Backup link state	State of the connection on the backup link (active or not)	value 1 = connected link value 0 = disconnected link
Primary link state	State of the connection on the primary link (active or not)	value 1 = connected link value 0 = disconnected link
Successful connections (backup link)	Number of successful connections on the backup link	From 0 to 4,294,967,295
Successful connections (primary link)	Number of successful connections on the primary link	From 0 to 4,294,967,295
Throughput bytes/sec	Total number of bytes per second flowing through the QLLC connection	From 0 to 4,294,967,295
Throughput frames/sec	Total number of frames per second flowing through the QLLC connection	From 0 to 4,294,967,295

FPX PassLan/IP features

Only one object is defined for the FPX PassLan/IP administration. This object contains an instance for each accredited gateway, defined by the TCP/IP address.

Each instance includes the following counters:



- Backup gateway
- Data bytes received
- Data bytes transmitted
- Primary gateway
- Throughput bytes received /sec
- Throughput bytes transmit /sec
- Total data bytes

The meaning of a counter is given by clicking on Explain>>.

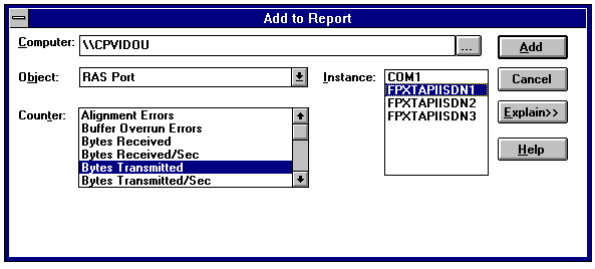
Counter	Description	Possible Values
Backup gateway	State of the backup IP gateway (pending connection)	1 = connected 0 = disconnected
Data bytes received	Number of data bytes received on this IP gateway	From 0 to 4,294,967,295
Data bytes transmitted	Number of data bytes transmitted on this IP gateway	From 0 to 4,294,967,295
Primary gateway	State of the primary IP gateway (pending connection)	1 = connected 0 = disconnected
Throughput bytes received/sec	Number of bytes received per second on this IP gateway	From 0 to 4,294,967,295
Throughput bytes transmitted/ sec	Number of bytes transmitted per second on this IP gateway	From 0 to 4,294,967,295
Total data bytes	Number of data bytes exchanged (transmitted and received) on this IP gateway	From 0 to 4,294,967,295

FPX RAS features

There are two different objects for the Microsoft RAS supplied with the Windows NT components:

- RAS Port
- RAS Total

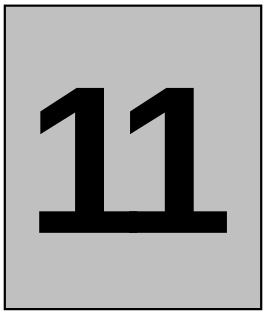
For example:
COM1, FPXTAPIISDN1, etc.



An instance is defined for each RAS port which has been configured with the Remote Access Service.

Refer to the Microsoft's Online Help for a description of the counters.

CHAPTER 11



FPX MPSupervisor

Windows NT

This chapter describes the FPX MPSupervisor, an object-oriented administrative product, and its associated elements. It fits perfectly with the Windows NT standard tools: Performance Monitor, Registry, Event Viewer, SNMP Service...

About this component

The FPX MPSupervisor, gives -in additionnal information from the standard tools- the Administrator a supervision system to administrate the FPX product via **S**imple **N**etwork **M**anagement **P**rotocol or **S**ystems **M**anagement **S**erver.

He can use :

- the SNMP extension DLLs and the **M**anagement **I**nformation **B**ase files
- the **Hypervisor** and **Hyper Config** utilities, delivered with FPX MPSupervisor

Once the adapter is loaded, the SNMP extension DLLs can be monitored to check the status of the plug, or the state of a particular link service, or the state of any IP gateway.
This component provides the following functionnalities:

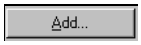
- Link level analysis (electrical interface, frame and packet levels)
- Statistics, logs and events
- Event and alert management,...

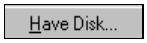
Note:
This component requires that Microsoft's TCP/IP stack and the SNMP Service be previously set on the computer.

Software installation

Before setting up the FPX MPSupervisor component, the FPX adapters must have been installed and configured on the computer. Follow the steps described in chapter 3 to install them correctly.

This product includes setup softwares that copy and install files onto the hard disk, according to the selected component.
The user can also follow these steps to install the component correctly:

- Insert the delivered CD-ROM into the appropriate drive.
- Run the *Control Panel* then double-click on the ***Network*** icon.
- From the main screen, select the *Services* tab, then click on 

to display the *Select Network Service* dialog box.
- Click on 

then enter the following path: "%**unit**%**\I386\sup**". Validate by clicking on 

to continue the automatic process.
- When the setup is complete, then check the SNMP Service is started: the utilities are added to the **Start Menu Programs.**

Supervising with the SNMP Service

Describing the proprietary MIBS

The FPXADM MIB

This MIB contains various tables describing all configurations of FPX products.

Object Name	Description	Possible Values
FpxMibDescription	MIB name	
FpxAdapterTrapFlag	State of the adapter trap flag	0 or 1 It can be set to 0 to disable trap generation when the FPX adapter configuration has changed or when the FPX adapter is down
FpxMibAdapterNumber	Number of FPX adapters configured	From 0 to n
FpxAdapterTable	Table describing the parameters of each FPX adapter configured	
FpxServiceTrapFlag	State of the service trap flag	0 or 1 It can be set to 0 to disable trap generation when an FPX service is stopping
FpxMibServiceNumber	Number of FPX services installed	From 0 to 10
FpxServiceTable	Table describing the parameters of each FPX service installed	
FpxDeviceTrapFlag	State of the device trap flag	0 or 1 It can be set to 0 to disable trap generation when an FPX device is stopping

It is accessible through the following tree:

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxadm (1)

FPX Adapters Parameters

The **FpxAdapterTable** contains the description of the FPX adapters configured on the Windows NT computer. Each entry contains the following information:

Object Name	Description	Possible Values
FpxAdapterIndex	Adapter index in the table	From 1 to n
FpxAdapterName	FPX adapter name	FPX01
FpxAdapterDesc	Adapter description	Cirel Systèmes FPX X25 Adapter *n*
FpxAdapterType	Adapter type	B, I, IM or S
FpxAdapterState	Adapter state	1: loaded 0: not loaded
FpxAdapterDPM	Dual port memory address	From A0000 to E8000
FpxAdapterIO	I/O port address	From 310 to 370
FpxAdapterIRQ	Interrupt level	From 3 to 15
FpxAdapterAChannel	A-channel interface type	ISDN V11 V28 V35

Object Name	Description	Possible Values
FpxAdapterBChannel	B-channel interface type	ISDN V11 V28 V35 MODEM

FPX Adapter Trap Flag

An SNMP trap is generated when the FPX adapter configuration has changed or when the FPX adapter is out-of-order. The **FpxAdapterTrapFlag** can be set to zero to disable trap generation.

FPX Services

The **FpxServiceTable** contains the description of the FPX services installed on the Windows NT computer. Each entry contains the following information:

Object Name	Description	Possible Values
FpxServiceIndex	Service index	From 1 to n
FpxServiceName	Service name (Entry name in the registry)	CirX25*n*, FpxStart, FpxLoadSvc, FpxMpSrv*n*
FpxServiceDispName	FPX service description (DisplayName value in the registry)	Example for FpxStart utility: Fpx Auto Start Utility
FpxServiceAdaptInd	Number of FPX adapters used by this service (FpxAdapterIndex from the FpxAdapterTable table)	0 None From 1 to n
FpxServiceState	Service State	1 Stopped 2 Start pending 3 Stop pending 4 Running
FpxServiceStartMode	Startup mode of the service (Start value in the registry)	2 Automatic 3 Manual 4 Disabled

FPX Service Trap Flag

An SNMP trap is generated when an FPX service is stopping. The **FpxServiceTrapFlag** can be set to zero to disable trap generation.

FPX Devices

The **FpxDeviceTable** contains the description of the FPX devices installed on the Windows NT Server. Each entry contains the following information:

Object Name	Description	Possible Values
FpxDeviceIndex	Device index	From 1 to n
FpxDeviceName	Device Name (Entry name in the registry)	Mip, FpxNdis, FpxTapi
FpxDeviceDispName	FPX device description (DisplayName value in the registry)	Example for Mip: Mip Driver for FPX series X.25 Adapters
FpxDeviceAdaptInd1	Number of the first FPX adapter used by this device. (FpxAdapterIndex in the FpxAdapterTable)	0 None From 1 to n

Object Name	Description	Possible Values
FpxDeviceAdaptInd2	Number of the second FPX adapter used by this device. (FpxAdapterIndex in the FpxAdapterTable)	0 None From 1 to n
FpxDeviceAdaptInd3	Number of the third FPX adapter used by this device. (FpxAdapterIndex in the FpxAdapterTable)	0 None From 1 to n
FpxDeviceAdaptInd4	Number of the fourth FPX adapter used by this device. (FpxAdapterIndex in the FpxAdapterTable)	0 None From 1 to n
FpxDeviceState	Device state	1 Stopped 2 Start pending 3 Stop pending 4 Running
FpxDeviceStartMode	Startup mode of the device (Start value in the registry)	0 Boot 1 System 2 Automatic 3 Manual 4 Disabled

FPX Device Trap Flag

An SNMP trap is generated when an FPX device is stopping. The **FpxDeviceTrapFlag** can be set to zero to disable trap generation.

The FPXMPS MIB

This MIB contains objects describing the configuration of each FPX MPServer installed, the configuration of the associated Bull hosts, and the FPX MPServer statistic objects.

Object Name	Description	Possible Values
MpsMibDescription	MIB name	
MpsTrapFlag	State of the configuration trap flag	0 or 1 It can be set to 0 to disable the trap generation when the FPX MPServer configuration has changed.
MpsNumber	Number of FPX MPServer installed	From 0 to 4
MpsTable	Table describing the parameters of each FPX MPServer installed	
MpsBullNumber	Total number of Bull hosts configured	From 0 to 40
MpsBullTable	Table describing the Bull hosts	
MpsStatNumber	FPX MPServer statistic instances	From 0 to 8
MpsStatTable	FPX MPServer statistics table	From 0 to 256

It is accessible through the following tree :

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxmps (2)

Servers table

The **FpxMpServer table** contains the configuration of each installed server.

Object Name	Description	Possible Values
MpsIndex	Server index	From 1 to 4
MpsName	Server name (service name)	FpxMpSrv1, FpxMpSrv2, FpxMpSrv3, FpxMpSrv4
MpsBoard	Name of the FPX adapter name used	FPX01
MpsSessNum	Number of allowed sessions	From 1 to 32
MpsBullName	Bull server name	BullNT1 (max 8 characters)
MpsBullState	Bull server state	0: Inactive 1: Active 2: Trace mode
MpsPadName	X.25/X.29 server name	PadNT1 (max 8 characters)
MpsPadState	X.25/X.29 server state	0: Inactive 1: Active 2: Trace mode
MpsNbX25Sess	Number of sessions reserved for the X.25 connections of the X.25/X.29 server	From 0 to 32
MpsNbX29Sess	Number of sessions reserved for the X.29 connections of the X.25/X.29 server	From 0 to 32
MpsNbBothSess	Number of non-dedicated sessions of the X.25/X.29 server	From 0 to 32
MpsNbBullHost	Number of Bull hosts configured for this FPX MPServer	From 0 to 10

MPS Trap Flag

A SNMP trap is generated when the configuration of a FPX MPServer has changed. The **MpsTrapFlag** can be set to zero to disable the trap generation.

BULL Hosts table

The **MpsBullTable** contains the description of each Bull host configured.

Object Name	Description	Possible Values
MpsBullIndex	Site index in the table	From 1 to 40
MpsBullMpsIndex	Index in the MpsTable of the FPX MPServer connecting to this host	From 1 to 4
MpsBullNetAddr	X.25 or ISDN network address of the host	1133010203 3357010203 ...
MpsBullName	Bull host name (optional)	DPSDEMO (max 15 characters)
MpsBullCallType	Type of host connection	0 normal 1 direct DNS 2 Calling handling
MpsBullLocAddr	Local network address	133000001

Object Name	Description	Possible Values
MpsBullFacField	Network facilities used for this host connection (including reverse charging and closed user group)	0001
MpsBullStations	Access rights of each workstation address for this host	i.e. D.D.D.N.N.U.U. ... D Dedicated N Non-dedicated U Unauthorized.

Statistics Table

The **MpsStatTable** contains the statistics for each configured MPServer

Object Name	Description	Possible Values
MpsStatIndex	Statistic instance index	From 1 to 256
MpsStatSrvIndex	FPX MPServer index of the MpsServer Table linked to this instance	From 1 to 4
MpsStatSrvType	Connection type	B: Bull P: Pad X: X25
MpsStatNetAddr	X.25 or ISDN network address of the Bull host	1133010203 3357010203 ...
MpsStatCallState	Host connection state	1 = Connected host 0 = Disconnected host
MpsStatActSessNumber	Number of active sessions	From 0 to 64 for a Bull host From 0 to 32 for a Pad or X25 host
MpsStatMaxSessNum	Maximum number of simultaneous sessions on this host since the FpxMpServer has been started up	From 0 to 64 for a Bull host From 0 to 32 for a Pad or X25 host
MpsStatClearSrv	Number of clears detected on server's side following a server error or a host connection reject	From 0 to 4,294,967,295
MpsStatClearLan	Number of clears detected on LAN's side following a LAN error	From 0 to 4,294,967,295
MpsStatClearWan	Number of clears detected on host's side following an FPX or a WAN error or a host connection reject	From 0 to 4,294,967,295
MpsStatThputMsg	Total number of messages per second flowing through the MPServer connection	From 0 to 4,294,967,295
MpsStatThputBytes	Total number of bytes per second flowing through the MpServer connection	From 0 to 4,294,967,295

The FPXQLLC MIB

This MIB contains the parameters and statistical information of each QLLC connection.

Object Name	Description	Possible Values
QllcMibDescription	MIB Name	

Object Name	Description	Possible Values
QllcTrapFlag	State of the trap flag	0 or 1 It can be set to 0 to disable trap generation when a QLLC connection is using the backup address to connect to the host or peer system.
QllcConnectionNumber	Number of connections	From 0 to 8
QllcCnctTable	Table describing the connection parameters and the statistics for each connection	

It is accessible through the following tree:

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxqllc (4)

QLLC Trap Flag

An SNMP trap is generated when a QLLC connection is using the backup access instead of the primary one. The **QllcTrapFlag** can be set to zero to disable trap generation.

QLLC Connections table

The **QllcCnctTable** contains the statistics of this connection.

Object Name	Description	Possible Values
QllcIndex	QLLC connection index	From 1 to 20
QllcName	QLLC connection name configured with the SNA Server Admin program	QLLC1, ASPARIS, etc.
QllcPrimNetAddr	Primary network address (described in SNA Server Admin)	1133020304
QllcBackNetAddr	Backup network address (described in FpxBackup)	0133020304
QllcPrimCnctOk	Number of successful connections done on the primary link	From 0 to 4,294,967,295
QllcBackCnctOk	Number of successful connections done on the backup link	From 0 to 4,294,967,295
QllcCnctFail	Number of connections failed on both primary and backup links	From 0 to 4,294,967,295
QllcPrimCnctState	Connection state of the primary link	1: connected link 0: disconnected link
QllcPrimRcvBytes	Number of bytes received on the primary link	From 0 to 4,294,967,295
QllcPrimSndBytes	Number of bytes transmitted on the primary link	From 0 to 4,294,967,295
QllcPrimRcvMsg	Number of messages received on the primary link	From 0 to 4,294,967,295
QllcPrimSndMsg	Number of messages transmitted on the primary link	From 0 to 4,294,967,295
QllcBackCnctState	Connection state of the backup link	1: connected link 0: disconnected link
QllcBackRcvBytes	Number of bytes received on the backup link	From 0 to 4,294,967,295

QllcBackSndBytes	Number of bytes transmitted on the backup link	From 0 to 4,294,967,295
QllcBackRcvMsg	Number of messages received on the backup link	From 0 to 4,294,967,295
FpxStatSndMsg	Number of messages transmitted on the backup link	From 0 to 4,294,967,295

The FPXX25 MIB

This MIB contains the parameters of each X.25 profile configured for the different FPX adapters.

Object Name	Description	Possible Values
X25MibDescription	MIB Name	
X25TrapFlag	State of the trap flag	0 or 1 It can be set to 0 to disable trap generation when the X.25 configuration or physical link state has changed.
X25ProfileNumber	Number of X.25 profiles	From 0 to n
X25ProfileTable	Table describing the X.25 profiles	
MacStatInstNumber	Number of MAC statistical instances Level 1	From 0 to 8
MacStatTable	Statistical table - Level 1	
LapStatInstNumber	Number of LAP statistical instances Level 2	From 0 to 12
LapStatTable	Statistical table - Level 2	
PlpStatInstNumber	Number of PLP statistical instances Level 3	From 0 to 256
PlpStatTable	Statistical table - Level 3	

It is accessible through the following tree:

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxx25 (5)

X.25 Trap Flag

A SNMP trap is generated when the X.25 configuration or the physical link state has changed (cable not plugged, for example). The **X25TrapFlag** can be set to zero to disable trap generation.

X.25 Profiles Table

The **X25ProfileTable** contains the description of the profiles configured on each adapter. Each table entry contains the following information:

Object Name	Description	Possible Values
ProfileIndex	Profile index	From 1 to 8
ProfileName	Profile Name	Profile for X.25/V24 connection Profile 1 for B-channel (ISDN connection) using the X.25 protocol, etc.

Object Name	Description	Possible Values
ProfileBoard	FPX adapter name (name given by the user when saving the FPX configuration)	FPX01
ProfilePrefix	Switching prefix used for this profile (only for FpxS, FpxM and FpxI)	33
ProfileFrmK	Frame window size	From 2 to 7 LAP-B and LAP-X and 1 for LAP-D
ProfileWSize	Packet window size	From 2 to 7
ProfileMaxPktSize	Maximum packet size	From 128 to 1024
ProfileThputClass	Throughput class	From 5 to 13
ProfileFirstIVC	First incoming logical channel	From 0 to 4095
ProfileFirstBVC	First two-way logical channel	From 0 to 4095
ProfileFirstOVC	First outgoing logical channel	From 0 to 4095
ProfileLastIVC	Last incoming logical channel	From 0 to 4095
ProfileLastBVC	Last two-way logical channel	From 0 to 4095
ProfileLastOVC	Last outgoing logical channel	From 0 to 4095

X.25 Statistics Table - Level 1

The **MacStatTable** contains statistical information at the physical level. Each table entry contains the following information:

Object Name	Description	Possible Values
MacStatIndex	Index of the MAC statistical instance	From 1 to 8
MacStatName	Name of the MAC statistical instance	FPX01/A-Channel (V28), etc.
MacStatPlugState	State of the physical link	1: plugged 0: not plugged
MacStatRcvBytes	Number of bytes received at the physical level	From 0 to 4,194,967,295
MacStatTransmittedBytes	Number of bytes transmitted at the physical level	From 0 to 4,194,967,295

X.25 Statistics Table - Level 2

The **LapStatTable** contains statistical information at the LAP level. Each table entry contains the following information:

Object Name	Description	Possible Values
LapStatIndex	Index of the LAP statistical instance	From 1 to 12
LapStatName	Name of the LAP statistical instance	FPX01/A-Channel LAP FPX01/D-Channel LAP, etc.
LapStatRcvBytes	Number of data bytes received at LAP level (link access control)	From 0 to 4,294,967,295
LapStatTransmittedBytes	Number of data bytes transmitted at LAP level (link access control)	From 0 to 4,294,967,295
LapStatRcvFrames	Number of frames received at LAP level (link access control)	From 0 to 4,294,967,295
LapStatTransmittedFrames	Number of frames transmitted at LAP level (link access control)	From 0 to 4,294,967,295

X.25 Statistics Table - Level 3

The **PlpStatTable** contains statistical information at the packet level. Each table entry contains the following information:

Object Name	Description	Possible Values
PLpStatIndex	Index of the PLP statistical instance	From 1 to 256
PLpStatName	Name of the PLP statistical instance	FPX01\1133010203 FPX02\3357010203, ...
PlpStatCallErrNumber	Number of failed connection attempts	From 0 to 4,294,967,295
PlpStatOpenSVC	Number of established VCs	From 0 to 4,294,967,295
PlpStatLastClearDiag	Latest clear diagnostic received on the X.25 link	From 0 to 255
PlpStatLastClearCause	Latest clear cause received on a virtual circuit	From 0 to 255
PlpStatRemoteClearNumber	Number of remote clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
PlpStatLocalClearNumber	Number of local clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
PlpStatRcvBytes	Number of data bytes received on a virtual circuit at packet level	From 0 to 4,294,967,295
PlpStatTransmittedBytes	Number of data bytes transmitted on a virtual circuit at packet level	From 0 to 4,294,967,295
PlpStatRcvPackets	Number of messages received on a virtual circuit at packet level	From 0 to 4,294,967,295
PlpStatTransmittedPackets	Number of messages transmitted on a virtual circuit at packet level	From 0 to 4,294,967,295

The FPXIP MIB

This MIB contains objects describing the FPX PassLan/IP driver configuration, the parameters of each accredited gateway and its associated statistics.

Object Name	Description	Possible Values
FpxIpMibDescription	MIB Name	
CfgTrapFlag	State of the configuration trap flag	0 or 1 It can be set to 0 to disable trap generation when the FPX PassLan/IP configuration has changed.
NdisIpAddr	IP address of the FPX adapter	128.1.1.2
NdisLocalNetAddr	Local network address	1133010203
NdisBoardList	List of the FPX adapters used	FPX01, FPX02, etc.
NdisUsePidList	PID use for each FPX adapter	YES, NO, etc. (in the adapter list order)
NdisTrcSysLevel	SYS trace level	0: none 1: errors 2: data 3: full
NdisTrcMacLevel	MAC trace level	0: none 1: errors 2: data 3: full

Object Name	Description	Possible Values
NdisTrcX25Level	X.25/PPP trace level	0: none 1: errors 2: data 3: full
BackupTrapFlag	State of the backup trap flag	0 or 1 It can be set to 0 to disable trap generation when a gateway connection is using the backup access.
GatewayNumber	Accredited gateway number	From 0 to 64
GatewayTable	Table describing each accredited gateway	
ConnectionNumber	Total number of configured connections	From 0 to 256
ConnectionTable	Table describing global parameters and the statistics for each accredited gateway	

It is accessible through the following tree:

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxip (3)

Backup Trap Flag

A SNMP trap is generated when a gateway is using the backup access instead of the primary one. The **BackupTrapFlag** can be set to zero to disable trap generation.

Gateways Table

The **GatewayTable** contains the global parameters and the statistics for each accredited gateway.

Object Name	Description	Possible Values
GtwIndex	Gateway index	From 1 to 64
GtwName	Gateway name	GTWPARIS
GtwIpAddress	Gateway IP address	128.1.1.3
GtwIpAddresRange	IP address range accepted by the driver	128.1.1.3 - 128.1.1.40
GtwUse	Gateway access	0: inbound 1: outbound 2: both
GtwProtocol	Protocol used	X.25, PPP, PPP-PAP, PPP-CHAP
GtwHighThreshold	Line-up threshold for bandwidth-on-demand	From 0 to 100 %
GtwLowThreshold	Line-down threshold for bandwidth-on-demand	From 0 to 100 %
GtwCnctNumber	Number of connections configured for this gateway	From 0 to 4
GtwAccRevCharg	Reverse charging acceptance	0: no 1: yes

Object Name	Description	Possible Values
GtwMainActiveCnct	Number of active connections on a primary link	From 0 to 4
GtwBackupActiveCnct	Number of active connections on a backup link	From 0 to 4
GtwExchangeBytes	Number of exchanged bytes (transmitted and received) on this gateway	From 0 to 4,294,967,295
GtwRcvBytes	Number of bytes received from this gateway	From 0 to 4,294,967,295
GtwSndBytes	Number of bytes transmitted to this gateway	From 0 to 4,294,967,295
GtwThputBytes	Number of bytes transmitted per second on this gateway	From 0 to 4,294,967,295

Connections Table

The **ConnectionTable** contains the parameters for each configured connection.

Object Name	Description	Possible Values
CnctName	Connection name	GTWPARIS/Cnx1
CnctGatewayIndex	Index of the gateway in the GatewayTable	From 1 to 64
CnctMainFpxName	FPX adapter name used for this connection (primary link)	FPX01
CnctMainOutNetAddr	Main network outgoing address	13301040404
CnctMainOutSubAddr	Main network outgoing sub-address	05
CnctMainInNetAddr	Main network incoming address	119201050505
CnctMainFacField	Network facilities used to connect the gateway (primary link) including reverse charging and CUG	00010105
CnctMainRetryNumber	Number of retries on the main address before using the backup address	From 1 to 999
CnctMainTimeout	Disconnection timeout value for this connection (main address)	From 1 to 999
CnctMainForbidenPort	Unauthorized ports on the main address	100 101 102 103
CnctMainAcceptedPort	Authorized ports on the main address	200 201 202
CnctBackFpxName	FPX adapter used for this connection (backup link)	FPX02
CnctBackOutNetAddr	Backup network outgoing address	013301040404
CnctBackOutSubAddr	Backup network outgoing sub-address	05
CnctBackInNetAddr	Backup network incoming address	119201050505
CnctBackFacField	Network facilities used to connect the gateway (backup link) including reverse charging and CUG	0105
CnctBackRetryNumber	Number of retries done on the backup address when connection failed	From 1 to 999
CnctBackTimeout	Disconnection timeout value for this connection (backup address)	From 1 to 999
CnctForbidenPort	Unauthorized ports on the backup address	100 101 102 103

Object Name	Description	Possible Values
CnctAcceptedPort	Unauthorized ports on the backup address	200 201 203

The PROXY MIB

This MIB contains objects describing the remote adapters FPX.

Object Name	Description	Possible Values
Description	MIB name	
RemFpxNumber	Number of remote FPX	From 1 to n
RemFpxTable	Table describing the parameters of each remote FPX installed	
MacStatNumber	Number of MAC statistics instances	From 1 to 2 fois n
MacStatTable	MAC statistics table	
LapStatNumber	Number of LAP statistics instances	From 1 to 3 fois n
LapStatTable	LAP statistics table	
PlpStatNumber	Number of PLP statistics instances	From 1 to X fois n
PlpStatTable	PLP statistics table	

It is accessible through the following tree :

iso (1) . org (3) . dod (6) . internet (1) . private (4) . enterprises (1) . cirel (1432) . fpxpro (6)

Fpx table

The **RemFpxTable** contains the configuration of each remote installed FPX.

Object Name	Description	Possible Values
Name	Name of the remote adapter FPX	FPX01
NetAddr	X.25 or ISDN network address of the remote adapter FPX	133010203
Facilities	Facility field of a called packet	0105
UserData	User data	
State	Remote adapter state	0 unknown 1 off 2 on
DPMAddress	Dual Port Memory Address	From A0000 to E8000
IOAddress	Input/Output port address used to communicate with the remote adapter	From 310 to 370
IRQLevel	Interrupt level to access the remote adapter	From 3 to 15
Type	Adapter type	B, I, IM or S
AChannel	Electrical interface on the A-channel (depends on the FPX used)	ISDN V11 V28 V35
BChannel	Electrical interface on the B-channel (depends on the FPX used)	ISDN V11 V28 V35 MODEM

Object Name	Description	Possible Values
Update	Statistics update of the remote adapter by changing the parameter Set=1	

Mac Statistics table - Level 1

The **MacStatTable** contains statistical information at the physical level. Each table entry contains the following information:

Object Name	Description	Possible Values
FpxIndex	Index of the MAC statistical instance	
InstName	Name of the MAC statistical instance	FPX01/A-Channel (V28), etc.
PlugState	State of the physical link	0: not plugged 1: CTS on 2: DSR on 3: CTS-DSR on
RcvBytes	Number of bytes received at the physical level	From 0 to 4,194,967,295
SentBytes	Number of bytes transmitted at the physical level	From 0 to 4,194,967,295

Lap Statistics table - Level 2

The **LapStatTable** contains statistical information at the LAP level. Each table entry contains the following information:

Object Name	Description	Possible Values
FpxIndex	Index of the LAP statistical instance	
InstName	Name of the LAP statistical instance	FPX01/A-Channel LAP
RcvBytes	Number of bytes received at the physical level	From 0 to 4,194,967,295
SentBytes	Number of bytes transmitted at the physical level	From 0 to 4,194,967,295
RcvFrames	Number of frames received at LAP level (link access control)	From 0 to 4,194,967,295
SentFrames	Number of frames transmitted at LAP level (link access control)	From 0 to 4,194,967,295

Plp Statistics table - Level 3

The **PlpStatTable** contains statistical information at the PLP level. Each table entry contains the following information:

Object Name	Description	Possible Values
FpxIndex	Index of the PLP statistical instance	
InstName	Name of the PLP statistical instance	FPX01\1133010203 FPX02\3357010203, ...

Object Name	Description	Possible Values
CallFailNumber	Number of failed connections attempts	From 0 to 4,194,967,295
OpenVCNumber	Number of established VCs	From 0 to 4,194,967,295
LastClearCause	Latest clear cause received on a virtual circuit	From 0 to 255
LastClearDiag	Latest clear diagnostic received on the X.25 link	From 0 to 255
RemoteClearNumber	Number of remote clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
LocalClearNumber	Number of local clears received on a virtual circuit at packet level	From 0 to 4,294,967,295
RcvBytes	Number of data bytes received on a virtual circuit at packet level	From 0 to 4,194,967,295
SentBytes	Number of data bytes transmitted on a virtual circuit at packet level	From 0 to 4,194,967,295
RcvPackets	Number of messages received on a virtual circuit at packet level	From 0 to 4,194,967,295
SentPackets	Number of messages transmitted on a virtual circuit at packet level	From 0 to 4,194,967,295

Using the SNMP extension DLLs

Overview

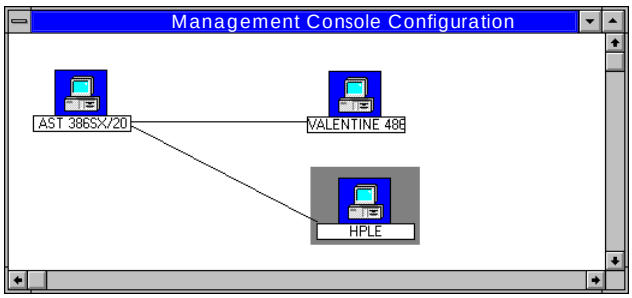
Simple Network Management Protocol is used to monitor and control hosts and gateways on an internetwork, so that the Administrator can set parameters on a remote host or gateway. The Windows NT SNMP Service allows a Windows NT computer to be monitored remotely, but does not include an *Agent* that can do the monitoring.

How does the SNMP Service works?

With this Service, a Windows NT machine can report its current status to an SNMP management system on a TCP/IP network, sending status information to a host in two instances: **when a management system requests information**
when a significant event occurs on the Windows NT machine.
The SNMP Service can handle requests from one or more hosts and report network information, called traps to a host.
On TCP/IP networks, each device has a unique name and IP address: the SNMP Service recognizes the host(s) to which the information are reported, and from which the requests are received.

When a network manager requests information about a device, the SNMP Service can be used to determine object values (MIBs), that represent various types of information about tis device.

Example of configuration



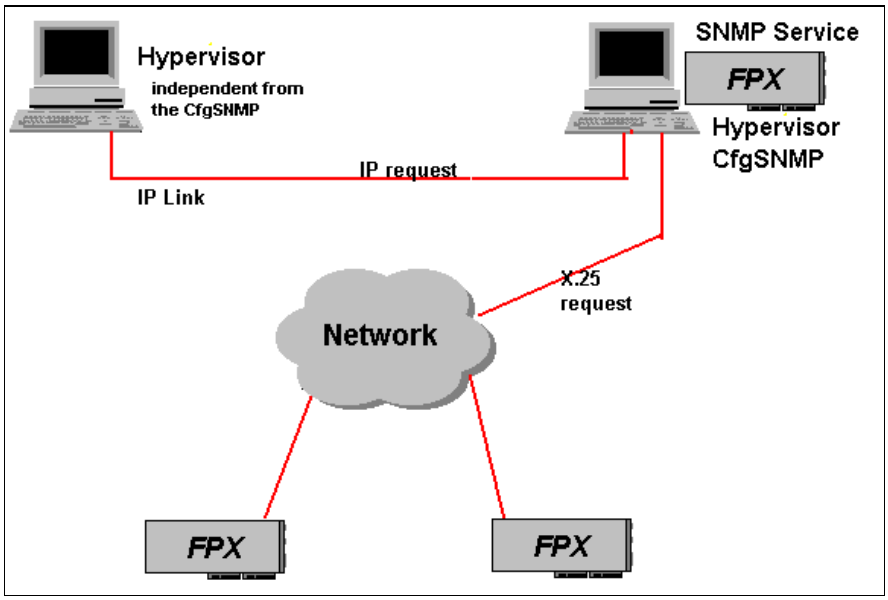
For example, the SNMP manager console is installed on a Windows for Workgroups computer labeled AST 386SX/20.

This console sends queries to the SNMP extension DLLs installed via the FPX MPSupervisor product on the Windows NT Server labeled HPLE.
The SNMP traps are transmitted to another Windows NT Server labeled VALENTINE.

The proprietary utilities

Principle

This diagram shows a basic example, allowing monitoring of remote adapter FPX.



Hypervisor Configuration (CfgSNMP)

Overview

The **SNMP Hyper Config** (CfgSNMP) tool describes the organization of a Company -whose FPX adapters- the Administrator would like to manage. The state of these FPX adapters is obtained through a non IP telecommunication network. The *Hypervisor* sends a request to the *SNMP Agent.* This *SNMP Agent* consults the FPX adapter -remote or local- via the telecommunication network and according to the answer, replies to the *Hypervisor* request. There is no configuration need for the NT machine. The configuration is used to describe non SNMP objects (non NT or NT through non IP network) as peripherals of the NT machine.

Menus description

The menus and their associated commands, described in the following table, are accessible by clicking. Some of these commands can be used by clicking directly on the shortcuts.

Menus/commands	Capabilities
File	
Save	Configure the Company organization
Print	
Print Preview	
Page Setup...	
Exit	Quit the program
Edit	
Cancel	Clear the screen as if using the Esc key
Cut	Remove an object
Copy	Copy the selected data to the clipboard
Paste	Paste the data contained in the clipboard
View	
Toolbar	Display or hide the Toolbar
Status Bar	Display or hide the Status bar
? (Help)	
Help Topics	Provide online information about commands and fields
About...	Display the version information

Toolbar

The toolbar is displayed above the application window, under the Menu bar. The various buttons are used to rapidly access to the different objects in the application, by clicking on the selected icon.
To display or not the toolbar, select the *View* menu, then the *Toolbar* command.

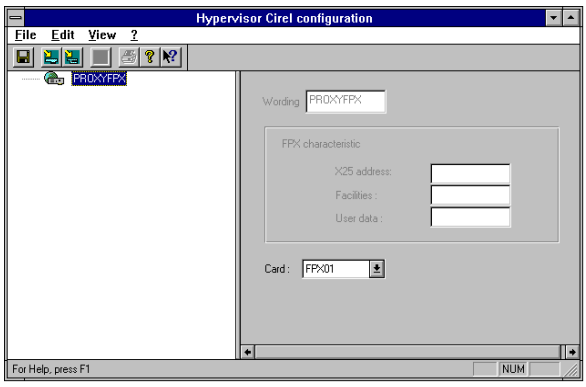
Save the Company organization.

Add an adapter FPX object.

Add an organization object.

Delete the object and those depending on it.

Creating an organization

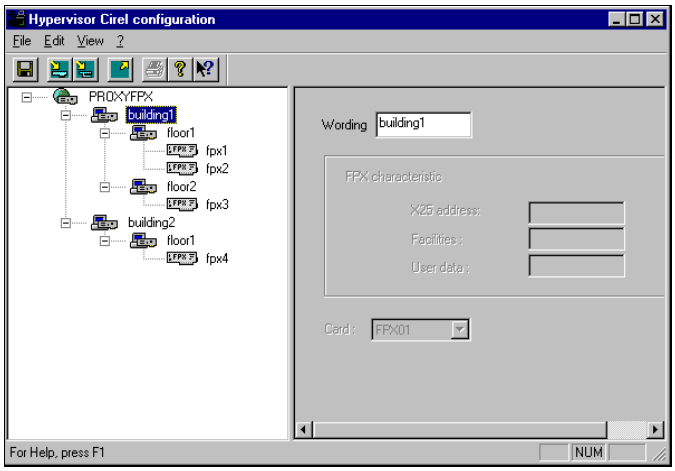


From the *Hypervisor Configuration* main screen, (from there, the Administrator can describe its Company organization):

- Click on the  button to add an organization object,
- Or click on the  button to add an adapter FPX object, then enter the associated parameters.

In the following example, the organization is made up of several FPX (fpx1, fpx2, fpx3, fpx4).

In fact, it is a tree-shaped description of a Company.



Note:
This tool can manage up to 500 adapters among 2000 objects.
Each branch shows an organization unit.
Each leaf shows a managed FPX adapter.

The whole set of organizations and FPX are objects handled by the *Configurator SNMP* program.

- For each organization, enter the label name (for example *buiding1*,...) in the *Wording* field.
- For each FPX, enter the label name (for example *fpx1*,...) and its associated characteristics in the *X25 address*, *Facilities*, and *User Data* fields.
- When the global definition is finished, click on  to save the structure.
- Stop and restart the SNMP service to update the proxy settings.

Hypervisor (Applet)

Menus description

The menus and their associated commands, described in the following table, are accessible by clicking.

The *Open* command can be used by clicking directly on the  shortcut.

Menus/commands	Capabilities
File	
Open	Access to the IP address (Ipconfig)
Exit	Quit the program
View	
Toolbar	Display or hide the Toolbar
Status Bar	Display or hide the Status bar
Split	Give the screen the correct proportion (vertical direction)
Refresh	Refresh the view
? (Help)	
About...	Display the version information

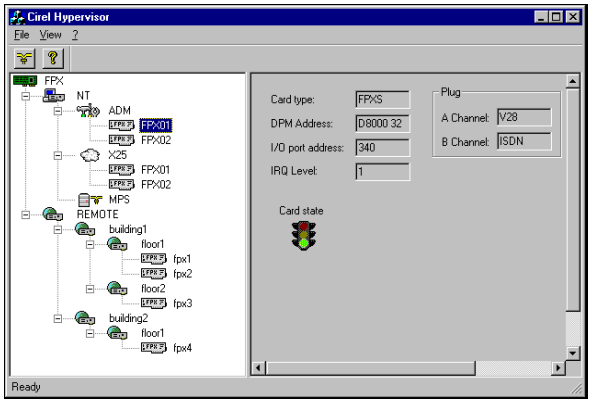
Toolbar

The toolbar is displayed above the application window, under the Menu bar. The  button is used to rapidly access to the IP address in the application, by clicking on the selected icon.
To display or not the toolbar, select the *View* menu, then the *Toolbar* command.

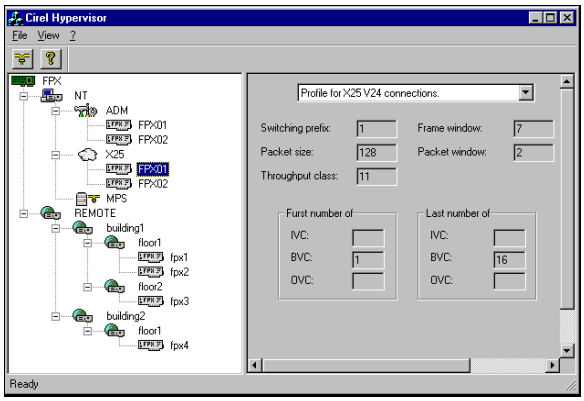
Inquiry

- From the *Hypervisor* main screen, click on the  button, then enter the *IP address* of the FPX (located on the machine with the SNMP Service).
- If the entered address is Ok, the Administrator can see via the MIB installed:
  - the local machine NT and its configuration
  - and the remote configurations (built previously via the Hypervisor Configuration).

Local machine labeled NT



This example shows the FPX01 adapter characteristics and its associated status.
The adapter has been properly loaded *(green light).*

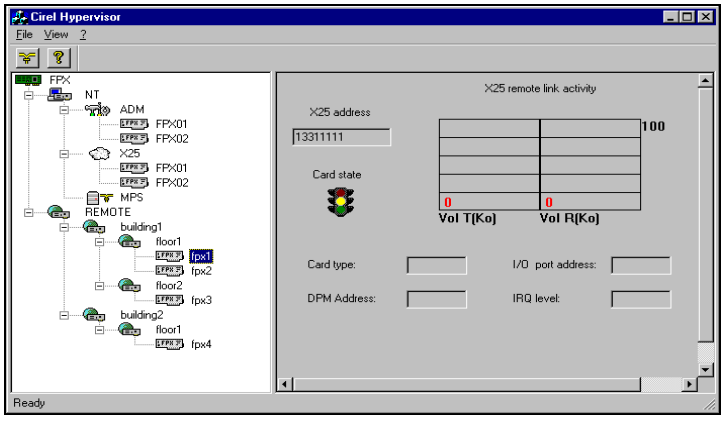


- Click on  to display the X.25 settings of the FPX01 (subscription).

The tree can be different, according the selection (adapter, services).

Remote machine labeled REMOTE

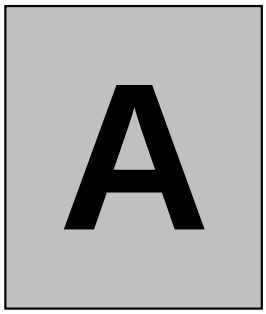
- Click on the FPX to be administrated to consult the status of the adapter, the activity,...: information that can be used by the Administrator to supervise the Company organization.



In this example, the adapter is found, but not loaded *(orange light).*

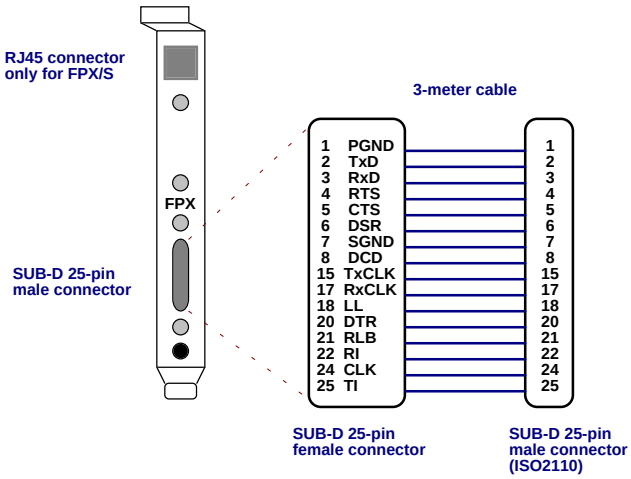
APPENDIX A

Cables

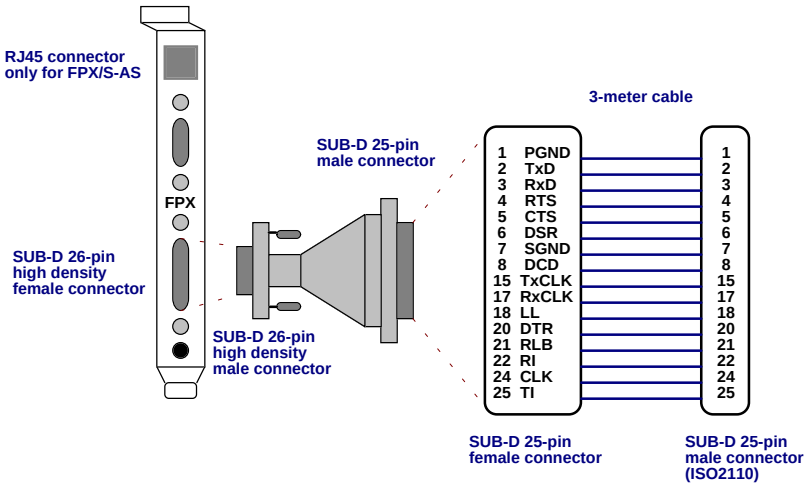


This appendix describes the pin-out diagrams for the cables.

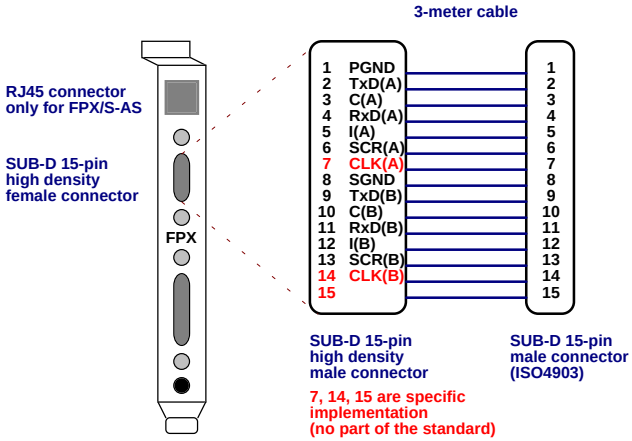
V28 cable (FPX/B & FPX/S)



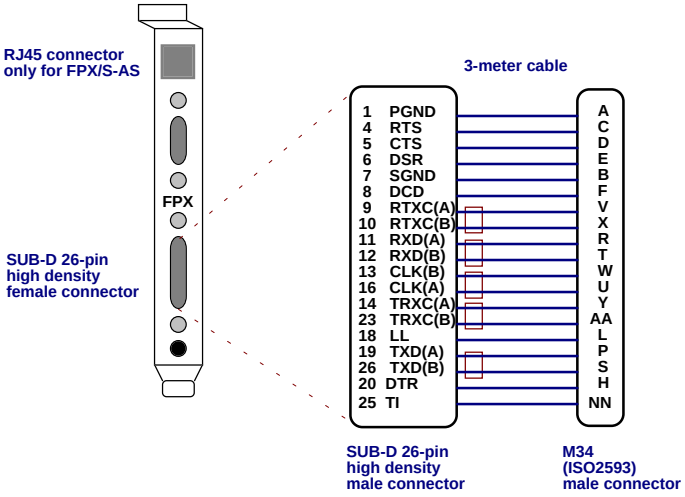
V28 cable (FPX/B-AS & FPX/S-AS)



V11 cable (FPX/B-AS & FPX/S-AS)



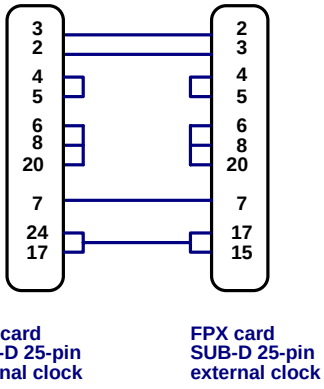
V35 cable (FPX/B-AS & FPX/S-AS)



The M34 connector is available in two formats:

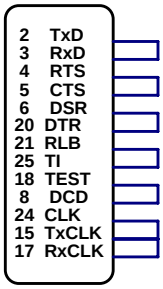
- US standard with a 1.6 mm pin-out diameter
- European standard with a 1 mm pin-out diameter

V28 null-modem cable



This cable must be used when two FPX cards are connected back-to-back through the V28 electrical interface.

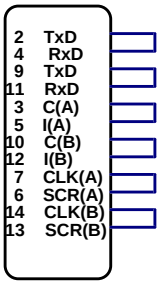
V28 loopback cable



SUB-D 25-pin connector

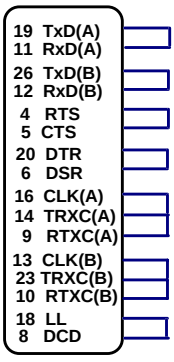
This loopback must be used when executing FPX selftests through the FPX Diagnostic Control Panel.

V11 loopback cable



SUB-D 15-pin connector

V35 loopback cable



SUB-D 26-pin connector

APPENDIX B

Error Logging

B

Loading errors

Code	Meaning
1	Invalid syntax
2	Incorrect adapter number
3	Load file not found
4	Error reading file
5	No answer or missing adapter
6	Unable to reinitialize adapter
7	Unexpected end of file
8	PEDATA too long
9	Unable to load adapter
10	Illegal module end attribute
11	Start address not found
12	MIP driver not started
13	Descriptor file not found
14	Descriptor file too long
15	Incorrect parameters in descriptor file
16	Invalid syntax in descriptor file
17	Error closing file
18	Incorrect adapter parameters
19	Software is already down-loaded
20	Incorrect selftests patterns
21	Incorrect I/O port address
22	Error initializing MIP driver dialog
23	Missing adapter or incorrect adapter configuration
24	Problem initializing MIP driver parameters
25	Adapter selftests failed
26	Configuration file not found
27	Error reading configuration file
28	Pre-loader file not found
29	Missing adapter in configuration file
30	Pool allocation incompatibility
31	Incorrect number of pools
32	Incorrect buffer size
33	Incorrect number of buffers in a pool
34	Incorrect pool allocation
35	Incorrect pool number
36	TMS reset
37	TMS boot failure
38	TMS starting failure
39	TMS error

Initializing errors (XINIT.CPT report file)

Initializer errors

Code	Meaning
1	Error number not found
2	Initialization ended successfully
3	Syntax: WXINIT filename adapter number
4	Incorrect adapter name
5	Unable to create XINIT.CPT report file
10	Configuration file not found
11	Configuration file is empty
12	Configuration file not compliant with:
13	Invalid header in configuration file
14	Invalid configuration file for an FPX adapter
15	Incorrect buffer length
16	Buffer allocation for a message failed
17	Missing parameters in configuration file

Dictionary errors

Code	Meaning
20	Dictionary file not found
21	Dictionary file is empty
22	Dictionary file not compliant with:
23	Dictionary size too big
24	Error in dictionary file, see below
25	Control block parameter not specified
26	Missing parameter or block name
27	Invalid syntax, name must be alphanumeric
28	Name too long (8 characters max.)
29	Incorrect procedure number
30	Control block parameter not found
31	Block brackets misuse (missing begin block)
32	Missing equal sign (=) after a parameter name
33	Missing or incorrect parameter attribute
34	Incorrect property for a parameter
35	Incorrect type for a parameter
36	Incorrect length for a parameter
37	Incorrect procedure number for a parameter
38	Incorrect iteration for a parameter
39	Control block parameter must be numeric
40	Unknown type
41	Block length too long
42	Missing global block
43	A control block parameter cannot be incremented
44	Beginning of block with no corresponding end of block
45	Parameter not found for the name:

Configuration errors

Code	Meaning
50	Error in configuration file
51	Number of estimated block occurrences not found
52	Data not compliant with dictionary
53	Record type not compliant with dictionary
54	Name not compliant with dictionary

Block errors

Code	Meaning
70	Number of block iterations incorrectly specified
71	Continuation block expected
72	Block iteration depth too big
73	Expecting block after a size parameter
74	Number of block iterations greater than the control parameter value

Parameter errors

Code	Meaning
80	Incorrect numeric value for a parameter
81	Type of parameter not already implemented
82	Expecting string value (in quotes)
83	String value length exceeding allowable limit
85	Value outside numeric interval
86	Incorrect hexadecimal string value
87	Hexadecimal string value length exceeding allowable limit
88	Block size parameter must be transmittable
100	Adapter not configured
101	Message buffer overflow
102	Memory allocation failure
103	Stopped by user
151	Already initialized
152	An error has been detected
200	Error communicating with FPX adapter
250	Initializing layer
251	Error in reference file:
252	Reference file not found
253	Missing configuration file name
254	A task name must have 6 characters
255	A task definition is expected: '*...'
256	No task defined
257	Missing ',' or message size
258	Missing ',' separator
259	Missing ';'at end of line
260	Incorrect dictionary file (.dic)

Code	Meaning
261	A layer name must have 6 characters
262	Initializing task
263	Unknown option
264	Unable to open report file
265	Task not found or already terminated
266	Terminating task
270	Incorrect command line option
271	Unknown task
272	Incorrect task termination order
273	Illegal ALL option
274	Task not selected
300	Error communicating with COM/DRIVER
400	Error communicating with COM/ADMIN ISDN

FPX PassLan/IP system events

Various system events are sent to the Event Viewer to help the user.

These events are classified in 3 categories:

- *Information*
  to help the user monitor driver activity: these events provide WAN information (successful/failed incoming and outgoing connections, disconnections with X.25 cause and diagnostic, etc.)

- *Warning*
  when a problem occurs without affecting driver activity: these events are used when a parameter has an incorrect value in the *Registry*, or when an incoming call is rejected because the gateway is not authorized, etc.

- *Error*
  when a severe error occurs and causes a gateway disconnection or a driver stopping: these events are used when a mandatory gateway parameter has an incorrect value in the *Registry,* or when communication with an FPX adapter has failed, etc.

Information events are only available when the X.25 trace level is set to **DATA** (Global parameters panel in the FPX PassLan/IP configuration program).
Warning and *Error* events are available at any X.25 trace level (Global parameters panel in the FPX PassLan/IP configuration program).

Note: To avoid saturation of the system log, do not set the X.25 trace level to DATA when using the product intensively.

The table below lists possible events and the following data associated with them:

Value:	Event value
Type:	Event type (Information, Warning or Error)
Trace:	X.25 trace level necessary to obtain this event (None, Data)
Info:	Additional information is sometimes available for an event No: no additional information Yes followed by a number: additional information is available; the number indicates the type of additional information)
Description:	Description of the event
Note:	Event note

When the *Info* parameter is set to Yes, double-click on this event inside the Event Viewer to show the *Event Detail* window that contains valuable information. Select the *Word* radio button and read the 4 bytes at offset 14. These 4 bytes provide additional information according to the number following Yes in the *Info* column.

X.25 Trace

Number	1st Byte	2nd Byte	3rd Byte	4th Byte	Note
1	00	00	00	FPX adapter Number (from 01 to 15)	FPX adapter number
2	Gateway Number (from 01 to 64)	Connection Number (from 01 to 04)	00	FPX adapter Number (from 01 to 15)	The Gateway Number corresponds to the position of the gateway in the allowed gateway list. The Connection Number corresponds to the number of connections defined for this gateway. FPX adapter number
3	Gateway Number (from 01 to 64)	Connection Number (from 01 to 04)	01 main address 02 backup address	FPX adapter Number (from 01 to 15)	The Gateway Number corresponds to the position of the gateway in the allowed gateway list. The Connection Number corresponds to the number of connections defined for this gateway. FPX adapter number
4	Gateway Number (from 01 to 64)	Connection Number (from 01 to 04)	Cause	Diagnostic	The Gateway Number corresponds to the position of the gateway in the allowed gateway list (00 when the gateway is not found). The Connection Number corresponds to the number of connections defined for this gateway (00 when the gateway is not found). Cause and diagnostic of the clear packet
5	XX	YY	ZZ	WW	Mip function retcode

List of events

The events are the same for the FPXTAPI, FPXNDIS and LLCX25 Drivers.
From the value = 1004 to the value = 1018, only the FPXNDIS is affected.

Value	Type	Trace	Info.	Description	Note
	Error	None	No	'Parameters' key not found in the registry	The FpxNdis driver is not installed in memory. Configure the PassLan/IP product and restart the computer. If the problem persists, reinstall the product.

Value	Type	Trace	Info.	Description	Note
1	Error	None	No	Incorrect adapter number in the registry	The FpxNdis driver is not installed in memory. Configure the PassLan/IP product and restart the computer. If the problem persists, reinstall the product.
2	Error	None	No	Incorrect IP local address	The FpxNdis driver is not installed in memory. Bindings between the TCP/IP protocol and the FpxNdis driver may not have been created. Select the Control Panel, click on the Network icon, check bindings between TCP/IP protocol and the driver, and restart the computer.
3	Error	None	No	Incorrect X121 local address	Configure the FPX PassLan/IP product. If the problem persists, reinstall the product.
4	Wng.	None	No	MacTrace, SysTrace or X25Trace key not found in the registry	Configure the FPX PassLan/IP product. If the problem persists, reinstall the product.
5	Error	None	No	'Gateways' key not found in the registry	The FpxNdis driver is not installed in memory. Configure the FPX PassLan/IP product and restart the computer. If the problem persists, reinstall the product.
6	Error	None	No	No allowed gateway	At least one gateway must be accredited using the FPX PassLan/IP configuration program.
7	Error	None	No	Gateway name too long	Modify the gateway name using FPX PassLan/IP configuration program.
8	Error	None	No	Subkey under 'Gateways' key not found in the registry	Configure the FPX PassLan/IP product. If the problem persists, reinstall PassLan/IP product.
9	Error	None	No	Incorrect IP address for a gateway	Modify this IP address using FPX PassLan/IP configuration program.
10	Error	None	No	Value of 'Use' key incorrect or key not found in the registry	Check this gateway again using FPX PassLan/IP configuration program.
11	Error	None	No	Incorrect X121 main address for a gateway	Check this gateway again using FPX PassLan/IP configuration program.
12	Error	None	No	Incorrect value for 'MainFacField' key or key not found in the registry	Check this gateway again using FPX PassLan/IP configuration program.
13	Error	None	No	Incorrect X121 backup address for a gateway	Check this gateway again using FPX PassLan/IP configuration program.
14	Error	None	No	Incorrect value for 'BackupFacField' key or key not found in the registry	Check this gateway again using FPX PassLan/IP configuration program.
15	Error	None	No	Incorrect value for 'AcceptRevCharg' key for a gateway in the registry	Check this gateway again using FPX PassLan/IP configuration program.

Value	Type	Trace	Info.	Description	Note
16	Error	None	No	Out of memory	The FpxNdis driver is not installed in memory. Restart your computer.
17	Wng.	None	Yes 1	Received incoming connection from unknown caller	No gateway has been accredited to accept this incoming call. Configure a new gateway using FPX PassLan/IP configuration program.
18	Wng.	None	Yes 2	Incoming call received but reverse charging not authorized	No gateway has been accredited to accept this incoming call. Configure a new gateway using FPX PassLan/IP configuration program.
19	Wng.	None	Yes 2	Incoming call received but no more context available	Incoming call discarded.
20	Wng.	None	Yes 3	Maximum call retries exhausted	Check this gateway, X.25 or ISDN Wan. Is there an accredited gateway on the remote server?
21	Wng.	None	Yes 3	Switching to backup access	
22	Error	None	No	Reconfiguration failed See following error	Dynamic reconfiguration of the FpxNdis driver has failed. Please configure the product again. If the problem persists, restart the computer.
23	Error	None	No	Illegal context (Invalid "AppRef")	The FpxNdis driver has received an invalid frame sent by an FPX adapter. The corresponding connection of this gateway is closed. Other connections are not affected.
24	Wng.	None	No	Received message for a free context	This can occur after a WAN clear. No effect on driver's activity.
25	Error	None	No	Received message for a closed context	This can occur after a WAN clear. No effect on driver's activity.
26	Error	None	No	Illegal Request (Invalid "Cont" or "Purge" message)	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
27	Error	None	No	Incorrect message length received from an FPX adapter	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.

Value	Type	Trace	Info.	Description	Note
28	Error	None	No	Message with invalid "Cmdu" field received from an FPX adapter	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
29	Error	None	No	Message with invalid "Interface" field received from an FPX adapter	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
30	Error	None	No	Message with incorrect buffer length received from an FPX adapter	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
31	Error	None	No	Message with invalid X.25 event received from an FPX adapter	The FpxNdis driver has received an invalid frame sent by an FPX adapter. All gateway connections using this FPX adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
32	Error	None	Yes 3	ACK_CONREQ message received for a context not in CALL_PENDING state	This gateway connection will be closed. Other connections are not affected.
33	Error	None	Yes 3	CON_CON message received for a context not in CALL_PENDING state	This gateway connection will be closed. Other connections are not affected.
34	Error	None	Yes 3	DATIND message received while another DATIND message is being received	This gateway connection will be closed. Other connections are not affected.
35	Error	None	Yes 3	DATIND message received with a fragment length bigger than the total length	This gateway connection will be closed. Other connections are not affected.
36	Error	None	Yes 3	DATIND message received for a context with no receipt credit	This gateway connection will be closed. Other connections are not affected.
37	Error	None	Yes 3	ACK-FLOWTREQ message received for a context not in FLOWT_PENDING state	No effect for this gateway connection: this message is lost.
38	Error	None	No	MEP_CONT message received with a fragment length + saved length >= total length	This gateway connection will be closed. Other connections are not affected.

Value	Type	Trace	Info.	Description	Note
39	Error	None	No	Incorrect ReceiveMip retcode	Incorrect status of ReceiveMip function caused by the FPX. All gateway connections using this adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
40	Error	None	No	Incorrect IRP status	Incorrect IRP status caused by the FPX adapter. All gateway connections using this adapter will be closed. Reloading this adapter may be required. Gateways using other FPX adapters are not affected.
41	Error	None	No	Incorrect SendMip retcode	The FpxNdis driver will send this request later.
42	Error	None	No	Incorrect OpenDevice retcode for an FPX adapter	The FpxNdis driver will send this request later. While this request has not been correctly sent, the FpxNdis driver considers that this FPX adapter is not operational.
43	Error	None	Yes 1	MIP_CNX_DEAD for a Mip context	An FPX adapter is out-of-order. All gateway connections using this FPX adapter will be closed. Reloading this adapter is mandatory. Gateways using other adapters are not affected.
44	Error	None	Yes 5	CloseDevice failed for an FPX adapter	An FPX adapter is out-of-order. All gateway connections using this FPX adapter will be closed. Reloading this adapter is mandatory. Gateways using other adapters are not affected.
52	Error	None	No	Unauthorized link Bindings with TCP/IP or Netbeui protocol are disabled.	Select Control Panel, click on Network icon, check bindings between the FpxNdis driver and the TCP/IP protocol and restart your computer.
53	Info.	Data	No	Incoming call with calling address	
54	Wng.	None	Yes 3	Incorrect length sent to the FPX adapter. (ignored)	No effect on this specific gateway.
55	Wng.	None	Yes 3	Timeout on FLOW_TRANSMIT_REQUEST event	An FPX adapter has not provided the transmission credit for this connection. When this event log is registered, the connection is closed. Other connections are not affected.
57	Error	None	No	Mip connection already opened	A Mip connection is already established with an FPX. All connections with it are closed. Connections with other FPX adapters are not affected. Reload this adapter to activate gateways associated with it.

Value	Type	Trace	Info.	Description	Note
59	Error	None	No	Invalid link - A binding MUST be disabled (Bloodhound ?)	Select the Control Panel, click on Network icon, check bindings between the FpxNdis driver and the protocols or services and restart your computer.
66	Wng.	None	Yes 3	Timeout on FLOW_TRANSMIT_REQUEST event (1st phase)	An FPX adapter has not provided transmission credit for this connection. When this event happens, no data are transmitted on this connection. Other connections are not affected.
67	Info.	Data	Yes 1	ConnectMip successful	
68	Info.	Data	Yes 1	ConnectMip failed	This FPX adapter is not loaded or is currently being loaded.
69	Info.	Data	Yes 1	X.25 Register request successful	Register request sent to NETX25 task towards the FPX adapter.
70	Info.	Data	Yes 1	X.25 Register request failed	Register request rejected by the FPX adapter.
71	Info.	Data	Yes 1	X.25 Deregister request successful	Deregister request sent to NETX25 task towards the FPX adapter.
72	Info.	Data	Yes 1	X.25 Deregister request failed	Deregister request rejected by the FPX adapter.
73	Info.	Data	Yes 3	X.25 CON_REQ message successful	Successful outgoing call request to an FPX adapter.
74	Info.	Data	Yes 3	X.25 CON_REQ message failed	Failed outgoing call request to an FPX adapter.
75	Info.	Data	Yes 3	X.25 CON_RES message successful	Incoming call accepted by the FpxNdis driver. A call response is sent to the FPX adapter.
76	Info.	Data	Yes 3	X.25 CON_RES message failed	Incoming call accepted by the FpxNdis driver. The call response is rejected by the FPX adapter.
77	Info.	Data	Yes 4	X.25 DIS_REQ message successful	Clear request sent to an FPX adapter.
78	Info.	Data	Yes 4	X.25 DIS_REQ message failed	Clear request rejected by the FPX adapter.
79	Info.	Data	Yes 1	Received X.25 Register ACK message	X.25 register request acknowledged by the FPX adapter.
80	Info.	Data	Yes 1	Received X.25 Register NACK message	X.25 register request rejected by the FPX adapter.
81	Info.	Data	Yes 3	X.25 CON_IND message successful	Incoming call received from the FPX adapter by the FpxNdis driver.
83	Info.	Data	Yes 3	X.25 CON_CON message successful	Outgoing call accepted by a remote gateway.
85	Info.	Data	Yes 4	X.25 DIS_IND message successful	Clear indication received from a remote gateway.
88	Error	None	Yes 1	ConnectMip failed -> Restart the computer	The FPX adapter may be reloaded when an IP flow is received or sent by the FpxNdis driver.

Value	Type	Trace	Info.	Description	Note
89	Error	None	No	Buffer already freed	A buffer deallocation is currently in progress but it is already free. No effect on other connections.
90	Error	None	No	PAP local user name too long	Check this gateway again using FPX PassLan/IP configuration program.
91	Error	None	No	PAP remote user name too long	Check this gateway again using FPX PassLan/IP configuration program.
92	Error	None	No	PAP local password too long	Check this gateway again using FPX PassLan/IP configuration program.
93	Error	None	No	PAP remote password too long	Check this gateway again using FPX PassLan/IP configuration program.
94	Error	None	No	CHAP local user ID too long	Check this gateway again using FPX PassLan/IP configuration program.
95	Error	None	No	CHAP remote user ID too long	Check this gateway again using FPX PassLan/IP configuration program.
96	Error	None	No	Secret too long	Check this gateway again using FPX PassLan/IP configuration program.
97	Error	None	Yes 3	Inbound call received while outgoing call is connecting	No effect for this connection
98	Error	None	Yes 3	Problem with unauthorized TCP/UDP ports	An application cannot establish a connection with a remote gateway because its TCP/UDP ports are not authorized for this gateway.
99	Error	None	Yes 3	Received incoming connection with unallowed Pid	Modify the Pid option using FPX PassLan/IP configuration program for the driver to accept this incoming call.
100	Info	Data	Yes 3	PPP not established.	PPP establishment in progress.
101	Info	Data	Yes 3	PPP established.	
1004	Info	Data	Yes 3	First incoming IP address	
1005	Info	Data	Yes 3	First outgoing IP address	
1009	Info	Data	Yes 3	Stac compression activated	
1014	Info	Data	Yes 3	Incorrect main DLCI for gateway	Check the configuration in FPX PassLan/IP.
1015	Info	Data	Yes 3	Incorrect backup DLCI for gateway	Check the configuration in FPX PassLan/IP.
1016	Info	Data	Yes 3	Unexpected Frame Relay encapsulation: xxxx	Check the encapsulation parameters in the gateway configuration.
1017	Info	Data	Yes 3	DLCI number xxxx activated	Frame Relay connection in progress
1018	Info	Data	Yes 3	DLCI number xxxx deactivated	Frame Relay connection closed

MAC Trace

Value	Type	Trace	Info.	Description	Note
102	Wng.	Error	Yes 3	Forbidden IP remote address (event log 103).	Data packet received with a forbidden IP remote address. Event log 103 shows this address.
103	Wng.	Error	Yes 3	Forbidden IP address: see at offset 14.	

Note: How is the **Incoming network address** within the *Connection configuration* dialog box filled in properly?

This can be easily done by using Event log 53 in the event viewer System log.
This event displays these messages:

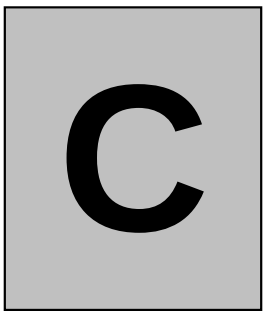
Info in Receive X25 section : Incoming call from 2***13301020304*** - Length 12

The first part (one or two digits) of this incoming address corresponds to the profile prefix used for this FPX adapter (refer to the FPX configuration program).
The following digits (in bold and italic here) is the incoming network address that can be used to fill in the connection dialog box for a specific gateway. To do this, execute the following steps:

- From the event viewer, note this address or select it with the arrow keys and then Control Enter.
- Go to the *Connection configuration* dialog box in the PassLan/IP configuration program
- Insert the incoming address in this window:

A P P E N D I X C

X.25 Clears description



X.25 Causes

Code (hexadecimal)	Meaning
0x00	[DTE] DTE originated call
0x01	[OCC] Number busy
0x03	[INV] Invalid facility request
0x05	[NC] Network congestion
0x09	[DER] Out-of-order
0x0b	[NA] Access barred
0x0d	[NP] Not obtainable
0x11	[RPE] Remote procedure error
0x13	[ERR] Local procedure error
0x19	[PCV] Reverse charging not subscribed to
0x21	[ ] Incompatible destination
0x29	[ ] Fast select acceptance not subscribed to
0x39	[ ] Missing ship (for mobile maritime service)
0xff	[ ] Unknown cause

X.25 Diagnostics

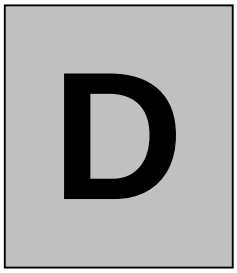
Code (hexadecimal)	Meaning
0x00	No additional information
0x01	Invalid P(S)
0x02	Invalid P(R)
0x10	Packet type invalid
0x11	Packet type invalid for state r1
0x12	Packet type invalid for state r2
0x13	Packet type invalid for state r3
0x14	Packet type invalid for state p1
0x15	Packet type invalid for state p2
0x16	Packet type invalid for state p3
0x17	Packet type invalid for state p4
0x18	Packet type invalid for state p5
0x19	Packet type invalid for state p6
0x1a	Packet type invalid for state p7
0x1b	Packet type invalid for state d1
0x1c	Packet type invalid for state d2
0x1d	Packet type invalid for state d3
0x20	Packet not allowed
0x21	Unidentifiable packet
0x22	Call on one-way logical channel
0x23	Invalid packet on a PVC
0x24	Packet on unassigned logical channel
0x25	Reject not subscribed to
0x26	Packet too short
0x27	Packet too long

Code (hexadecimal)	Meaning
0x28	Invalid general format identifier
0x29	Restart with non-zero general format identifier
0x2a	Packet type not compatible with facility
0x2b	Unauthorized interrupt confirmation
0x2c	Unauthorized interrupt
0x2d	Unauthorized reject
0x30	Timer expired
0x31	Timer expired for incoming call
0x32	Timer expired for clear indication
0x33	Timer expired for reset indication
0x34	Timer expired for restart indication
0x40	Call setup, call clearing or registration problem
0x41	Facility/Registration code not allowed
0x42	Facility parameter not allowed
0x43	Invalid called address
0x44	Invalid calling address
0x45	Invalid facility/registration length
0x46	Incoming call barred
0x47	No logical channel available
0x48	Call collision
0x49	Duplicate facility requested
0x4a	Non-zero address length
0x4b	Non-zero facility length
0x4c	Facility not provided when expected
0x4d	Invalid CCITT specified DTE facility
0x50	Miscellaneous
0x51	Improper cause code from DTE
0x52	Non-aligned byte
0x53	Inconsistent Q-bit setting
0x70	International problem
0x71	Remote network problem
0x72	International protocol problem
0x73	International link out-of-order
0x74	International link busy
0x75	Transit network facility problem
0x76	Remote network facility problem
0x77	International routing problem
0x78	Temporary routing problem
0x79	Unknown called DNIC
0x7a	Maintenance action
0x80	Clear request from DTE-C
0x81	Clear response
0x82	Reselect request
0x83	Loss of characters
0x84	Break request from DTE-C
0x85	Reset request from DTE-C
0x86	Invalid PAD parameters
0x88	Unknown number cause received from Telex
0x89	Out-of-order cause received from Telex
0x8a	Missing cause received from Telex
0x8b	Unauthorized access cause received from Telex
0x8c	Busy cause received from Telex
0x8d	Telex communication break
0x90	Trouble caused by TRANSPAC
0x91	Trouble caused by TRANSPAC
0x92	Trouble caused by TRANSPAC
0x93	Trouble caused by TRANSPAC

Code (hexadecimal)	Meaning
0x94	Trouble caused by TRANSPAC
0x95	Line not in service or maintenance in progress
0x96	Line not in service or maintenance in progress
0x97	Modem powered off or looped, or terminal powered off
0x98	Circuit 105 not provided by DTE
0x99	Frame level not provided yet
0x9a	Restart in progress
0x9b	SARM received by the DTE when established
0x9c	DISC received by the DTE when established
0x9d	DM received by the DTE when established
0x9e	SABM received by the DTE when established
0x9f	CMDR/FRMR received by the DTE when established
0xa0	Invalid N(R)
0xa1	Inconsistent F Bit received
0xa2	Command unknown or too long
0xa3	Response unknown or too long
0xa4	No response for N2 SARM
0xa5	No response for N2 I-frame
0xa6	Reset received
0xa7	N(S) already received in the window
0xa8	No response for N2 reset
0xa9	Too many errors in line
0xaa	No more flags following the error
0xab	Closing signal lm
0xac	Loopback
0xad	No frame received during T3
0xb0	Unknown service
0xb1	Missing resources
0xb2	Maximum number of simultaneous calls reached for this service
0xb3	Access to the requested service is not allowed
0xc0	No dial tone
0xc1	No response for 5 call backs
0xc2	Call stepping dial time is too long (1min)
0xc3	Busy tone detected
0xc4	The called subscriber does not provide 2100 Hz
0xc5	Frame level cannot be established
0xc6	Phone communication break
0xca	Failed calling ISDN on synchronous dial-in port
0xcb	TRANSPAC/ISDN channel not available on SDP
0xff	Unknown diagnostic

APPENDIX D

PAD profile

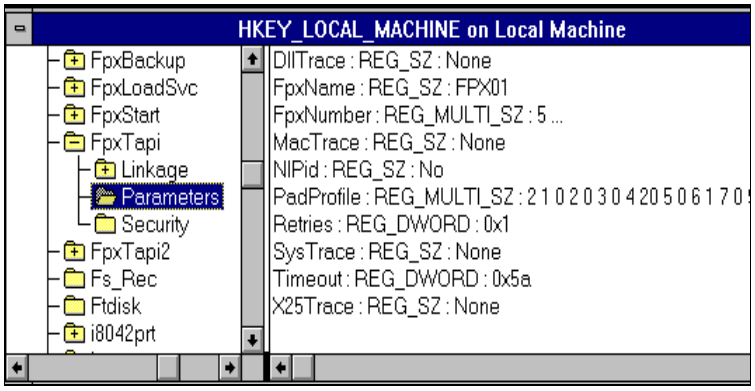


This appendix describes the value of parameters for the default PAD profile used by the FPX RAS Support when accepting asynchronous connections.

Registry location

- Click on the ***Windows NT Diagnostic*** icon in the Administration Tools group on NT3.51 or
- Click on START, then run **Regedit**.

- In the *Tool* menu, select the *Registry Editor* command.
- Go to the **HKEY_LOCAL_MACHINE** window.
- Select **SYSTEM** key, then **CurrentControlSet**, **Services.**



The PadProfile is set in the **Parameters** section of the **FpxTapi** key.

It is defined as a multi-string and includes the following elements:

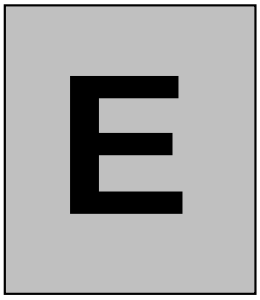
- 2 SET command
- 1 0 Parameter 1, value 0
- 2 0 Parameter 2, value 0
- 3 0 Parameter 3, value 0
- 4 20 Parameter 4, value 20
- 5 0 Parameter 5, value 0
- etc.

PAD parameters

Parameter	Meaning
1	Escape character
2	Echo
3	Data forwarding character
4	Idle delay timer (1/20 second)
5	Flow control (PAD to terminal)
6	PAD result code control
7	PAD action on break receipt
8	Discard output
9	Padding characters after carriage return
10	Line folding
11	Terminal transmission speed
12	PAD flow control (by terminal)
13	Line feed insertion after carriage return
14	Padding characters after line feed
15	Editing
16	Character delete function
17	Line (buffer) delete function
18	Line display function
19	Editing PAD result codes
20	Echo mask
21	Parity treatment
22	Page wait

APPENDIX E

ISDN connection sample trace



This appendix shows a trace generated by the FPX diagnostic Tools.

How to get the trace

- From the *FPX Diagnostic Tools Panel* dialog box, select *Traces* in the *Tools* menu

Sample trace

LAPD level information asked on : Mar 21 10:51:31 1996

-- From ISDN -- ☞ *Starting physical level establishment*
ISDN: Layer 1 Activation Request From Terminal.

-- From ISDN --
ISDN: Layer 1 Activated.

- From Network - ☞ *Checking all TEI(s)*

LAPD: Sapi 63 Tei 127 C
FE FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 0
Msg_Type : ID CHK REQUEST
Ai_Ind : 127

- From Terminal- ☞ *Asking for a TEI*
LAPD: Sapi 63 Tei 127 C
FC FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 11340
Msg_Type : ID REQUEST
Ai_Ind : 127

- From Network -
LAPD: Sapi 63 Tei 127 C
FE FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 11340
Msg_Type : ID ASSIGNED
Ai_Ind : 64

☞ *TEI has been assigned*

- From Network -
LAPD: Sapi 63 Tei 127 C
FE FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 0
Msg_Type : ID CHK REQUEST
Ai_Ind : 64

☞ *Checking the assigned TEI*

- From Terminal-
LAPD: Sapi 63 Tei 127 C
FC FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 61709
Msg_Type : ID CHK RESPONSE
Ai_Ind : 64

- From Network -
LAPD: Sapi 63 Tei 127 C
FE FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 0
Msg_Type : ID CHK REQUEST
Ai_Ind : 64

- From Terminal-
LAPD: Sapi 63 Tei 127 C
FC FF 03
Unnumbered - UI Tei Management Procedure
LM_Header : 0F
RI_Ind : 478
Msg_Type : ID CHK RESPONSE
Ai_Ind : 64

-- From ISDN --
ISDN: Layer 1 Deactivated.

-- From ISDN --
ISDN: Layer 1 Activation Request From Terminal.

-- From ISDN --
ISDN: Layer 1 Activated.

☞ *Physical level established*

```
- From Network -
LAPD: Sapi 63   Tei 127   C
                FE FF 03
        Unnumbered  - UI Tei Management Procedure
                LM_Header       : 0F
                RI_Ind          : 0
                Msg_Type        : ID CHK REQUEST
                Ai_Ind          : 127

- From Terminal-
LAPD: Sapi 63   Tei 127   C
                FC FF 03
        Unnumbered  - UI Tei Management Procedure
                LM_Header       : 0F
                RI_Ind          : 8127
                Msg_Type        : ID CHK RESPONSE
                Ai_Ind          : 64

- From Terminal-
LAPD: Sapi 63   Tei 127   C
                FC FF 03
        Unnumbered  - UI Tei Management Procedure
                LM_Header       : 0F
                RI_Ind          : 7088
                Msg_Type        : ID CHK RESPONSE
                Ai_Ind          : 3

- From Terminal-                                  ☞ Starting frame level establishment
LAPD: Sapi 0   Tei 64   C   P
                00 81 7F
        Unnumbered  - SABME

- From Network -                                  ☞ Frame level established
LAPD: Sapi 0   Tei 64   R   F
                00 81 73
        Unnumbered  - UA

- From Terminal-                                  ☞ Calling an SDP to access X.25
LAPD: Sapi 0   Tei 64   C   Nr0   Ns0                network from ISDN network
                00 81 00 00
        Information - INFO    Cref: 1   Pdes: 8
                08 01 01 05 04 02 88 90 A1 18 01 83 6D 03
                80 50 30 70 09 80 33 36 30 38 36 34 36 34
                7C 02 88 90 7D 02 C1 FF
Q931: SETUP                                      ☞ SDP number: 36 08 64 64
                BearerCap               :02 88 90
                Sending Complete        :
                Channel Id              :01 83
                Calling SubAddress      :03 80 50 30
                Called  Address         :09 80 33 36 30 38 36 34 36 34
                Low Layer Compat.       :02 88 90
                High Layer Compat.      :02 C1 FF
                ----------------------

- From Network -
LAPD: Sapi 0   Tei 64   R   Nr1
                00 81 01 02
        Supervisory - RR
```

- From Network -
LAPD: Sapi 0 Tei 64 C Nr1 Ns0
02 81 00 02
Information - INFO Cref: 1 Pdes: 8
08 01 81 02 18 01 89
Q931: CALL PROCEEDING
Channel Id :01 89

☞ *Call proceeding*

- From Terminal-
LAPD: Sapi 0 Tei 64 R Nr1
02 81 01 02
Supervisory - RR

- From Network -
LAPD: Sapi 0 Tei 64 C Nr1 Ns1
02 81 02 02
Information - INFO Cref: 1 Pdes: 8
08 01 81 07
Q931: CONNECT

☞ *Call connected*

- From Terminal-
LAPD: Sapi 0 Tei 64 R Nr2
02 81 01 04
Supervisory - RR

☞ *Data transfer into B-channel is now possible*

- From Terminal-
LAPD: Sapi 0 Tei 64 C Nr2 P
00 81 01 05
Supervisory - RR

- From Network -
LAPD: Sapi 0 Tei 64 R Nr1 F
00 81 01 03
Supervisory - RR

☞ *Layer 2 supervision*

- From Terminal-
LAPD: Sapi 0 Tei 64 C Nr2 P
00 81 01 05
Supervisory - RR

- From Network -
LAPD: Sapi 0 Tei 64 R Nr1 F
00 81 01 03
Supervisory - RR

- From Terminal-
LAPD: Sapi 0 Tei 64 C Nr2 Ns1
00 81 02 04
Information - INFO Cref: 1 Pdes: 8
08 01 01 45 08 02 80 90
Q931: DISCONNECT
Cause :02 80 90

☞ *Disconnect request from terminal*

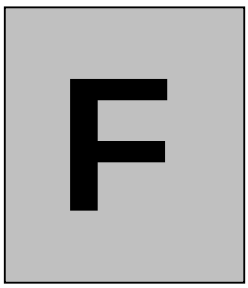
☞ *80: Coding standard=CCITT Location=User*

☞ *90: Normal event, normal clearing*

```
- From Network -
LAPD: Sapi 0   Tei 64   R   Nr2
                  00 81 01 04
          Supervisory - RR

- From Network -
LAPD: Sapi 0   Tei 64   C   Nr2   Ns2
                  02 81 04 04
          Information - INFO    Cref: 1   Pdes: 8
                  08 01 81 4D 08 02 87 90
Q931: RELEASE                                          ☞ 80: Coding standard=CCITT
                  Cause                  :02 87 90         Location=International network
                  ----------------------                ☞ 90: Normal event, normal clearing

- From Terminal-
LAPD: Sapi 0   Tei 64   R   Nr3
                  02 81 01 06
          Supervisory - RR

- From Terminal-                                       ☞ Release confirmed
LAPD: Sapi 0   Tei 64   C   Nr3   Ns2
                  00 81 04 06
          Information - INFO    Cref: 1   Pdes: 8
                  08 01 01 5A
Q931: RELEASE COMPLETE
                  ----------------------

- From Network -
LAPD: Sapi 0   Tei 64   R   Nr3
                  00 81 01 06
          Supervisory - RR

- From Network -                                       ☞ Disconnect level 2
LAPD: Sapi 0   Tei 64   C   P
                  02 81 53
          Unnumbered  - DISC

- From Terminal-
LAPD: Sapi 0   Tei 64   R   F
                  02 81 73
          Unnumbered  - UA

-- From ISDN --
ISDN: Layer 1 Deactivated.
```

APPENDIX F

Glossary



This glossary lists and defines technical terms used in this manual.

ACTLU

Activate Logical Unit. SNA command sent by the SSCP to an LU to activate a session and establish session parameters.

ACTPU

Activate Physical Unit. SNA command sent by the SSCP to activate a PU, so that any logical units controlled by this PU are available to the SNA network.

Active session

The session in which a user issues commands to be executed by the computer. An active session occupies the full screen.

Adapter

Circuit card added to a PC to perform a specialized function such as accessing a communication line.

Alert

A message sent to indicate an abnormal event or failure.

API

Application Programming Interface. The formally-defined programming language interface between an IBM system control program and the user of the program.

APPC

Advanced Program-to-Program Communications defines a session between an application program in a host computer and an application program in the same host or a different one.

ASCII

American Standard Code for Information Interchange. An 8-bit code developed by the American National Standard Institute for the exchange of information between communications devices. ASCII currently consists of 128 codes that represent the English alphabet, punctuation, and certain control characters, and an additional 128 codes called the extended character set that includes a number of European characters, graphics characters, and scientific characters.

Asynchronous

A transmission mode that uses start/stop bits to define a character and separate it from other characters.

Bits per second (bps)

This is how transmission speeds are measured. There are eight bits in a byte, so a transmission at 8000 bits per second means that the user is sending 1000 bytes (characters) per second.

BSC

Binary Synchronous Communication. A character-oriented, half-duplex data communications protocol. BSC is the older of IBM's two transmission modes and is currently being replaced by SNA/SDLC.

BTU

Basic Transmission Unit. A standard unit of information transmitted over an SNA network, it consists of the TH, the RH and the RU.

CCITT

The International Telegraph and Telephone Consultative Committee. An international body responsible for setting communications standards such as X.25.

CCN

Cluster Control Node.

CICS

Customer Information Control System. A mainframe database application.

Click

To quickly press and release a mouse button.

Client

A computer using services available through an SNA Server. While running applications such as a 3270 emulator, the client uses the SNA Server to access host or peer systems on the SNA network.

CMS

Conversational Monitor System. An interactive mainframe system that resides under the VM operating system.

Code Page

The technical term for a code set such as ANSI or EBCDIC.

Command

The control information sent from a primary station to another.

Controller

An intermediary device connecting terminals and other devices to the mainframe. It is also known as a Control Unit.

Control Unit

See *Controller*.

CPI-C

Common Programming Interface for Communications. An SAA-adherent API that allows peer-to-peer communications among programs in an SNA environment.

CSV

Common Service Verb. An application programming interface that provides ways of translating characters, tracing, and sending network management information to a host.

CTS

Clear to Send. It is activated by the modem as a reply to request to send, when the link is ready to transmit data. The PC will typically activate "data terminal ready" (DTR) when the communications software is loaded. When the connection to the remote modem has been made, the modem will usually return "data set ready" (DSR).

CUCN

CommUnication Controller Node. It is responsible for network management.

DACTLU

DeACTivate Logical Unit. An SNA command that is sent to deactivate the session between the SSCP and a LU.

DACTPU

DeACTivate Physical Unit. An SNA command that is sent to deactivate the session between the SSCP and a PU.

Data

Any representation such as characters or analog quantities to which meaning is, or might be, assigned.

Data Circuit

(1) ISO: A pair of associated transmit and receive channels that provide a means of two-way data communication. (2) In SNA, synonym for link connection.

Data Link

In SNA, the combination of the link connection and the link stations joining two adjacent network nodes.

DCE

Data Circuit Terminating Equipment. A device that sends to, and receives data from, the DCE on an X.25 network. When a user makes an X.25 connection using a PC, then the user is usually the DTE, and the system being called is the DCE.

Device

(1) A printer, terminal, control unit, front-end processor or any of the units or equipment that connect to a mainframe computer. (2) Any component that is part of a PC system, such as a mouse, keyboard, monitor, etc.

Dialup

Access to a switched network, usually through a dial telephone.

DLC

Data Link Control. A communications protocol used for PCs to exchange information with each other and with mainframe devices. It is frequently used over token-ring networks.

DLL

Dynamic Link Library. An operating-system mechanism that automatically links executable code to an application program.

DSR

Data-Set-Ready. It is activated by the modem (DCE) as a reply to "data terminal ready".

DTE

Data Terminal Equipment. A device that sends to, and receives data from, the DCE on an X.25 network.

DTR

Data-Terminal-Ready. It is activated by the terminal (DTE) when it is ready to communicate (terminal on).

EBCDIC

Extended Binary Coded Decimal Interchange Code. The standard code used to define characters on large IBM systems.

EBCDIC code page

A set of characters and values which define the mainframe's host characters for a particular language. There are separate EBCDIC code pages for all major languages.

EISA

Extended Industry Standard Architecture.

Extended Memory

In Intel 286 based computers and higher, memory above one megabyte.

FCS

Frame Check Sequence. It is used to control frame integrity information.

FEP

Front-End Processor. A device that relieves a host computer of processing tasks such as a message handling, code conversion, and error control (such as controllers, PCs, etc.)

Format 0 XID

A type of XID that supplies minimal information about the node. Format 0 XIDs have a fixed length. They can be used for 3270 and LUA communication and cannot be used for APPC.

Format 3 XID

A type of XID that supplies more detailed information about the node than a Format 0 XID. Format 3 XIDs have a variable length. They can be used for 3270 and LUA communications, and are the only type of XID that can be used for APPC.

Full Duplex

A communication mode in which the signal flows in both directions at the same time. This means that the user can transmit and receive data simultaneously.

Gateway

A device that provides a connection between dissimilar communications systems, such as between a LAN workstation and a mainframe.

Half Duplex

A communication mode in which the signal flows in both directions, but only one direction at a time.

HDLC

High level Data Link Control. This is a link layer protocol used to transmit information over a X.25 network.

HLLAPI

High-Level Applications Programming Interface. The PC or workstation, instead of the user, interacts with the mainframe application.

Host session

Interactive exchanges between the PC and the mainframe. It can be either a display or printer session.

IBM

International Business Machines.

IEEE

Institute of Electrical and Electronics Engineers. An organization that maintains the standards for the 802.2 protocol.

I-frame

Information frame. A standard unit of information transmitted over an SNA network. For 802.2 or SDLC communication, an I-frame is equivalent to a BTU.

IMS

Information Management System.

Interrupt

Suspending a process, such as execution of a computer program, that is triggered by an external event and performed in such a way that the process can be resumed.

IRQ

Interrupt request lines. Hardware lines over which devices send signals to get the attention of the processor when the device is ready to accept or send information.

ISA

Industry Standard Architecture.

ISO

International Standards Organization defining seven functional layers : physical, data link, network, transport, session, presentation and application.

LAN

Local Area Network, a data network connecting multiple PCs so they can share peripherals and data. Each PC on a LAN has a special adapter, and is connected to the other PCs on the LAN by cable, infrared, or radio links. A LAN has network protocol software to handle the flow of information. The most common types of network protocol software are Novell NetWare, Microsoft NetBIOS, etc.

LAPB

Link Access Protocol Balanced.

Leased Line

A leased connection to an X.25 network; the user does not need to dial the X.25 network to make a call.

LLC

Logical Link Control.

LU

Logical Unit. A port through which a user communicates with a mainframe system. LUs are used by the mainframe VTAM application to identify the peripheral devices connected to the mainframe.

LUA

Logical Unit Application. A conventional LU application or the interface that these applications use. LUA allows workstations to communicate with host applications using LU 0, 1, 2 or 3 protocols.

MAC

Media Access Control. The layer of the IEEE 802 standards that deals with network access and collision detection. In the IEEE standards, the MAC layer lies between the physical layer and the logical link control layer.

Modem

Modulator/demodulator. A device that allows transmission of data between computers over telephone lines.

NAU

Network Addressable Unit. It defines a device, a line or a program.

NCP

Network Control Program. An IBM program that supports communication controllers in single-domain, multiple-domain and interconnected networks.

Node

An endpoint of a link or a junction common to two or more links in a network. They can be host processors, communication controllers, cluster controllers or terminals.

NPSI

Network Packet Switched Interface. It provides translation and simulation functions for the terminal using the X.25 network.

NRZ

Non return to Zero. Data encoding method used for sending information across communications lines. The opposite of NRZI.

NRZI

Non return to Zero Inverted. Data encoding method used for sending information across communications line. The opposite of NRZ.

Packet

A transmission unit of fixed maximum size, used as the basic unit on a packet-switched network. A packet contains both a header and data.

Protocol

A system of rules and regulations to control data flow. A protocol ensures that all the data sent arrive at the correct destination intact.

PSDN

Packet-Switched Data Network. The protocol used on packet-switching networks is X.25.

PU

Physical Unit. A network-addressable unit that provides the services needed to use and manage a particular device, such as a communications link device. A PU is implemented with a combination of hardware, software and microcode.

PVC

Permanent Virtual Circuit. A type of circuit used by an X.25 connection, where the circuit is constantly active, and the destination address is preset.

QLLC

Qualified Logical Link Control. A protocol used to have SNA sessions on X.25 networks.

RH

Request/Response Header.

RU

Request/Response Unit. In SNA, a message that controls the session, data flow and function management aspects of the SNA protocol.

RUI

Request Unit Interface. A basic interface that allows programs to acquire and release control of conventional LUs. The RUI also reads and writes Request/Response Headers (RHs), transmission headers (THs) and request unit (RU) data.

SAA™

Systems Application Architecture. Guidelines created by IBM to help developers standardize applications so they can operate in different environments with minimal modifications to programs.

SAP

Service Access Point.

SDLC

Synchronous Data Link Control. A type of link service used to manage synchronous data transfer over standard telephone lines (switched lines) or leased lines.

SDP

Access to Public Switched Data Network using the B-channel.
This access refers to the X.31 Case A recommendation. See also *X.31*.

SID

Security Identifier. It is required to gain access to an invoked program when using security.

SLI

Session Level Interface. A higher-level interface that facilitates the opening and closing of SNA sessions with host LU 0, LU 1, LU 2, and LU 3 application programs. In an SLI, application programs can control data traffic at a logical message level.

SNA

System Network Architecture. A collection of rules that brings uniformity to communications systems and the ways they interact. These rules define various functions that allow data to be transferred from one computer to another, in a form that is usable by the receiving computer.

SON

Session Outage Notification.

SSCP

System Service Control Point. (1) A host-system network component that provides network services for dependent nodes. (2) An SNA network component that helps control and maintain communication flow between PUs and LUs on the network. Multiple SSCPs may work together in order to coordinate communications.

SVC

Switched Virtual Circuit. A type of circuit used by an X.25 connection, where the circuit is not constantly active, but is called and cleared dynamically. The destination address is supplied when the circuit is called.

TCAM

TeleCommunication Access Method.

TH

Transmit Header.

TP

Transaction Program. An application program that uses APPC to exchange data with another TP on a peer-to-peer basis.

TSO

Time Sharing Option. Option providing for interactive time sharing from remote terminals.

VM

Virtual Machine.

VM/CMS

Virtual Machine/Conversational Monitor System.

VTAM

Virtual Telecommunications Access Method. A set of IBM mainframe programs that control communications between mainframe applications and the terminals and computers that connect to the mainframe.

WAN

Wide Area Network. A high-speed communications system, consisting of hardware (computers and peripherals) and software (programs and files), that provides communications services and allows resources to be shared over a larger geographic area than that served by a LAN.

X.25

The CCITT standard used for communication over a packet-switching network. X.25 uses the QLLC protocol.

X.31

The CCITT standard used to support packet mode terminal equipment by ISDN. Two main services are defined:

- Case A: access to PSDN (via a synchronous dial-in port)
- Case B: use of an ISDN virtual circuit (X.25 on D-channel)

XID

Exchange Identification. An identifier that is exchanged between nodes on an SNA network, so the nodes can recognize each other and establish link and node characteristics for communicating. See also *Format 0 XID and Format 3 XID*.

3270

The information display system for IBM hosts (mainframes); the system includes terminals, printers and controllers with which the user can access host functions.

3270 terminal emulation

The running of software so that a PC acts as a 3270 terminal, displaying information from a host system (mainframe). Emulation software can also allow a PC to send print jobs from a host system to a printer connected to the PC.

5250 terminal emulation

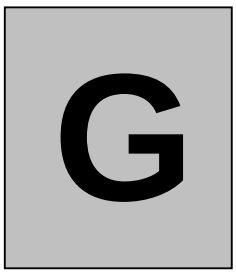
The running of software so that a PC acts as a 5250 terminal, interacting with an AS/400 system.

802.2

The logical link control protocol used for communications over a token-ring or Ethernet network. The 802.2 protocol is an IEEE standard.

APPENDIX G

Customer Services



This appendix explains how to gather information in order to contact the Technical Support Service.

TECHNICAL SUPPORT INFORMATION FORM

Company :

Name :

Address :

Phone Number :

Fax Number :

Country :

Cirel

Date :

Time :

FPX PRODUCT INFORMATION	FPX CONFIGURATION
Product(s) Name(s) :	**Type :**
	IRQ :
	I/O :
Product(s) Version(s) :	**DPM :**
	Interface Type (V28, V35, V11,...) **:**
	External Modem : Yes ☐ No ☐
	Modem Type :
PC CONFIGURATION	**PRODUCT CONFIGURATION**
Make & Model :	**OS :**
Processor :	**Version :**
RAM Memory :	**LAN Protocol** (Netbeui, IP,...) **:**
LAN Adapter :	**WAN Protocol** (QLLC, SDLC, PPP,...) **:**
Specific Adapter :	**Connection Type** (X25, ISDN, LL,...) **:**
Display Type :	**First Setup ☐ or Upgrade ☐**
Bus Type :	**Host Computer :**

Problem Description :

Comments & Suggestions :