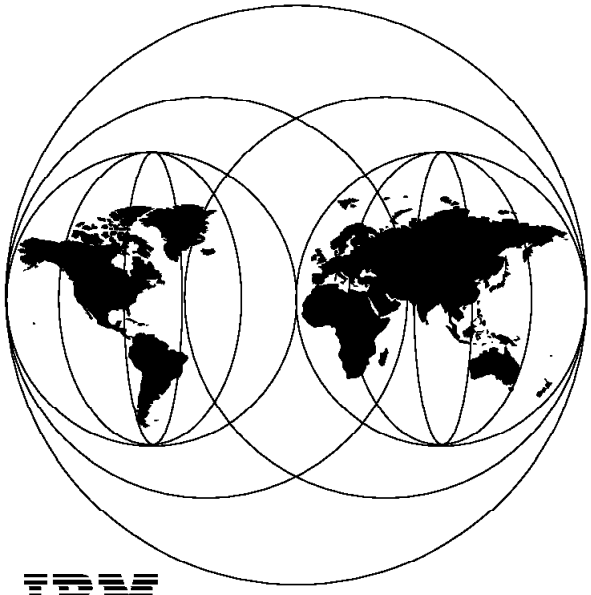
SG24-2111-00

Exploring the IBM eNetwork Communications Suite

August 1997



IBM
International Technical Support Organization
Raleigh Center

SG24-2111-00

International Technical Support Organization

Exploring the IBM eNetwork Communications Suite

August 1997

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix B, “Special Notices” on page 297.

First Edition (August 1997)

This edition applies to Version 1.0 of the IBM eNetwork Communications Suite, Program Number 5801-AAR, Feature Number 2345, Part Number 39F1693, for use with the Windows NT, Windows 95 and Windows 3.x Operating Systems.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 678
P.O. Box 12195
Research Triangle Park, NC 27709-2195

Contents

Preface

The IBM eNetwork Communications Suite combines the power of several successful communication software packages to provide access to corporate mainframe systems, application and mail servers, and also the Internet. This redbook helps you understand the concept and the components of the eNetwork Communications Suite and assists you in planning for a roll-out of, or a migration to this product.

This redbook covers the installation, integration and corporate usage of the IBM eNetwork Communications Suite. In particular, new features of the FTP Software TCP/IP protocol stack and FTP Software TCP/IP applications are discussed, such as IP security and IP Version 6 support. Those and other new features and functions are covered in detailed sections, explaining their use and the overall design.

Finally, the use of the other components of the suite - Netscape Navigator, Personal Communications for Windows, Lotus Notes Mail Client - in conjunction with the new TCP/IP stack is presented in case studies.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the Systems Management and Networking ITSO Center, Raleigh. The leader of this project was Martin Murhammer.

Martin Murhammer is a Senior Information Technology Availability Professional at the ITSO Raleigh Center. Before joining ITSO in 1997, he was a Systems Engineer in the Systems Service Center at IBM Austria. He has 12 years of experience in the personal computing environment including areas such as heterogeneous connectivity, server design, system recovery, and Internet solutions. He is a Certified OS/2 Engineer and a Certified LAN Server Engineer and has previously coauthored six redbooks during residencies at the ITSO Raleigh and Austin Centers.

Tamas Gaidosch is a System Engineer in IBM Hungary, specializing in networking software solutions. He has four years of experience in networked computing environments and system administration. He holds a degree in Computer Science. His areas of expertise include operating systems (OS/2 LAN Server, Windows, AIX), networks (TCP/IP, X.25) and self-service banking software.

Jason Meaden is a Software Support Specialist in IBM Australia. He specializes in TCP/IP, VisualAge and Operating System support. Prior to

working for IBM he owned a small consulting business called Tiara Information Services in Perth, Western Australia. It specialized in online services, information resource technology and OS/2 support. He has over seven years of experience in Internet and other online services.

Thanks to the following people for their invaluable contributions to this project:

Julian Over, Karl Wozabal, Mick Lugton, Barry Nusbaum, Gail Wojton
Systems Management and Networking ITSO Center, Raleigh

Fiona Collins
International Technical Support Organization, Cambridge Center

John Connor, Gerald Young, Karen Tracey, Jim Duncan, Lou Shannon
IBM Research Triangle Park

Steve Wise
IBM Austin

Shishir Belbase
FTP Software, Inc.

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 313 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

  For Internet users `http://www.redbooks.ibm.com`
  For IBM Intranet users `http://w3.itso.ibm.com`

- Send us a note at the following address:

  `redbook@vnet.ibm.com`

Chapter 1. A Short Introduction to TCP/IP and the Internet

Many excellent publications have been written on the topic of TCP/IP and the Internet. The aim of this chapter therefore is to provide only a short overview for the benefit of those readers who may not be familiar with the topic or who may desire a quick refresh.

We have included a selection of publications on advanced TCP/IP and Internet topics for your reference in Appendix C, “Related Publications” on page 301.

1.1 Why TCP/IP?

The need to interconnect networks that use different protocols was recognized early in the 1970s during a period when the use and development of networking technology was increasing. The rapid growth in networking over the past three decades has allowed users greater access to resources and information as well as causing significant problems when merging, or interconnecting, different types of networks. Open protocols and common applications were required, leading to the development of a protocol suite known as *Transmission Control Protocol/Internet Protocol* (TCP/IP) which originated with the U.S. Department of Defense (DoD) in the mid-1960s and took its current form around 1978.

An interesting article about the history of the Internet can be found at the following URL:

`http://www.isoc.org/internet-history/`

1.2 The Growth of TCP/IP

In the early 1980s TCP/IP became the backbone protocol in multivendor networks such as ARPANET, NFSNET and regional networks. The protocol suite was integrated into the University of California at Berkeley′s UNIX operating system and became available to the public for a nominal fee. From this point on TCP/IP has become widely used due to its inexpensive availability in UNIX and its spread to other operating systems, resulting in increasing use in both local area network (LAN) and wide area network (WAN) environments.

Today, TCP/IP provides the ability for corporations to merge differing physical networks while giving users a common suite of functions. It allows interoperability between equipment supplied by multiple vendors on multiple platforms, and it provides access to the Internet. In fact, the Internet, which

has become the largest computer network in the world, is based on the TCP/IP protocol suite.

The Internet consists of large international, national and regional backbone networks, that allow local and campus networks and individuals access to global resources. Use of the Internet has grown rapidly over the last few years, as illustrated in Table 1.

Table 1. Internet Growth. The source of these figures can be found at the following URLs:

`http://info.isoc.org/guest/zakon/Internet/History/HIT.html#Growth`
`http://www.nw.com/zone/WWW/dist-bynum.html`

Date	Hosts	Networks	Domains
July 1989	130,000	650	3,900
July 1992	992,000	6,569	16,300
July 1993	1,776,000	13,767	26,000
July 1995	6,642,000	61,538	120,000
July 1996	12,881,000	134,365	488,000
January 1997	16,146,000	n/a	828,000

As opposed to the Internet, the term *Intranet* has evolved recently to describe TCP/IP networks that are entirely under the control of a private authority or company. Those Intranets may or may not have connections to other independent Intranets (which would then be referred to as *extranets*) or the Internet. They may or may not be fully or partially visible to the outside depending on the implementation.

So why has the use of TCP/IP grown at such a rate? The reasons include the availability of common application functions across differing platforms and the ability to access the Internet, but the primary reason is that of interoperability. The open standards of TCP/IP allow corporations to interconnect or merge different platforms. An example is the simple case of allowing file transfer capability between an MVS/ESA host and, perhaps, a Hewlett Packard workstation.

TCP/IP also provides for the routing of multiple protocols from and to diverse networks. For example, a requirement to connect isolated networks using IPX, AppleTalk and TCP/IP protocols using a single physical connection can be accomplished by using routers utilizing TCP/IP protocols.

One further reason for the growth of TCP/IP is the popularity of the socket programming interface, which is the programming interface between the

TCP/IP transport protocol layer and TCP/IP applications. A large number of applications today have been written for the TCP/IP socket interface.

1.3 Internet Standards and Request for Comments (RFC)

We mentioned in the previous section that the Internet is a large multinational, multivendor, multiplatform network. That might give reason to ask some questions, such as:

- Are there any standards for such a diverse network?
- Who establishes and reviews them?
- Who assigns network addresses?
- Who manages the Internet?

The Internet Activities Board (IAB) is the non-profit, coordinating committee for Internet design, engineering and management. The IAB members are committed to making the Internet function effectively and evolve to meet a large-scale, high-speed future. The IAB sets the Internet standards and manages the Request For Comments (RFC) publication process.

RFC is the mechanism through which the Internet protocol suite has been evolving. For example, an Internet protocol can have one of six states: standard, draft standard, proposed standard, experimental, informational and historic. In addition, an Internet protocol has one of five statuses: required, recommended, elective, limited use and not recommended. By communicating using the RFC, new protocols are being designed and implemented by researchers from both academic institutions and commercial corporations. At the same time, some old protocols are being superseded by new ones.

The RFC standards are described in the ″Internet Official Protocol Standards″ RFC, currently RFC 2000.

The task of coordinating the assignment of values to the parameters of protocols is delegated by the Internet Architecture Board (IAB) to the Internet Assigned Numbers Authority (IANA). These protocol parameters include op-codes, type fields, terminal types, system names, object identifiers, and so on. The ″Assigned Numbers″ RFC, currently RFC 1700, documents these protocol parameters.

To obtain registered IP addresses (see 1.5.1.1, “IP Addressing” on page 6) and domain names (see 1.7.5, “Domain Name System (DNS)” on page 23), you need to contact the Internet Network Information Center (InterNIC), the administrative body for the Internet.

Registration is available online at the NIC Web site using the following URL:

http://rs.internic.net/about-rs.html

1.4 TCP/IP Architecture

TCP/IP, as a set of communications protocols, is based on layers. Unlike SNA or OSI that distinguish seven layers of communication, there are only four layers in the TCP/IP model. They enable heterogeneous systems to communicate by performing network-related processing such as message routing, network control, error detection and correction.

The layering model of TCP/IP is shown in Figure 1, with an explanation of each layer following thereafter:

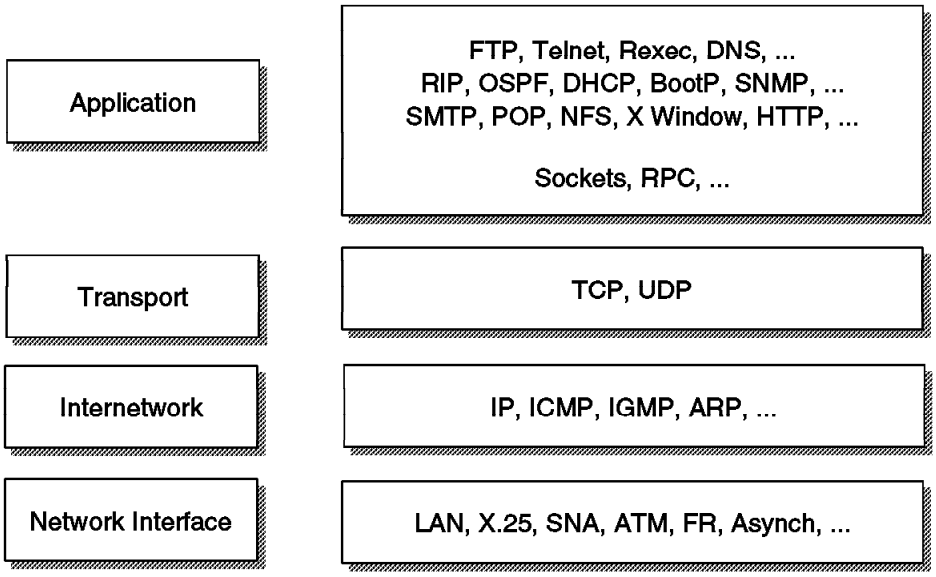


Figure 1. TCP/IP - Architecture Model: Layers and Protocols

Application Layer

The application layer is provided by the program that uses TCP/IP for communication. Examples of applications are Telnet, FTP, e-mail, Gopher and SMTP. The interface between the application and transport layers is defined by port numbers and sockets and is described in more detail in 1.6.1, “Ports and Sockets” on page 17.

Transport Layer

The transport layer provides communication between application programs. The applications may be on the same host or on different

hosts. Multiple applications can be supported simultaneously. The transport layer is responsible for providing a reliable exchange of information. The main transport layer protocol is TCP. Another is the User Datagram Protocol (UDP), which provides a connectionless service in comparison to TCP, which provides a connection-oriented service. That means that applications using UDP as the transport protocol have to provide their own end-to-end flow control. Usually, UDP is used by applications that need a fast transport mechanism.

Internet Layer

The Internet layer provides communication between computers. Part of communicating messages between computers is a routing function that ensures that messages will be correctly delivered to their destination. The Internet Protocol (IP) provides this routing function. Examples of Internet layer protocols are IP, ICMP, IGMP, ARP and RARP.

Network Interface Layer

The network interface layer, sometimes also referred to as the link layer, data link layer or network layer, is implemented by the physical network that connects the computers. Examples are LAN (IEEE 802.x standards), Ethernet, X.25, ISDN, ATM, frame relay, or asynch.

Note that the RFCs actually do not describe or standardize any network layer protocols per se, they only standardize ways of accessing those protocols from the Internet layer.

1.5 TCP/IP Internet Layer Protocols

This section provides a short overview of the most important and common protocols of the TCP/IP Internet layer.

1.5.1 Internet Protocol (IP)

IP is the layer that hides the underlying physical network from the upper-layer protocols. It is an unreliable, best-effort and connectionless packet delivery protocol. Note that best-effort means that the packets sent by IP may be lost, out of order, or even duplicated, but IP will not handle these situations. It is up to the higher-layer protocols to deal with these situations.

One of the reasons for using a connectionless network protocol was to minimize the dependency on specific computing centers that used hierarchical connection-oriented networks. The DoD intended to deploy a network that would still be operational if parts of the country were destroyed. During earthquakes, this has been proved to be true for the Internet.

1.5.1.1 IP Addressing

IP uses IP addresses to specify source and target hosts on the Internet. (For example, we can contrast an IP address in TCP/IP with a fully qualified NETID.LUNAME in SNA.) An IP address consists of 32 bits, which is usually represented in the form of four decimal numbers, one decimal number for each byte (or octet). For example:

```
00001001 01000011 00100110 00000001        a 32-bit address
    9       67       38       1            decimal notation (9.67.38.1)
```

An IP address consists of two logical parts: a network address and a host address. An IP address belongs to one of four classes depending on the value of its first four bits. This is shown in Figure 2.

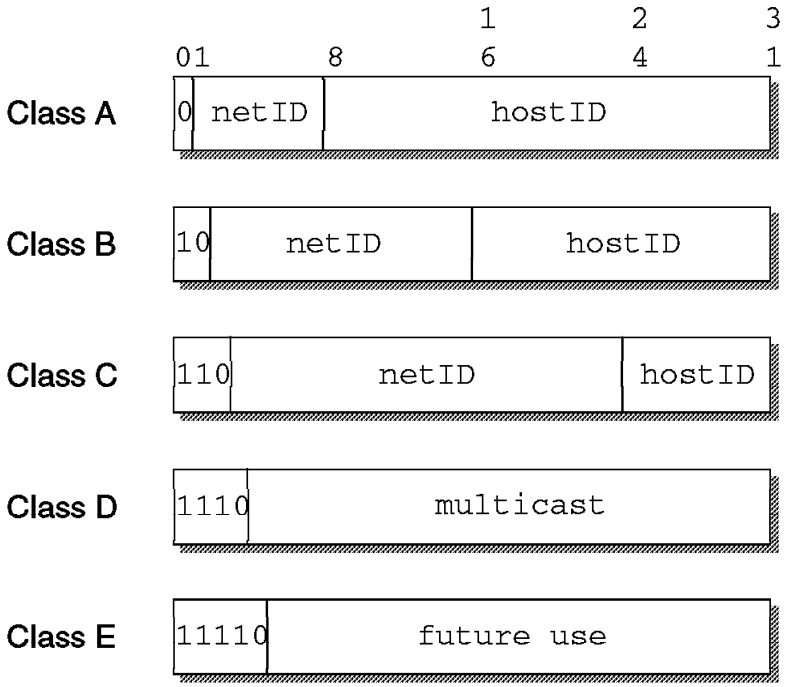


Figure 2. IP - Assigned Classes of IP Addresses

The following address space is defined for IP:

- Class A addresses use 7 bits for the <network> and 24 bits for the <host> portion of the IP address. That allows for 126 (2**7-2) networks with 16777214 (2**24-2) hosts each; a total of over 2 billion addresses.
- Class B addresses use 14 bits for the <network> and 16 bits for the <host> portion of the IP address. That allows for 16382 (2**14)

networks with 65534 (2**16-2) hosts each; a total of over 1 billion addresses.

- Class C addresses use 21 bits for the <network> and 8 bits for the <host> portion of the IP address. That allows for 2097150 (2**21) networks with 254 (2**8-2) hosts each; a total of over half a billion addresses.
- Class D addresses are reserved for multicasting (a sort of broadcasting, but in a limited area, and only to hosts using the same class D address).
- Class E addresses are reserved for future use.

Some values for these host IDs and network IDs are pre-assigned and cannot be used for actual network or host addressing:

all bits 0 Stands for *this*: this host (IP address with <host address>=0) or this network (IP address with <network address>=0). When a host wants to communicate over a network, but does not yet know the network IP address, it may send packets with <network address>=0. Other hosts on the network will interpret the address as meaning *this network*. Their reply will contain the fully qualified network address, which the sender will record for future use.

all bits 1 stands for *all*: all networks or all hosts. For example:

128.2.255.255

means all hosts on network 128.2 (class B address).

This is called a directed broadcast address because it contains both a valid <network address> and a broadcast <host address>.

Loopback The class A network 127.0.0.0 is defined as the loopback network. Addresses from that network are assigned to interfaces that process data inside the local system and never access a physical network (loopback interfaces).

1.5.1.2 IP Subnets

Due to the explosive growth of the Internet, the principle of assigned IP addresses became too inflexible to allow easy changes to local network configurations. Those changes might occur when:

- A new type of physical network is installed at a location.
- Growth of the number of hosts requires splitting the local network into two or more separate networks.
- Growing distances require splitting a network into smaller networks, with gateways between them.

To avoid having to request additional IP network addresses in these cases, the concept of subnets was introduced. The assignment of subnets can be done locally, as the whole network still appears to be one IP network to the outside world.

Recall that an IP address consists of the pair <network address><host address>. For example, let us take a class A network; the address format is shown in Figure 3:

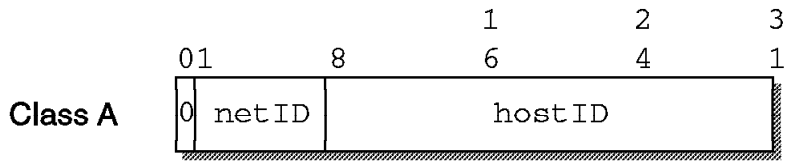


Figure 3. IP - Class A Address without Subnets

Let us use the following IP address:

```
00001001 01000011 00100110 00000001        a 32-bit address
   9       67       38       1             decimal notation (9.67.38.1)

         9.67.38.1          is an IP address  (class A)  having

         9                  as the <network address>
           67.38.1          as the <host address>
```

Subnets are an extension of this by considering a part of the <host address> to be a subnetwork address. IP addresses are then interpreted as <network address><subnetwork address><host address>.

For example, we may wish to choose the bits from 8 to 25 of a class A IP address to indicate the subnet addresses, and the bits from 26 to 31 to indicate the actual host addresses. Figure 4 shows the subnetted address that has been derived from the original class A address:

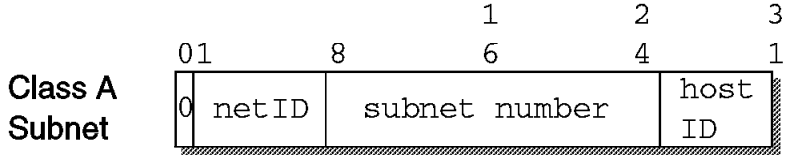


Figure 4. IP - Class A Address with Subnet Mask and Subnet Address

We normally use a bit mask, known as the subnet mask, to identify which bits of the original host address field indicate the subnet number. In the above example, the subnet mask is 255.255.255.192 in decimal notation (or 11111111 11111111 11111111 11000000 in bit notation). Note that, by convention, the <network address> is masked as well.

For each of these subnet values, only (2**18)-2 addresses (from 1 to 262143) are valid because of the all bits 0 and all bits 1 number restrictions. This split will therefore give 262142 subnets each with a maximum of (2**6)-2 or 62 hosts.

You will notice that the value applied to the subnet number takes the value of the full byte with non-significant bits being set to zero. For example, the hexadecimal value 01 in this subnet mask assumes an 8-bit value 01000000 and gives a subnet value of 64 and not 1 as it might seem.

Applying this mask to our sample class A address 9.67.38.1 would break the address down as follows:

```
 00001001 01000011 00100110 00000001 = 9.67.38.1 (class A address)
 11111111 11111111 11111111 11------   255.255.255.192 (subnet mask)
===================================  logical_AND
 00001001 01000011 00100110 00------ = 9.67.38  (subnet base address)
```

This leaves a host address of:

```
-------- -------- -------- --000001 = 1        (host address)
```

IP will recognize all host addresses as being on the local network for which the logical_AND operation described above produces the same result. This is important for routing IP datagrams in subnet environments (see 1.5.1.4, “IP Routing” on page 10).

Note that the actual subnet number would be:

```
-------- 01000011 00100110 00------ = 68760    (subnet number)
```

You will notice that the subnet number shown above is a relative number, that is, it is the 68760th subnet of network 9 with the given subnet mask. This number bears no resemblance to the actual IP address that this host has been assigned (9.67.38.1) and has no meaning in terms of IP routing.

The division of the original <host address> part into <subnet> and <host> parts can be chosen freely by the local administrator; except that the values of all zeroes and all ones in the <subnet> field are reserved for special addresses.

Note: Because the range of available IP addresses is decreasing rapidly, many routers support the use of all zeroes and all ones in the <subnet> field, though this is not coherent with the standards.

1.5.1.3 IP Datagram

The unit of transfer of a data packet in TCP/IP is called an IP datagram. It is made up of a header containing information for IP and data that is only relevant to the higher level protocols. IP can handle fragmentation and re-assembly of IP datagrams. The maximum length of an IP datagram is 65,535 bytes (or octets). There is also a requirement for all TCP/IP hosts to support IP datagrams of size up to 576 bytes without fragmentation.

The IP datagram header is a minimum of 20 bytes long:

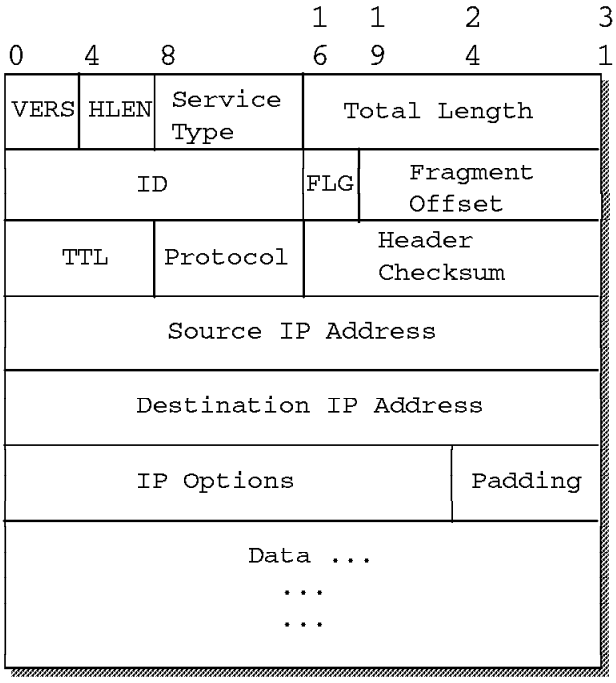


Figure 5. IP - Format of an IP Datagram Header

We do not elaborate on the format of the IP datagram header. You can find this information in the listed publications.

1.5.1.4 IP Routing

There are two types of IP routing: direct and indirect.

Direct Routing: If the destination host is attached to a physical network to which the source host is also attached, an IP datagram can be sent directly, simply by encapsulating the IP datagram in the physical network frame. This is called direct delivery and is referred to as direct routing.

Indirect Routing: Indirect routing occurs when the destination host is not on a network directly attached to the source host. The only way to reach the destination is via one or more IP gateways. (Note that in TCP/IP terminology, the terms gateway and router are used interchangibly for a system that actually performs the duties of a router.) The address of the first of these gateways (the first hop) is called an indirect route in the context of the IP routing algorithm. The address of the first gateway is the only information needed by the source host.

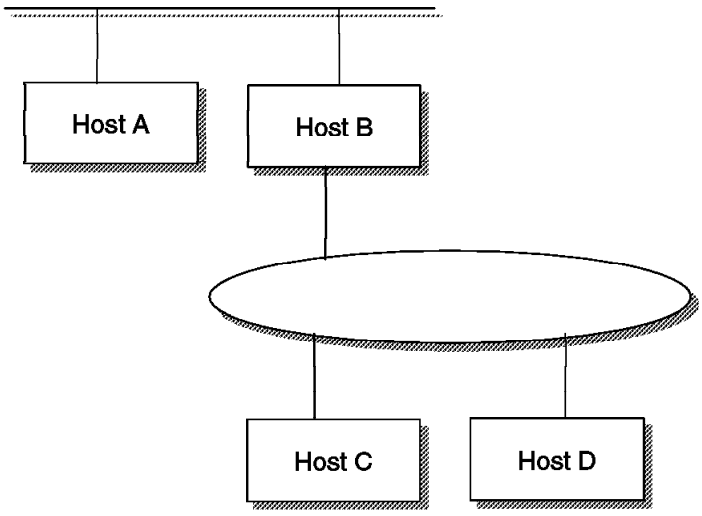


Figure 6. IP - Direct and Indirect Routes. (Host C has a direct route to hosts B and D, and an indirect route to host A via gateway B.)

IP Routing Table: The determination of available direct routes is derived from the list of local interfaces available to IP and is composed by IP automatically at initialization. A list of networks and associated gateways (indirect routes) needs to be configured to be used with IP routing if required. Each host keeps the set of mappings between the following:

- Destination IP network address(es)
- Route(s) to next gateway(s)

These are stored in a table called the IP routing table. Three types of mappings can be found in this table:

1. The direct routes, for locally attached networks
2. The indirect routes, for networks reachable via one or more gateways
3. The default route, which contains the (direct) route to be used in case the destination IP network is not found in the mappings of type 1 and 2 above

See the network in Figure 7 for an example configuration.

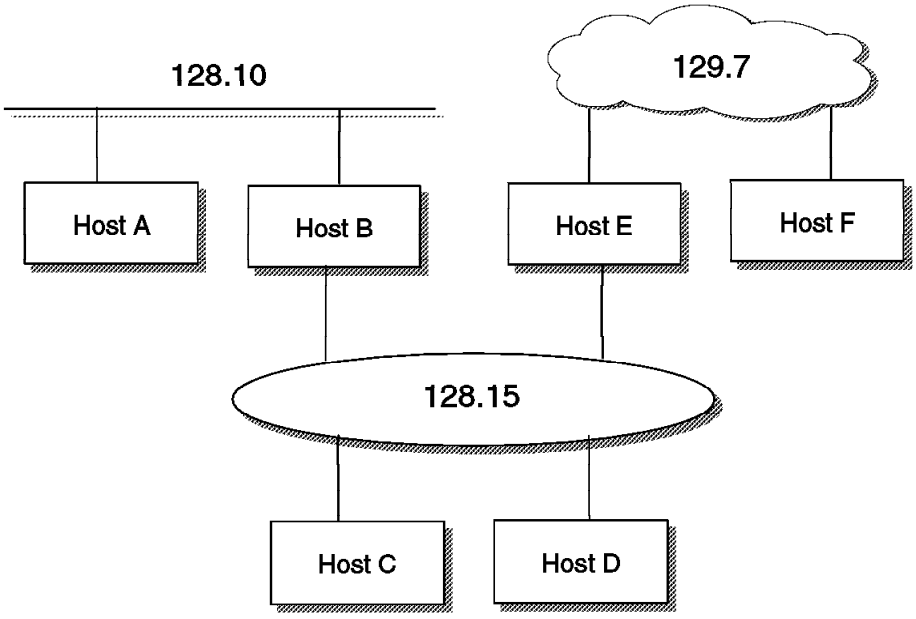


Figure 7. IP - Routing Table Scenario

The routing table of host D might contain the following (symbolic) entries:

```
destination      router    interface

    129.7.0.0    E         lan0
    128.15.0.0   D         lan0
    128.10.0.0   B         lan0
    default      B         lan0
    127.0.0.1    loopback  lo
```

The routing table of host F might contain the following (symbolic) entries:

```
destination      router    interface

    129.7.0.0    F         wan0
    default      E         wan0
    127.0.0.1    loopback  lo
```

IP Routing Algorithm: IP uses a unique algorithm to route an IP datagram. It is called the IP routing algorithm which is illustrated in the figure below, including support of subnets:

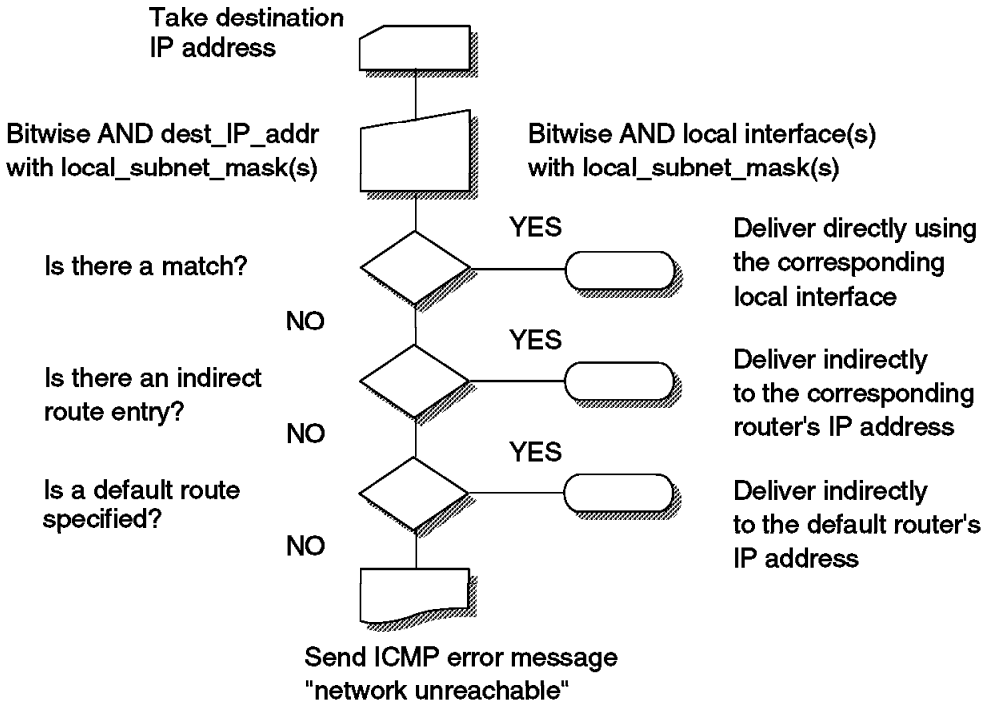


Figure 8. IP - Routing Algorithm (with Subnets)

Notes:

1. This is an iterative process. It is applied by every host handling a datagram, except for the host to which the datagram is finally delivered.
2. Routing tables and the routing algorithm are local to any host in an IP network. In order to be able to forward IP datagrams on behalf of other hosts, routers need to exchange their routing table information with

other routers in the network. This is done using special routing protocols, some of which are discussed in 1.9, “TCP/IP Routing Protocols and Techniques” on page 30.

1.5.2 The Future Version of IP (IPv6)

It has been mentioned in 1.5.1.1, “IP Addressing” on page 6 that the address space of the current version of IP, IP Version 4 or IPv4 allows for almost four billions of valid addresses. One might think that this should be sufficient to cope with the growth of many more years. The truth is that, due to the impacts of growth as well as the restrictions of subnetting, the IP address space will be nearing exhaustion by the year 2005, or so.

Apart from the problem of running out of IP addresses, there are other requirements that should be met by the next generation of IP:

- Allow encapsulation of its own or other protocols
- Incorporate class of service to distinguish between different types of traffic
- Provide for enhanced multicasting capabilities
- Provide for authentication and encryption
- Provide a mechanism for autoconfiguration
- Preserve the virtues of IPv4, such as globally unique addressing, datagram service, independence from physical network characteristics, flexible topology, free available standards
- Provide for transition from IPv4
- Be compatible with IPv4

That has led to the initiative of defining a new version of IP which is now named IP Version 6 or IPv6 but has gone by the name of IPng (next generation IP) for some time. The specifications of IPv6 and associated protocols and issues can be found in RFCs 1883 to 1886.

IPv6 uses 128-bit addresses instead of the 32-bit addresses of IPv4 which provides a large enough address space. It also fulfills the other requirements as listed above.

IPv6 is just facing its initial implementations in commercially available TCP/IP products, but there are no IPv6 networks available to the general public yet. Internet providers are, however, expected to open IPv6 networks in the 1998 timeframe.

For a more detailed discussion of IPv6 within this redbook, please refer to 4.2, “Implementing and Using IPv6” on page 147. More information about IPv6 networks can be found at the following URLs:

```
http://playground.sun.com/ipng/
http://www-6bone.lbl.gov/6bone/
```

1.5.3 Internet Control Message Protocol (ICMP)

Although ICMP is shown in Figure 2 on page 6 as being in the same protocol layer as IP, it is actually an integral part of IP. ICMP is occasionally used for reporting some errors in datagram delivery.

Perhaps one of the most useful commands available on all TCP/IP implementations is the Packet INternet Groper (PING) application. PING uses ICMP to send an Echo datagram to a specified IP address and wait for it to return. This is very useful for debugging purposes and also for knowing if a remote host can be reached from the local host.

1.5.4 Interfacing with the Network Layer

Though the network interface layer itself is not covered by the TCP/IP standards, the RFCs do specify certain methods to access that layer from the higher layers. Before we describe some of the protocols that interface with the network layer, we need to distinguish between different types of networks that the Internet layer can be connected with:

Multiaccess broadcast networks

In a network of this type, any system (TCP/IP host) can have multiple connections to other hosts simultaneously, and it can also send information to all other hosts on the same network with a single, special kind of message (broadcast). Local area networks (LANs) typically represent this type of network. Protocols such as ARP, ProxyARP, RARP, BootP and DHCP are used with this type of network. We will briefly describe some of them in this and following sections.

Multiaccess non-broadcast networks

In a network of this type, any host can have multiple connections to other hosts simultaneously but there are no broadcast mechanisms in place. Examples of this type of network are X.25, Frame Relay and AnyNet Sockets over SNA.

Point-to-point networks

In a network of this type, a host can only have one connection to one other host at any time, and there are no broadcast mechanisms in place. Examples of this type of network are SNAlink and asynchronous connections (using SLIP or PPP which are briefly described in this section).

Notes:

1. The term *connection* in the three paragraphs before applies to any single IP interface of a host in any of the network types mentioned. For instance, a host could have multiple point-to-point interfaces and thus more than one connection at a time, but still only one per interface.
2. Some publications only distinguish between broadcast and non-broadcast networks.

1.5.4.1 Hardware Address Resolution (ARP and RARP)

The Address Resolution Protocol (ARP) maps Internet addresses to hardware addresses. When an application attempts to send data over a TCP/IP network capable of broadcasting, IP requests the appropriate hardware address mapping using ARP. If the mapping is not in the mapping table (ARP cache), an ARP broadcast packet is sent to all the hosts on the network requesting the physical hardware address for the host. For more information about ARP, see RFC 826.

An exception to the rule constitutes the Asynchronous Transfer Mode (ATM) technology where ARP cannot be implemented in the physical layer as described above. Therefore, an ARP server is used with which every host has to register upon initialization in order to be able to resolve IP addresses to hardware addresses.

Some network hosts do not know their IP addresses when they are initialized. This can especially be true in the case of a host needing to be booted from diskette. Reverse ARP (RARP) can be used by, for example, a diskless workstation to determine its own IP address. In this case the workstation would already know its hardware address (discovered at initialization) and would broadcast a request to a RARP server to map the addresses. It is necessary to have a RARP server in your network in order to implement RARP.

1.5.4.2 Serial Line Interface Protocol (SLIP)

The Serial Line Internet Protocol (SLIP) allows you to set up a point-to-point connection between two TCP/IP hosts over a serial line, for example, a serial cable or an RS-232 connection into a modem and over a telephone line. You can use SLIP to access a remote TCP/IP network (such as a service provider′s network) from your local host or to route datagrams between two TCP/IP networks. For more information about SLIP, see RFC 1055.

SLIP has several deficiencies, such as:

- Only being able to transport IP datagrams. (It can not be used to route other protocols.)
- Having no ability to determine the address of the host at the other end of the connection. (Both hosts must know each other's addresses.)
- Having no error correction or data compression facility, therefore being unreliable across noisy and low speed lines.

SLIP is not an Internet standard, but it is in widespread use. Due to the fact that most implementations incorporate SLIP and that for many applications the issues listed above are not important, it is a good choice for remote connection (or dial-in access). However, for use between hosts across a dynamic environment such as a large WAN, the problems are a major consideration and make SLIP an inadequate protocol to link routers.

1.5.4.3 Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) is an Internet standard that has been developed to overcome the problems associated with SLIP. PPP allows addresses to be negotiated across a connection instead of being statically defined; this is not broadcasting because the negotiation is limited to a single link rather than to all hosts. PPP implements reliable delivery of datagrams over both synchronous and asynchronous serial lines. It also allows compression to be negotiated and can be used to route a wide variety of network protocols. For more information about PPP, see RFCs 1717 and 1661.

Note: Do not confuse the terms point-to-point connection and Point-to-Point Protocol (PPP). A point-to-point connection is a link between two specific interfaces, while PPP is a protocol used to communicate over the link.

1.6 TCP/IP Transport Layer Protocols and Interfaces

This section provides a brief overview of the protocols of the TCP/IP transport layer.

1.6.1 Ports and Sockets

Each process that wants to communicate with another process identifies itself to the TCP/IP protocol suite by one or more ports. A port is a 16-bit number, used by the host-to-host protocol to identify to which higher-level protocol or application program (process) it must deliver incoming messages.

As some higher level programs are themselves protocols, standardized in the TCP/IP protocol suite, such as Telnet and FTP, they use the same port number in all TCP/IP implementations. (Port 23 is used by a Telnet server; ports 20 and 21 are used by an FTP server.) Those assigned port numbers

are called well-known ports and the standard applications are called well-known services.

The well-known ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA) and on most systems can only be used by system processes or by programs executed by privileged users. The assigned well-known ports occupy port numbers in the range 0 to 1023. The ports with numbers in the range 1024-65535 are not controlled by the Internet central authority and on most systems can be used by ordinary user-developed programs.

Confusion due to two different applications trying to use the same port numbers on one host is avoided by writing those applications to request an available port from TCP/IP. Because this port number is dynamically assigned, it may differ from one invocation of an application to the next.

UDP, TCP and ISO TP-4 all use the same port principle. To the extent possible, the same port numbers are used for the same services on top of UDP, TCP and ISO TP-4.

Let us first consider the following terminologies:

- A socket is a special type of file handle that is used by a process to request network services from the operating system.
- A socket address is the triple:

  ```
  {protocol, local-address, port number}
  ```

  In the TCP/IP suite, for example:

  ```
  {tcp, 193.44.234.3, 12345}
  ```

- A conversation is the communication link between two processes.
- An association is the 5-tuple that completely specifies the two processes that constitute a connection:

  ```
  {protocol, local-address, local-port, foreign-address,foreign-port}
  ```

  In the TCP/IP suite, for example, a valid association could be:

  ```
  {tcp, 193.44.234.3, 1500, 193.44.234.5, 21}
  ```

- A half-association is either:

  ```
  {protocol, local-address, local-port}
  ```

  or

  ```
  {protocol, foreign-address, foreign-port}
  ```

  which specifies each half of a connection.

- The half-association is also called a socket or a transport address. That is, a socket is an endpoint for communication that can be named and addressed in a network.

The socket interface is one of several application programming interfaces (APIs) to the communication protocols. Designed to be a generic communication programming interface, it was first introduced by the 4.2BSD UNIX system. Although it has not been standardized, it has become a de facto industry standard.

The socket interface is differentiated by the services that are provided to applications: stream, datagram, and raw sockets services.

Stream socket interface (SOCK_STREAM)
Defines a reliable connection-oriented service (over TCP for example). Data is sent without errors or duplication and is received in the same order as it is sent. Flow control is built-in to avoid data overruns. No boundaries are imposed on the exchanged data, which is considered to be a stream of bytes. An example of an application that uses stream sockets is the File Transfer Protocol (FTP).

Datagram socket interface (SOCK_DGRAM)
Defines a connectionless service (over UDP, for example). Datagrams are sent as independent packets. The service provides no guarantees; data can be lost or duplicated, and datagrams can arrive out of order. An example of an application that uses datagram sockets is the Network File System (NFS).

Raw socket interface (SOCK_RAW)
Allows direct access to lower layer protocols such as IP and ICMP. This interface is often used for testing new protocol implementations. An example of an application that uses raw sockets is the PING command.

1.6.2 User Datagram Protocol (UDP)

UDP is basically an application interface to IP. It provides no additional reliability, flow-control or error recovery. It simply serves as a multiplexer/demultiplexer for sending/receiving IP datagrams, using ports to direct the datagrams.

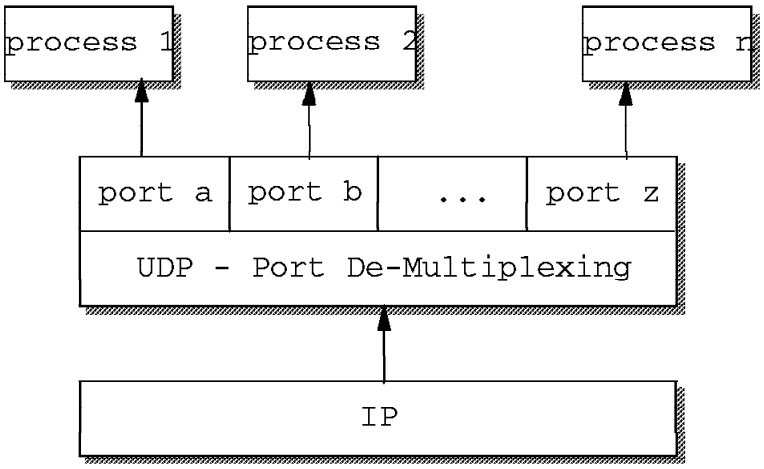


Figure 9. UDP - Demultiplexing Based on Ports

1.6.3 Transmission Control Protocol (TCP)

We have previously discussed IP, the unreliable connectionless packet (datagram) system that forms the basis of the TCP/IP protocol suite. TCP is the higher level protocol that provides reliability, flow control and some error recovery. Most of the TCP/IP application protocols, such as Telnet and FTP, use TCP as the underlying protocol.

TCP is a connection-oriented, end-to-end reliable protocol providing logical connections between pairs of processes. Within TCP, a connection is uniquely defined by a pair of sockets (that is, by a pair of processes, on the same or different systems, that are exchanging information).

The two processes communicate with each other over the TCP connection (InterProcess Communication - IPC), as shown in Figure 10 on page 21.

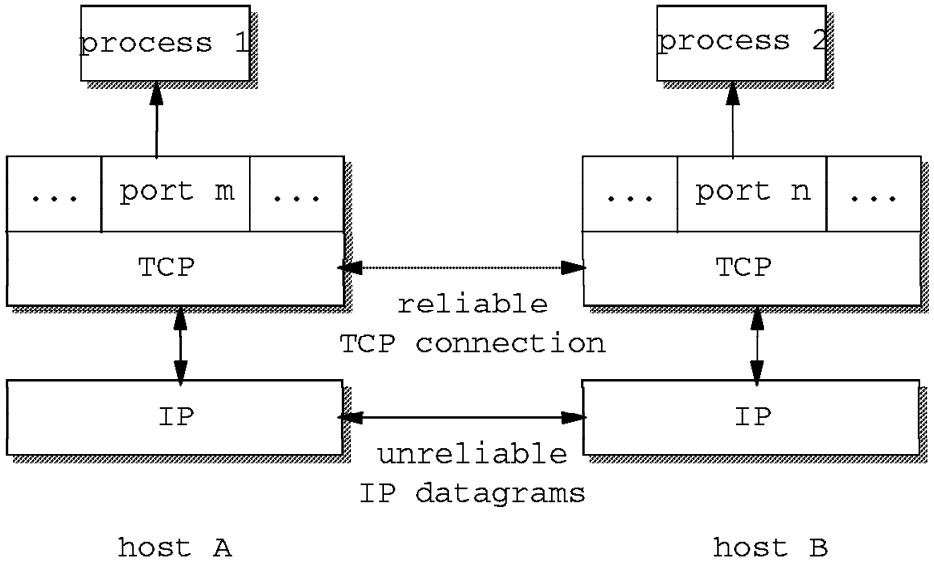


Figure 10. TCP - Connection between Processes. (Processes 1 and 2 communicate over a TCP connection carried by IP datagrams.)

1.7 TCP/IP Application Protocols

One of the reasons why TCP/IP is so popular is that there are many simple and useful standard applications available. We summarize several common TCP/IP applications in this section.

1.7.1 Remote Login and Terminal Emulation (Telnet)

Telnet (teletypewriter network) is the virtual terminal protocol in TCP/IP. It allows users of one host to log into a remote host and interact as normal terminal users of that host. Telnet is a line-oriented protocol using the ASCII character set. Though initially designed for terminal emulation, Telnet is also used as the underlying protocol for file transfer (FTP control sessions) and e-mail (SMTP) operations.

For readers who are familiar with SNA, we can relate Telnet in TCP/IP to the terminal emulators (3270 or 5250 types) in SNA. In fact, all of the IBM TCP/IP product implementations provide Telnet support of 3270 terminal emulation in addition to the many other terminal emulation protocols, such as the widely used DEC VT terminal emulation types.

3270 terminal emulation differs from normal Telnet operation in the following ways:

1. It uses block-mode rather than line-mode.
2. It uses the EBCDIC character set rather than the ASCII character set.
3. It uses special key functions such as ATTN and SYSREQ.

A 3270 Telnet (TN3270) server must support those characteristics during initial client/server session negotiations. TN3270 sessions can represent either display or printer devices.

Originally TN3270 sessions were identified as non-SNA devices to a mainframe computer. The TN3270E extensions (see RFC 1647) define methods to map TN3270 sessions to specific SNA logical unit (LU) names thus effectively turning them into SNA devices. This eases the use of certain applications and allows users to be assigned the same LUs whenever they connect to the server.

1.7.2 File Transfer Protocols (FTP and TFTP)

File Transfer Protocol (FTP) provides the function of transferring files between two TCP/IP hosts. Since FTP is built on the services of TCP in the transport layer, it provides a reliable and end-to-end connection during the file transfer operation. Security is provided by the normal user ID and password authentication.

Trivial File Transfer Protocol (TFTP) is a somewhat simplified companion of FTP. It operates on UDP and therefore does not guarantee reliable end-to-end connection or delivery. It also offers only limited security based on client hostname authorization. Nonetheless, TFTP is quite commonly used in conjunction with BOOTP to distribute startup program code to diskless network stations. (See 1.8.1, “Bootstrap Protocol (BOOTP)” on page 29 for more information on BOOTP.)

1.7.3 Remote Printing (LPR and LPD)

The line printer requester (LPR) allows access to printers on other computers running the line printer daemon (LPD) as though they were on your computer. The clients provided (LPR, LPQ, LPRM or LPRMON or LPRPORTD) allow the user to send files or redirect printer output to a remote host running a remote print server (LPD). Some of these clients can also be used to query the status of a job, as well as to delegate a job. For more information about remote printing, see RFC 1179.

1.7.4 Remote Command Execution (REXEC and RSH)

Remote shell (RSH) and remote execution (REXEC) are similar protocols that allow you to run programs and commands on different computers. The results are received and displayed on the local host. This can be useful for small computers to harness the power of large systems.

1.7.5 Domain Name System (DNS)

Recall that TCP/IP hosts are addressed by 32-bit IP addresses that are represented in decimal notation. For example, to Telnet to a remote host with IP address of 9.67.38.1, the users would typically enter `telnet 9.67.38.1`. This was both very cumbersome and error-prone.

Very quickly, this evolved to the use of symbolic high-level machine names. That is, instead of typing `telnet 9.67.38.1`, one would now enter `telnet small`, where small would then be internally translated to the IP address 9.67.38.1.

This introduces the problem of maintaining the mappings between IP addresses and high-level machine names in a coordinated and centralized way.

Initially, host names to address mappings were maintained by the Internet Network Information Center (InterNIC, previously NIC) in a single file (HOSTS.TXT) which was fetched by all hosts using FTP. Most hosts would have a copy of that file, which may or may not be current or correct.

Due to the explosive growth in the number of hosts, this mechanism became too complicated and time-consuming, and was replaced by a new concept: the domain name system (DNS).

The domain concept lies in decentralizing the naming mechanism by distributing responsibility (and authority) for mapping between names and addresses. For example, consider the internal structure of a large organization. As the chief executive cannot do everything, the organization will probably be partitioned into divisions, each of them having autonomy within certain limits. Specifically, the executive in charge of a division has authority to make direct decisions, without permission from his chief executive.

Domain names are formed in a similar way, and will often reflect the hierarchical delegation of authority used to assign them. For example, consider the name:

`small.itso.raleigh.ibm.com`

Here, itso.raleigh.ibm.com is the lowest-level domain name, a subdomain of raleigh.ibm.com, which again is a subdomain of ibm.com, a subdomain of com. We can also represent this naming concept by a hierarchical tree (see Figure 11 on page 24).

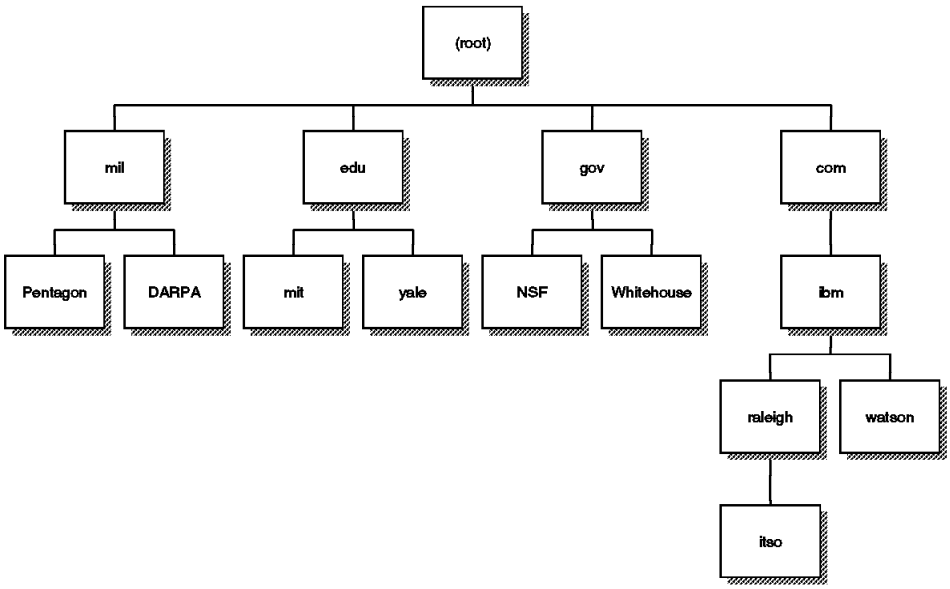


Figure 11. Hierarchical Name space. (Chain of authority in assigning domain names.)

Table 2 shows some of the top-level domains of today's Internet domain name space.

Table 2. DNS - Some Top-Level Internet Domains

Domain Name	**Meaning**
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	US Military
net	Major network support centers
org	Non-profit organizations
country code	ISO standard 2-letter identifier for country-specific domains

1.7.5.1 Mapping Domain Names to IP Addresses

The mapping of names to addresses consists of independent, cooperative systems called name servers. A name server is a server program answering requests from the client software, called a name resolver.

There are various types of implementations of the resolve functions and the name server functions (for example, full versus stub resolvers, and primary, secondary versus cache name servers). We do not elaborate on them.

Conceptually, all Internet domain servers are arranged in a tree structure that corresponds to the naming hierarchy in Figure 11 on page 24. Each leaf represents a name server that handles names for a single subdomain. Links in the conceptual tree do not indicate physical connections. Instead, they show which other name server a given server can contact.

Figure 12 shows the domain name resolution process:

- A user program issues a request such as the gethostbyname() sockets call. (This particular call is used to ask for the IP address of a host by passing the hostname.)
- The resolver formulates a query to the name server.
- The name server checks to see if the answer is in its local authoritative database or cache, and if so, returns it to the client. Otherwise, it will query the other available name server(s).

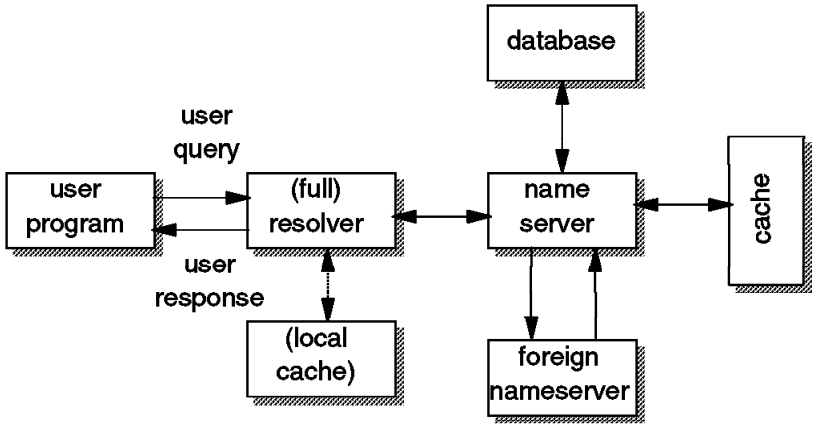


Figure 12. DNS - Resolver and Domain Name Server

1.7.5.2 Inverse Mapping

In some cases, it may be necessary to find a hostname for a given IP address. This is called inverse mapping and is a standard function of most

DNS servers available today. A special domain, in-addr.arpa, is being used for inverse name queries.

1.7.5.3 Transport

The query/reply messages are transported by either UDP or TCP.

1.7.6 Dynamic DNS (DDNS)

The Dynamic Domain Name System (DDNS) is a protocol that defines extensions to the Domain Name System to enable DNS servers to accept requests to update the DNS database dynamically and securely.

Note: DDNS currently is an Internet Draft (ID) which means that there is no standard specified yet. Nonetheless, IBM has fully implemented DDNS in its OS/2 Warp Server products.

These extensions define mechanisms for adding and deleting a set of names and associated resource records. Further, DDNS uses DNS security extensions to authenticate hosts that request to create or update entries in the DDNS server database. Without client authentication, another host could impersonate an unsuspecting host by remapping the address entry for the unsuspecting host to that of its own. Once the remapping occurs, important data, such as logon passwords and mail intended for the host would unfortunately be sent to the impersonating host instead.

IBM implements fail-safe RSA public-key digital signature technology to secure the DNS database updates so that the database entries cannot be changed by unauthorized hosts.

1.7.7 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol is an electronic mail protocol with both client (sender) and server (receive) functions. Since SMTP is a rather old protocol, many aspects of modern electronic mail are missing in its definitions. It basically assumes that messages would only consist of plain text in 7-bit US ASCII format with a line length of no more than 1000 characters. For more information about SMTP, see RFCs 821, 822 and 974.

1.7.8 Multipurpose Internet Mail Extensions (MIME)

To overcome the shortcomings of SMTP, a new architecture has been defined that allows for a much greater variety of what can be contained in an electronic message, such as:

- 8-bit text and lines longer than 1000 characters
- International code pages and character sets
- Binary and multimedia objects, such as:
  - Fonts

– Images, audio and video objects

MIME is defined in RFCs 2045 to 2049 and currently has a state of draft standard. MIME does not solely apply to electronic mail; rather it defines a way to incorporate different objects in any electronic message. For instance, it is used widely throughout the Internet today by means of browsing the World Wide Web (see 1.10.3, “The World Wide Web (WWW)” on page 34).

1.7.9 Post Office Protocol (POP)

The Post Office Protocol is an electronic mail protocol with both client (sender/receiver) and server (storage) functions. POP allows mail for multiple users to be stored in a central location until a request for delivery is made by an electronic mail program. For more information about POP, see RFC 1725.

1.7.10 Remote Procedure Call (RPC)

Remote Procedure Call is a standard developed by SUN Microsystems and used by many vendors of UNIX systems.

RPC is an application programming interface (API) available for developing distributed applications. It allows programs to call subroutines that are executed at a remote system. The caller program (called client) sends a call message to the server process, and waits for a reply message. The call message includes the procedure′s parameters and the reply message contains the procedure′s results.

Sun-RPC consists of the following parts:

- RPCGEN: A compiler that takes the definition of a remote procedure interface and generates the client stubs and the server stubs.
- XDR (eXternal Data Representation): A standard way of encoding data in a portable fashion between different systems. It imposes a big-endian byte ordering and the minimum size of any field is 32 bits. This means that both the client and the server have to perform some translation.
- A run-time library.

The concept of RPC is very similar to that of an application program issuing a procedure call:

- The caller process sends a call message and waits for the reply.
- On the server side, a process is dormant awaiting the arrival of call messages. When one arrives, the server process extracts the procedure parameters, computes the results and sends them back in a reply message.

The RPC Call Message consists of several fields, such as:

- Remote program number
- Remote program version number
- Remote procedure number

1.7.10.1 Portmap

The Portmap or Portmapper is a server application that will map a program number and its version number to the Internet port number used by the program. Portmap is assigned the reserved (well-known service) port number 111.

Portmap only knows about RPC programs on the host it runs on. In order for Portmap to know about the RPC program, every RPC program should register itself with the local Portmapper when it starts up.

The RPC client (caller) has to ask the Portmap service on the remote host about the port used by the desired server program.

1.7.11 Network File System (NFS)

The Network File System (NFS) enables machines to share file systems across a network. It allows authorized users to access files located on remote systems as if they were local. It is designed to be machine-independent, operating system-independent, and transport protocol-independent. This is achieved through implementation on top of RPC.

1.7.12 X Window System

The X Window System (hereafter referred to as X) is one of the most widely used graphical user interface (GUI), or bitmapped window display systems.

Current X releases contain two numbers: a version number indicating major protocol or standards revisions, and a release number indicating minor changes. At the time of this book′s publication, the latest version is X11 Release 6, also known as X11R6.

The X Window System uses sockets to communicate over a TCP/IP network.

There are two main components in X that communicate with each other:

1.7.12.1 X-Server

A dedicated program that provides display services on a graphic terminal, on behalf of a user, at the request of the user′s X-client program. It controls the screen and handles the keyboard and the mouse (or other input devices) for one or more X-clients. Equally, it is responsible for output to the display,

the mapping of colors, the loading of fonts and the keyboard mapping. Typically X-server programs run on high-performance graphics PCs and workstations, as well as X terminals, that are designed to run only the X-server program.

1.7.12.2 X-Client

The actual application is designed to employ a graphical user interface to display its output. Typically, many X-clients compete for the service of one X-server per display per user. Xterm and Xclock are two examples of X-clients.

1.8 TCP/IP Configuration and Management Protocols

This section provides a brief overview of some of the protocols used to configure and manage TCP/IP networks.

1.8.1 Bootstrap Protocol (BOOTP)

The BOOTstrap Protocol (BOOTP) enables a client workstation to initialize with a minimal IP stack and request its IP address, a gateway address and the address of a name server from a BOOTP server. Once again, a good example of a client that requires this service is a diskless workstation. If BOOTP is to be used in your network, then you must make certain that both the server and client are on the same physical LAN segment. BOOTP can only be used across bridged segments when source routing bridges are being used, or across subnets if you have a router capable of BOOTP forwarding, also known as a BOOTP relay agent.

1.8.2 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is based on BOOTP and extends the concept of a central server supplying configuration parameters to hosts in the network. DHCP adds the capability to automatically allocate reusable network addresses to workstations or hosts, and it supports the following functions.

Automatic Allocation
DHCP assigns a permanent address to a host.

Dynamic Allocation
DHCP assigns a leased IP address for a limited period of time. This is the only mechanism that allows automatic reuse of addresses that had been previously assigned but are no longer in use.

Manual Allocation
The host's address is manually configured by the network administrator.

You may have more than one DHCP server in your network, each server containing a pool of addresses and leases in local storage. A client may be configured to broadcast a request for address assignment and will select the most appropriate response from those servers that answer the request. One big potential advantage with DHCP is a reduction in the workload required to manually configure addresses for all workstations in a segment.

According to RFC 1541, a DHCP server does not need to be in the same subnet or on the same physical segment as the client which would then require the use of a BOOTP relay agent.

1.8.3 Simple Network Management Protocol (SNMP)

With the growth in size and complexity of the TCP/IP-based networks, the need for network management became very important. The current network management framework for TCP/IP consists of the following:

1. Structure and Identification of Management Information (SMI) describes how managed objects contained in the Management Information Base (MIB) are defined.
2. Management Information Base, second version (MIB-II) describes the managed objects.
3. SNMP defines the protocol used to manage these objects.

A network management station executes network management applications that monitor and control network elements such as hosts, gateways and terminal servers. These network elements use a management agent to perform the network management functions requested by the network management stations. SNMP is used to communicate management information between the network management stations and the agents in the network elements.

1.9 TCP/IP Routing Protocols and Techniques

This section provides a brief overview of some of the protocols used to update routing tables among routers in TCP/IP networks. This process is called dynamic routing because the routers take care that updates are sent automatically according to protocol specifications.

In contrast to that, static routing would require system administrators to enter all required routing information at every host and gateway in order for a TCP/IP internetwork to function as desired.

1.9.1 Routing Information Protocol (RIP)

The Routing Information Protocol creates and dynamically maintains network routing tables. RIP arranges to have gateways and routers periodically broadcast their routing tables to neighbors. Using this information, a RouteD server can update a host′s routing tables. For example, RouteD determines if a new route has been created, if a route is temporarily unavailable or if a more efficient route exists. For more information about routing using RIP, see RFC 1058.

The Routing Information Protocol Version 1 is commonly known as RIP. It uses a distance vector algorithm, which means it calculates the best path to a destination based on the number of hops in the path. Each hop represents a router through which a datagram must pass in order to reach the destination.

RIP is widely used and easy to implement, but it is known to have several limitations:

- The maximum number of hops is 15 (16 refers to an unreachable destination), making RIP inadequate for large networks that may have more than 15 routers on any single path.
- RIP is not a secure protocol. It does not authenticate the source of any routing updates it receives.
- RIP can not choose the best path based on delay, cost, reliability or load.
- RIP does not support variable length subnet masks.
- RIP can take a relatively long time (compared to other protocols such as OSPF) to converge, or stabilize its tables after an alteration to the network configuration has occurred.

The Routing Information Protocol Version 2 (RIP-2) was created in order to fix some of the limitations of RIP. It is still less powerful than protocols such as OSPF, but it has the advantages of being easy to implement and having a lower network overhead. This overhead includes network traffic and CPU time. RIP-2 can interoperate with RIP, and it is able to implement variable length subnetting.

1.9.2 Open Shortest Path First (OSPF)

OSPF is a complex protocol utilizing a link state, shortest path first algorithm. In a link-state protocol, each router broadcasts link status information to each of its neighboring routers instead of distance vector information. Each neighboring router then propagates the status information to its own neighbors until the information has been sent to every router in the network. Each router then uses the status information to build a

complete routing table utilizing a calculated cost for each link based on load, time delays, or reliability.

The biggest advantage of OSPF in comparison to either RIP or RIP-2 is that of the time taken to converge after a change to the network. The link-state protocols will always stabilize the propagated routing tables much faster than the distance vector protocols.

OSPF supports variable length subnetting and multicasting (a broadcast mechanism that only sends to a number of specific hosts rather than every one in the network). It also introduces the concept of *areas*, where the Autonomous System is divided into areas, each responsible for its own topology. Area topology is not propagated to other areas; border routers maintain connectivity between the separate areas across an OSPF backbone, reducing the amount of routing information which must be exchanged.

See RFC 1583 for more information about OSPF.

1.9.3 Classless Inter-Domain Routing (CIDR)

It has been mentioned in 1.5.1.1, “IP Addressing” on page 6 that due to the impact of growth, the IP address space will be near exhaustion very soon if addresses continue to be assigned as they are requested or as they used to be. We have pointed out that the next version of IP, IPv6, will easily overcome that problem (see 1.5.2, “The Future Version of IP (IPv6)” on page 14), but what can be done until IPv6 is fully deployed?

One idea was to use a range of class C addresses instead of a single class B address. The problem there is that each network must be routed separately because standard IP routing understands only class A, B and C network addresses (see 1.5.1.4, “IP Routing” on page 10).

Within each of these types of network, subnetting can be used to provide better granularity of the address space within each network, but there is no way to specify which multiple class C networks are actually related (see 1.5.1.2, “IP Subnets” on page 7). The result of this is termed the *routing table explosion* problem: A class B network of 3000 hosts requires one routing table entry at each backbone router, whereas the same network, if addressed as a range of class C networks, would require 16 entries.

The solution to this problem is a scheme called Classless Inter-Domain Routing (CIDR). CIDR is described in RFCs 1518 to 1520.

CIDR does not route according to the class of the network number (hence the term classless) but solely according to the high order bits of the IP

address which are termed the IP prefix. Each CIDR routing table entry contains a 32-bit IP address and a 32-bit network mask, which together give the length and value of the IP prefix. This can be represented as <IP_address network_mask>. For example, to address a block of eight class C addresses with one single routing table entry, the following representation would suffice: <192.32.136.0 255.255.248.0>. This would, from a backbone point of view, refer to the class C network range from 192.32.136.0 to 192.32.143.0 as one single network because of the identical IP prefix, as illustrated in Figure 13:

```
 11000000 00100000 10001000 00000000 = 192.32.136.0 (class C address)
 11111111 11111111 11111--- --------   255.255.248.0 (network mask)
=================================== logical_AND
 11000000 00100000 10001--- -------- = 192.32.136  (IP prefix)

 11000000 00100000 10001111 00000000 = 192.32.143.0 (class C address)
 11111111 11111111 11111--- --------   255.255.248.0 (network mask)
=================================== logical_AND
 11000000 00100000 10001--- -------- = 192.32.136  (same IP prefix)
```

Figure 13. Classless Inter-Domain Routing - IP Supernetting Example

This process of combining multiple networks into a single entry is referred to as *supernetting* because routing is based on network masks that are shorter than the natural network mask of an IP address, in contrast to subnetting (see 1.5.1.2, “IP Subnets” on page 7) where the subnet masks are longer than the natural network mask.

CIDR is implemented and used in today’s Internet backbone routers based on the Border Gateway Protocol (BGB-4). It is scarcely used at the local network level where splitting up the available address space is more of a problem than expanding the address space.

Note: CIDR in itself does not constitute a routing protocol. It is a method of interpretation of IP addresses that can be employed by routing protocols to achieve the goals previously described.

1.10 Internet User Applications and Protocols

This section provides a brief overview of some of the protocols and applications that have made the task of using the Internet both easier and very popular over the past couple of years.

1.10.1 Network News

One application that is particularly popular on the Internet is Network News, also known as Usenet News. Based on the Network News Transfer Protocol (NNTP), users on the Internet can view and contribute to news groups covering topics such as science, education, computers, business, politics, recreation, sports, and many more. News groups are stored on news servers. NNTP is used for both server-to-server and client-to-server communication.

Clients use a news agent application, such as the IBM NewsReader/2, to retrieve articles from one or more news groups, and to post articles to one or more news groups.

For more information about NNTP, see RFC 977.

1.10.2 Gopher

Gopher is a client/server protocol designed for information location and retrieval. The client function provides a menu-driven interface to access the files stored on a Gopher server. The server function allows descriptive names to be assigned to the files. Thus, making it easier to identify the content of each file. Gopher was designed at the University of Minnesota.

For more information about Gopher, see RFC 1436.

1.10.3 The World Wide Web (WWW)

The World Wide Web is a global hypertext system that was initially developed in 1989 by Tim Berners-Lee at the European Laboratory for Particle Physics, CERN in Switzerland to facilitate an easy way of sharing and editing research documents among a geographically dispersed group of scientists.

In 1993 the Web started to grow rapidly which was mainly due to the National Center for Supercomputing Applications (NCSA) developing a Web browser program called Mosaic, an X Windows-based application. This application provided the first graphical user interface to the Web and made browsing more convenient.

Today there are Web browsers and servers available for nearly all platforms. You can get them either from an FTP site for free or buy a licensed copy. The rapid growth in popularity of the Web is due to the flexible way people can navigate through world wide resources in the Internet and retrieve them. To get an idea of the growth of the Web, Table 3 on page 35 presents some statistics.

The number of Web servers is also increasing rapidly and the traffic over port 80, which is the well-known port for HTTP Web servers, on the NSF backbone has had a phenomenal rate of growth too. The NSFNET was converted back to a private research network in 1995, therefore comprehensive statistics of backbone traffic are not as easily available anymore, if they are at all.

Table 3. Growth of The World Wide Web. The source of these figures can be found at the following URL:

`http://www.mit.edu/people/mkgray/net/web-growth-summary.html`

Date	Web Sites	Web Traffic	FTP Traffic	E-mail Traffic
June 1993	130	0.5	42.9	6.4
June 1994	2,738	6.1	35.2	6.4
March 1995	n/a	23.9	24.2	4.9
June 1995	23,500	n/a	n/a	n/a
June 1996	230,000	n/a	n/a	n/a
January 1997	650,000	n/a	n/a	n/a

1.10.4 Hypertext Transfer Protocol (HTTP)

The Hypertext Transfer Protocol is a protocol designed to allow the transfer of Hypertext Markup Language (HTML) documents. HTML is a tag language used to create hypertext documents. Hypertext documents include links to other documents that contain additional information about the highlighted term or subject. Such documents may contain other elements apart from text, such as graphic images, audio and video clips, and even virtual reality worlds (which are described in VRML, a scripting language for that kind of element).

HTTP is based on request-response activity. A client, running an application called a browser, establishes a connection with a server and sends a request to the server in the form of a request method. The server responds with a status line, including the message′s protocol version and a success or error code, followed by a message containing server information, entity information and possible body content.

An HTTP transaction is divided into four steps:

1. The browser opens a connection.
2. The browser sends a request to the server.
3. The server sends a response to the browser.

4. The connection is closed.

On the Internet, HTTP communication generally takes place over TCP connections. The default port is TCP 80, but other ports can be used. This does not preclude HTTP from being implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used, but the mapping of the HTTP request and response structures onto the transport data units of the protocol in question is outside the scope of this document.

Except for experimental applications, current practice requires that the connection be established by the client prior to each request and closed by the server after sending the response. Both clients and servers should be aware that either party may close the connection prematurely, due to user action, automated timeout, or program failure, and should handle such closing in a predictable fashion. In any case, the closing of the connection by either or both parties always terminates the current request, regardless of its status.

What we have just described means that, in simple terms, HTTP is a connectionless protocol. For example, to load a page including two graphics, a graphic-enabled browser will open three TCP connections: one for the page, and two for the graphics. Most browsers, however, are able to handle several of these connections simultaneously.

HTTP is stateless, because it keeps no track of the connections. If a request depends on the information exchanged during a previous connection, then this information has to be kept outside the protocol.

1.10.5 The Advent of Java

Java is an important new technology in the world of the Internet. In summary, it is a simple, robust, object-oriented, platform-independent, multithreaded, dynamic general-purpose programming environment for creating applications for the Internet and Intranet. Java includes the components described in the following sections.

1.10.5.1 Java Language

Java is a programming language developed by Sun Microsystems, which is object-oriented, distributed, interpreted, architecture-neutral, and portable. Java can be used to create downloadable program fragments, so-called *applets*, that augment the functionality of a Java-capable browser such as HotJava or Netscape Navigator.

1.10.5.2 Java Virtual Machine

The Java Virtual Machine (JVM) is an abstract computer that runs compiled Java programs (or precisely, interprets Java byte-code that has been produced by a Java compiler). JVM is virtual because it is generally implemented in software on top of a real hardware platform and operating system. In this way, it is architecture-neutral and platform-independent. All Java programs should be compiled to run in a JVM.

The following diagram describes in simple terms how Java is implemented:

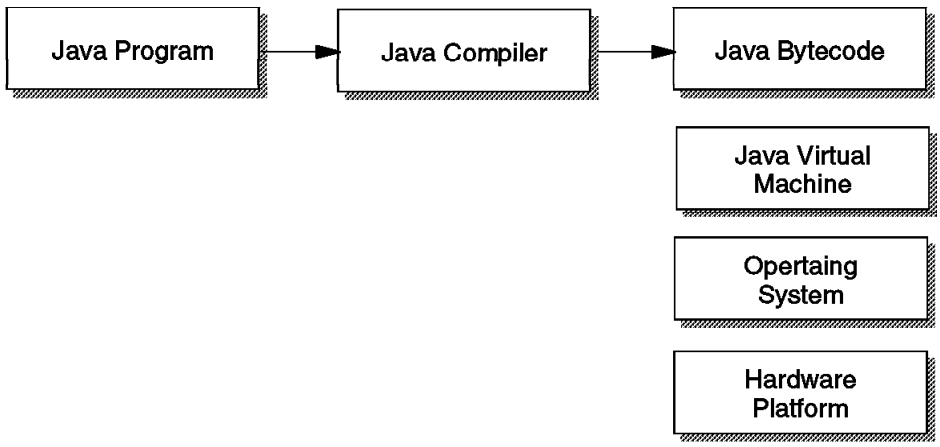


Figure 14. Implementation of Java

1.10.5.3 HotJava

HotJava is a Java-enabled Web browser, developed by Sun Microsystems, that lets you view Java applets.

1.10.5.4 JavaOS

JavaOS is a highly compact operating system, developed by JavaSoft, which is designed to run Java applications directly on microprocessors in anything from personal computers to pagers. JavaOS will run equally well on a network computer, a PDA, a printer, a game machine, or countless other devices that require a very compact OS and the ability to run Java applications.

1.10.5.5 Java Beans

An initiative called Java Beans is brewing a similar set of APIs that will make it easy to create Java applications from reusable components. Java

Beans will be used in a wide range of applications, from simple widgets to full-scale, mission-critical applications. Many software vendors including IBM have announced plans to support it.

1.10.5.6 JavaScript

JavaScript is an HTML extension and programming language, developed by Netscape, which is a simple object-based language compatible with Java. JavaScript programs are embedded as source directly in an HTML document. They can control the behavior of forms, buttons and text elements.

JavaScript is used to create dynamic behavior in elements of the Web page. In addition, it can be used to create forms whose fields have built-in error checking routines.

For more information about Java, check out the following URLs:

```
http://ncc.hursley.ibm.com/javainfo/
http://java.sun.com/
```

1.11 TCP/IP and Internet Security

In this section we briefly introduce some concepts and protocols that allow you to establish various degrees of security in TCP/IP networks.

One may say that the Internet is great because there is so much information out there that can be accessed very easily and quickly. Electronic communication has become a lot easier because of the Internet, no doubt, but it can also be a dangerous thing at times.

Imagine that someone could get into your system and destroy data at random just because you forgot to implement security that could have prevented it. Or, worse, imagine someone could tap into your communication, learn your passwords and then use your account information to do electronic shopping.

One of the major concerns when providing commercial services on the Internet is providing for transaction security and communications security.

Information exchanges are secure if all the following are true:

- Messages are confidential.
- The information exchange has integrity.
- Both sender and receiver are accountable.
- You can authenticate both parties in the exchange.

There are certainly other ways of compromising information on the Internet that one might think of, so how should one go ahead to protect oneself against them?

1.11.1 Secure Sockets Layer (SSL)

SSL is a security protocol that was developed by Netscape Communications Corporation, along with RSA Data Security, Inc. The primary goal of the SSL protocol is to provide a private channel between communicating applications which ensures privacy of data, authentication of the partners and integrity.

SSL provides an alternative to the standard TCP/IP socket API which has security implemented within it. Hence, in theory it is possible to run any TCP/IP application in a secure way without changing it. In practice, SSL is so far only implemented for HTTP connections.

In fact the protocol is composed of two layers:

- At the lower layer is the SSL Record protocol. It is used for data encapsulation.
- On the upper layer is the SSL Handshake protocol used for initial authentication and transfer of encryption keys.

The SSL protocol addresses the following security issues:

Privacy
After the symmetric key is established in the initial handshake, the messages are encrypted using this key.

Integrity
Messages contain a message authentication code ensuring the message integrity.

Authentication
During the handshake, the client authenticates the server using an asymmetric or public key.

SSL requires each message to be encrypted and decrypted and therefore has a high performance and resource impact. In addition, since only the server is authenticated, SSL is not suitable for applications, such as electronic banking, which require that the server authenticate their clients.

1.11.2 Firewalls

One way to deal with network security is the installation of a specialized server, a so-called *firewall*. Firewalls tend to be seen as a protection between the Internet and a private network. But generally speaking a firewall should be considered as a means to divide the world into two or

more networks: one or more secure network and one or more non-secure network.

Imagine a company where all the departments are connected to the internal network, including sales, accounts, development and human resources departments. The administrator would like to be able to restrict access from the development department machines to the human resources department machines and from the sales department to the development department.

In order to provide maximum security, a good firewall design is paramount:

- Anything not explicitly permitted should default to denied.
- Increasing complexity leads to bugs, which lead to opportunities.
- The server should be kept in a physically secure environment.
- Provide extensive logging.
- Turn off known problems and non-essential daemons (applications and services).

Most of the firewalls available today offer one or more of the following services, some of which we briefly describe in the paragraphs following the list below:

- Filtering gateways
- Proxy application layer gateways
- Circuit layer gateways (SOCKS servers)
- Domain name server hiding
- Mail handling
- Auditing and logging

Multiple technologies are needed to provide capabilities and protection. The IBM Secure Network Gateway (SNG), for instance, is based on IBM′s technology and has been used for nearly ten years to protect internal IBM networks.

1.11.2.1 Screening Filters

The screening filter looks at each IP packet flowing through it, controlling access to machines and/or ports in the private network and possibly limiting access from the private network to the Internet. Screening filters operate at the IP layer and cannot control access at the application layer.

1.11.2.2 Proxy Servers

Proxy servers are used to control access to or from the private network relaying only acceptable communications from known users.

Users in the private network can access an application, such as FTP, in the proxy server using their usual utilities (clients). Users authenticate

themselves to the proxy server and can then access the application on the desired machine in the public network. Proxy servers can also be used from the public network to access applications in the private network, but this exposes login names and passwords to attackers in the public network.

1.11.2.3 SOCKS Servers

SOCKS servers are like proxy servers without the requirement for double connections. With SOCKS, users can benefit from secure communications without needing to be aware that it is happening.

Users have to use new versions of applications called SOCKSified clients. The SOCKSified client code directs its requests to the SOCKS port on the firewall. Sessions are broken at the firewall, as they are with proxy servers. With SOCKS, however, the connection to the destination application is created automatically once the user is validated.

Both the client and the SOCKS server need to have SOCKS code. The SOCKS server acts as an application-level router between the client and the real application server. SOCKS is for outbound sessions only. It is simpler for the private network user, but does not have secure password delivery so it is not intended for sessions between public network users and private network applications.

The majority of Web browsers are SOCKSified and you can get SOCKSified TCP/IP stacks for most platforms. For additional information, refer to the following URLs:

```
http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com
```

1.11.3 IP Security Architecture (IPSec)

IPSec describes several security mechanisms that address security, authentication and encryption at the IP layer rather than on upper transport or application layers. The IP Security Architecture defines two specific headers to provide security services for IP datagrams. Those may be applied either separately or combined.

1.11.3.1 IP Authentication Header (AH)

The IP Authentication Header (AH) can be used to provide connectionless integrity and data origin authentication for IP datagrams, and optionally to provide anti-replay integrity. This header protects an entire IP datagram, including all immutable fields in the IP header. AH does not provide confidentiality (no encryption).

1.11.3.2 IP Encapsulating Security Payload (ESP)

The Encapsulating Security Payload (ESP) can be used to provide confidentiality, data origin authentication, connectionless integrity, anti-replay integrity, and limited traffic flow confidentiality. Unlike AH, ESP provides security only for the protocols encapsulated by it, not the protocol that carries it.

For a more detailed discussion of IPSec within this redbook, please refer to 4.1, “Implementing and Using IP Security (IPSec)” on page 139. For more information on IPSec, please refer to RFCs 1825-1827.

1.12 Transporting Other Protocols over TCP/IP

We have so far regarded the TCP/IP network and transport protocols as a means of communications for TCP/IP applications. In reality, those protocols can also be employed to connect systems that run applications that normally would not have anything to do with TCP/IP. Those applications would expect to communicate over protocols such as NetBIOS, SNA or IPX.

Whenever an application or a protocol is made to use a transport protocol other than the one(s) it has originally been designed for, we call that non-native transport.

1.12.1 NetBIOS over TCP/IP

RFCs 1001 and 1002 define a way how to support applications using the NetBIOS API to use a TCP/IP network for transport. Essentially, NetBIOS is not a protocol but an application programming interface that knows very little about any underlying networking protocols. NetBIOS is used mostly in LAN environments and is there implemented to use the IEEE 802.2 interface. That renders NetBIOS unusable for TCP/IP networks because it cannot be routed in that way.

RFC 1001/1002 implementations of NetBIOS over TCP/IP alleviate that problem and have become increasingly important with the presence of operating systems such as OS/2 Warp Server, Windows NT and Windows 95 which partly rely on NetBIOS for communications.

1.12.2 SNA over TCP/IP

The IBM Multiprotocol Transport Network Architecture (MPTN) defines another way of using any transport network for any kind of application. The ultimate goal and great benefit of MPTN is that applications remain unchanged even if their native transport network is replaced by a non-native transport network.

In a specific implementation of MPTN, a TCP/IP network can be used to transport SNA applications using either dependent or independent logical unit (LU) communication, and it also supports Advanced-Program-to-Program Communication (APPC) and Advanced-Peer-to-Peer Networking (APPN).

Another implementation, MPTN likewise supports the transport of TCP/IP sockets applications over SNA networks.

1.12.3 IPX over TCP/IP

In a similar way as with NetBIOS over TCP/IP (RFC 1001/1002), RFC 1234 describes a way to transport the Novel Internet Packet Exchange (IPX) protocol over IP. However, in this case IPX datagrams are encapsulated in UDP datagrams before being sent over an IP network. This makes a whole TCP/IP network appear as a single IPX network to NetWare servers and requesters.

IPX offers functions to NetWare servers and IPX routers that are similar to the functions that IP provides for TCP/IP networks. Therefore, a connectionless delivery over UDP is desired when sending IPX over IP.

Chapter 2. Product Overview

In this chapter, we introduce the components of the IBM eNetwork Communications Suite, and highlight their main features. The applications that make up the suite have been selected because they have proven reliable, and have been accepted by the industry as leaders in their field.

The applications have been bundled together into one package to make the implementation of the IBM eNetwork Communications Suite in your enterprise a smooth one. This has been achieved by developing a single installation interface, and support across the following Windows platforms: Windows 3.x, Windows 95 and Windows NT 4.0.

A brief overview of the eNetwork Communications Suite functions is provided in Table 4.

Table 4. eNetwork Communications Suite Functional Overview

Function	Windows NT	Windows 95	Windows 3.x
TCP/IP Stack	N	Y	Y
AnyNet Support	Y	N	Y
APPC Support	Y	Y	Y
FTP Client	Y	Y	Y
FTP Server	Y	Y	Y
NFS Client	Y	Y	Y
NFS Server	N	N	N
Telnet Client	Y	Y	Y
LPR Client	Y	Y	Y
LPD Server	Y	Y	Y
X Window Server	N	N	N
Remote Command	Y	Y	Y
Remote Copy	Y	Y	Y
Scripting Tools	Y	Y	Y
3270/5250 Connectivity	Personal Communications		
Web Browser	Netscape Navigator and Plug-ins		
Mail Client	Lotus Notes, Netscape Mail		
NNTP Client	Netscape News		

2.1 TCP/IP Stack and Applications from FTP Software

The 16-bit and 32-bit TCP/IP protocol stack and applications from FTP Software bring a fast and effective TCP/IP solution to your workstations, regardless of which version of Windows you have deployed. These applications provide all the tools you require to connect to your corporate Intranet, or the Internet. They allow you to connect from the office via your existing LAN, or by using the dialer to connect to an Internet service provider by modem.

You and your mobile workforce can also use the tools to connect to your corporate Intranet from a laptop computer at home, or in the field. The built-in security of the FTP Software TCP/IP protocol stack and applications means that you can be confident that only those people authorized to access your sensitive corporate data are gaining access.

The seamless integration of this security ensures that the authorized user is not burdened by a degradation in the usability or functionality of the applications.

2.1.1 IP Security Architecture (IPSec)

The FTP Software TCP/IP protocol stack on Windows 95 implements IP security using a shared secret-based data encryption method. A shared secret means each party in the transaction has a unique phrase that only they and the other party are aware of. For each host that you wish to communicate with in a secure manner, you need to contact the system administrator of that site, and exchange the unique phrases needed to set up the IP security. Each host then encrypts the shared secret and sends it to the remote host for verification. If the verification is successful, the session starts, and the TCP/IP traffic between the two hosts will be protected.

2.1.2 IP Version 6 (IPv6) - The Next Generation IP

The FTP Software TCP/IP protocol stack supports the next generation of IP known as IP Version 6 or IPv6. IPv6 solves the main problem with IPv4 which is an increasing demand on address space. At the same time, IPv6 also solves many other restrictions handed down from the previous version, while remaining compatible with IPv4. This allows for easy migration to IPv6 in your enterprise.

For more information on IPv6, please refer to 4.2, “Implementing and Using IPv6” on page 147.

2.1.3 TCP/IP Applications

Regardless of which platform you install the eNetwork Communications Suite on, the Network Access Suite will contain a number of advanced products that will increase your productivity under Windows and TCP/IP.

Some of these applications replace the existing applications of the same name, or function. Others are available only with the FTP Software Network Access Suite. The applications that are enhanced versions of existing tools contain functions and support not available with the standard tools supplied with Windows.

The folder containing the application shortcuts to the Network Access Suite will look similar to Figure 15.

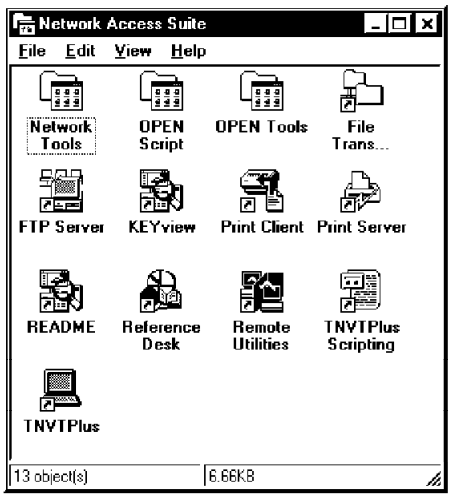


Figure 15. Network Access Suite

The main components included with the Network Access Suite are as follows:

File Transfer

The ability to transfer files quickly and easily is very important. The File Transfer Protocol application in the Network Access Suite allows you to connect to a remote FTP site and transfer files to and from that remote site. It also allows you to set your own machine up as an FTP server within the network. In this way, you can allow others to access the files on your system. Detailed customization, and user ID and password security means that you can control exactly who has access to which files. In combination with the IP security offered with the FTP

Software TCP/IP Protocol Stack, you can achieve an unparalleled level of security and confidence.

Printing

The FTP Software TCP/IP Network Access Suite includes a print server and a print client. The print server allows you to configure printers to be made available on the TCP/IP network for other clients to print to. These printers must be accessible to your workstation. They can be local or other network devices. As an example, you may have a printer on your desk that is attached locally to your workstation, and a high quality printer available on the existing NetBIOS network in your department. If you have correctly installed the support for these printers on your workstation, you can share the devices on the TCP/IP network and allow other users to print to those devices. You could even access them from a laptop computer that had dialed in to your TCP/IP network.

The print client can be used to print documents directly to a properly configured printer on your system. It can also be used to manage LPR printing, if the printer has been configured using the LPR protocol.

InterDrive

FTP Software′s InterDrive Client enables you to connect to resources on your network that have been shared using the Network File System (NFS). You can assign drive letters to remote hard disk volumes on machines that do not have support for NetBIOS. This is typical for UNIX-based systems such as AIX which do not generally install NetBIOS support as part of their network protocol stack. Using the InterDrive Client is very straightforward. You access resources, and map network drives through the network neighborhood just as you do with a NetBIOS network. You can also access resources on an NFS server using the Universal Naming Convention (UNC) method. You will need at least one NFS server on your network to take advantage of the InterDrive Client.

KEYView

The KEYView application is not specifically TCP/IP related. It is a universal file viewer. It supports many file types, including document, spreadsheet, pictures, HTML, and multimedia formats. It also supports compression and encoding. The compression formats include ZIP and TAR. The encoding formats supported are UUencode, and BinHex.

These features make it ideal for use with TCP/IP applications. The Internet consists of many different types of systems, and file formats. Having a viewer that can handle these many formats makes it easy to view the files and documents you are working with on the Internet. The KEYView application also installs itself as an Explorer extension.

This ensures its features are always available even when navigating through your own local system.

TNVTPlus

This advanced Telnet application allows you to connect to another remote host system, and run commands on that remote host. You can also transfer files, save a transcript of the session, and print the details. TNVTPlus supports the following terminal types for connecting to the remote host:

- VT420
- VT320
- VT52
- WYSE-60
- WYSE-50
- SCO ANSI
- IBM-PC

Many different protocols are also supported for transferring files to and from the remote host. They are as follows:

- Z-Modem
- Y-Modem
- X-Modem
- Kermit

The terminal interface is easily configurable. Settings such as color mapping, word wrap, code page, character sets, keyboard, printing, and display options are all easily set through the Telnet Connection Properties window.

Remote Utilities

The Remote Utilities are two functions in one application. The first is Remote Command. This allows you to execute commands on a remote system, and have the results displayed to you on your local system.

The second part of the application is Remote Copy. This allows you to move files to or from a remote system. In both cases, you will need to have the appropriate permissions on the remote systems to allow these procedures.

OpenScript

OpenScript is a scripting language that is similar to Visual Basic. It allows you to create detailed scripts for tasks that you perform

regularly. OpenScript is a very powerful language, and a full tutorial is outside the scope of this publication. If you are familiar with Visual Basic, or Word Basic, the transition to OpenScript will be very easy. If you have no previous experience with these products, there is ample online documentation to enable you to learn the OpenScript language.

The Network Access Suite also contains a folder called Network Tools. This folder contains the applications Network Time, Query, and Retriever. These functions are also found in the Secure Client for Windows Application set, and are described in detail in 2.1.4, "TCP/IP Stack Functions."

2.1.4 TCP/IP Stack Functions

The FTP Software TCP/IP protocol stack can be installed to replace the existing Microsoft TCP/IP stack included in Windows 95 and Windows 3.x. In a forthcoming release, there may also be a replacement for the Microsoft TCP/IP stack in Windows NT. This extra functionality is referred to as the Secure Client for Windows Applications set.

In Table 5 we provide a comparative overview of the features of the different TCP/IP protocol stacks.

Table 5 (Page 1 of 2). TCP/IP Stack Functional Comparison

Function	**Secure Client 3.0 for Windows 95**	**Microsoft TP/IP for Windows 95**	**OnNet16 2.5 for Windows 3.x**	**Microsoft TCP/IP for Windows NT**
Simple/Advanced Configuration	Y	N	Y	N
DHCP Client	Y	Y	Y	Y
IPv6 Support	Y	N	N	N
Mobile IP	Y	N	N	N
IP Security	Y	N	N	N
Dialer	Y	Y	Y	Y
Packet Trace Facility	Y	N	Y	N
Network Time	Y	N	Y	N
Ping	Y	Y	Y	Y
Traceroute	Y	Y	Y	Y?
Host	Y	N	Y	N
Finger	Y	N	Y	N
Whois	Y	N	Y	N

Table 5 (Page 2 of 2). TCP/IP Stack Functional Comparison				
Function	**Secure Client 3.0 for Windows 95**	**Microsoft TP/IP for Windows 95**	**OnNet16 2.5 for Windows 3.x**	**Microsoft TCP/IP for Windows NT**
Quote	Y	N	Y	N
Statistics	Y	N	Y	N
Administrative tools	Y	N	Y	N
NetBIOS over TCP/IP	Y	Y	Y	Y
PPP/SLIP Support	Y	Y	Y	Y
NIS Support	Y	N	Y	N
SOCKS Support	Y	N	Y	N
Java Agent Responder	Secure Listener	N	N	N

In Figure 16 you can see the objects used to start these new stack functions.

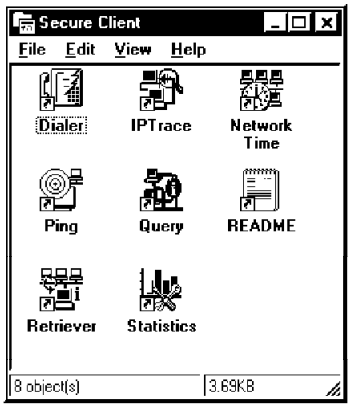


Figure 16. Secure Client for Windows Applications

Some of the following functions take specific advantage of the extra functionality available only in the FTP Software TCP/IP protocol stack, and as such are not installable if you are using Windows NT.

Dialer

The FTP Software Dialer is designed to enable you to create custom connections to your Internet Service Provider, or other remote TCP/IP server such as your corporate Intranet server. Supported protocols

are PPP and SLIP. The PPP protocol also supports PAP and CHAP authentication, as well as the older login style authentication.

IPTrace

With this powerful diagnostic tool, you can determine if there are problems with your network. It gives a running display of the network traffic, and allows you to capture that data, and interrogate the packet information.

Ping

Ping is a useful tool for determining the status of the link between two systems on an internetworked environment. Because the Ping application uses a protocol very low in the stack, it can be used to determine the status of the underlying network layer.

For example, if you cannot Telnet to a remote host, but are able to ping that same host, you could determine that the routes and physical connections are available, and the problem is probably in the application layer.

As well, if you can ping a remote host by its IP address, but not by using its fully qualified hostname, then you have either configured the domain name server incorrectly, the server is not functioning, or the hostname is not registered with the server.

There are many other examples of using the Ping application to determine the network status. For more information, refer to the online documentation or a system management manual.

Statistics

This diagnostic utility will also help resolve problems that you may be having with your TCP/IP installation, or network status. To use the Statistics application, create a session that contains sets of views from the following list:

- ARP
- Connections
- ICMP
- Interface
- IP
- Memory
- Name Resolution
- Routing
- TCP

- UDP

Along with these views, the following can be graphed, and added to the diagnostic sessions:

- ICMP Packets Received
- ICMP Packets Sent
- IP Packets Received
- IP Packets Sent
- Memory Allocated
- Memory in Use %
- TCP Segments Received
- TCP Segments Retransmitted
- TCP Segments Sent
- UDP Packets Received
- UDP Packets Sent

If you require any specific information on the usage of the information these statistics present in determining your network status, it is suggested that you purchase a separate systems management manual.

Note: Windows NT provides some of the aforementioned utilities, such as Ping, Netstat and the System Performance Monitor, matching some, but not all, of the functionality contained in the Ping and Statistics applications. Windows NT also provides a Dialer application capable of PPP connections.

The following three applications are also available under Windows NT:

Network Time

The Network Time application allows you to configure your workstations so that they synchronize their system time with that of a known time server on the network. You can configure the Network Time application to synchronize the system time at each startup, or at regular intervals.

Query

Query presents the option to perform the following network requests:

- Finger
- Whois
- Quote

- Host
- DNS
- NIS

The information is presented in an easy-to-understand format, and can be logged to a text file for archive, or further study. An example of the easy-to-use interface and the results it returns can be seen in Figure 17.

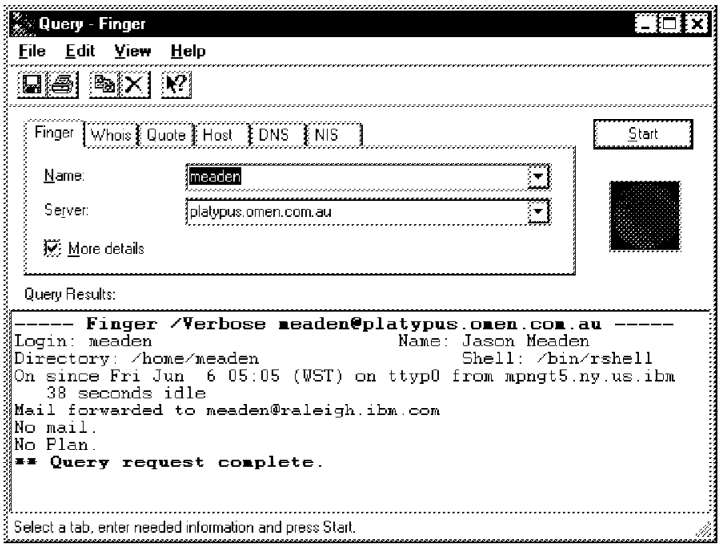


Figure 17. Network Access Suite - Query Application Interface

Retriever

This useful tool is for gathering information about your system that your network administrator, or technical support staff may require to diagnose any possible system problem you may be experiencing.

The types of information it gathers includes system information such as:

- Basic system configuration
- Environment variables
- Application information
- Type of network card and drivers installed
- Registry information
- Installation logs

This information is saved to a text file which you then send to the appropriate technical support.

2.1.5 Custom Install Manager

Custom Install Manager allows you, as administrator, to set up installation options for clients on your network based on individual or group requirements. Once you have planned the roll out of the FTP Software within your enterprise, you create install options based on the needs of groups, or individuals within the company.

You may have a marketing unit that requires only the connectivity of TCP/IP without the need for the FTP server, Print server, or other advanced features. You would create a custom installation set for that group that excluded those functions. On the other hand, your technical department will probably require those advanced services, and the extra tools such as Ping, and Query. You create a separate custom installation set for that group.

Within each distinct group, you may have an individual who requires a slightly different installation. For example, one employee in the marketing unit may require the FTP Server to make certain documents available for the rest of the enterprise. With Custom Install Manager, you can create a custom install set for just that one user.

2.2 Netscape Navigator

The Internet has existed for some time, and always contained vast amounts of information of interest to even the general population. The reason it long remained the realm of the military, scientists, and university students, was that it was difficult to use, and required a number of different tools that were complicated to configure.

The overwhelming popularity and explosive growth of the Internet can be attributed to the World Wide Web. It takes the wealth of information available on the Internet, and makes it easy to access, easy to use, and fun to explore. The user friendly interface of the Netscape Navigator makes it the single tool you require to access the disparate information resources available on the Internet today.

The rich multimedia now being used in WWW pages have created enormous potential for exciting, interactive Internet advertising, and information presentation. Powerful search engines on large online databases, coupled with the interface of Netscape Navigator give you the ability to find exactly what you are looking for, without having to wade through irrelevant data. This makes the information easy to find, thus saving valuable time.

2.2.1 Web Browser

The features of the World Wide Web are increasing rapidly, with the introduction of important extensions to HTML, the language used to write Web pages. Most recently, the widespread adoption by the industry of Java as a tool to create exciting, easy-to-use, and importantly, cross-platform applications for the Internet user has created another powerful reason to be making use of the World Wide Web. To take advantage of these features a Web browser that is up-to-date, and supports the most recent innovations is required.

The IBM eNetwork Communications Suite provides this in the form of Netscape Navigator. Netscape Navigator includes support for Java applets, and JavaScript. It also supports recent enhancements to the HTML language used to create Web pages. The pages you view with Netscape Navigator will be accurate representations of the original, and will allow you to take full advantage of the information they contain. These features have made Netscape Navigator the industry leader in Web browser software.

2.2.2 Netscape Plug-Ins

Certain types of data cannot be easily represented using HTML, or are too difficult to convert into Java. For this reason, they require specially designed Netscape plug-ins. These are external modules that are automatically called by Netscape as required. They provide the extra flexibility required to present the information in a usable format.

The IBM eNetwork Communications Suite provides three of the most popular Netscape plug-ins as part of the package.

2.2.2.1 FirstFloor Smart Bookmarks

The FirstFloor Smart Bookmarks package is designed to help you organize and track your favorite World Wide Web sites. It uses agent technology to keep up-to-date references to your favorite sites. It can tell you when a page has been updated, or changed.

2.2.2.2 Adobe Acrobat Reader

Adobe Acrobat Reader allows you to view files saved as Portable Document Format (PDF) within your Netscape Navigator. The PDF format is very popular, it allows the information to be presented in an easy-to-use and read format. It includes text formatting not available in standard HTML, and provides the ability to search, resize, and print the data.

2.2.2.3 IBM techexplorer Hypermedia

The IBM techexplorer Hypermedia Browser is a powerful tool for displaying, and formatting mathematical, scientific, and technical symbols within World

Wide Web documents. It is based on, and includes a large subset of the TeX and LaTeX markup languages.

2.2.3 Netscape Mail

An important function of the Netscape Navigator is e-mail. This allows your users to communicate with other users on your Intranet, or with external users on the Internet.

The Netscape Mail component is not limited to only sending plain text messages. It can also be used to send files as attachments to others. You can send presentations, documents created with your word processor, archives of files and data. The file will arrive at the recipient's system in the format you originally sent it in. This means your document, or other data does not lose formatting information included with the original document.

2.2.4 Netscape News

Netscape Navigator also includes support for Newsgroups. Newsgroups, often referred to as UseNet, are made up of several thousand special interest discussion groups. These groups cover almost every topic you can imagine. They include groups for discussing software, hardware, and other technical issues. Thousands of hobbies, sports and other recreational activities are also covered.

Netscape Navigator presents these groups in a simple-to-use fashion. The groups can be sorted in a variety of ways to make it easier for you to follow. The unread messages are highlighted so that next time you start Netscape News, you do not read the same messages again. The messages can also be threaded. This makes it easier to follow a particular discussion through the forum.

2.3 IBM Personal Communications for Windows

IBM Personal Communications for Windows is a powerful package designed to solve your host connectivity problems. Personal Communications for Windows is a host terminal emulation package that provides 5250 and 3270 emulation. You can connect to AS/400 and S/390 systems, establish client/server connections using CPI-C and APPC (LU 6.2), perform file transfer operations, and set your local workstation printer up as a host printer.

Personal Communications allows you to take advantage of High Performance Routing (HPR) over token-ring and Ethernet connections. This gives you reliable routing around network outages, congestion control and data integrity.

AnyNet allows applications to communicate over different network transports, and interconnected networks without modification. You can reduce the number of transport networks, thus reducing the complexity of the network. The AnyNet functionality in Personal Communications allows SNA applications such as 3270 and 5250 emulators, and APPC and CPI-C applications to communicate over a TCP/IP network.

Note: AnyNet SNA/APPC over TCP/IP is currently supported with Personal Communications for Windows NT and Windows 3.x. Future versions of Personal Communications will also support Windows 95.

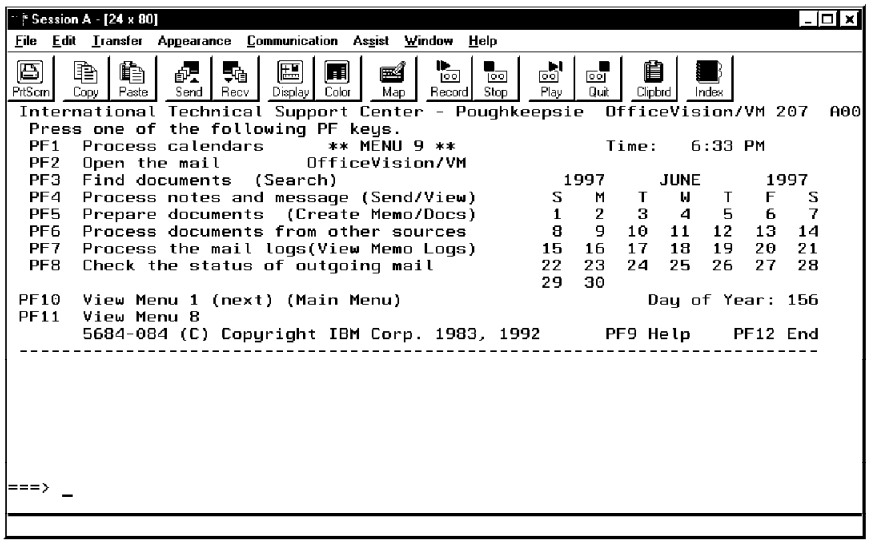


Figure 18. Personal Communications for Windows

Personal Communications for Windows as included in this release of the IBM eNetwork Communications Suite, comes with the full range of Personal Communications administrative and problem determination aids, APPC and CPI-C utilities, the Personal Communications library, and emulator utilities such as ZipPrint and CM Mouse.

For a full list of available connectivity options with IBM Personal Communications for Windows, refer to the *eNetwork Communications Suite for Windows Installation Guide* in the section titled *"*Connecting with Personal Communications*"*.

2.3.1 CM Mouse

CM Mouse is an extension to the Personal Communications application. It allows you to use your mouse to navigate the host session. You do this by

creating macros that you assign to mouse actions, or a pop-up menu that you can use with your mouse, or other pointing device.

2.3.2 Library Reader for Windows

The IBM Library Reader for Windows is a graphical viewer for documents created in BookManager format. BookManager files are hypertext documents that allow you to read, search, print, and manipulate the information they contain.

You can bookmark pages to follow up later, and for easier reference. You can also makes notes which you attach to a page of information for later use, much like tagging a page in a normal book with a yellow post-it sticker.

The IBM Library Reader for Windows allows you to organize your online books into bookshelves. You can keep related publications in separate bookshelves to make them easier to locate.

2.4 Lotus Notes Mail Client

Lotus Notes has long been recognized as the leader in groupware applications. It is a powerful application that will meet all your groupware needs. The Lotus Notes family is a scalable solution. If your enterprise consists of several dozen workstations that require nothing more than a powerful, full featured e-mail application, then the Lotus Notes Mail Client will meet that demand.

If your enterprise is a much larger organization that needs powerful e-mail access and the ability to run Notes applications, then Notes Desktop will give your users this ability.

Your enterprise may be a global company with tens of thousands of workstations, hundreds of mobile users, and staff all over the world. You require the ability to be able to share your data within the organization, and with your suppliers, and customers. You want all the power of Lotus Notes Desktop, calendaring and scheduling, and the ability to publish your Notes databases on the Internet. For this, you require the full product known as Lotus Notes.

Your enterprise will require a Lotus Domino Server to take advantage of the features in the Lotus Notes Mail Client. If you require the additional features of the other Lotus Notes products, they are available under a separate license agreement, and you should contact your local IBM sales representative for more information.

2.5 Other Members of the eNetwork Software Family

The IBM eNetwork Communications Suite is a member of the eNetwork Software Family. The eNetwork Software Family is a range of client/server applications that provide the tools you need for your information access, collaboration, and electronic commerce.

Some of the other components available as part of the eNetwork Software Family are described in the following sections:

2.5.1 eNetwork Communications Server

eNetwork Communication Server is an enterprise class solution for connecting diverse applications and network environments. It provides support for key client/server APIs such as APPC and CPI-C. Communication Server is available for AIX, OS/2, Windows NT, and OS/390.

2.5.2 ARTour

Advanced Radio Communications on Tour (ARTour) is a wireless client/server interface for users on the move. It makes network resources available to mobile users without modification to their existing network-enabled software. Features that make ARTour ideal for mobile computing include:

- Wireless connectivity allowing mobile users to take full advantage of the same network resources they would have in the office
- Data reduction which improves response times and bandwidth usage
- Encryption to ensure security, and protect data privacy

2.5.3 Host On-Demand

IBM Host On-Demand is a Java-based solution supporting Telnet3270 protocols. It enables clients to connect to your centralized host applications using any Java-enabled platform. This platform could include the users existing Java-enabled Web browser.

Some of these applications are used in our corporate scenarios. If you require more information on the full range of products available as part of the eNetwork Software Family, refer to the URL:

`http://www.networking.ibm.com/eNetwork/enethome.html`.

Chapter 3. Installation and Configuration

In this chapter, we describe the installation and configuration of the IBM eNetwork Communications Suite on the supported platforms. The three Windows platforms supported by this release of the IBM eNetwork Communications Suite are:

- Windows NT 4.0
- Windows 95
- Windows 3.1 / Windows for Workgroups

The installation procedure across each platform is very similar. This makes your job of installing the product across multiple platforms very easy. However, if you are going to be installing on multiple platforms, we suggest you read the installation guidelines for each platform, as there are some minor differences.

The following information should be read in conjunction with the *eNetwork Communications Suite for Windows - Installation Guide*, GC31-8528-00 included with the IBM eNetwork Communications Suite.

3.1 Installing on Windows NT

To begin the installation of any of the components of the eNetwork Communications Suite, place the IBM eNetwork Communications Suite CD-ROM into the drive. Windows NT should automatically start the setup application, and you will see an installation screen similar to Figure 19 on page 62. Since the Windows NT version does not yet allow you to install the FTP Software TCP/IP protocol stack, that option will not be available.

If you are installing from a LAN CD-ROM, or you have disabled autorun, then you will need to start the setup program manually. To do this, click on the **Start** button in Windows NT, then select **Run**. In the field marked Open:, type `X:SETUP.EXE` where `X:` is the drive letter of your CD-ROM or shared device.

If you have reviewed your hardware and software requirements, and you have decided which components you are ready to install, then you should now be ready to continue to the installation of the individual components. There is no requirement to follow the installation order that we have set here. However, we present screen captures and other examples to highlight important steps in the installation and configuration process. To avoid confusion, we suggest you follow the same installation order as we have.

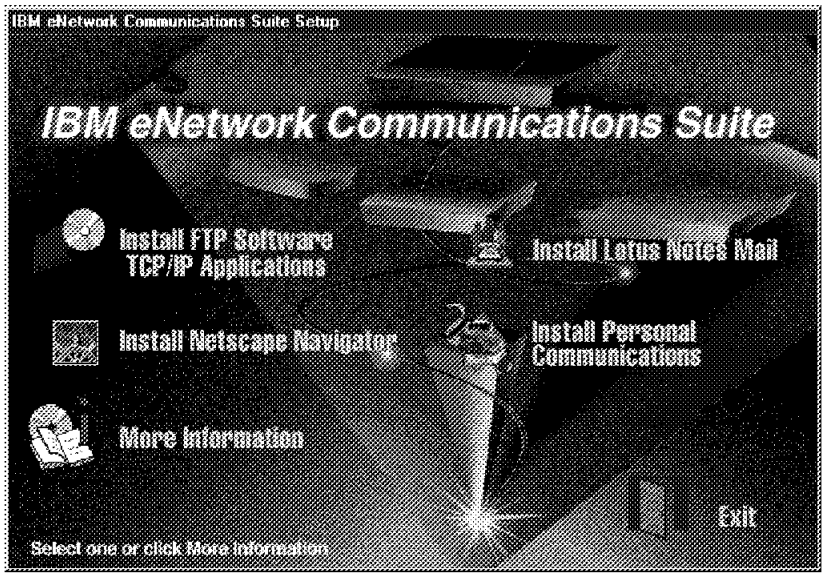


Figure 19. IBM eNetwork Communications Suite Setup Panel (Windows NT)

3.1.1 Prerequisites

Before commencing the installation of the IBM eNetwork Communications Suite for Windows NT, you should be aware of some prerequisites for the product. By ensuring that you meet these requirements now, you will save yourself a great deal of time and effort in the future.

3.1.1.1 Software Requirements

The installation of the IBM eNetwork Communications Suite for Windows NT requires the following software:

- Microsoft Windows NT 4.0
- Lotus Notes Server 3.0 or higher, available on the network

Windows NT 4.0 can be either the Server or the Workstation release. The Lotus Notes server is only required if you are planning to install the Lotus Notes Mail Client. The Lotus Notes server does not need to be installed on the same workstation, but should be accessible from the workstation via the existing network infrastructure.

3.1.1.2 Hardware Requirements

Before beginning the installation of the IBM eNetwork Communications Suite, ensure that your system has or exceeds the following minimum hardware requirements.

- Intel 33 MHz 80486 processor
- 16 MB of system RAM
- 90 - 120 MB of free disk space for entire suite
- Supported CD-ROM drive and drivers
- LAN adapter (with device drivers supporting NDIS or ODI), in case of LAN attachment
- Hayes-compatible modem capable of 9600 bps attached to standard switched telephone line, in case of dial-up attachment
- Supported audio card and drivers

It should be noted that the above list represents the minimum hardware requirements of the eNetwork Communications Suite. If you are installing the complete suite, then we strongly recommend you have at least 32 MB of system RAM, and an Intel Pentium-based processor.

Some of the components of the minimum hardware requirement list are optional. The LAN adapter card is only needed if you are using a LAN connection as part of your network. A modem is not required if you are not taking advantage of the dial-up facilities available in this suite. The audio card is only necessary if you wish to utilize the multimedia features of the IBM eNetwork Communications Suite. You do not need a CD-ROM in the machine you are installing the IBM eNetwork Communications Suite on. You can use a shared CD-ROM on your network. If so, then you will need to map the network CD-ROM drive to a local drive letter, and install from there. Do not start the installation through the Network Neighborhood method.

3.1.2 Installing the Windows NT TCP/IP Protocol Stack

At the time of writing, you have to use the protocol stack shipped with Windows NT, because the FTP Software stack is not currently available in the Windows NT version of the eNetwork Communications Suite. A future release of the IBM eNetwork Communications Suite for Windows NT may include a native TCP/IP protocol suite from FTP Software.

You can check to see if TCP/IP is installed on your system by looking at the Protocols tab of the Network object from Control Panel. To view this tab, click on the **Start** button, then select **Settings**, and then **Control Panel**. When the Control Panel folder opens, double-click the **Network** object to open the Network Settings, then click on the **Protocols** tab. You should see a Network Settings application that looks similar to Figure 20 on page 64. You may have other protocols also loaded and they will appear in this section, too.

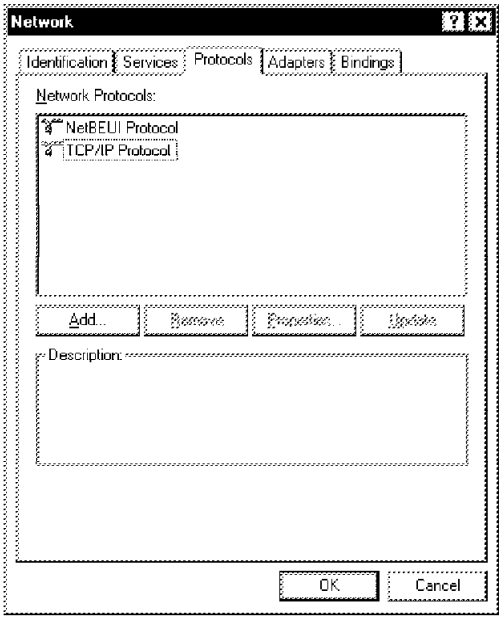


Figure 20. Network Settings Application

If you are having trouble installing or configuring the Microsoft TCP/IP protocol stack, please contact your system administrator, or your local Microsoft Technical Support office.

3.1.3 Installing the FTP Software TCP/IP Applications

The following instructions guide you through the process of installing the FTP Software TCP/IP applications component of the eNetwork Communications Suite.

1. From the IBM eNetwork Communications Suite Setup panel, click on **Install FTP Software TCP/IP Applications**. This will give you the Network Access Suite Setup Wizard. Network Access Suite is the name of the FTP Software TCP/IP applications suite in Windows NT. You should read the brief welcome message, and the installation notes for last-minute changes to the installation procedure. Once you have done this, click on the button marked **Next** to continue with the installation.
2. The installation wizard will now ask you what type of installation you wish to perform. The choices available to you are:

   Full This will install all components of the Network Access Suite onto your system.

Custom This option will give you the opportunity to select which components of the Network Access Suite you wish to install.

Administrator Select this option to install the files onto a server. This will allow you to install the FTP Software TCP/IP Application Suite and Protocol stack onto other client machines.

3. If you select the **Full** option, you will only be asked which directory you wish to place the data files in. Change the destination directory, or accept the default by selecting **Next**.

   If you selected the **Custom** option, you will be asked for a destination directory. Change the selection, or accept the default as above. The installation program will now ask you to choose which components to install. You should choose only those options you require for the workstation you are installing onto. For details on the usage of a particular component, refer to Chapter 2, "Product Overview" on page 45. Once you have made your selection, click **Next** to continue.

   If you selected the **Administrator** option, you will be prompted for the destination directory. Change this directory, or accept the default.

4. The installation program will now display a list of the components it is going to install. You can change the selection by selecting **Back**. To continue with copying the files to your hard disk, click **Next**. The installation program will now copy the files to your hard disk and update the shortcuts and registry information.

5. Once the copying is complete, it will give you the option to restart your computer. Select **Yes** and then wait for the system to reboot.

Once your system has rebooted, you can continue with the installation of the other components of the eNetwork Communications Suite.

3.1.4 Installing Personal Communications for Windows NT

The installation of the Personal Communications product has many options that may not be required in every installation scenario. If you are not familiar with all these options, we suggest you check with your system administrator for the correct settings and options for connecting to your host.

If you require detailed information on the configuration of Personal Communications, refer to Appendix C, "Related Publications" on page 301 for information on other IBM publications available.

3.1.4.1 Installation Steps

To install the full product you need about 31 MB of free disk space on your hard drive. Follow these steps carefully to successfully install the Personal Communications product:

1. Start the eNetwork Communications Suite Setup panel as described in 3.1, “Installing on Windows NT” on page 61.
2. Click on **Install Personal Communications**. The Setup Wizard will bring up the IBM Personal Communications Setup dialog box, where you can select the components you want to install:
   - IBM Library Reader is an online documentation (book) viewer for the BookManager-formatted files.
   - Netware for SAA Client is an alternative emulator connectivity option. Refer to your system administrator to see if you require this option to be installed.
   - Personal Communications is a full-function 3270 and 5250 terminal emulation package.
3. Once you have chosen the products you wish to install, click on **Next**.
4. Check that the components you have chosen are listed in the Current Settings section of the confirmation panel, and click **Next** if they are correct.
5. If you have chosen to install the IBM Library Reader, that part of the installation will be started first. If you have not elected to install the Library Reader, you can skip these next few steps and go to step 14 on page 67. Read the brief installation instructions, then choose **Continue**.
6. Click on **OK** to confirm the installation of the Library Reader.
7. The next dialog box will ask you which components of the Library Reader you wish to install. You will need to select at least the Program Files. If you are unfamiliar with the Library Reader, we suggest you also install the online documentation.

   At this dialog box, you can also elect to change the default installation directories. Once you have made your selections, click **Install** to continue.
8. The installation program will now commence copying the files to your hard drive. When the installation program prompts for startup defaults, you can change the settings, or accept those defaults by selecting **OK**.
9. When the installation program has finished copying the files it requires, it will advise you to reboot the machine or run your AUTOEXEC.BAT file. Click the **OK** button, then **Exit** to close the Library Reader installation program.

10. The next dialog box will again advise you to reboot Windows NT. At this point, select the radio button for **Yes, I want to restart my computer now**. Then click **OK**.
11. Once the system has rebooted, start the IBM eNetwork Communications Suite Setup panel again, and select **Install Personal Communications**.
12. Once again the setup wizard will ask which components you wish to install. Do not select the IBM Library Reader again. Click on **Next** to continue the installation.
13. Click on **Next** to reconfirm your selections.
14. You will now be at the Personal Communications installation wizard. Read the information on this panel, and click **Next** to continue.
15. Select the installation type you want:
    - Run Personal Communications from my workstation: This will result in a stand-alone installation, with all the files copied to your local drive.
    - Run Personal Communications from a server: This will install the program files from a shared server drive, keeping only your session profiles, keyboard and macro files and other configuration information on your workstation or in a personal directory on a server.
    - Install Personal Communications on a server: All the files on the CD-ROM are copied to the network drive that you specify. You cannot choose any installation options.

    Click on **Next** to continue.
16. Specify the functions you want to install:
    - 3270: Your workstation can emulate a S/390 terminal (display and/or printer). The emulator APIs (EHLLAPI, PCSAPI, DDE and SRPI) are installed.
    - 5250: Your workstation can emulate an AS/400 terminal (display and/or printer). The emulator APIs are installed.
    - Communication APIs: The APIs include the protocols that let you use SNA communications. These protocols include IEEE 802.2, SDLC, SNA-over-Async, and Twinaxial attachments, and the APPC and CPI-C programming interfaces.

    Click on **Next** to continue.
17. Choose the installation directory. Click on **Next**.

18. Choose to install a subset or all of the emulators functions, as explained below:

    Full Installs all the functions of the emulators you chose, including the optional utilities, the help files and publications, all the printer-definition files and tables, and the sample programs. The Communications APIs without the associated help file or publications are installed even if you did not choose them in the Choose Components window. You need the SNA protocols to run the emulator. For example, if you use only TCP/IP, choose **Custom** and deselect the APIs.

    Custom Allows you to choose which subcomponents to install when the Custom Installation window appears.

    Note: If you want to use Cyrillic, Greek or Turkish language support, you must choose Custom and then select **Language choice** in the Custom Installation window.

    Minimal Installs only the main functions of the emulators you chose, including the help file but not the publications. If you make this choice, you must have protocols installed other than those provided by the Communications APIs, for example a TCP/IP protocol stack.

    Click on **Next** to continue.

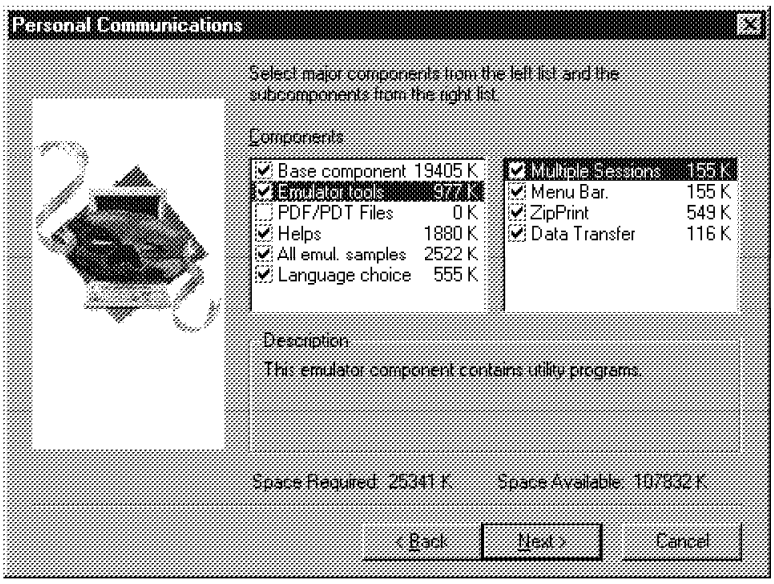


Figure 21. Personal Communications Component and Subcomponent Selection (Windows NT)

19. If you chose to do a custom installation, at this point you can select the components and subcomponents you wish to install, as shown in Figure 21. Make your selections and click on **Next**.

20. The wizard is ready to install the product now. You have a chance to change the destination directory and the required disk space is displayed. You can go back to the function selection window (step 19) by unchecking Continue with installation. If all settings are correct, click on **Next** to continue.

21. Accept the default program folder name or specify another one by typing it in, or by selecting from the list. Click on **Next** to continue.

22. Click on **OK** on the two information boxes. You will be asked whether you want to install the Personal Communications IEEE 802.2 interface for the LAN. Follow the instructions on the screen to install this interface (see Figure 22).

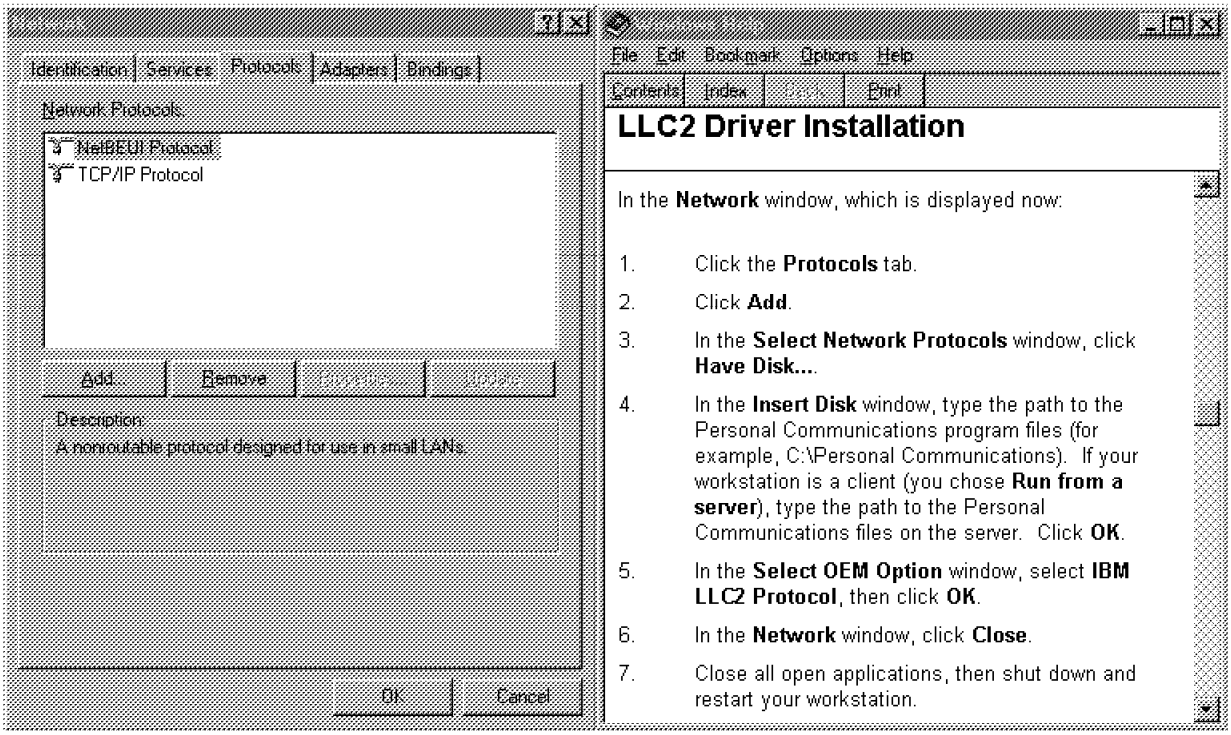


Figure 22. Personal Communications LLC2 Driver Installation (Windows NT)

23. Close all your applications and reboot your computer.

You can start your first emulator session by selecting **IBM Personal Communications** from the Windows NT Start menu, and then selecting **Start or Configure Session**.

3.1.5 Installing Netscape Navigator for Windows NT

The installation of the Netscape Navigator consists of a number of separate steps:

1. Installation of Netscape Navigator
2. Configuration of Netscape Preferences
3. Configuration of Netscape Mail and Netscape News
4. Installation of Netscape Plug-Ins

We explain each of the above steps in detail in the following sections.

3.1.5.1 Installation of Netscape Navigator

To begin the installation, you should start from the IBM eNetwork Communications Suite Setup panel as described in 3.1, “Installing on Windows NT” on page 61. From there, follow these steps to install the Netscape Navigator:

1. Click on **Install Netscape Navigator**. This will start the Netscape Navigator Setup program. Read the brief welcome message, then click on **Next** to continue.
2. Your next option is the destination directory. Click on **Browse** to change the destination, or click on **Next** to accept the default.
3. You will now be asked if you wish to install the CoolTalk application for Netscape Navigator. If you have a properly configured sound card with a suitable microphone, you can choose to install this option as well. To do so, click on **Yes**. If you do not wish to install the CoolTalk application, then click **No** and continue with the installation of the Netscape Navigator. The installation program will now commence copying the files to your hard disk.
4. If you chose to install the CoolTalk application, you will be asked if you wish to enable the CoolTalk Watchdog. This program will listen for incoming connections from other users who are using CoolTalk, and automatically start the CoolTalk application. If you have a permanent connection to your network, you should select this option.
5. Once the files have been copied to the hard disk, the installation program will ask if you wish to connect to the Netscape homepage to continue with the installation. Select **No**, as we will be explaining the configuration of the Netscape Navigator in this section.

6. The installation program will now ask if you wish to view the README file. You should choose **Yes**, as it may contain important last-minute information not found in this publication or the program documentation.
7. Click on **OK** once the setup has completed. This will close the installation program, and give you the opportunity to view the README file.
8. Close the README file once you have finished reading it.

Now that the above steps have been completed, you should have a folder open on your desktop that looks similar to Figure 23.

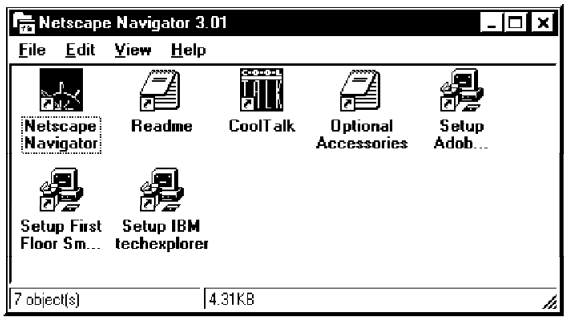


Figure 23. Netscape Navigator Folder (Windows NT)

If you have a direct connection to the Internet, you will now be able to use the Netscape Navigator without any further configuration. Most of the general preferences are simply cosmetic changes, and do not require alteration. If you require information on these settings, select **Options/General Preferences** and press F1, or click on **Help**.

3.1.5.2 Configuration of Netscape Preferences

Double-click on the **Netscape Navigator** object to start the Netscape Navigator. The application should start, and load an introduction page that welcomes you to the eNetwork Communications Suite. You can read this information now, or the next time you start the Navigator.

If you are connected to the Internet via a proxy server or other firewall device, then you need to configure this in the Netscape preferences. If you are not sure, then contact your system administrator who can give you the correct details. As an example, we show you how to configure the Netscape Navigator to use a proxy server. We assume the details of the proxy server are as follows:

Proxy Server: proxy.au.ibm.com
Port: 80

1. From the Netscape menu, select **Options** with your mouse. Then select **Network Preferences** from the drop-down menu.
2. Click on the **Proxies** tab of the Preferences notebook.
3. Click the radio button for **Manual Proxy Configuration** and then select **View**.
4. In the Manual Proxy Configuration notebook, fill in the name of the proxy server next to those protocols that the proxy server supports. In our case, it is FTP and HTTP. Type in the port number as well.
5. Generally, if you have a proxy server, it is only required for sites outside of your internal network. Check with your system administrator, but in most cases, you can tell Netscape not to use the proxy server for connecting to machines within your own domain. If so, place the domain name of your network into the section called No Proxy For. In our example, this was au.ibm.com. Once completed, you should have a configuration similar to Figure 24.
6. Click on **OK** to apply these changes. Click on **OK** again to close the Network Preferences notebook.

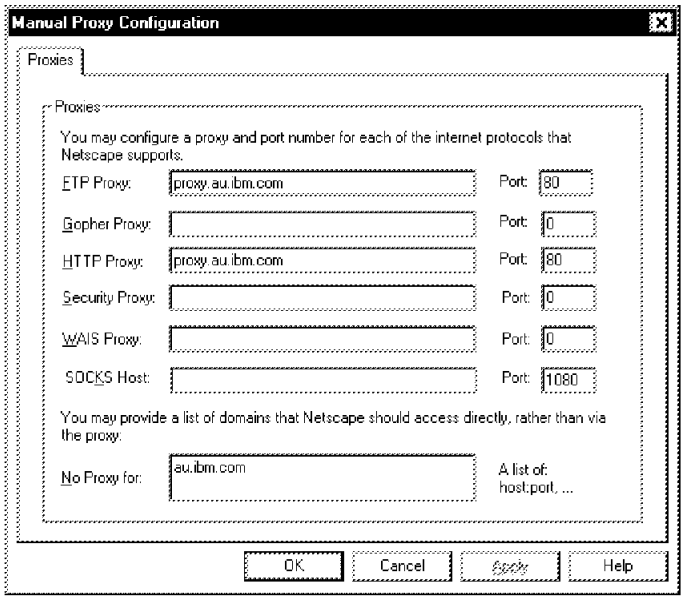


Figure 24. Manual Proxy Configuration Setup (Windows NT)

3.1.5.3 Configuration of Netscape Mail and Netscape News

To configure the Netscape Mail and News functions, you will need some information from your system administrator. Of the many options that can be configured, this is the most basic information required. If you do not have any or all of this information, you will not be able to use the Netscape Mail or Netscape News effectively.

SMTP Mail Server This is the fully qualified hostname of the server that you will be using to send your new e-mail messages to for delivery.

For example: mail.raleigh.ibm.com

POP3 Mail Server This is the fully qualified hostname of the server that you will collect your new e-mail messages from. Often, this will be the same as the SMTP mail server.

For example: pop3.raleigh.ibm.com

POP3 User Name This is your user ID for the POP3 mail server. While it is often the same as the first part of your e-mail address, it does not need to be.

For example: meaden

POP3 Mail Password This is your password for collecting your e-mail from the POP3 mail server. It will probably be assigned to you by the system administrator.

For example: password

NNTP News Server This is the fully qualified hostname of the news server you will use to send and receive messages from the Internet newsgroups.

For example: news.raleigh.ibm.com

Email Address This is your full e-mail address that you will use for electronic mail on either the Internet, your Intranet, or both.

For example: meaden@raleigh.ibm.com

Your Name This is generally your first and last name. If the same e-mail address is being used by many people in the same section, it will often represent the name of the department, or their purpose.

For example: Software Support

Once you have these details, start the configuration with the following steps:

1. Select **Options** from the Netscape menu. From the pull-down menu, select **Mail and News Preferences**.
2. Select the tab marked **Servers** from the Preferences notebook.
3. In the field called Outgoing Mail (SMTP) Server type in the name of your mail server.
4. Press the Tab key, or use the mouse to move to the next field called Incoming Mail (POP3) Server. In this field, type the name of your POP3 mail server.
5. Press the Tab key, or use the mouse to move to the next field called POP3 User Name. In this field, type your POP3 mail user ID.
6. Press the Tab key, or use the mouse to move to the field called News (NNTP) Server. In this field, type the name of your news server.
7. Once those details are complete, your Servers Preferences should look similar to Figure 25. Select the **Identity** tab from the Preferences notebook to continue the configuration.

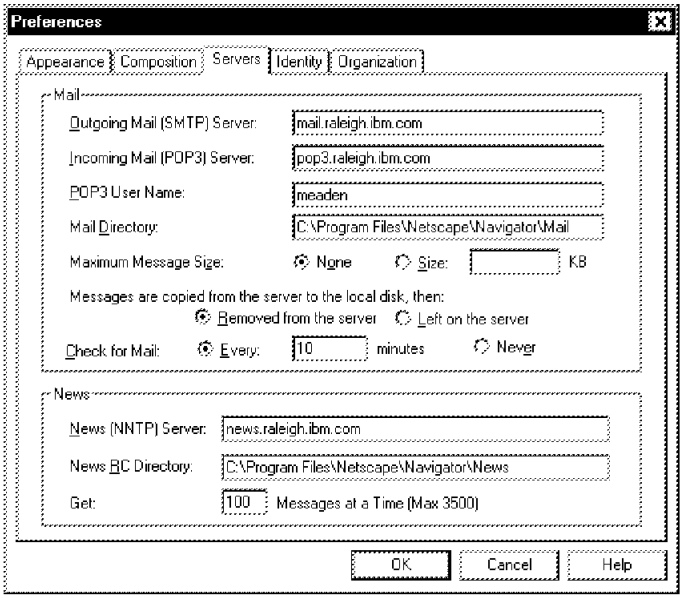


Figure 25. Netscape Preferences - Servers (Windows NT)

8. In the field titled Your Name, type in the user name, or other name you have selected for this e-mail account.
9. Use the Tab key or the mouse to move to the next field called Your Email. In this field, type the e-mail address of the account.

10. Double-check that your configuration looks similar to Figure 26 on page 75. If so, select **OK** to save the changes.

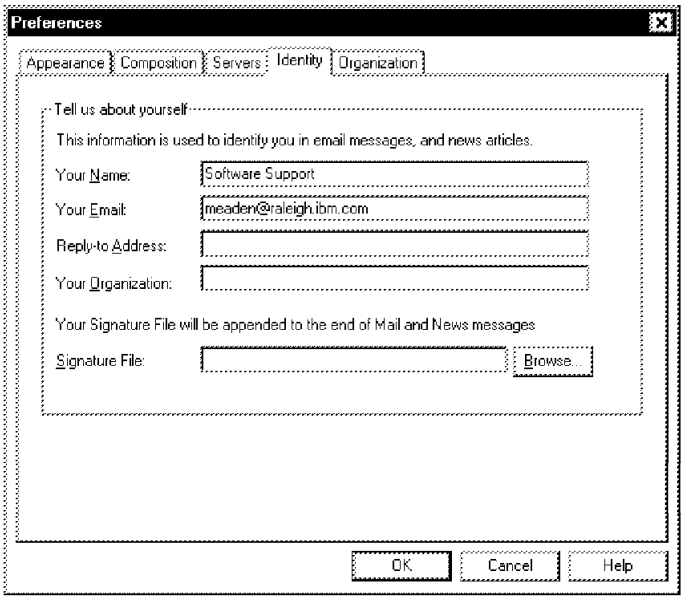


Figure 26. Netscape Preferences - Identity (Windows NT)

Your Netscape Mail and Netscape News are now properly configured and ready to run.

3.1.5.4 Installation of Netscape Plug-Ins

To install the Netscape plug-ins, ensure the IBM eNetwork Communications Suite CD-ROM is in the CD-ROM drive. The following information is for installing the Adobe Acrobat Plug-In for Netscape Navigator:

1. From the Netscape Navigator folder (Figure 23 on page 71) double-click on the **Setup Adobe Acrobat** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Read the Adobe license carefully, and choose **Accept** if you agree to the terms of the license. If you choose **Decline** to indicate you do not accept the license agreement, the installation will end.
4. The installer will now ask for an installation directory. Accept the default directory by selecting **Install**. You can change the destination directory by typing over the existing installation path with your preferred location.

5. Click on **OK** when you receive a notification about the registration procedure.
6. At the prompt for Name and Organization, you should enter the details of yourself, the license owner, or the end user. Select **OK** when complete.
7. The Adobe Acrobat Installer will now commence copying the files to your hard disk. Click on **OK** once the installation has completed.

The Adobe Acrobat Reader Plug-In has now been successfully installed.

To install the First Floor Smart Bookmarks plug-in, follow these instructions:

1. From the Netscape Navigator folder (Figure 23 on page 71) double-click on the **Setup First Floor Smart Bookmarks** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Once the setup wizard has started, read the brief welcome screen and click **Next** to continue.
4. At the User Information section, you should complete the details in the same way as for the Adobe Acrobat installation. If the section marked Serial is not already filled in, check your product documentation for this number. If it is already filled in, then leave the current value as is.
5. Confirm your earlier input by selecting **Yes**, or change the details by selecting **No.**.
6. You will now be asked which type of installation you wish to perform. For most users, the default Typical installation will be sufficient, and you should select that option. Click on **Next** to continue.
7. If the destination directory you chose does not yet exist, the installation application will ask if it can create it for you. Choose **Yes** and continue with the installation.
8. The installation will now ask you which Internet Browser you are using. The default selection is **Netscape 2.0 or later**. Do not change that setting, as this is the correct choice. Click **Next** to continue the installation.
9. The installation wizard will now double-check the options you selected. If you have nothing you wish to change, press **Next**.
10. The installation wizard will now copy the files to your hard disk.
11. Once it has finished copying the files, the installation wizard will advise you it has completed, and give you the option to view the README. Select **Finish** and the installation will end and present you with the

application README file. Read through this file in case there have been any last-minute changes.

The First Floor Smart Bookmarks Plug-In has now been successfully installed.

The final plug-in included with the IBM eNetwork Communications Suite is the IBM techexplorer Plug-In. To install this product, follow these steps:

1. From the Netscape Navigator folder (Figure 23 on page 71) double-click on the **Setup IBM techexplorer** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Once the setup wizard has started, read the brief welcome screen and select **Next** to continue.
4. Read the license agreement carefully, and choose **Yes** if you agree with the terms and conditions.
5. The setup wizard will now ask for an installation path. You can change the default by clicking **Browse** or accept the default by clicking **Next**.
6. If the selections on the next screen match your preferred settings, then select **Next**.
7. The setup wizard will then copy the files to your hard disk, then open the README file.
8. Read this information carefully, in case there has been any last-minute changes. Close the README once you have finished viewing it.
9. Select **Finish** from the setup wizard.

The installation of the IBM techexplorer is now complete. All these plug-ins are automatically loaded when the Netscape Navigator is started. If the Netscape Navigator encounters a WWW page that requires one of the plug-ins, they will be invoked automatically.

3.1.6 Installing Lotus Notes Mail Client for Windows NT

This section assists you in installing the Lotus Notes Mail Client. If your organization has access to a Lotus Notes server, and you wish to take advantage of the powerful e-mail capabilities of the Lotus Notes Mail Client, read this section carefully.

1. Start the IBM eNetwork Communications Suite Setup panel as described in 3.1, “Installing on Windows NT” on page 61, click on Install Lotus Notes Mail.

2. Read the Software Agreement carefully, and click on **I Agree** if you accept the terms of the agreement.

3. The next screen is a welcome panel. In the fields provided, type in your name, and the company name. Click on **Next** to continue with the installation.

4. The installation wizard will ask you to confirm the information you typed in on the previous panel. Click on **Yes** to confirm the information, or take this opportunity to go back and correct it.

5. Select **Standard Install** from the Install Option dialog. You can change the default installation path from this dialog by clicking **Browse** next to the program or data folder path. You can select **Next** to continue the installation.

6. The installation wizard will now ask you which program folder you want the application shortcut installed to. Accept the default, highlight a new selection, or create a new folder. Once you have made any changes, select **Next**.

7. Before copying the files to your hard disk, the installation will ask that you shut down any other running applications. Other applications may have files open that are replaced by the installation of the Lotus Notes Mail Client. Close any other running applications and then click **Yes** to continue.

8. The installation program will now commence copying the files to your hard drive. When finished, it will advise you that the installation is complete. Click **Done** to exit the installation.

The installation of the Lotus Notes Mail Client is now complete. Start the Notes client to commence the configuration. For details on configuring your Lotus Notes Mail Client with the correct settings, refer to your Notes administrator.

3.2 Installing on Windows 95

To begin the installation of any of the components of the eNetwork Communications Suite, place the IBM eNetwork Communications Suite CD-ROM into the drive. Windows 95 should automatically start the setup application, and you will see an installation screen similar to Figure 27 on page 79

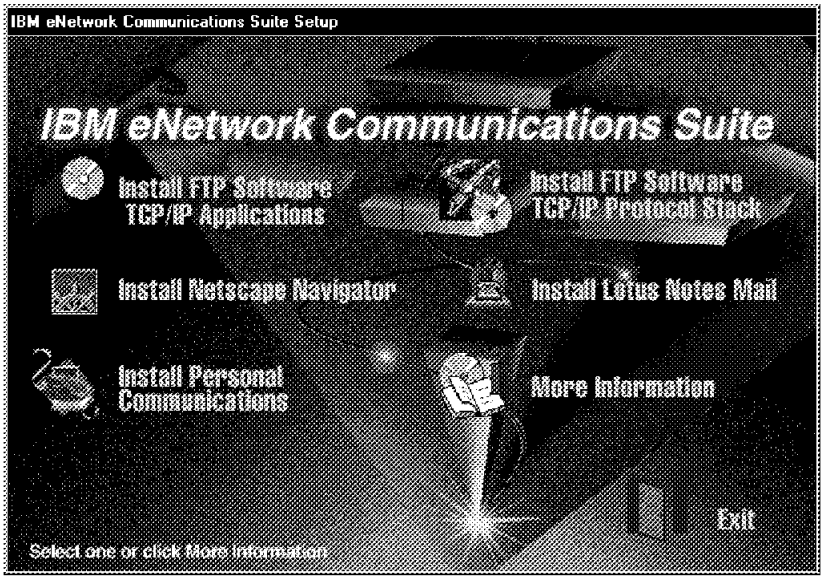


Figure 27. IBM eNetwork Communications Suite Setup Panel (Windows 95)

If you are installing from a network CD-ROM, or you have disabled the autorun feature, start the setup program manually. To do this, select **Run...** from the Start menu and type in `X:SETUP.EXE`, where `X:` is the drive letter of your CD-ROM.

3.2.1 Prerequisites

The next sections explain the eNetwork Communications Suite for Windows 95 system requirements.

3.2.1.1 Hardware Requirements

The following minimum hardware requirements should be met:

- Intel 80486 33 Mhz or higher microprocessor
- 8 MB RAM (16 MB recommended)
- 96 MB disk space for the entire suite
- CD-ROM drive
- For a LAN connection, a LAN adapter with NDIS or ODI device driver
- For a dial-up connection, any Hayes-compatible modem, supporting 9600 bps or higher, and a switched telephone line.

The CD-ROM drive may be a shared one on your LAN. If you plan to install from a shared CD-ROM drive, map it to a drive letter first. Do not start the installation by the Network Neighborhood method.

3.2.1.2 Software Requirements

The installation of the eNetwork Communications Suite requires the following software:

- Microsoft Windows 95
- Lotus Notes Server V3.0 or higher (for the Lotus Notes Mail Client only)

Before you start installing the software, verify the following:

- Your computer is properly connected to a modem, an ISDN card, or a LAN.
- In case of a LAN connection, the driver software for the network card is installed and running.
- Have the Windows 95 installation media easily accessible.

3.2.1.3 Information Needed for a LAN Connection

Some of this information may not be required if your network uses Dynamic Host Configuration Protocol (DHCP) or does not use Windows Internet Naming Service (WINS) name servers. See your network administrator if you need help with this information:

- Host name an IP address of your computer
- Subnet mask of your network
- Domain name of your network
- IP address(es) of default router(s)
- Type of name resolution (DNS, NIS, and/or WINS)
- IP address(es) of DNS or NIS server(s)
- IP address(es) of WINS server(s)
- Your user name on network hosts

3.2.2 Installing the FTP Software TCP/IP Protocol Stack

To install the entire product, also called the Secure Client, you might need up to 14 MB of available disk space on your computer. The Setup program lets you choose to install a subset of the components.

If you already have a TCP/IP protocol stack installed on your computer, this installation program replaces it with the FTP Software TCP/IP protocol stack.

The Secure Listener program is not installed by default. To install the Secure Listener, you must select either a Full or a Custom installation, and select the Secure Listener in the list of components.

For more information about Secure Client Version 3.0 see 2.1, “TCP/IP Stack and Applications from FTP Software” on page 46, and the README file, which is available on the Secure Client program menu after you install Secure Client 3.0.

3.2.2.1 Installation Steps

Begin the installation from the eNetwork Communications Suite Setup panel as described in 3.2, “Installing on Windows 95” on page 78.

1. Click on **Install FTP Software TCP/IP Protocol Stack** on the eNetwork Communications Suite Setup panel. The setup wizard will appear. Click on **Installation Notes** to read last-minute information. When finished, close the Notepad window and click on **Next** to continue the installation.
2. Select an installation type:
   - Typical installs all components except the Secure Listener.
   - Full installs all the components.
   - Custom lets you choose the components you want to install.
   - Administrator installs the product on a file server.
3. Accept the default installation folder or click on **Change** and specify another folder. Click on **Next** to continue.
4. Choose the location of your data files by clicking on **Change**, or accept the default and click on **Next**.

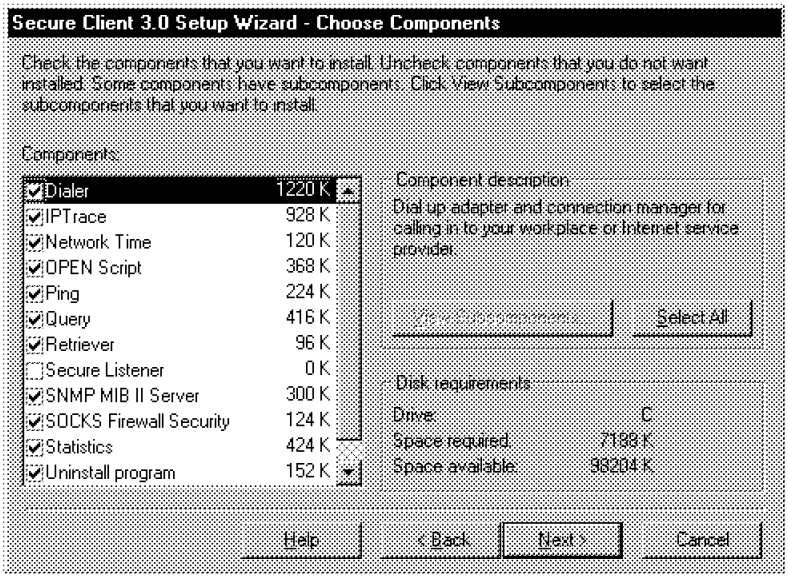


Figure 28. Component Selection

5. Go to the next step if you have not selected Custom as the installation type; otherwise choose the components you want to install, in the dialog box shown in Figure 28. After you finish, click on **Next** to continue.
6. In the **Copy File** dialog box you can verify which components are to be installed and eventually cancel the installation, leaving the system unmodified. In order to install, click on **Next**.
7. After the files have been copied, click on **Next** to start the wizard, which will let you configure the protocol stack.
8. If you use a dial-up connection, select the adapter type. Follow the wizard's instructions to install and configure the appropriate adapter. If you use LAN connection only, click on **Cancel**.

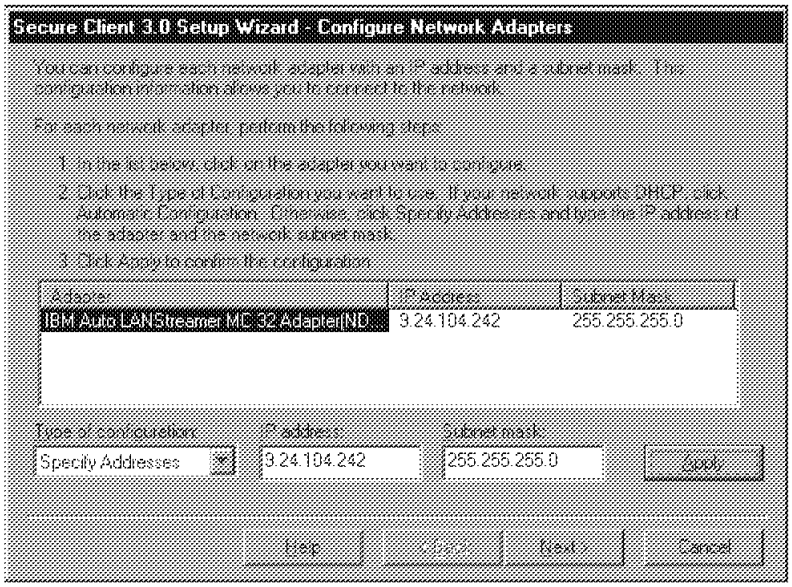


Figure 29. Secure Client Installation - Configure Network Adapter

9. In the Configure Network Adapter dialog box, shown on Figure 29, select the configuration type and specify the IP address and network mask for each of your network adapters. If you selected DHCP as the configuration type for an adapter, the IP address and Subnet mask fields will be disabled for that adapter. Click on **Next** to continue.

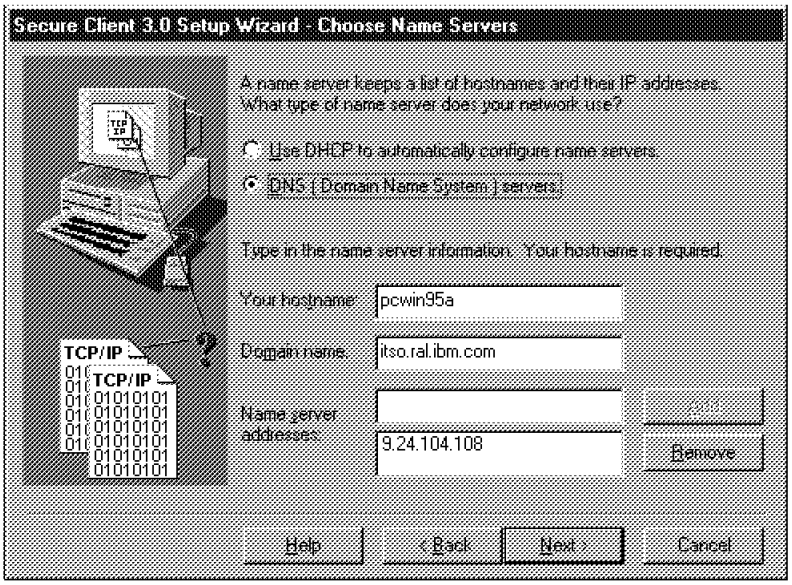


Figure 30. Secure Client Installation - Choose Name Servers

10. Configure your name servers, in the dialog box shown in Figure 30. If you have configured DHCP on the previous panel, consider using the automatic name server configuration at this point. If you are not sure, ask your network administrator.

11. Specify your hostname. In case you selected DNS as the type of name server, also specify the domain name and the IP address(es) of the name server(s). Click on **Next** to continue.

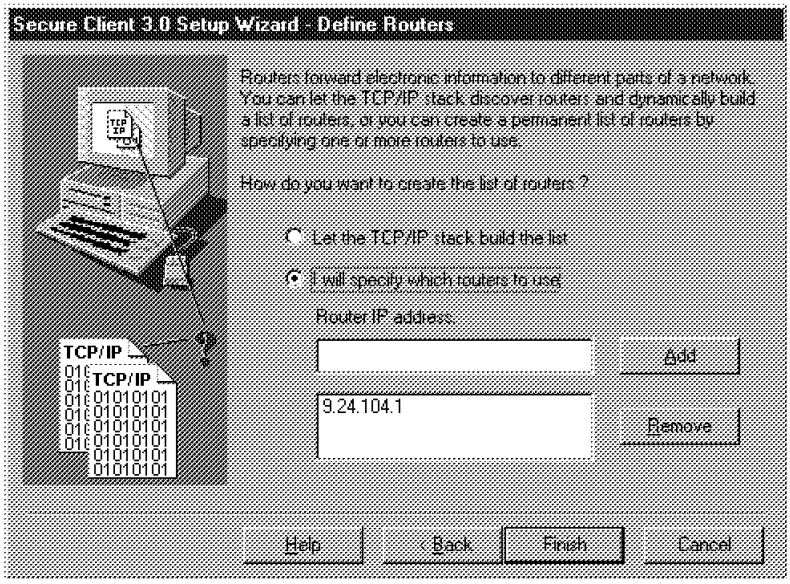


Figure 31. Secure Client Installation - Define Routers

12. In this dialog box specify the IP address(es) of your router(s). If you selected DHCP at step 9 on page 83, it makes sense to let the TCP/IP stack build the list. If in doubt, consult your network administrator.
13. Click on **Finish** to complete the installation. If you selected Full installation at step 2 on page 81 or you selected to install the Secure Listener at step 5 on page 82, continue with the next step. Otherwise go to step 19 on page 86
14. The Secure Listener Setup Wizard Welcome window appears, as shown in the figure below:

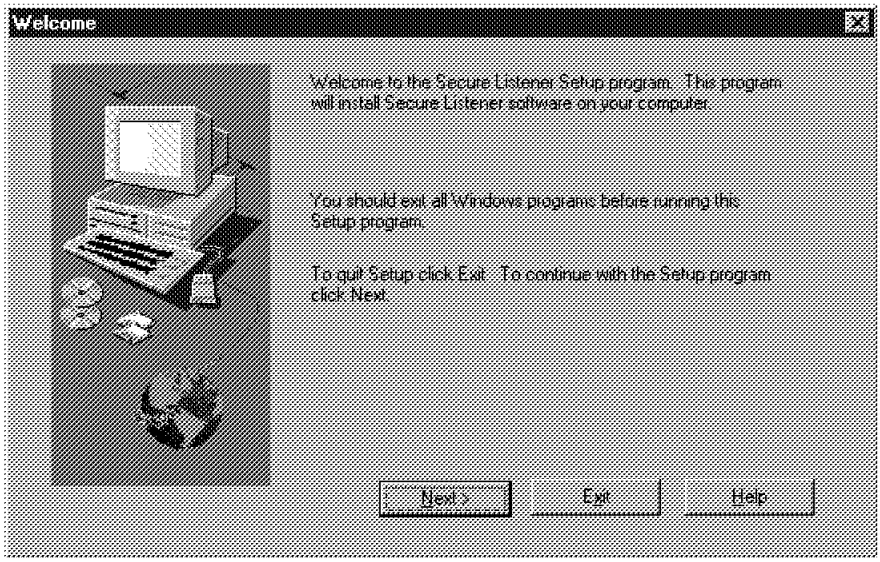


Figure 32. Secure Listener Welcome Window

Click on **Next** to continue with the installation.

15. Select the destination path for this product, or accept the default. Click on **Next** to continue.
16. Click on **Yes** in the Confirm Java Installation dialog box. The Java Development Kit (JDK) 1.02 will be installed.
17. Click on **Readme** for important last-minute information about the Secure Listener. After you have done this, close the Notepad window and click on **Exit**.
18. An information box pops up telling you that the Secure Client installation has completed successfully. Click on **OK** to continue.
19. Click on **Yes** to restart the system.

You have now installed the FTP Software TCP/IP protocol stack. A folder shown in Figure 33 on page 87 has been created, containing the shortcuts to the different components.

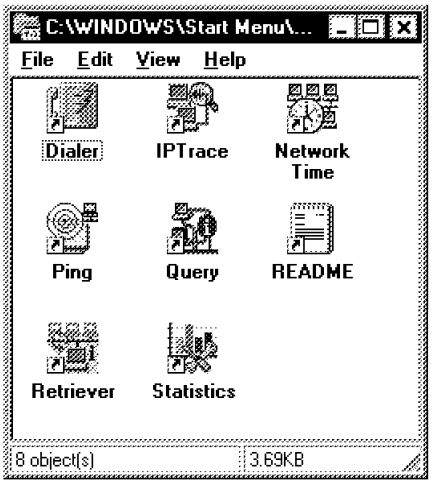


Figure 33. Secure Client Folder

3.2.2.2 Verifying the Installation

Verify your TCP/IP network connection by contacting another computer in the network. Start the Ping application and enter the host name or the IP address of an active computer on your network. (You cannot start Ping from an MS-DOS command prompt.) A response from the remote computer indicates that the installation was successful.

Some debugging hints:

- If you can ping a remote host by its IP address, but not by its host name, verify your name server settings.
- If you can ping a host that is on the same subnet as your machine, but you cannot ping hosts on other subnets or networks, check your router settings.
- You can use the Traceroute application as a last resort to track down connectivity problems. Use it carefully, because it generates significant network loads. Traceroute can be accessed by clicking the corresponding tab on the Ping application window.

3.2.3 Installing the FTP Software TCP/IP Applications

Begin the installation from the eNetwork Communications Suite Setup panel as described in 3.2, “Installing on Windows 95” on page 78. The following instructions guide you through the process of installing the FTP Software TCP/IP applications component of the eNetwork Communications Suite.

1. From the IBM eNetwork Communications Suite Setup panel, click on **Install FTP Software TCP/IP Applications**. This will give you the Network Access Suite Setup Wizard. Network Access Suite is the name of the FTP Software TCP/IP applications suite in Windows 95. You should read the brief welcome message, and the installation notes for last-minute changes to the installation procedure. Once you have done this, click on the button marked **Next** to continue with the installation.
2. The installation wizard will now ask you what type of installation you wish to perform. The choices available to you are:

   Full This will install all components of the Network Access Suite onto your system.

   Custom This option will give you the opportunity to select which components of the Network Access Suite you wish to install.

   Administrator Select this option to install the files onto a server. This will allow you to install the FTP Software TCP/IP Application Suite and Protocol stack onto other client machines.
3. If you select the **Full** option, you will only be asked which directory you wish to place the data files in. Change the destination directory, or accept the default by clicking **Next**.

   If you select the **Custom** option, you will be asked for a destination directory. Change the selection, or accept the default as above. The installation program will now ask you to choose which components to be installed. You should choose only those options you require for the workstation you are installing onto. For details on the usage of a particular component, refer to Chapter 2, “Product Overview” on page 45. Once you have made your selection, click **Next** to continue.

   If you select the **Administrator** option, you will be prompted for the destination directory. Change this directory, or accept the default.
4. The installation program will now display a list of the components it is going to install. You can change the selection by clicking **Back**. To continue with copying the files to your hard disk, click **Next**.
5. The installation program will now copy the files to your hard disk and update the shortcuts and registry information.
6. Once the copying is complete, it will give you the option to restart your computer. Select **Yes** and then wait for the system to reboot.

A folder shown on Figure 34 on page 89 has been created with the shortcuts to the components of the Network Access Suite.

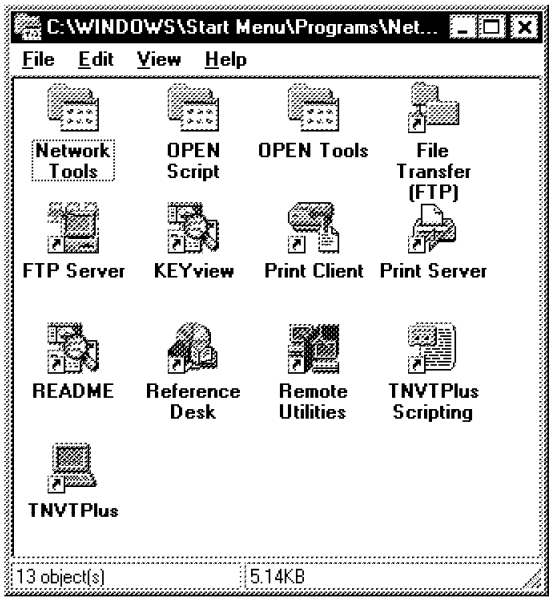


Figure 34. Network Access Suite Folder

Once your system has rebooted, you can continue with the installation of the other components of the eNetwork Communications Suite.

3.2.4 Installing Personal Communications for Windows 95

The installation of the Personal Communications product has many options that may not be required in every installation scenario. If you are not familiar with all these options, we suggest you check with your system administrator for the correct settings and options for connecting to your host.

If you require detailed information on the configuration of Personal Communications, refer to Appendix C, “Related Publications” on page 301 for information on other IBM publications available.

To install the full product you need about 31 MB of free disk space on your hard drive.

3.2.4.1 Installation Steps

Begin the installation from the eNetwork Communications Suite Setup panel as described in 3.2, “Installing on Windows 95” on page 78. Follow the steps below to successfully install this product.

1. Click on **Install Personal Communications** on the eNetwork Communications Suite Setup window. The Setup Wizard will bring up

the IBM Personal Communications Setup dialog box, shown in Figure 35 on page 90, where you can select the components you want to install:

- IBM Library Reader is an online documentation (book) viewer for the BookManager-formatted files.
- CM Mouse is a utility that maps mouse actions to host screen actions. It helps you easily navigate the host screens. It provides macro definition and playback functions combined with screen recognition capabilities.
- Personal Communications is a full-function 3270 and 5250 terminal emulation package.

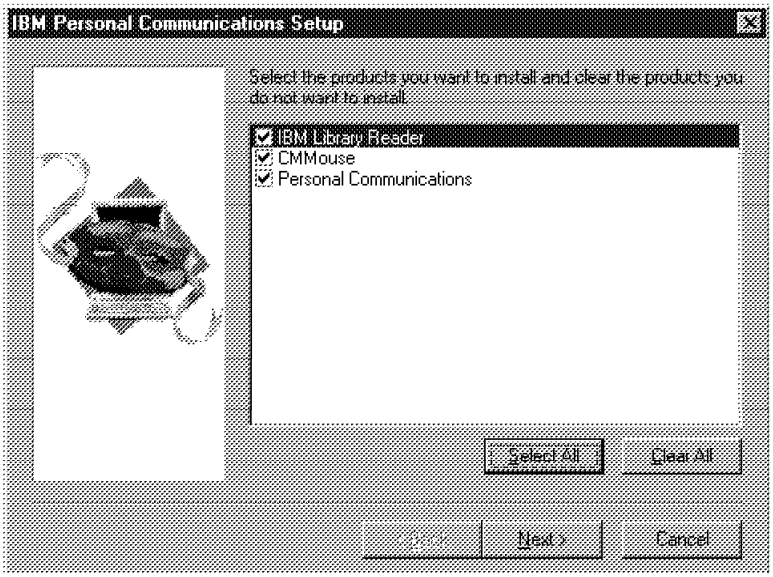


Figure 35. IBM Personal Communications Setup

If you want to install the IBM Library Reader, you must install it and reboot your computer before installing any other component. Go to the next step if you want to install the IBM Library reader; otherwise go to step 10 on page 92.

2. Tick *only* the IBM Library Reader check box on the IBM Personal Communications Setup dialog box and click on **Continue**.
3. On the next dialog box the Setup Wizard will show the component to be installed. Click on **Next**.
4. Read the message on the Installation Instructions window and click on **Continue**.

5. Click on **OK** in the Install window.

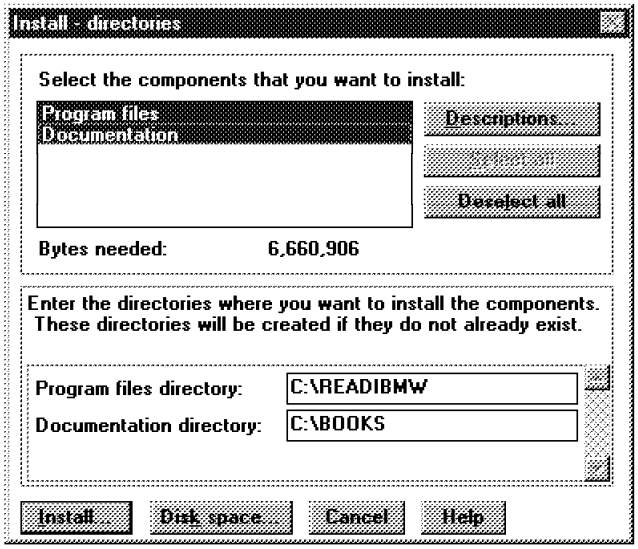


Figure 36. IBM Library Reader Installation - Directories

6. At the Install - directories dialog box select the components you want to install, and change the destination directories if needed. Click on **Install**.

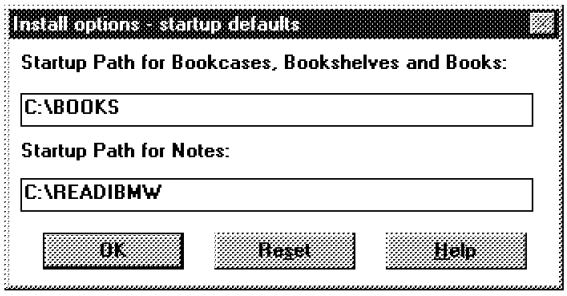


Figure 37. IBM Library Reader Installation - Options

7. At the Install options - startup defaults dialog box change the startup paths of the product if needed. Click on **OK** to continue.
8. At the Installation and Maintenance dialog box click on **OK** to continue.
9. Reboot your system. To continue with the installation, repeat the first installation step, then go to the next step.

10. Tick the check box in front of the products you want to install. Click on **Next** to continue.
11. On the next dialog box the Setup Wizard will show the components to be installed. Click on **Next** to continue.
12. If you selected to install CM Mouse, go to the next step; otherwise go to step 16.
13. At the CM Mouse Installation dialog box select the components you want to install and change the destination paths if needed. You can specify which sample files you want to install after clicking on **Samples...**. You can also configure CM Mouse by clicking on **Configure...** and making your selections at the CM Mouse Configuration dialog box. The default setting will fit your needs in most cases. Click on **Install** to continue.

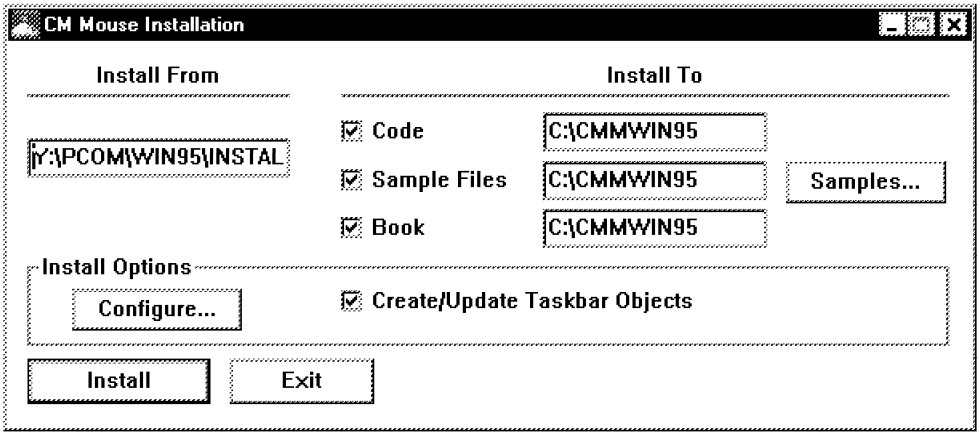


Figure 38. CM Mouse Configuration Panel

Note: The CM Mouse application uses APIs supported by Personal Communications. To get CM Mouse support, the Personal Communications installation might ask if you want the AUTOEXEC.BAT file to be modified to call PCSVARS.BAT. Click on **Yes**.

14. Select the task bar group you wish to place the CM Mouse icons in, then click on **OK**. Click on **OK** again on the Install Status message box.
15. Click on **Exit** on the CM Mouse Installation dialog box.

    You have finished the CM Mouse installation. Go to the next step if you selected to install the Personal Communications emulators.
16. Click **Next** in the Personal Communications AS/400 and 3270 message box.

17. Select the installation type you want:

    - Run Personal Communications from my workstation: This will result in a stand-alone installation, with all the files copied to your local drive.
    - Run Personal Communications from a server: This will install the program files from a shared server drive, keeping only your session profiles, keyboard and macro files and other configuration information on your workstation or in a personal directory on a server.
    - Install Personal Communications on a server: All the files on the CD-ROM are copied to the network drive that you specify. You cannot choose any installation options.

    Click on **Next** to continue.

18. Specify which functions do you want to install:

    - 3270: Your workstation can emulate an S/390 terminal (display and/or printer). The emulator APIs (EHLLAPI, PCSAPI, DDE and SRPI) are installed.
    - 5250: Your workstation can emulate an AS/400 terminal (display and/or printer). The emulator APIs are installed.
    - Communication APIs: The APIs include the protocols that let you use SNA communications. These protocols include IEEE 802.2, SDLC, SNA-over-Async, and Twinaxial attachments, and the APPC and CPI-C programming interfaces.

    Click on **Next** to continue.

19. Choose the installation directory and click on **Next**.

20. Choose to install part or all of the emulator′s functions:

    Full Installs all the functions of the emulators you chose, including the optional utilities, the help files and publications, all the printer-definition files and tables, and the sample programs. The Communications APIs without the associated help file or publications are installed even if you did not choose them in the Choose Components window. You need the SNA protocols to run the emulator. For example, if you use only TCP/IP, choose **Custom** and deselect the APIs.

    Custom Allows you to choose which subcomponents to install when the Custom Installation window appears.

    Note: If you want to use Cyrillic, Greek or Turkish, you must

choose **Custom** and then select **Language choice** in the Custom Installation window.

Minimal Installs only the main functions of the emulators you chose, including the help file but not the publications. If you make this choice, you must have protocols installed other than those provided by the Communications APIs, for example a TCP/IP protocol stack.

Click on **Next** to continue.

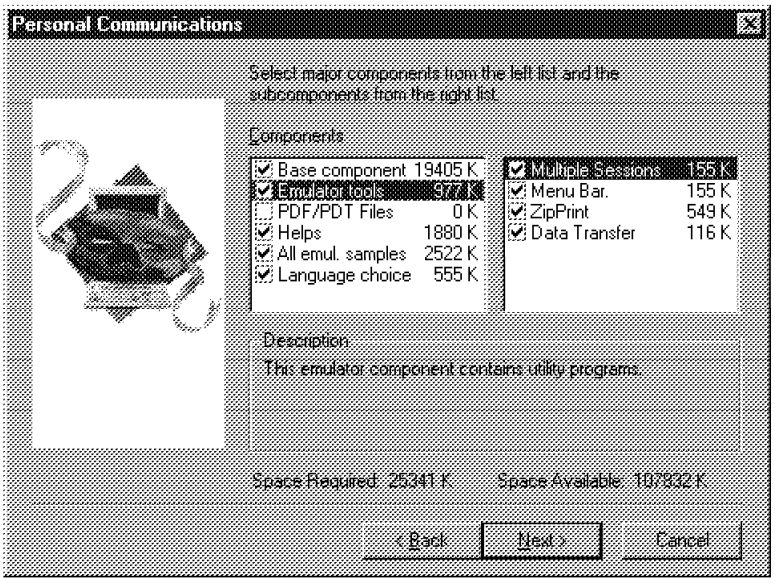


Figure 39. Personal Communications Component and Subcomponent Selection (Windows 95)

21. If you chose Custom Installation, at this point you can select the components and subcomponents you wish to install, as shown in Figure 39. Make your selections and click on **Next**.
22. The Wizard is ready to install the product now. You have a chance to change the destination directory and the required disk space is displayed. You can go back to the function selection window (step 21) by unchecking Continue with installation. If all settings are correct, click on **Next** to continue.
23. Accept the default program folder name or specify another one by typing in or by selecting from the list. Click on **Next** to continue.
24. Click on **OK** on the two information boxes. You will be asked whether you want to install the Personal Communications IEEE 802.2 interface for

the LAN. Follow the instructions on the screen to install this interface (see Figure 40 on page 95).

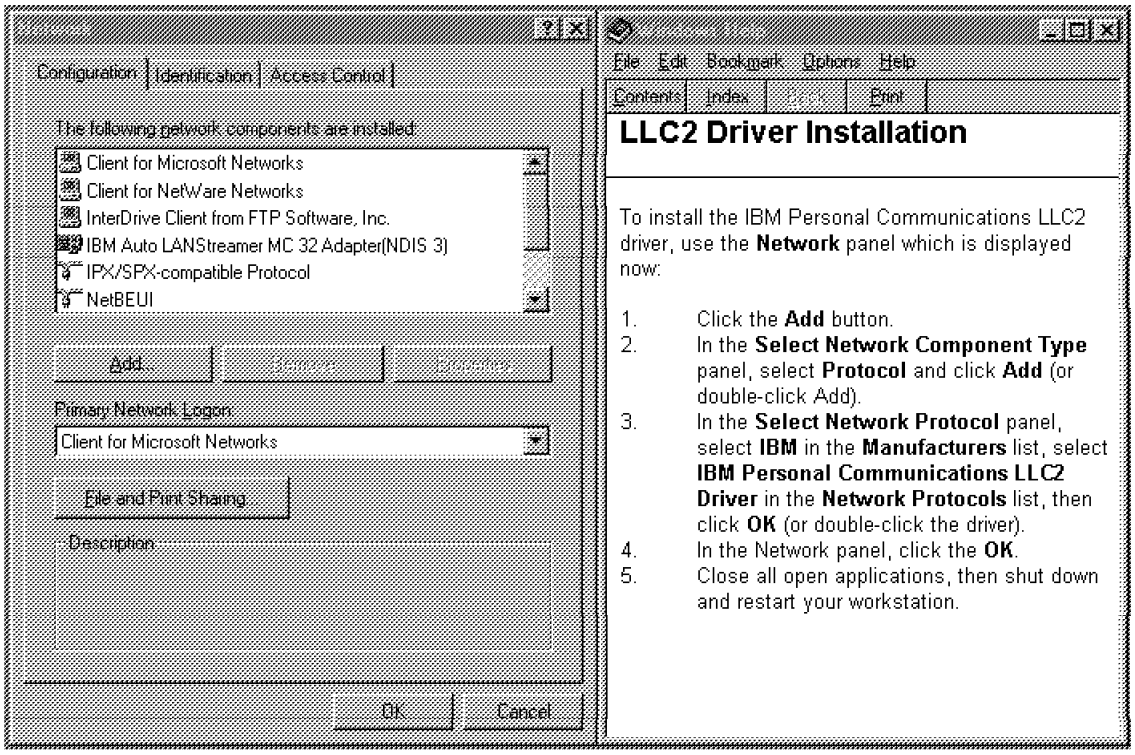


Figure 40. Personal Communications LLC2 Driver Installation (Windows 95)

25. Close all your applications and reboot your computer.

You can start your first emulator session by selecting **IBM Personal Communications** from the Windows 95 Start menu, and then selecting **Start or Configure Session**.

3.2.5 Installing Netscape Navigator for Windows 95

The installation of the Netscape Navigator consists of a number of separate steps:

1. Installation of Netscape Navigator
2. Configuration of Netscape Preferences
3. Configuration of Netscape Mail and Netscape News
4. Installation of Netscape Plug-Ins

We explain each of the above steps in detail in the following sections.

3.2.5.1 Installation of Netscape Navigator

To begin the installation, you should start from the IBM eNetwork Communications Suite Setup panel as described in 3.1, “Installing on Windows NT” on page 61. From there, follow these steps to install the Netscape Navigator:

1. Click on the item **Install Netscape Navigator**. This will start the Netscape Navigator Setup program. Read the brief welcome message, then click on **Next** to continue.
2. Your next option is the destination directory. Click on **Browse** to change the destination, or click on **Next** to accept the default.
3. You will now be asked if you wish to install the CoolTalk application for Netscape Navigator. If you have a properly configured sound card with a suitable microphone, you can choose to install this option as well. To do so, click on **Yes**. If you do not wish to install the CoolTalk application, then click **No** and continue with the installation of the Netscape Navigator. The installation program will now commence copying the files to your hard disk.
4. If you chose to install the CoolTalk application, you will be asked if you wish to enable the CoolTalk Watchdog. This program will listen for incoming connections from other users who are using CoolTalk, and automatically start the CoolTalk application. If you have a permanent connection to your network, you should select this option.
5. Once the files have been copied to the hard disk, the installation program will ask if you wish to connect to the Netscape homepage to continue with the installation. Select **No**, as we explain the configuration of the Netscape Navigator in this section.
6. The installation program will now ask if you wish to view the README file. You should choose **Yes**, as it may contain important last-minute information not found in this publication or the program documentation.
7. Click on **OK** once the setup has completed. This will close the installation program, and give you the opportunity to view the README file.
8. Close the README file once you have finished reading it.

Now that the above steps have been completed, you should have a folder open on your desktop that looks similar to Figure 41 on page 97.

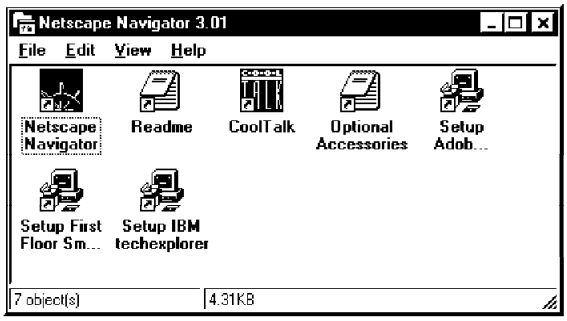


Figure 41. Netscape Navigator Folder (Windows 95)

If you have a direct connection to the Internet, you will now be able to use the Netscape Navigator without any further configuration. Most of the general preferences are simply cosmetic changes, and do not require alteration. If you require information on these settings, select **Options/General Preferences** and click F1, or click on **Help**.

3.2.5.2 Configuration of Netscape Preferences

Double-click on the **Netscape Navigator** object to start the Netscape Navigator. The application should start and load an introduction page that welcomes you to the eNetwork Communications Suite. You can read this information now, or the next time you start the Navigator.

If you are connected to the Internet via a proxy server or other firewall device, then you need to configure this in the Netscape preferences. If you are not sure, then contact your system administrator, who can give you the correct details. As an example, we show you how to configure the Netscape Navigator to use a proxy server. We assume the details of the proxy server are as follows:

Proxy Server: proxy.au.ibm.com
Port: 80

1. From the Netscape menu, select **Options** with your mouse. Then select **Network Preferences** from the drop-down menu.
2. Click on the **Proxies** tab of the Preferences notebook.
3. Click the radio button for **Manual Proxy Configuration** and then click on **View**.
4. In the Manual Proxy Configuration notebook, fill in the name of the proxy server next to those protocols that the proxy server supports. In our case, it is FTP and HTTP. Type in the port number as well.

5. Generally, if you have a proxy server, it is only required for those sites outside of your internal network. Check with your system administrator, but in most cases, you can tell Netscape not to use the proxy server for connecting to machines within your own domain. If so, place the domain name of your network into the section called No Proxy For. In our example, this was au.ibm.com. Once completed, you should have a configuration similar to Figure 42.

6. Click on **OK** to apply these changes. Click on **OK** again to close the Network Preferences notebook.

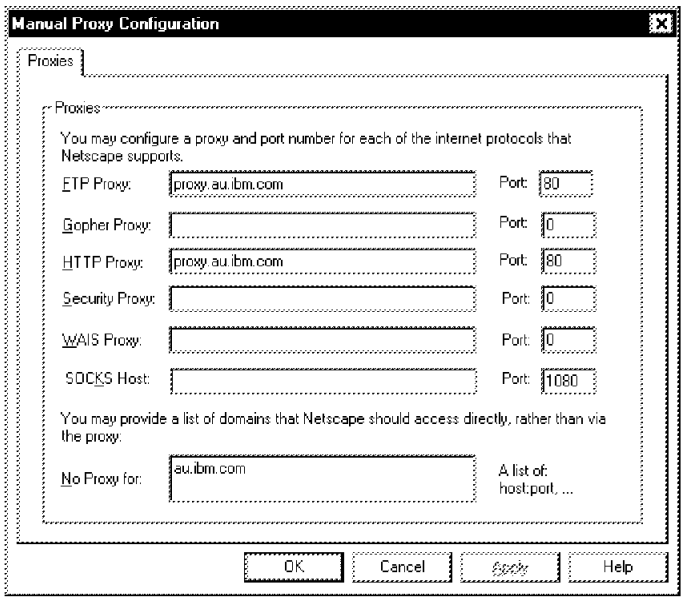


Figure 42. Manual Proxy Configuration Setup (Windows 95)

3.2.5.3 Configuration of Netscape Mail and Netscape News

To configure the Netscape Mail and News functions, you will need some information from your system administrator. Of the many options that can be configured, this is the most basic information required. If you do not have any or all of this information, you will not be able to use the Netscape Mail or Netscape News effectively.

SMTP Mail Server This is the fully qualified hostname of the server that you will be using to send your new e-mail messages to for delivery.

For example: mail.raleigh.ibm.com

POP3 Mail Server This is the fully qualified hostname of the server that you will collect your new e-mail messages from. Often, this will be the same as the SMTP mail server.

For example: pop3.raleigh.ibm.com

POP3 User Name This is your user ID for the POP3 mail server. While it is often the same as the first part of your e-mail address, it does not need to be.

For example: meaden

POP3 Mail Password This is your password for collecting your e-mail from the POP3 mail server. It will probably be assigned to you by the system administrator.

For example: password

NNTP News Server This is the fully qualified hostname of the news server you will use to send and receive messages from the Internet newsgroups.

For example: news.raleigh.ibm.com

Email Address This is your full e-mail address that you will use for electronic mail on either the Internet, your Intranet, or both.

For example: meaden@raleigh.ibm.com

Your Name This is generally your first and last name. If the same e-mail address is being used by many people in the same section, it will often represent the name of the department, or their purpose.

For example: Software Support

Once you have these details, start the configuration with the following steps:

1. Selecting **Options** from the Netscape menu. From the pull-down menu, select **Mail and News Preferences**.
2. Select the tab marked **Servers** from the Preferences notebook.
3. In the field called Outgoing Mail (SMTP) Server type in the name of your mail server.
4. Click the Tab key, or use the mouse to move to the next field called Incoming Mail (POP3) Server. In this field, type the name of your POP3 mail server.
5. Click the Tab key, or use the mouse to move to the next field called POP3 User Name. In this field, type your POP3 mail user ID.

6. Click the Tab key, or use the mouse to move to the field called News (NNTP) Server. In this field, type the name of your news server.

7. Once those details are complete, your Servers Preferences should look similar to Figure 43. Select the **Identity** tab from the Preferences notebook to continue the configuration.

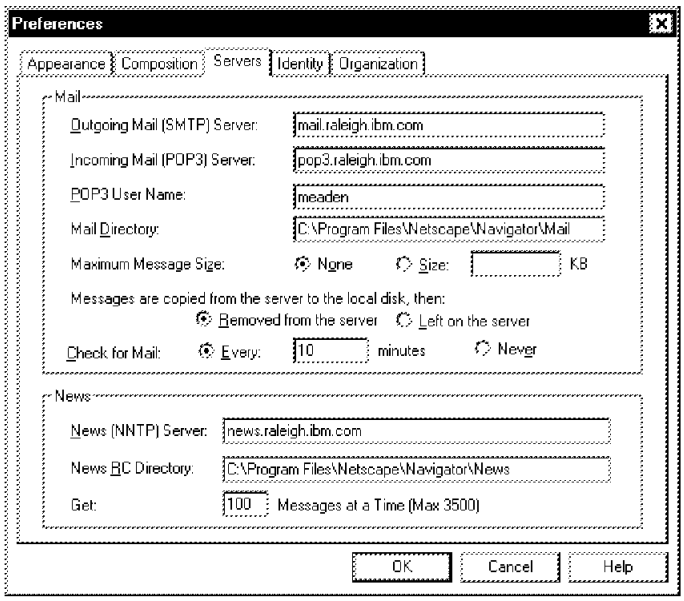


Figure 43. Netscape Preferences - Servers (Windows 95)

8. In the field titled Your Name, type in the user name, or other name you have selected for this e-mail account.

9. Use the Tab button or the mouse to move to the next field called Your Email. In this field, type the e-mail address of the account.

10. Double-check that your configuration looks similar to Figure 44 on page 101. If so, click **OK** to save the changes.

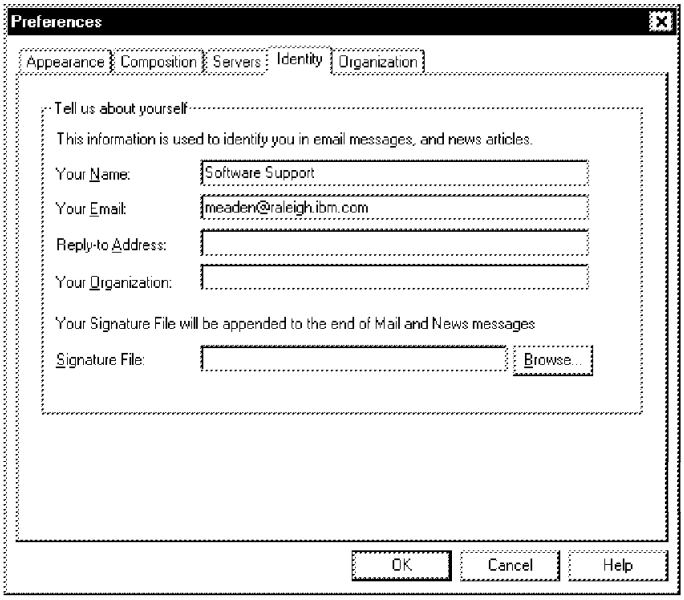


Figure 44. Netscape Preferences - Identity (Windows 95)

Your Netscape Mail and Netscape News are now properly configured and ready to run.

3.2.5.4 Installation of Netscape Plug-Ins

To install the Netscape plug-ins, ensure the IBM eNetwork Communications Suite CD-ROM is in the CD-ROM drive. The following information is for installing the Adobe Acrobat Plug-In for Netscape Navigator:

1. From the Netscape Navigator folder (Figure 41 on page 97) double-click on the **Setup Adobe Acrobat** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Read the Adobe license carefully, and click on **Accept** if you agree to the terms of the license. If you click **Decline** to indicate you do not accept the license agreement, the installation will end.
4. The installer will now ask for an installation directory. Accept the default directory by clicking **Install**. You can change the destination directory by typing over the existing installation path with your preferred location.
5. Click on **OK** when you receive a notification about the registration procedure.

6. At the prompt for Name and Organization, you should enter the details of yourself, the license owner, or the end user. Click **OK** when complete.
7. The Adobe Acrobat Installer will now commence copying the files to your hard disk. Click on **OK** once the installation has completed.

The Adobe Acrobat Reader Plug-In has now been successfully installed.

To install the First Floor Smart Bookmarks plug-in, follow these instructions:

1. From the Netscape Navigator folder (Figure 41 on page 97) double-click on the **Setup First Floor Smart Bookmarks** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Once the setup wizard has started, read the brief welcome screen and click on **Next** to continue.
4. At the User Information section, you should complete the details in the same way as for the Adobe Acrobat installation. If the section marked Serial is not already filled in, check your product documentation for this number. If it is already filled in, then leave the current value as is.
5. Confirm your earlier input by selecting **Yes**, or change the details by selecting **No**.
6. You will now be asked which type of installation you wish to install. For most users, the default Typical installation will be sufficient, and you should select that option. Click on **Next** to continue.
7. If the destination directory you chose does not yet exist, the installation application will ask if it can create it for you. Choose **Yes** and continue with the installation.
8. The installation will now ask you which Internet Browser you are using. The default selection is **Netscape 2.0 or later**. Do not change that setting, as this is the correct choice. Click on **Next** to continue the installation.
9. The installation wizard will now double-check the options you selected. If you have nothing you wish to change, click on **Next**.
10. The installation wizard will now copy the files to your hard disk.
11. Once finished copying the files, the installation wizard will advise you it has completed, and give you the option to view the README. Click on **Finish** and the installation will end, and present you with the application README file. Read through this file in case there have been any last-minute changes.

The First Floor Smart Bookmarks Plug-In has now been successfully installed.

The final plug-in included with the IBM eNetwork Communications Suite is the IBM techexplorer Plug-In. To install this product, follow these steps:

1. From the Netscape Navigator folder (Figure 41 on page 97) double-click on the **Setup IBM techexplorer** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Once the setup wizard has started, read the brief welcome screen and click on **Next** to continue.
4. Read the license agreement carefully, and select **Yes** if you agree with the terms and conditions.
5. The setup wizard will now ask for an installation path. You can change the default by clicking **Browse** or accept the default by clicking **Next**.
6. If the selections on the next screen match your preferred settings, then select **Next**.
7. The setup wizard will then copy the files to your hard disk, then open the README file.
8. Read this information carefully in case there has been any last-minute changes. Close the README once you have finished viewing it.
9. Select **Finish** from the setup wizard.

The installation of the IBM techexplorer is now complete. All these plug-ins are automatically loaded when the Netscape Navigator is started. If the Netscape Navigator encounters a WWW page that requires one of the plug-ins, they will be invoked automatically.

3.2.6 Installing Lotus Notes Mail Client for Windows 95

This section assists you in installing the Lotus Notes Mail Client. If your organization has access to a Lotus Notes server, and you wish to take advantage of the powerful e-mail capabilities of the Lotus Notes Mail Client, read this section carefully.

1. Start the IBM eNetwork Communications Suite Setup panel as described in 3.2, “Installing on Windows 95” on page 78 and click on **Install Lotus Notes Mail**.
2. Read the Software Agreement carefully, and click on **I Agree** if you accept the terms of the agreement.

3. The next screen is a welcome panel. In the fields provided, type in your name and the company name. Click on **Next** to continue with the installation.
4. The installation wizard will ask you to confirm the information you typed in on the previous panel. Click on **Yes** to confirm the information, or take this opportunity to go back and correct it.
5. Select **Standard Install** from the Install Option dialog. You can change the default installation path from this dialog by selecting **Browse** next to the program or data folder path. You can select **Next** to continue the installation.
6. The installation wizard will now ask you which program folder you want the application shortcut installed to. Accept the default, highlight a new selection, or create a new folder. Once you have made any changes, select **Next**.
7. Before copying the files to your hard disk, the installation will ask that you shut down any other running applications. Do this, then select **Yes** to continue.
8. The installation program will now commence copying the files to your hard drive. When finished, it will advise you that the installation is complete. Click on **Done** to exit the installation.

The installation of the Lotus Notes Mail Client is now complete. Start the Notes client to commence the configuration. For details on configuring your Lotus Notes Mail Client with the correct settings, refer to your Notes administrator.

3.3 Installing on Windows 3.x

To begin the installation of any of the components of the eNetwork Communications Suite place the IBM eNetwork Communications Suite CD-ROM into the drive and start the SETUP.EXE program (which is located in the root directory of the CD-ROM) either from the File Manager or by choosing **Run...** from the Program Manager′s File menu. The eNetwork Communications Suite for Windows 3.x Setup panel will be displayed (see Figure 45 on page 105).

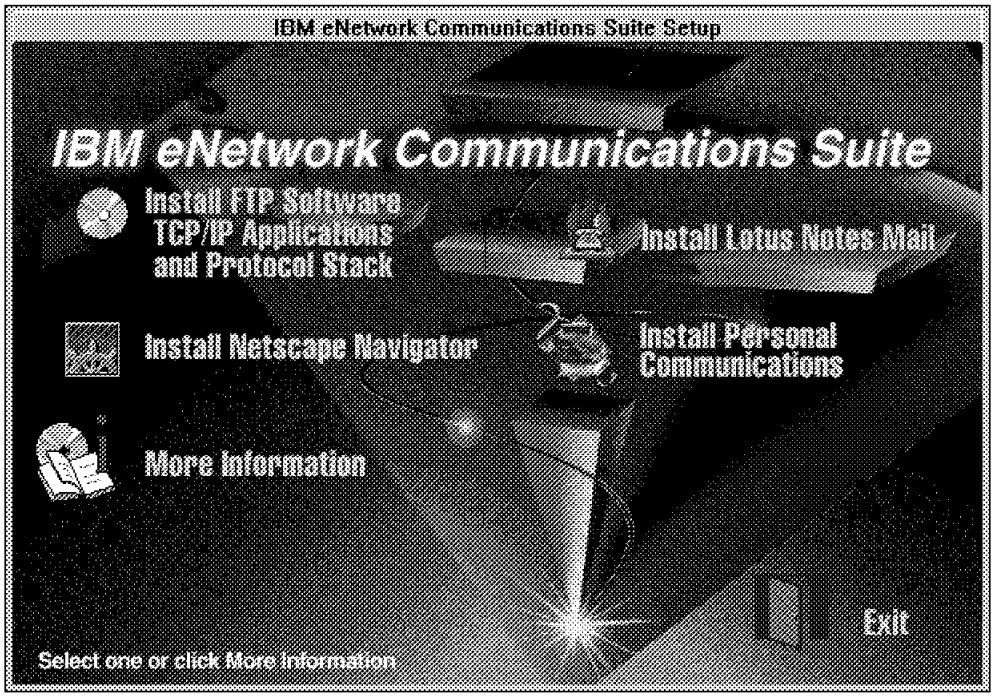


Figure 45. IBM eNetwork Communications Suite Setup Panel (Windows 3.x)

3.3.1 Prerequisites

The eNetwork Communications Suite for Windows 3.x has the following system requirements:

3.3.1.1 Hardware Requirements

The following minimum hardware requirements should be met:

- Intel 80486 33 MHz or higher microprocessor
- 8 MB RAM
- 78 MB disk space for the entire suite
- CD-ROM drive
- For a LAN connection, a LAN adapter with NDIS or ODI device driver
- For a dial-up connection, any Hayes-compatible modem, supporting 9600 bps or higher, and a switched telephone line.

The CD-ROM drive may be a shared one on your LAN.

3.3.1.2 Software Requirements

The installation of the eNetwork Communications Suite for Windows 3.x requires the following software:

- Either PC DOS or MS DOS, Versions 5.0 and higher
- Microsoft Windows 3.x. or Windows for Workgroups 3.11
- Lotus Notes Server V3.0 or higher (for the Lotus Notes Mail Client only)

Before you start installing the software, verify the following:

- Your computer is properly connected to a modem, an ISDN card, or a LAN.
- In case of a LAN connection, the driver software for the network card is installed and running.
- You have the Windows 3.x installation media easily accessible.

3.3.1.3 Information Needed for a LAN Connection

Some of this information may not be required if your network uses Dynamic Host Configuration Protocol (DHCP) or does not use Windows Internet Naming Service (WINS) name servers. See your network administrator if you need help with this information.

- Host name an IP address of your computer
- Subnet mask of your network
- Domain name of your network
- IP address(es) of default router(s)
- Type of name resolution (DNS, NIS, and/or WINS)
- IP address(es) of DNS or NIS server(s)
- IP address(es) of WINS server(s)
- Your user name on network hosts

3.3.2 Installing the FTP Software TCP/IP Applications and Protocol Stack

You will need approximately 10 MB of free disk space in order to install the full product.

3.3.2.1 Installation Steps

The installation on the Windows 3.x platform is slightly different from the Windows 95 and Windows NT platforms. Follow the steps below to install the product:

1. At the eNetwork Communications Suite Setup panel (see Figure 45 on page 105) click on **Install FTP Software TCP/IP Applications and Protocol Stack**.
2. Wait for the Welcome window to show up. Click on **Installation Notes...** to get last-minute information about the product. After you save read the notes, close the MS-Write window and click on **Continue**.
3. At the New Installation dialog box select an installation type:

   Express Installs the entire product, with a single network interface.

   Custom Lets you choose which components you want to install. You can configure more network interfaces with this option.

   Click on **Continue**.
4. The default destination directory C:PCTCP is shown. You can change it by selecting or typing in a new directory. Click on **Continue**.
5. Select the location for the online books, either your hard drive or your CD-ROM. If you select the hard drive, the books will be copied to the destination directory. Click on **Continue**.

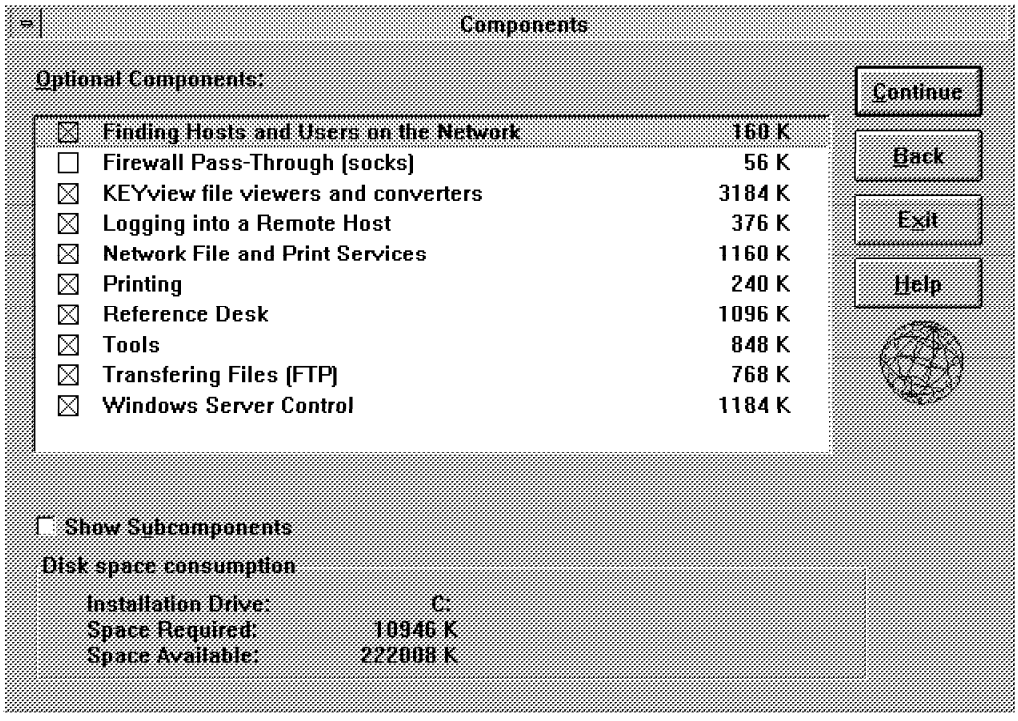


Figure 46. FTP Software Protocol Stack Installation - Component Selection

6. If you selected **Custom** at step 3, you will see the dialog box shown on Figure 46, where you can select the individual components you wish to install. After you make your selections, click on **Continue**.

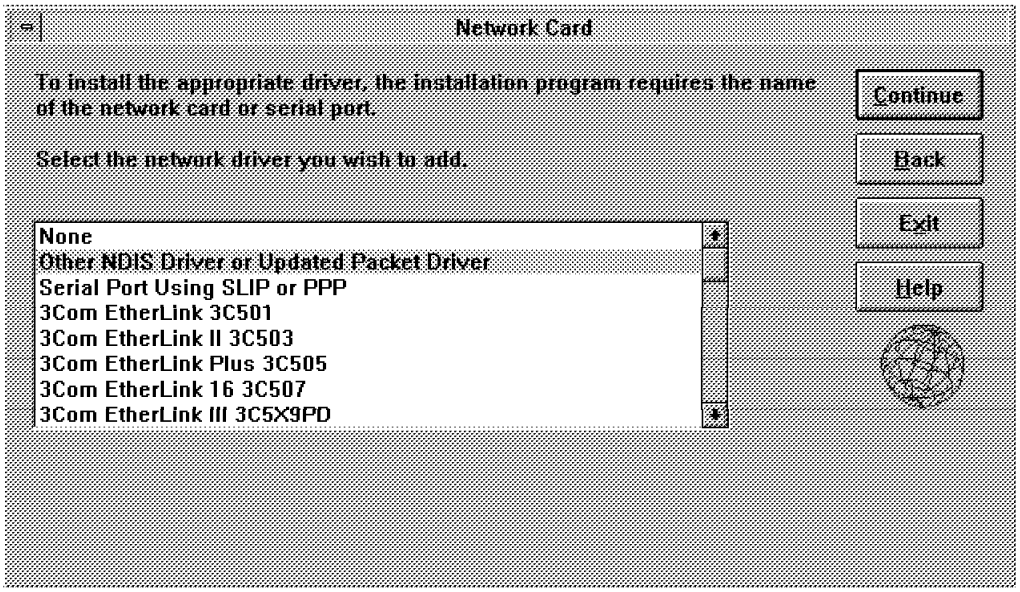


Figure 47. FTP Software Protocol Stack Installation - Network Card Selection

7. If your network card driver software is not already installed, you are presented with a list of network cards (see Figure 47). If your card is not in the list, select **Other NDIS Driver or Updated Packet Driver**. When the Setup program prompts you, insert the disk containing a network card driver (supplied by the manufacturer of your network card). If you cannot determine the type of network card installed in your computer, you can continue with the installation and use the Configure application later to specify this information.

   Select **Serial Port Using SLIP or PPP** for any serial (dial-up) connection, including ISDN.

   Click on **Continue** after making your selection.

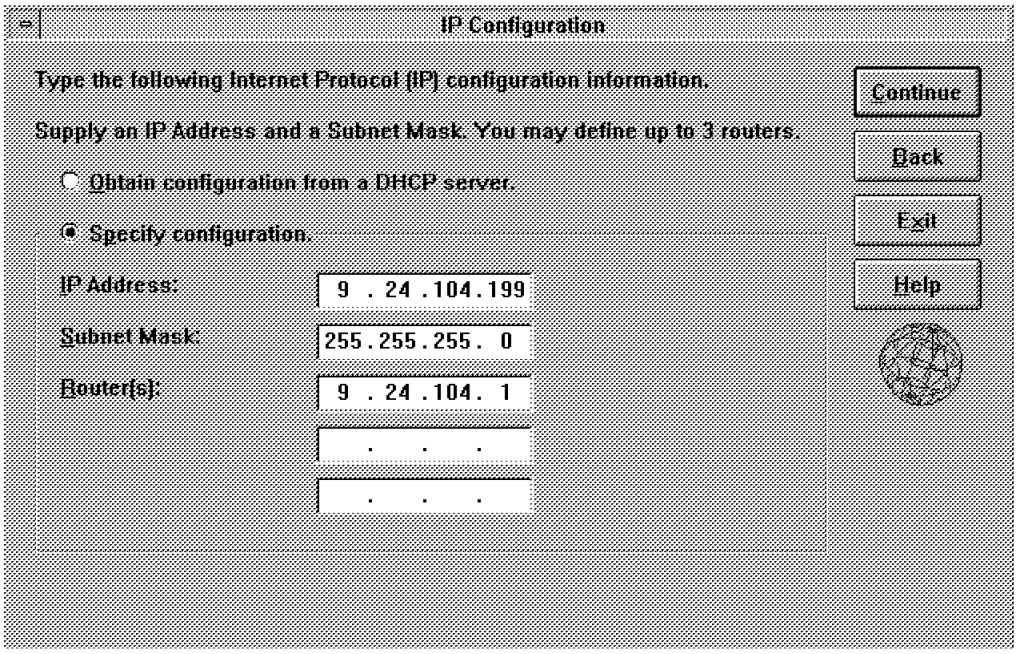


Figure 48. FTP Software Protocol Stack Installation - IP Configuration

8. At the IP Configuration panel select whether you will use DHCP (Dynamic Host Configuration Protocol) or you will specify the configuration manually. In the latter case, provide the IP address and the network mask of your computer and the addresses of up to three routers.
9. At the Name Server Configuration panel select the type of the name server (DNS or NIS) and type in the corresponding configuration information. Click on **Continue**.

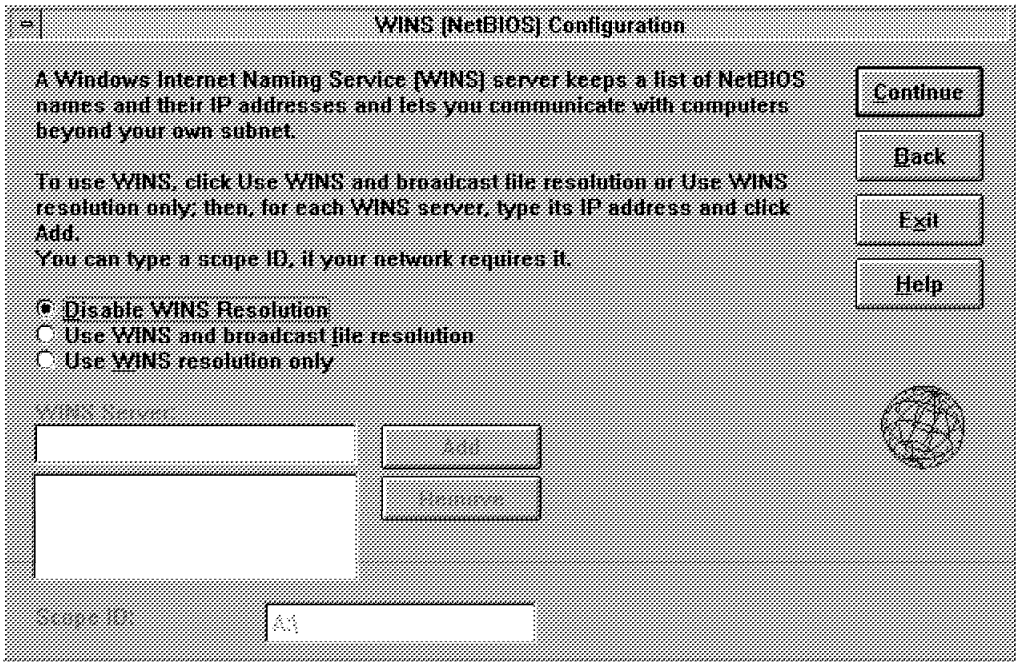


Figure 49. FTP Software Protocol Stack Installation - WINS Configuration

10. At the WINS (NetBIOS) Configuration panel specify whether Windows Internet Naming Service (WINS) should be used or not. If you want to use WINS resolution, you have two choices:

    - Use WINS and broadcast file resolution: NetBIOS will use primarily the WINS server(s), but if a given name cannot be resolved by the WINS server(s), it will use broadcasts.
    - Use WINS resolution only: NetBIOS will not use broadcasts to resolve hostnames.

    If you chose to use WINS, provide the IP address(es) of the WINS server(s) and the scope ID if needed. When using TCP/IP to handle NetBIOS traffic, all computers that will communicate with each other using NetBIOS broadcasts must use the same scope ID. See your network administrator for help.

    After completing this panel, click on **Continue**.

11. Type in your user ID on remote hosts. Click on **Continue**.
12. Select your time zone. Click on **Continue**.
13. Click on **Continue** to begin copying the files and complete the installation.

14. At the Update DOS System Files dialog box click on **Yes**. Backup copies of the system files will be made.

15. At the Setup Complete dialog box read the information and click **OK**.

16. Click on **Restart System**.

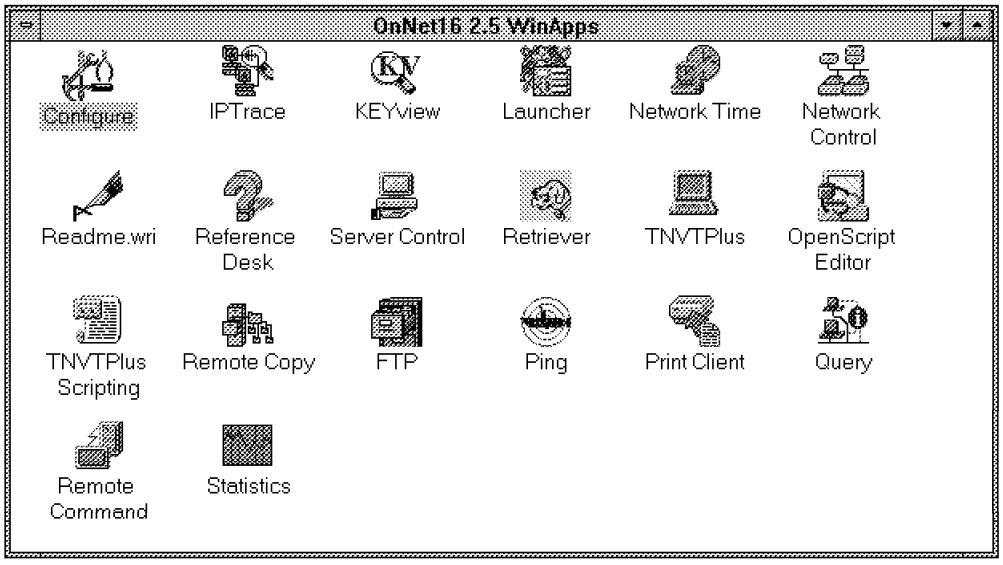


Figure 50. FTP Software Applications Program Group

The FTP Software TCP/IP applications and protocol stack installation has completed. You can access its functions from the OnNet16 2.5 WinApps program group, which looks similar to Figure 50.

Note: From now on Windows 3.x will start up with the Automatic Logon panel, where you can specify your user ID and password for the InterDrive Client to automatically log you on whenever you mount an NFS drive or printer.

3.3.3 Installing Personal Communications for Windows 3.x

Personal Communications for Windows 3.x comes with a variety of associated products:

- LAN Support Program (LSP) provides APIs to support network application programs on different network adapters.
- APPC Networking Services enables applications on your computer to communicate with partner applications on a wide variety of IBM and non-IBM systems that support Advanced Peer-to-Peer Program

Communications (APPC). This product also supports Common Programming Interface for Communications (CPI-C) APIs.

- AnyNet enables application programs to communicate over different types of networks and across interconnected networks. This helps reducing the number of network protocols in use and the complexity of the network management.
- IBM Library Reader is an online documentation (book) viewer for the BookManager formatted files.
- CM Mouse is a utility that maps mouse actions to host screen actions. It helps you easily navigate the host screens. It provides macro definition and playback functions combined with screen recognition capabilities.

The install program guides you through the installation steps of these associated products.

Begin the installation from the eNetwork Communications Suite Setup panel, shown on Figure 45 on page 105. Click on **Install Personal Communications**. The setup wizard will bring up the IBM Personal Communications Setup dialog box, where you can select the components you want to install. Make your selections and click on **Continue**. If you plan to use the IBM Library Reader, install it *first*.

In the following paragraphs we describe the installation steps for the individual components that are included in Personal Communications for Windows 3.x. We assume that you have already selected the component you want to install and the wizard has just started the installation process. Although you can select to install several components at the same time, we recommend selecting just one, installing it, then rebooting and continuing with the next component. In this way you will get greater control over the installation process.

Note: You will have to reboot anyway after the IBM Library Reader installation in order to be able to use the installed books.

3.3.3.1 Installing the IBM Library Reader

If you want to install the IBM Library Reader, you must install it and reboot your computer before installing any other component.

The installation steps are the following:

1. Tick *only* the IBM Library Reader check box on the IBM Personal Communications Setup dialog box. Click on **Next** to continue.

2. On the next dialog box the Setup Wizard will show the component to be installed. Click on **Next** to continue.
3. Read the message on the Installation Instructions window and click on **Continue**.
4. Click on **OK** on the Install dialog box.

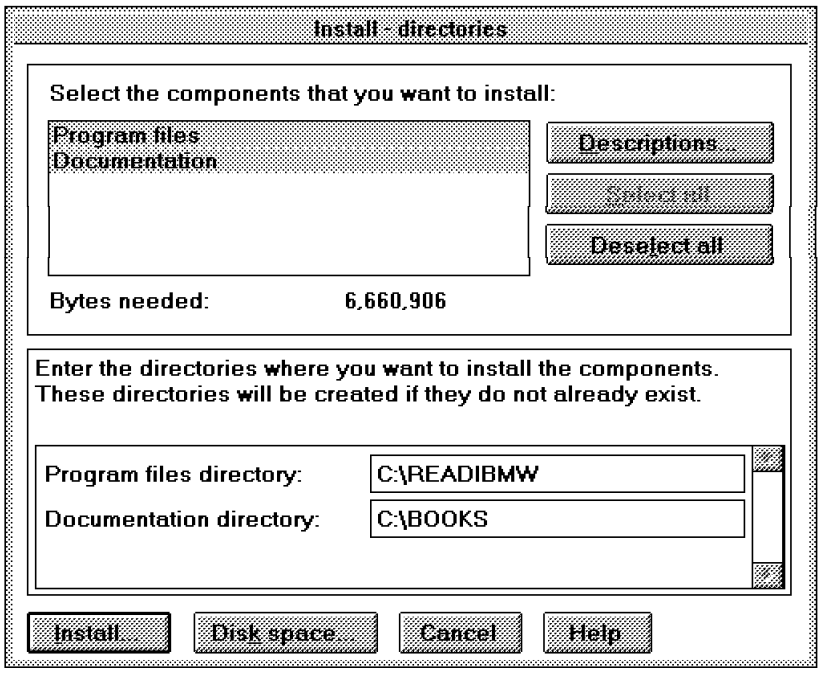


Figure 51. IBM Library Reader - Component Selection

5. At the Install - directories dialog box select the components you want to install, and change the destination directories if needed. You have to select the **Program files** in order to install the product. The Documentation item is optional. Click on **Install** to continue.

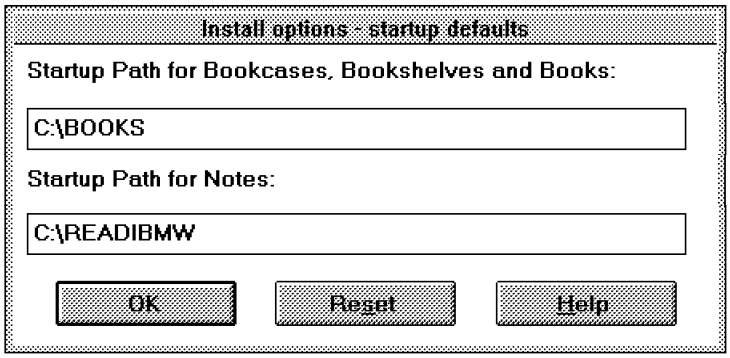


Figure 52. IBM Library Reader - Startup Defaults

6. At the Install options - startup defaults dialog box change the startup paths of the product if needed. Click on **OK** to continue.
7. At the Installation and Maintenance dialog box click on **OK** to continue.
8. Reboot your system.

The IBM Library Reader is now ready to use. A program group named Library Reader for Windows has been created. You can access the online books by double-clicking on either the **Library Reader for Windows** or the **List of Bookcases** icon.

3.3.3.2 Installing the LAN Support Program (LSP)

Please have your LAN adapter driver diskette with the NDIS drivers easily accessible. As an alternative, you will be able to specify the path to the driver if it is stored on other media, such as your hard disk.

1. Press Enter on the Welcome screen.
2. Read the information about LSP, then press Enter.
3. Press Enter again after reading what you need for the LSP installation. Because you are installing from a CD-ROM to your hard disk, you will need neither the backup copy of the original LSP diskettes nor a formatted system diskette.

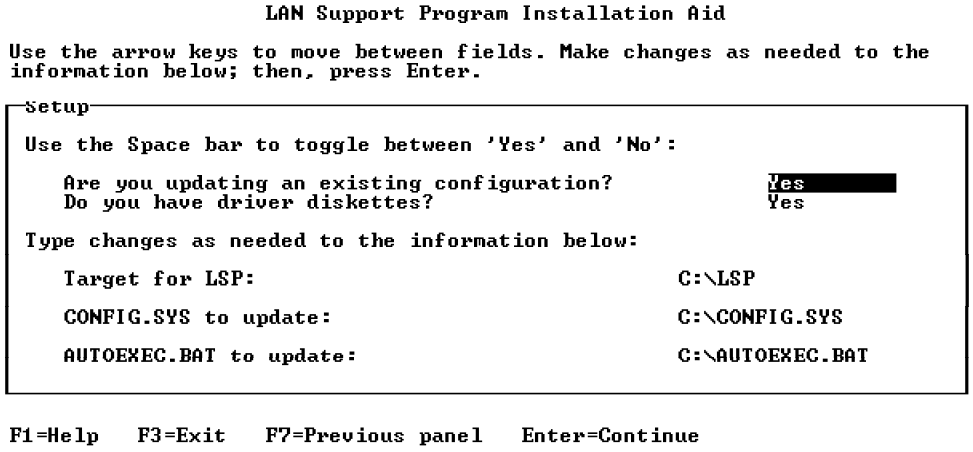


Figure 53. DOS LAN Support Installation - Setup Panel

4. At the Setup panel (see Figure 53) answer No to the question "Are you upgrading an existing configuration?" if this is the first time you install LSP. Answer Yes to the question "Do you have a driver diskette?" if you want NDIS support to be installed.

   You can change the target directory and the default CONFIG.SYS and AUTOEXEC.BAT files locations if needed.

   Press Enter to continue.

5. If you wanted NDIS support at the previous step, insert your LAN adapter driver diskette with the NDIS driver in the floppy drive. At the Process Driver Diskette panel change the path to the DOS NDIS files if needed. Press Enter to continue.

6. At the Information panel press F7 if you have additional driver diskettes; otherwise press Enter to continue.

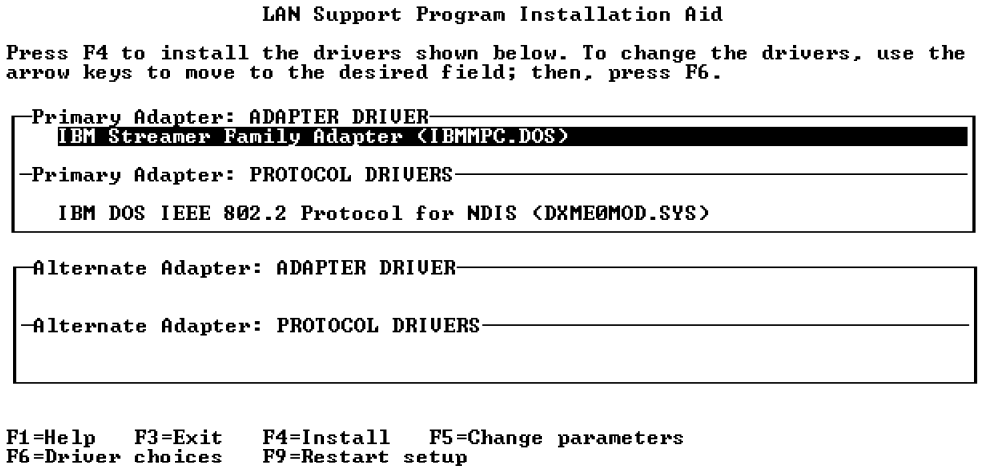


Figure 54. DOS LAN Support Installation - Driver Selection

7. You are presented with a screen shown on Figure 54, where you can select your adapter and protocol driver for both the primary and alternate LAN adapters. You can also change the default parameters for the drivers if needed. After you are done, press F4 to install the selected drivers.
8. If there is a diskette in your diskette drive, remove it. Then restart your computer for the changes to take effect.

Note: If besides LSP you selected other components to install, the Setup Wizard will take you directly to the next component installation.

3.3.3.3 Installing APPC Networking Services

Install this component following the steps below:

1. At the Install dialog box, click on **OK**.
2. At the Install - directories dialog box select the APPC Networking Services components you wish to install. You can also change the installation directories at this point. After making your selections, click on **Install...** to continue

   Note: Selecting **Base** is mandatory.
3. The installation program commences copying the files. After you are done, it pops up a dialog box asking whether you wish to do the configuration of the product at this time. If your answer is **Yes**, the Networking Services Configuration panel will be shown. You will receive step-by-step instructions for the configuration process. Ask your network administrator for assistance if you are not certain about the

parameters. After finishing with the configuration, click on **OK** to confirm the creation of the configuration file and the modifications of your system files.

4. At the Installation and Maintenance dialog box click on **OK** to acknowledge the successful installation of the APPC Networking Services.
5. Click on **Exit** at the Installation window and restart your computer for the changes to take effect.

The APPC Networking Services installation has completed. You can access the product's functions from the IBM APPC Networking Services program group.

3.3.3.4 Installing AnyNet

Follow these steps to install this component:

1. The installation program brings up the Information window. Read the material presented, it contains important information about AnyNet installation prerequisites in case of specific scenarios such as using APPC Networking Services. When finished, click on **Continue**.
2. At the Installation and Maintenance window select the desired installation mode:
   - AnyNet Workstation Setup to install the product and the accompanying documentation on a workstation.
   - AnyNet Code Server Setup to install a server for network distribution of AnyNet products and documentation.
3. Select **Install...** from the Action menu.
4. At the Install dialog box leave the Update CONFIG.SYS/AUTOEXEC.BAT check box ticked. Click on **OK** to continue.

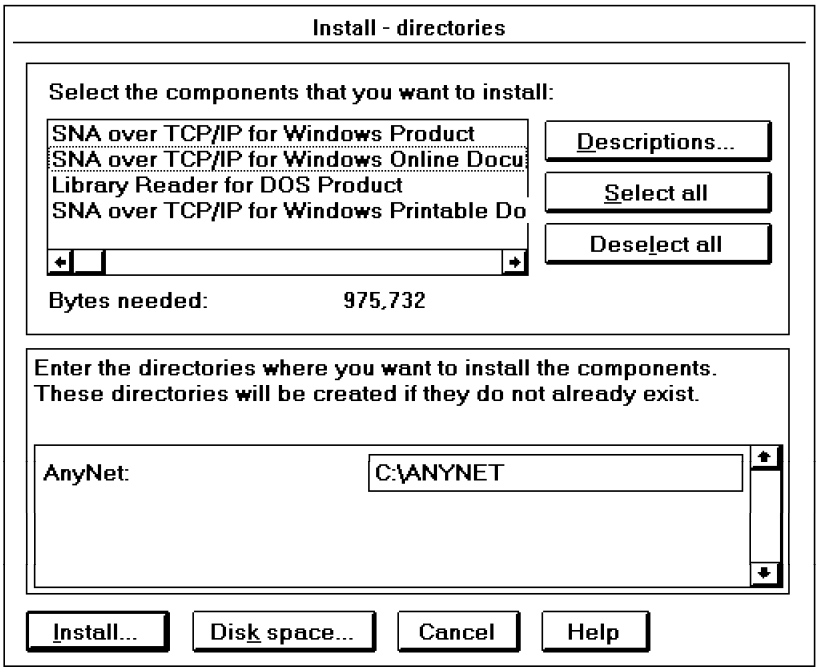


Figure 55. AnyNet Installation - Directories

5. At the Install - directories dialog box specify which subcomponents you want to install. After you are done, click on **Install** to continue. During the installation you will be asked whether you have the IBM TCP/IP for DOS product installed. Make sure you have the FTP Software TCP/IP protocol stack installed before you install AnyNet, then answer yes to this question. The installation process will continue.

   Note: A TCP/IP product is needed to run AnyNet. Ensure that such a product is installed before attempting to run AnyNet.

6. Specify a directory in which IBM Library Reader or BookManager/Read is installed. Select **OK**. The installation will continue.

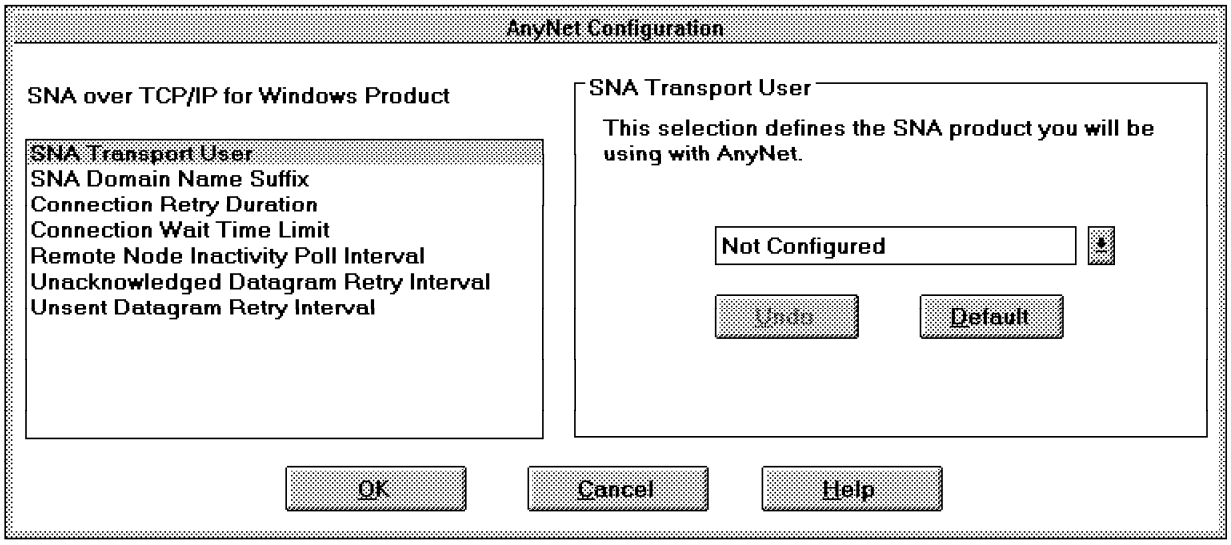


Figure 56. AnyNet Installation - Configuration

7. After the product files have been successfully copied, the AnyNet Configuration window will pop up. See your network administrator if you are uncertain about the configuration data that applies to your system. After configuring AnyNet, click on **OK** to continue.
8. Click **OK** on the message box to acknowledge that modifications have been made to your AUTOEXEC.BAT and CONFIG.SYS files.
9. Click **OK** on the message box that informs you about the successful completion of the installation.
10. Reboot your computer to make the changes effective.

During the installation a program group called AnyNet has been created. Included in this program group are the configuration tool and a README file.

3.3.4 Installing Netscape Navigator for Windows 3.x

The installation of the Netscape Navigator consists of a number of separate steps:

1. Installation of Netscape Navigator
2. Configuration of Netscape Preferences
3. Configuration of Netscape Mail and Netscape News
4. Installation of Netscape Plug-Ins

We explain each of the above steps in detail in the following sections. These steps are practically the same as in the case of the installation for Windows NT and for Windows 95. We repeat them here for your convenience.

3.3.4.1 Installation of Netscape Navigator

To begin the installation, you should start from the IBM eNetwork Communications Suite Setup panel as described in 3.1, “Installing on Windows NT” on page 61. From there, follow these steps to install the Netscape Navigator:

1. Click on the item **Install Netscape Navigator**. This will start the Netscape Navigator Setup program. Read the brief welcome, then click on **Next** to continue.
2. Your next option is the destination directory. Click on **Browse** to change the destination, or click on **Next** to accept the default.
3. You will now be asked if you wish to install the CoolTalk application for Netscape Navigator. If you have a properly configured sound card with a suitable microphone, you can choose to install this option as well. To do so, click on **Yes**. If you do not wish to install the CoolTalk application, then choose **No** and continue with the installation of the Netscape Navigator. The installation program will now commence copying the files to your hard disk.
4. If you chose to install the CoolTalk application, you will be asked if you wish to enable the CoolTalk Watchdog. This program will listen for incoming connections from other users who are using CoolTalk, and automatically start the CoolTalk application. If you have a permanent connection to your network, you should select this option.
5. Once the files have been copied to the hard disk, the installation program will ask if you wish to connect to the Netscape homepage to continue with the installation. Select **No**, as we explain the configuration of the Netscape Navigator in this section.
6. The installation program will now ask if you wish to view the README file. You should choose **Yes**, as it may contain important last-minute information not found in this publication, or the program documentation.
7. Click on **OK** once the setup has completed. This will close the installation program, and give you the opportunity to view the README file.
8. Close the README file once you have finished reading it.

Now that the above steps have been completed, you should have a program group open in the Program Manager that looks similar to Figure 57 on page 121.

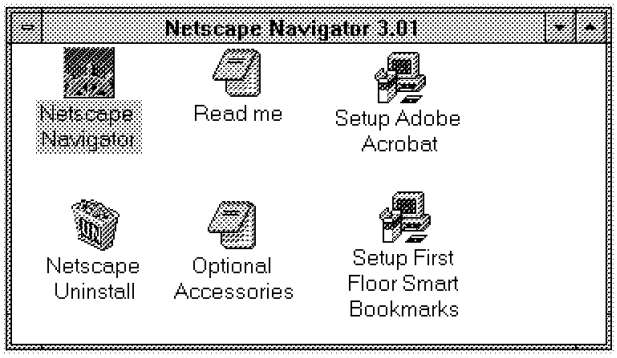


Figure 57. Netscape Navigator Program Group

If you have a direct connection to the Internet, you will now be able to use the Netscape Navigator without any further configuration. Most of the general preferences are simply cosmetic changes, and do not require alteration. If you require information on these settings, select **Options/General Preferences** from the menu bar, and press F1, or click on **Help**.

3.3.4.2 Configuration of Netscape Preferences

Double-click on the **Netscape Navigator** object to start the Netscape Navigator. The application should start and load an introduction page that welcomes you to the eNetwork Communications Suite. You can read this information now, or the next time you start the Navigator.

If you are connected to the Internet via a proxy server or other firewall device, then you need to configure this in the Netscape preferences. If you are not sure, then contact your system administrator who can give you the correct details. As an example, we show you how to configure the Netscape Navigator to use a proxy server. We assume the details of the proxy server are as follows:

Proxy Server: proxy.au.ibm.com
Port: 80

1. From the Netscape menu, select **Options** with your mouse. Then select **Network Preferences** from the drop-down menu.
2. Click on the **Proxies** tab of the Preferences notebook.

3. Click the radio button for **Manual Proxy Configuration** and then click **View**.

4. In the Manual Proxy Configuration notebook, fill in the name of the proxy server next to those protocols that the proxy server supports. In our case, it is FTP and HTTP. Type in the port number as well.

5. Generally, if you have a proxy server, it is only required for those sites outside of your internal network. Check with your system administrator, but in most cases, you can tell Netscape not to use the proxy server for connecting to machines within your own domain. If so, place the domain name of your network into the section called No Proxy For. In our example, this was au.ibm.com. Once completed, you should have a configuration similar to Figure 58.

6. Click on **OK** to apply these changes. Click on **OK** again to close the Network Preferences notebook.

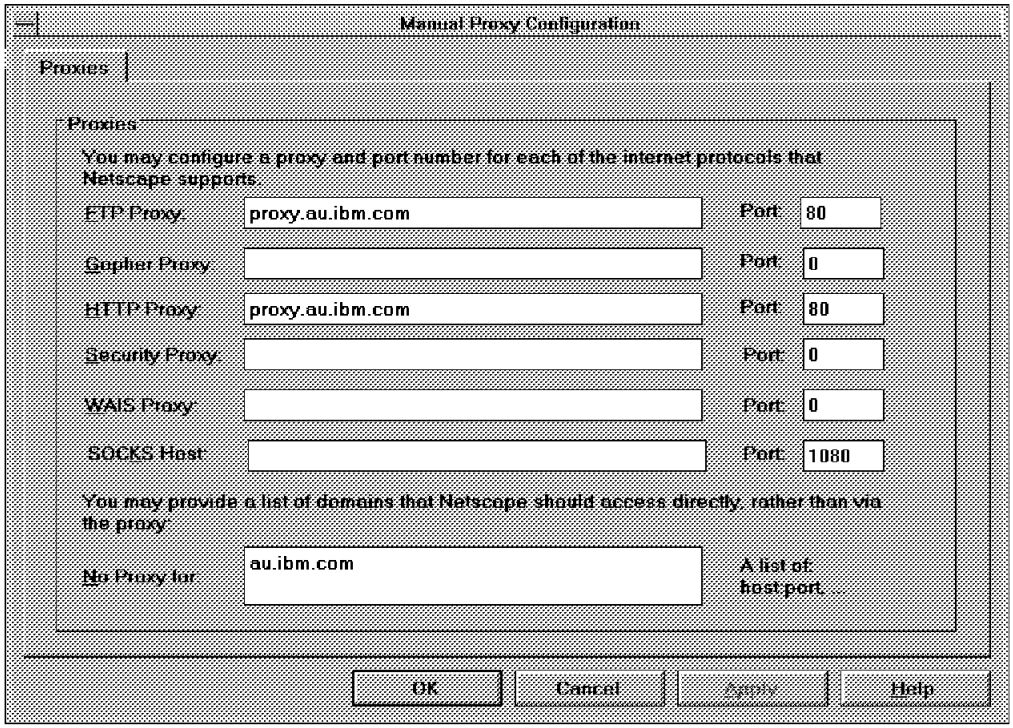


Figure 58. Manual Proxy Configuration Setup (Windows 3.x)

3.3.4.3 Configuration of Netscape Mail and Netscape News

To configure the Netscape Mail and News functions, you will need the following information from your system administrator. Of the many options that can be configured, this is the most basic information required. If you do not have any or all of this information, you will not be able to use the Netscape Mail or Netscape News effectively.

SMTP Mail Server This is the fully qualified hostname of the server that you will be using to send your new e-mail messages to for delivery.

For example: mail.raleigh.ibm.com

POP3 Mail Server This is the fully qualified hostname of the server that you will collect your new e-mail messages from. Often, this will be the same as the SMTP mail server.

For example: pop3.raleigh.ibm.com

POP3 User Name This is your user ID for the POP3 mail server. While it is often the same as the first part of your e-mail address, it does not need to be.

For example: meaden

POP3 Mail Password This is your password for collecting your e-mail from the POP3 mail server. It will probably be assigned to you by the system administrator.

For example: password

NNTP News Server This is the fully qualified hostname of the news server you will use to send and receive messages from the Internet newsgroups.

For example: news.raleigh.ibm.com

Email Address This is your full e-mail address that you will use for electronic mail on either the Internet, your Intranet, or both.

For example: meaden@raleigh.ibm.com

Your Name This is generally your first and last name. If the same e-mail address is being used by many people in the same section, it will often represent the name of the department, or their purpose.

For example: Software Support

Once you have these details, start the configuration with the following steps:

1. Selecting **Options** from the Netscape menu. From the pull-down menu, select **Mail and News Preferences**.
2. Select the tab marked **Servers** from the Preferences notebook.
3. In the field called Outgoing Mail (SMTP) Server type in the name of your mail server.
4. Press the Tab key, or use the mouse to move to the next field called Incoming Mail (POP3) Server. In this field, type the name of your POP3 mail server.
5. Press the Tab key, or use the mouse to move to the next field called POP3 User Name. In this field, type your POP3 mail user ID.
6. Press the Tab key, or use the mouse to move to the field called News (NNTP) Server. In this field, type the name of your news server.
7. Once those details are complete, your Servers Preferences should look similar to Figure 25 on page 74. Select the **Identity** tab from the Preferences notebook to continue the configuration.

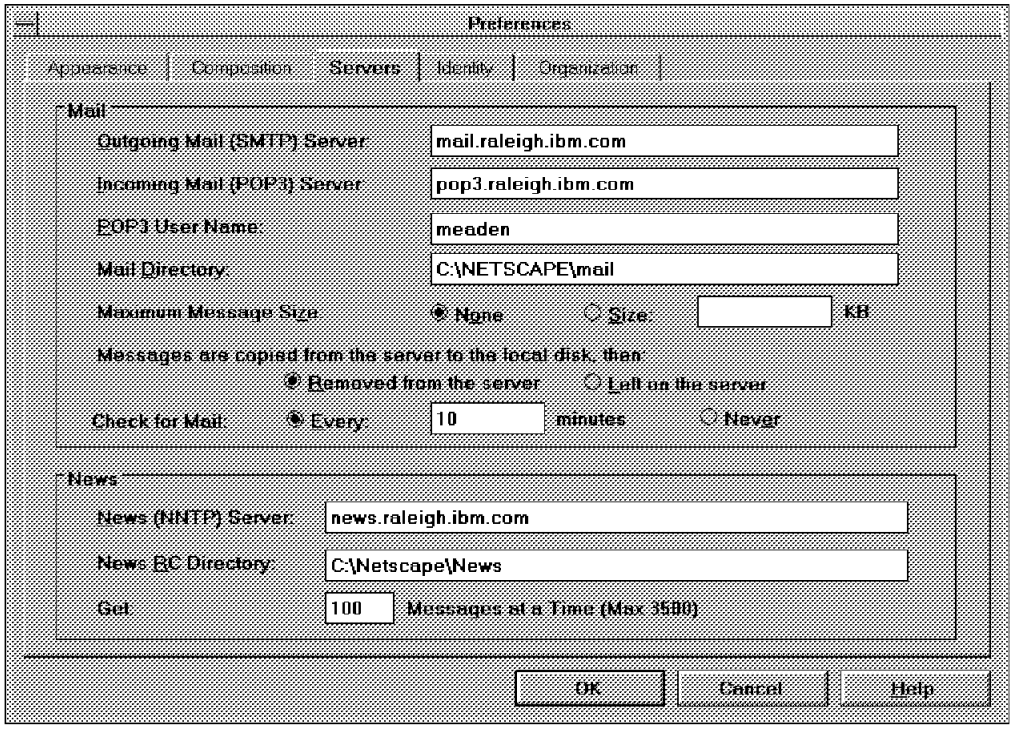


Figure 59. Netscape Preferences - Servers (Windows 3.x)

8. In the field titled Your Name, type in the user name, or other name you have selected for this e-mail account.
9. Use the Tab key or the mouse to move to the next field called Your Email. In this field, type the e-mail address of the account.
10. Double-check that your configuration looks similar to Figure 60. If so, click **OK** to save the changes.

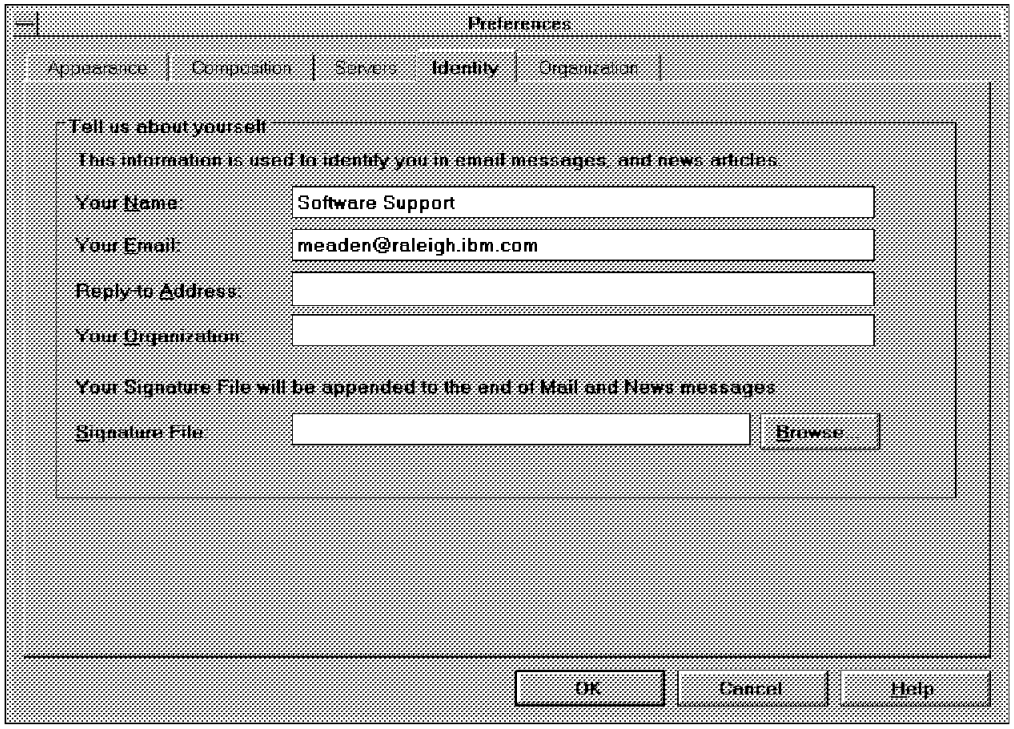


Figure 60. Netscape Preferences - Identity (Windows 3.x)

Your Netscape Mail, and Netscape News are now properly configured and ready to run.

3.3.4.4 Installation of Netscape Plug-Ins

To install the Netscape Plug-Ins, ensure the IBM eNetwork Communications Suite CD-ROM is in the CD-ROM drive.

Note: The IBM techexplorer plug in is not available in the Windows 3.x environment.

The following information is for installing the Adobe Acrobat Plug-In for Netscape Navigator:

1. From the Netscape Navigator program group (Figure 57 on page 121) double-click on the **Setup Adobe Acrobat** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Read the Adobe license carefully, and select **Accept** if you agree to the terms of the license. If you select **Decline** to indicate you do not accept the license agreement, the installation will end.
4. The installer will now ask for an installation directory. Accept the default directory by selecting **Install**. You can change the destination directory by typing over the existing installation path with your preferred location.
5. Click on **OK** when you receive a notification about the registration procedure.
6. At the prompt for Name and Organization, you should enter the details of yourself, the license owner, or the end user. Click **OK** when complete.
7. The Adobe Acrobat Installer will now commence copying the files to your hard disk. Click on **OK** once the installation has completed.

The Adobe Acrobat Reader Plug-In has now been successfully installed.

To install the First Floor Smart Bookmarks plug-in, follow these instructions:

1. From the Netscape Navigator folder (Figure 57 on page 121) double-click on the **Setup First Floor Smart Bookmarks** object.
2. Click on **OK** to confirm you have the CD-ROM inserted.
3. Once the setup wizard has started, read the brief welcome screen and click **Next** to continue.
4. At the User Information section, you should complete the details in the same way as for the Adobe Acrobat installation. If the section marked Serial is not already filled in, check your product documentation for this number. If it is already filled in, then leave the current value as is.
5. Confirm your earlier input by selecting **Yes**, or change the details by selecting **No**.
6. You will now be asked which type of installation you wish to perform. For most users, the default Typical installation will be sufficient, and you should select that option. Click on **Next** to continue.
7. If the destination directory you chose does not yet exist, the installation application will ask if it can create it for you. Choose **Yes** and continue with the installation.

8. The installation will now ask you which Internet Browser you are using. The default selection is **Netscape 2.0 or later**. Do not change that setting, as this is the correct choice. Click **Next** to continue the installation.
9. Select your time zone and click on **Next** to continue.
10. The installation wizard will now double-check the options you selected. If you have nothing you wish to change, click **Next**.
11. The installation wizard will now copy the files to your hard disk.
12. Once finished the file copy, the installation wizard will advise you it has completed, and give you the option to view the README. Select **Finish** and the installation will end, presenting you with the application README file. Read through this file in case there have been any last-minute changes.

The First Floor Smart Bookmarks plug-in has now been successfully installed.

All these plug-ins are automatically loaded when the Netscape Navigator is started. If the Netscape Navigator encounters a WWW page that uses one of the plug-ins, it will be invoked automatically.

3.3.5 Installing the Lotus Notes Mail Client for Windows 3.x

This section assists you in installing the Lotus Notes Mail Client. If your organization has access to a Lotus Notes Server, and you wish to take advantage of the powerful e-mail capabilities of the Lotus Notes Mail Client, read this section carefully.

1. Start the IBM eNetwork Communications Suite Setup panel as described in 3.3, “Installing on Windows 3.x” on page 104, and click on **Install Lotus Notes Mail**.
2. The next screen is a welcome panel. In the fields provided, type in your name, and the company name. Click on **Next** to continue with the installation.
3. The installation will ask you to confirm the information you typed in on the previous panel. Click on **Yes** to confirm the information, or take this opportunity to go back and correct it.
4. Select **Standard Install** from the Install Option dialog. You can change the default installation path from this dialog by typing in the program and/or data directory path. Click on **Next** to continue the installation.
5. The installation program will now ask you which program group you want the application icons installed to. Accept the default, highlight a

new selection, or create a new program group. Once you have made any changes, click on **Next** to continue.

6. The installation program is now ready to copy the files to your hard disk. Click on **Yes** to continue.
7. When finished, it will advise you that the install is complete. Click **Done** to exit the installation.

The installation of the Lotus Notes Mail Client is now complete. Start the Notes client to commence the configuration. For details on configuring your Lotus Notes Mail Client with the correct settings, refer to your Notes administrator.

3.3.6 Multiple Protocol Support

Although the design of DOS and Windows 3.x does not make them very suitable for robust multiprotocol networking, it is possible to run multiple protocol stacks under these environments. Specifically we will consider the concurrent use of the NetBIOS, TCP/IP and IEEE 802.2 interfaces on a single Windows 3.x system. The products involved are:

- DOS LAN Services for NetBIOS support
- FTP Software TCP/IP protocol stack for TCP/IP support
- Personal Communications for IEEE 802.2 support

The system on which we installed and tested these products is an IBM PS/2 Model 80. We used drive C: for all the products and used the default installation directories.

Important

Make backup copies of your original system files and also back up these files after each product installation step. In this way you can always restore an already correct configuration. The files involved are CONFIG.SYS, AUTOEXEC.BAT, PROTOCOL.INI, SYSTEM.INI, WIN.INI.

Follow the steps below to successfully install these products:

1. Install DOS LAN Services. Select the virtual redirector for Windows 3.x. support.
2. Reboot your computer and verify the NetBIOS connectivity by logging on to the network and accessing some shared resources.
3. Install the FTP Software TCP/IP protocol stack. See 3.3.2, “Installing the FTP Software TCP/IP Applications and Protocol Stack” on page 106 for details. At the end of the installation a dialog box titled Network Driver

Availability will pop up. Select **Primary Network**. Verify that the Chain network ″IBM DOS LAN Services″ check box is ticked.

4. Reboot and verify that the TCP/IP stack is operational by pinging an active host on the network. Also check that DOS LAN Services is still operational.

5. Install the LAN Support Program component of the Personal Communications. See 3.3.3, “Installing Personal Communications for Windows 3.x” on page 111 for details. Select **IEEE 802.2 NDIS support (DXME0MOD driver)**. You will need the LAN adapter’s driver diskette for this.

6. Make sure that your system files look like the examples below. Use a plain text editor to make changes if necessary.

   a. CONFIG.SYS file. It should contain the following drivers:

```
DEVICE=C:NETPROTMAN.DOS /I:C:NET      1
DEVICE=C:\NET\IBMTOK.DOS      2
DEVICE=C:\NET\DLSHELP.SYS      3
DEVICE=C:\PCTCP\DIS_PKT.GUP      4
DEVICE=C:\LSP\DXMA0MOD.SYS 001      5
DEVICE=C:\LSP\DXME0MOD.SYS N ,8,0,6,6   6
```

   Notes:

   1 This is the protocol manager. It must be the first driver. The /I switch specifies the directory where the PROTOCOL.INI file is located. The LAN Support Program installation utility changes this to C:LSP, so you have to edit this line to make the protocol manager use the PROTOCOL.INI file in the C:NET directory.

   2 This is the token-ring network driver.

   3 This is the DOS LAN Services driver.

   4 This is the MAC/DIS to Packet Driver converter needed for TCP/IP support.

   5 This is the interrupt arbiter.

   6 This is the IEEE 802.2 NDIS driver. The parameters are set by the LAN Support Program installation (see Figure 54 on page 116).

   b. AUTOEXEC.BAT file. It should contain the following relevant statements:

```
C:NETNET START   1
SET PCTCP=C:\PCTCP\PCTCP.INI
C:\PCTCP\VXDINIT.EXE   2
```

Notes:

1 This command calls the NETBIND protocol binder. Make sure that you remove any other NETBIND calls from the file.

2 This is the resident VxD loader for the Windows 3.x TCP/IP protocol stack.

c. PROTOCOL.INI file. Note that you should use the PROTOCOL.INI located in the C:NET directory (see **1** at 6a on page 129). Edit the file to look like this:

```
[network.setup]
version=0x3100
netcard=ibm$ibmtra,1,IBM$IBMTRA
transport=ibm$netbeui,IBM$NETBEUI
lana0=ibm$ibmtra,1,ibm$netbeui

[protman]
DriverName=PROTMAN$
PRIORITY=ibm$NETBEUI

[IBM$IBMTRA]
DriverName=IBMTOK$

[IBM$NETBEUI]
DriverName=netbeui$
SESSIONS=20
NCBS=20
BINDINGS=IBM$IBMTRA
LANABASE=0

[PKTDRV]
DriverName=PKTDRV$
intvec=0x60
chainvec=0x62
BINDINGS=IBM$IBMTRA
class=17

[DXME0]
DriverName=DXME0$
Bindings=IBM$IBMTRA
```

d. SYSTEM.INI file. This is located in the Windows 3.x base directory, usually C:WINDOWS. Check for the following lines under the [386Enh] section:

```
device=C:PCOMWINVpollD.386
device=C:\PCOMWIN\VslanD.386
device=C:\PCOMWIN\VdoshllD.386
device=C:\PCOMWIN\VpcsrtrD.386
device=C:\PCOMWIN\Vint21hD.386
device=C:\PCOMWIN\VvprtD.386
```

After you have completed, reboot your computer.

7. Install the emulator component of Personal Communications. See 3.3.3, “Installing Personal Communications for Windows 3.x” on page 111for details on how to do this. After the installation is done, restart Windows 3.x.

8. Check the IEEE 802.2 connectivity by configuring accordingly and starting a host emulator session. See your network administrator for parameter values needed for this type of connection.

Now your Windows 3.x system supports all three protocols. Note that the necessary drivers consume a considerable amount of conventional memory. You might have problems running your DOS applications, especially when you use a number of other device drivers also. Loading some of the drivers into high memory might help. Try this method carefully; there is no general rule that guarantees success.

3.4 Aspects of Systems Management

The eNetwork Communications Suite contains several components to make it easier to incorporate it into systems management policies and architectures that may be in place in larger networks. One of them provides for SNMP management, the other, in a somewhat limited way, for software distribution. The problem with the eNetwork Communications Suite today is that the components have not yet been fully integrated to facilitate, for instance, an automated and unattended installation of the whole product. This is subject to change in future releases. In this section, we address the systems management capabilities that are already available with eNetwork Communications Suite and provide alternative ways where practical.

3.4.1 The SNMP MIB-II Server

The FTP Software TCP/IP protocol stack includes an SNMP agent (a term we prefer to use over the term SNMP server) that runs as a Windows 95 network service. This agent allows an SNMP manager application, such as TME 10 NetView for AIX, to access and change system information in a client running FTP Software TCP/IP protocol stack. The information that a manager can see and/or change is contained in a database called the

Management Information Base (MIB). See 1.8.3, “Simple Network Management Protocol (SNMP)” on page 30 for more information on SNMP.

To install and configure the SNMP MIB-II Server, follow the instructions below:

1. Select **SNMP MIB-II Server** from the list of components during the installation of the FTP Software TCP/IP protocol stack, as shown in Figure 28 on page 82.
2. After the installation has completed and the system restarted, double-click on the **Network** object in the Control Panel folder or select **Properties** from the Network Neighborhood context menu to enter the Network setup panel.
3. From the Configuration tab, click on **Add**, select **Service** and then click on **Add** once more.
4. From the list of Manufacturers, select **FTP Software, Inc.**, and **SNMP MIB_II Server from FTP Software, Inc.** from the list of Network Services. Then click on **OK**.
5. Now select **SNMP MIB_II Server from FTP Software, Inc.** from the list of installed network components (you may have to scroll down the list to locate it) and click on **Properties**. The following panel will appear:

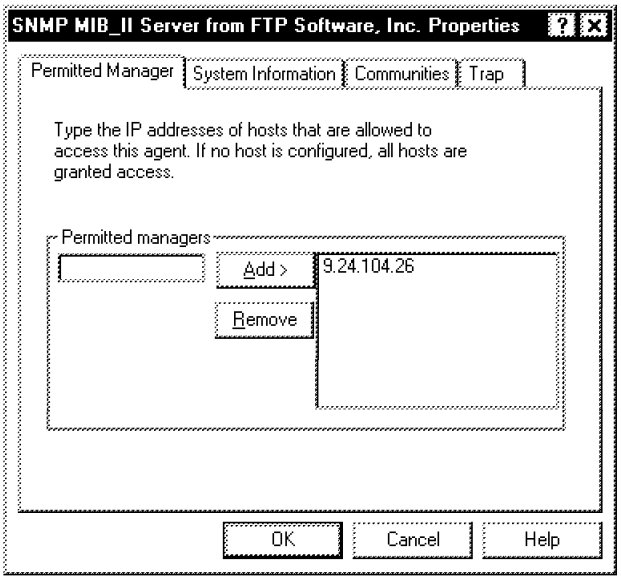


Figure 61. SNMP MIB-II Server Configuration

6. On the Permitted Manager tab, add the IP addresses or host names of SNMP managers that should be allowed to access the SNMP agent (server) on your system.
7. On the System Information tab, enter the name and location for a contact person that a network administrator can turn to in case there are problems with your system.
8. On the Communities tab, enter the SNMP communities that your system participates in. The default is *public*.
9. On the Trap tab, add the IP addresses or host names of SNMP manager systems that should receive unsolicited error messages (SNMP traps) that the SNMP agent (server) on your system generates.
10. Restart your workstation to enable the SNMP MIB-II Server.

3.4.2 Automated Installation and Software Distribution

One of the problems that faces a system administrator is how to install the product on every client in an enterprise, and to manage those systems easily. The eNetwork Communications Suite has a number of options available for installation across an enterprise. Which option you choose depends upon the size of your organization.

3.4.2.1 Shared CD-ROM Installation

If your organization has an existing network that enables the client machines to connect to a shared CD-ROM, then you can install from that shared resource. Simply assign the shared CD-ROM resource as a drive letter, then change to that drive and start the respective installation program. Follow the installation instructions in Chapter 3, “Installation and Configuration” on page 61.

3.4.2.2 Server Installation

Most of the applications that make up the eNetwork Communications Suite, the exception being Netscape Navigator, can be installed as server installations by using an option of the setup program that will copy all files from the product CD-ROM to a shared directory on a file server. This allows you to install the features you require onto each client machine from the server. The client machine will still require access to the server via an existing network infrastructure.

The advantage that this method has over the shared CD-ROM installation is that some of the components allow you to store all application files on the server and then actually run the application from the server. Only a minimum of files and data are kept on the client machine. The applications

that allow this are Lotus Notes Mail Client and IBM Personal Communications.

The FTP Software TCP/IP protocol stack and applications allow you to install to the file server. You then install a copy of those applications onto the client machine.

3.4.2.3 Using Custom Install Manager

As an example, the FTP Software TCP/IP protocol stack and applications contain a function called the Custom Install Manager (CIM). This feature allows you to create groups of systems with common requirements. When you install the client on a system, you specify which of these groups the system will belong to. The custom install manager will then install the predefined components. Basically, CIM creates a SETUP.INF file based on your parameters and uses that as an input file for the client setup program.

3.4.2.4 Pre-Built Installation Image

This method will save you considerable time if you are planning to install a large number of client machines. The machines must be nearly identical. To create an installation image, build a machine with the chosen operating system, and install the components you require. This will be used as the basis for all the machines you are installing onto. The next time you require a machine with this image, you copy the entire contents of this machine to the machine to be duplicated. All you will need to do is change the minor configuration details that vary for each individual machine. Such details include the TCP/IP address, e-mail address and Personal Communications setup.

To copy the contents of one machine to another, there are a couple of tools available. LapLink is a popular utility for copying files across a serial or parallel port. The best method would be to boot from DOS diskettes on both machines, and run the LapLink program from those floppies. This will ensure that the operating system of each machine does not have any open files that will cause those files to be skipped. This method will only work with a FAT formatted drive.

You could also compress the entire hard disk partition to a single file, and then copy that compressed file to a server. You could create bootable diskettes that contain a basic network requestor that would connect to that server and then uncompress the image to the client machine. This has the extra benefit of freeing up the source machine. It also means that the source and destination machine do not need to be physically near each other.

3.4.3 Specialized System Management Software

If you are planning a very large corporate implementation, and you wish to be able to monitor end user machines, install and update software on the remote machines and perform other complex administration tasks, you should install separate system administration software.

An example of this type of software is TME 10 from Tivoli. TME 10 has many features, including:

- Distributing software to remote users
- Changing the configuration of a remote user's installation
- Updating applications on a remote system
- Automating tasks and applications on the remote system
- Monitoring resources across the network

For more information on TME 10, contact your IBM sales representative or refer to the URL:

`http://www.tivoli.com/`

3.5 The eNetwork Communications Suite and Dynamic IP Configuration

Dynamic IP has become more popular as a way of reducing the configuration required at an end user machine. Other benefits include allowing the system administrator to change the TCP/IP details of a remote system, without having access to the physical hardware. If the network requires a change in its subnet, or IP address allocation, the client machines will be updated automatically at next startup. If a mobile user often connects from several different sites in different subnets, then automatic configuration means that he or she will be able to connect from those sites without having to reconfigure the details of his or her TCP/IP stack manually.

It is also ideal for dial-up point-to-point connections where, for example, your company may have several hundred mobile users, but only 50 inbound dial-up lines. Instead of using up precious address space by giving each user his or her own fixed IP address, you assign only 50 IP addresses to those lines. The end user gets one of those IP addresses from the group each time he or she logs on.

3.5.1 Configuring DHCP

The FTP Software TCP/IP protocol stack includes support for DHCP configuration for IPv4. You will require at least one Dynamic Host Configuration Protocol (DHCP) server on the network. Within the setup of

the FTP Software TCP/IP protocol stack, you have to set up the interface to use Automatic Configuration. To configure this, follow the instructions below:

1. Click on the **Start** button under Windows 95.
2. Choose **Settings** and **Control Panel**. When the Control Panel folder is open, double-click on the **Network** object.
3. Select **TCP/IP Stack FTP Software, Inc. (FTPTCP96)** from the list of installed network components and then click on **Properties**.
4. Select the page for either **IP Configuration** or **Routers**.
5. In both sections select **Automatic configuration** to enable the use of DHCP.

Your configuration notebook should look similar to the examples in Figure 62. When the interface is initialized, the DHCP client code is executed and will attempt to get the details it requires from a DHCP server. These details include, among others, the host's own IP address, subnet mask, and broadcast address.

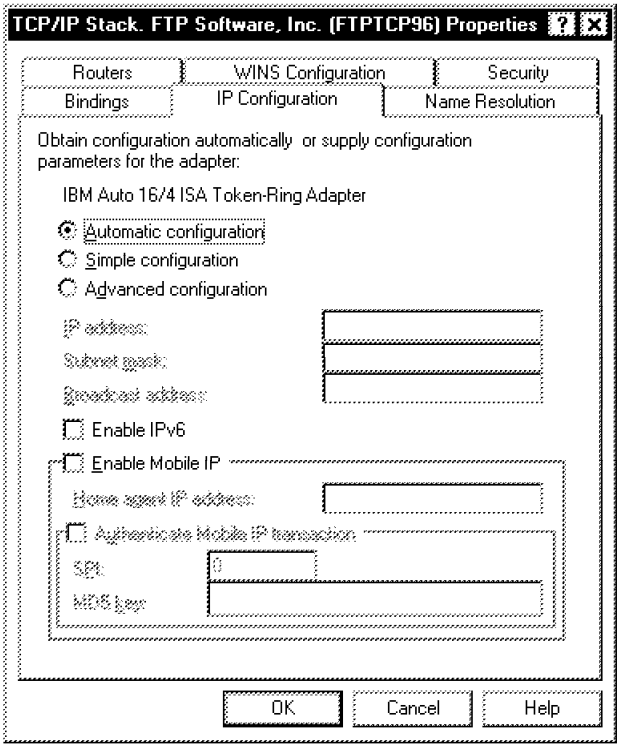


Figure 62. Automatic Interface Configuration with DHCP

It is also possible to set up the interface so that it receives its routing information from the DCHP server or by capturing router discovery packets. In that case, also set the router information to Automatic, as shown in Figure 63 on page 137.

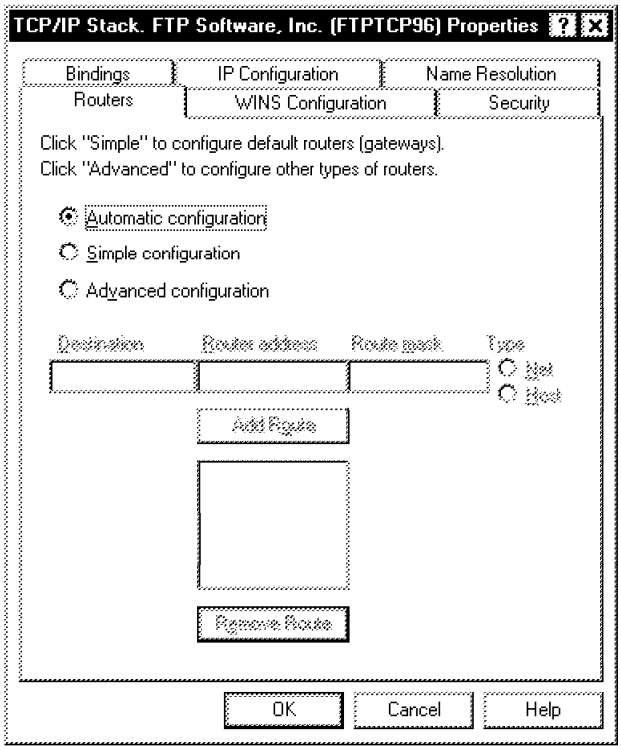


Figure 63. Automatic Router Configuration

For more information on DHCP, refer to RFC 1541, ″Dynamic Host Configuration Protocol″.

If you are using IPv6, then a different scheme is employed to obtain basic IP address and subnet information. At initialization of the interface, the host creates its own unicast address called a link local-use address, using the hardware address of the interface (for instance the IEEE 802 MAC address on a LAN), and appending it to the format prefix for link local-use addresses (1111 1110 10). If an IPv6 router exists on the network, it will advertise its subnet prefix on the network, and the host will use that information to update its link local-use address. In this way, each host will have a unique address on the network based on the assumption that the MAC address is a globally unique identifier.

You can then use DHCP to obtain additional configurations, such as name server and application server addresses, but the specifications for DHCP over IPv6 have not yet been finalized.

If you require more information, refer to RFC 1884, ″IP Version 6 Addressing Architecture″.

Chapter 4. Exploring Special Features

In this chapter we explain in detail some of the special features of the eNetwork Communications Suite and their implications for an enterprise-wide implementation. These special features rely on the FTP Software TCP/IP protocol stack, which is currently only available in the Windows 95 version of the IBM eNetwork Communications Suite.

Because many of these special features are still evolving as the standards are updated and amended by the Internet Engineering Task Force (IETF), there will be constant references to RFCs and other Internet documents.

For details on the latest standards, and their current status, please refer to the ″Internet Official Protocol Standards″ document. The latest version of this document is available from the following URL:

`ftp://ds.internic.net/std/std1.txt`

4.1 Implementing and Using IP Security (IPSec)

IP security standards currently rely on a key-based system for security. Key-based encryption is divided into two types: asymmetric and symmetric.

Asymmetric encryption works by having a pair of keys, one of which is public, and the other private. Data encrypted with the public key can only be decrypted by the corresponding private key. Conversely, data encrypted with the private key can only be decrypted by the corresponding public key. In this situation, the public key is distributed as needed and the private key is never disclosed to anyone other than the owner.

The symmetric encryption method works by setting a secret key that is known only to the parties who require the ability to encrypt and decrypt the data. The secret key should never be disclosed to anyone who is not authorized to decrypt the data. The implementation of the IP Security Architecture relies on a symmetric data encryption method.

The idea behind IPSec was to provide for authentication and encryption on the IP layer rather than using a variety of security protocols, such as SSL, on higher layers. Whereas application layer security protocols would only benefit a certain set of applications, IP layer security can be employed by any application and higher layer protocol.

IPSec is based on the concept of security associations which are defined by a Security Parameters Index (SPI), a sending user ID, and a destination IP

address. Security parameters include, among other information, the following:

- Authentication algorithm
- Cryptographic key(s) used with that authentication algorithm
- Encryption algorithm
- Cryptographic key(s) used with that encryption algorithm

Security associations are normally one-way, which means that there have to be two security parameter indexes for authenticated/encrypted sessions between any two hosts.

More information on IP Security can be found at the following URLs:

`http://ds.internic.net/rfc/rfc1825.txt`
`http://ds.internic.net/rfc/rfc1826.txt`
`http://ds.internic.net/rfc/rfc1827.txt`

4.1.1 Using IP Authentication Header (AH)

AH is used to create an encrypted header placed in an IP datagram for authentication, but the data itself is not encrypted. Each host with which you wish to communicate securely must supply a secret key. The remote host must also be aware of your secret key.

When negotiating a link, your key is used to process the datagram using a symmetric authentication algorithm known as Message Digest 5 (MD5). The resulting authentication data is placed in the Authentication Header. Fields in any protocol header that may change en route are treated as zero. The receiving system verifies this data by also combining the datagram with your secret key, applying the MD5 algorithm, then comparing the resulting data with the authentication header. In this way IP Security Architecture can provide source authentication and confirmation of the integrity of the data.

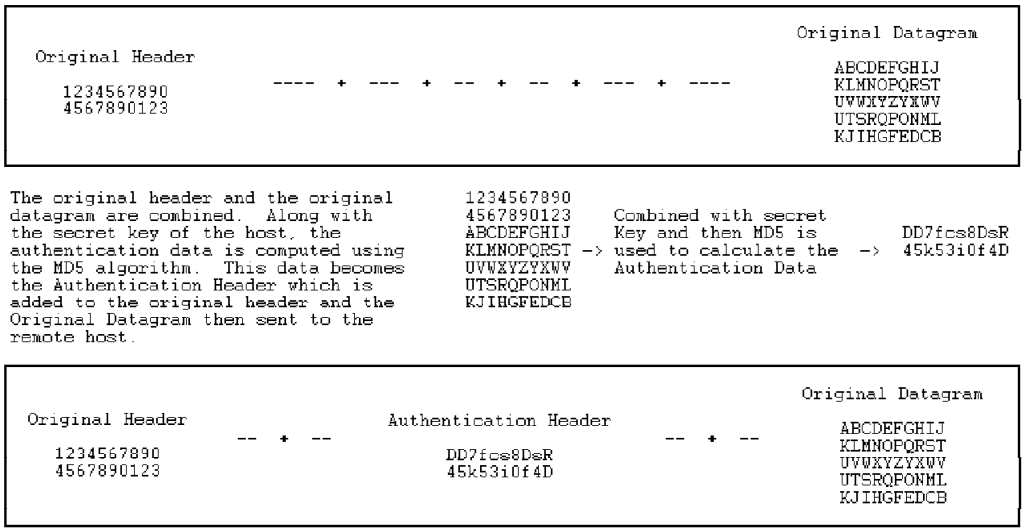


Figure 64. IP Security Using the Authentication Header

In the IP header, AH is identified by protocol number 51, assigned by the IANA.

4.1.2 Using Encapsulated Security Payload (ESP)

ESP is used to encrypt the data contained in an IP datagram which may be any protocol that IP can carry and the actual application data carried by those protocols.

ESP has two modes of operation:

Transport Mode

In this mode, ESP is used, as described above, to encrypt data contained in an IP datagram. This ESP payload is then placed in an IP datagram with a clear text (non-encrypted) header for normal delivery.

When negotiating a link, the original transport-layer frame (UDP, TCP, ICMP) of an IP datagram is encapsulated into ESP, and your key is used to process it using an encryption algorithm, such as DES. The resulting encrypted ESP is placed in the clear text IP datagram as the last payload (after any preceding headers, such as, for instance, AH). The receiving system strips off the clear text IP datagram and any preceding headers and decrypts the ESP with your secret key. The information from the IP header and the decrypted transport headers is combined and determines which application the user data should be delivered to.

Tunnel Mode

In this mode, ESP is used to encrypt a whole IP datagram including data as well as headers. Thus, the endpoints of the original datagram become hidden from the outside. This payload is then placed in a new IP datagram with clear text headers for delivery between the endpoints of the tunnel. Typically, such endpoints could be special routers connected to external networks that perform the encryption and decryption functions on behalf of workstations in the internal networks.

When negotiating a link, the original IP datagram is encapsulated into ESP, and your key is used to process it using an encryption algorithm, such as DES. The resulting encrypted datagram is placed in the clear text IP datagram as the last payload (after any preceding headers, such as, for instance, AH). The receiving system strips off the clear text IP datagram and any preceding headers and decrypts the ESP with your secret key. The resulting original IP datagram is then processed like any normal datagram.

ESP can be combined with AH to provide authentication as well as encryption. In this case, AH can be used in several ways:

1. To authenticate an IP datagram in ESP transport mode.
2. To authenticate an encrypted IP datagram in ESP tunnel mode.
3. To authenticate the (unencrypted) IP datagrams used between the endpoints of the tunnel.
4. In a combination of 2 and 3.

In the IP header, ESP is identified by protocol number 50, assigned by the IANA.

4.1.3 Configuring IP Security

To configure IP Security to communicate with the remote host you will need to complete a security association for the remote host. IP Security is currently only available on the Windows 95 version of the IBM eNetwork Communications Suite.

1. Click on the **Start** button, then select **Settings** then **Control Panel**.
2. Once the control panel folder has opened, double-click on the **Network** object.
3. From the configuration tab, select the component called **TCP/IP Stack. FTP Software, Inc. (FTPTCP96)** and then select **Properties**.
4. From the configuration notebook, select the tab marked **Security**.
5. Check the box marked **Enable IP Security**.

6. You will be presented with a dialog box like Figure 65 on page 143 asking for an IP security number. Type any combination of numbers and letters, until the **OK** push button gets enabled. Then click on this button. This information is a seed for generating the security association numbers. You will be presented with this panel each time you reboot your system to re-initialize the random number seed. This remains active as long as you have IP Security enabled.

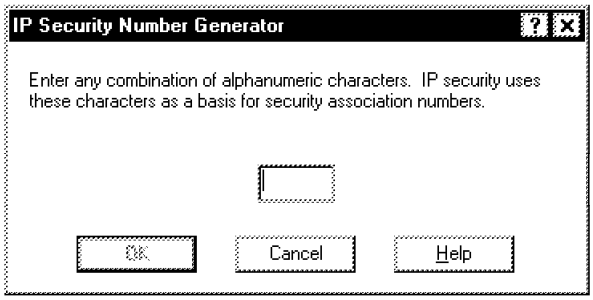


Figure 65. IP Security Number Generator

7. Click on the **Add** button to add the remote host security details. In the Security Association dialog box, there will be a number of fields for the local host. These should already be filled in with your local IP address, a local host Security Parameters Index (SPI) and the local host shared secret. You can change these details, or accept the defaults. The latter is recommended in order to provide for maximum randomness of the secret key.
8. You will now need to contact the remote host to collect the information you need to complete the remote host fields. It is important that the data be entered correctly, as any variation in the data will cause the connection to fail.
9. The remote host will also need to complete the details in the same manner. They should ensure that the details of your host are correctly entered into their remote host section.
10. Click on **OK** to save this association. You have to specify a password to be used for additional authorization as long as IP Security is enabled.

    Note: Yes, this means one more logon panel at system startup and every time you enter the IP Security configuration panel.

4.1.3.1 Using the International Export Version

Once completed, each host should have a security association dialog box similar to Figure 66 on page 144.

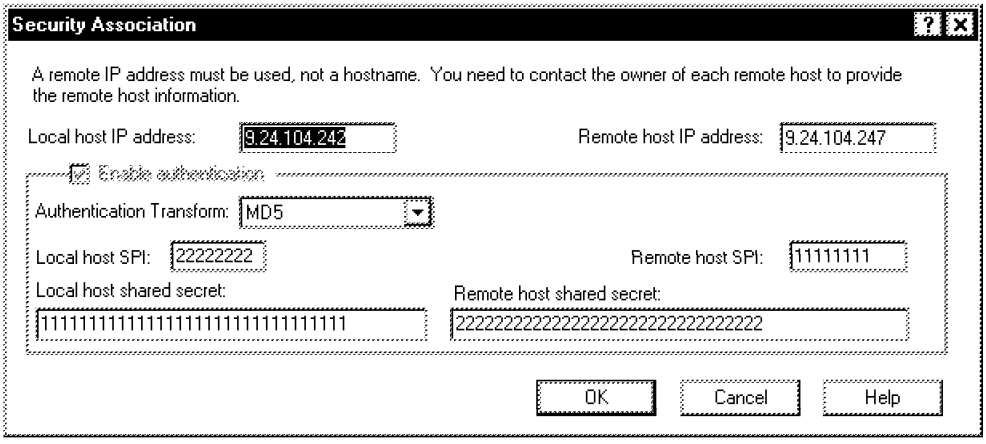


Figure 66. IP Security - Creating a Security Association

You can use the IPTrace application of the FTP Software TCP/IP protocol stack to verify that IPSec-AH is actually being used.

4.1.3.2 Using the U.S. Export Controlled Version

If you are using the Export Controlled version that is only available to customers within the United States and Canada, then you will have the ability to encrypt the datagram as well as provide authentication. In that case your Security Association dialog box will look like Figure 67 on page 145. It contains the fields for inputting the encryption keys and SPI for the datagram encryption algorithm to use.

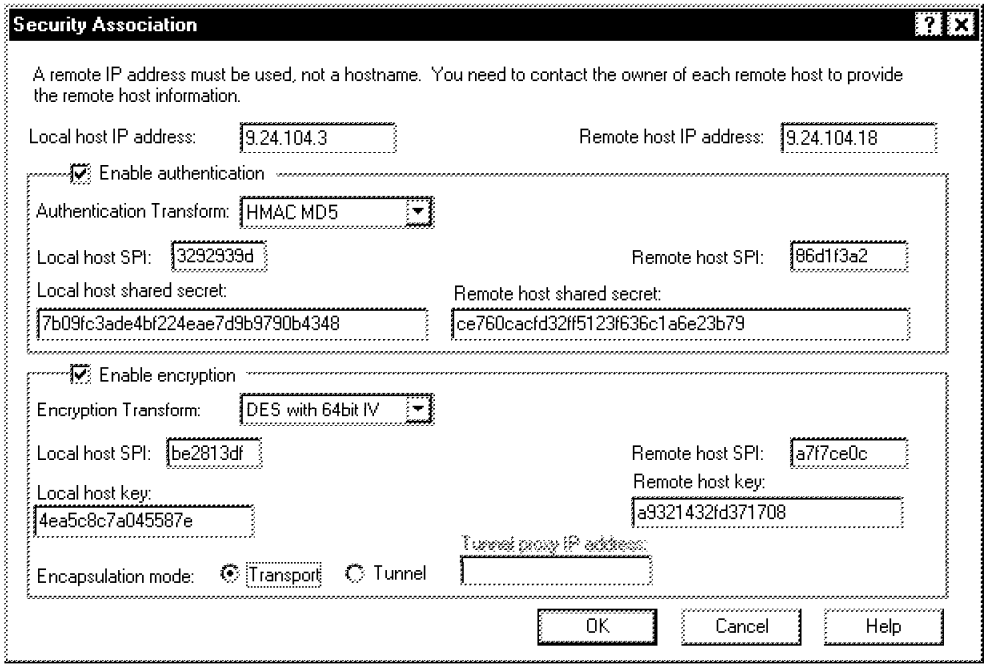


Figure 67. IP Security - Creating a Security Association (Export Controlled)

You can use the IPTrace application of the FTP Software TCP/IP protocol stack to verify that IPSec-ESP is actually being used. If you then compare, for instance, an FTP session between two IPSec systems to an FTP session between the same systems without IPSec enabled, you will realize the effect of having all application data and higher level protocols encrypted rather than transmitted in clear text.

4.1.3.3 Some Thoughts on Key Management

If your organization is planning to implement IP Security, there are some factors that you should consider:

- At present the Internet standards do not define an automatic process for distribution of secret keys in a secure manner. For each pair of hosts with which you wish to have communication in a secure manner, you will need to manually exchange the secret keys. This process is not practical on anything but a small scale. The secret keys are necessarily complicated, and not easily human-readable. This introduces the problem of an error being made while entering the keys.
- Most methods of exchanging keys are also nonsecure. Cutting and pasting the key into an e-mail message would be the simplest and most efficient method of key distribution, but unless the mail is secure itself, it

is open to the possibility of being intercepted. Many e-mail packages keep the data in plain text on the host system, or server. This makes the secret key information vulnerable.

A possible means of exchanging keys in a secure manner is the use of a separate encrypted communications channel. An example of an encrypted communications channel is Secure Sockets Layer (SSL). SSL is a client/server based method of secure communication. SSL was developed by Netscape Communications Corporation as an open, non-proprietary protocol. The SSL client is Netscape Navigator, which is included in the IBM eNetwork Communications Suite. For the server, IBM offers the Internet Connection Secure Server (ICSS). ICSS is available under a separate license agreement. For more information on SSL, refer to the following URL:

`http://home.netscape.com/assist/security/ssl/index.html`

- Each datagram needs to be combined with a secret key, and then processed with the MD5 algorithm to determine the authentication header. This process adds a slight overhead to the processing time per datagram. This delay is reproduced at the receiving end of the datagram where the data must again be combined with the secret key for processing, and then compared with the original authentication header.

  The same holds true for ESP where the actual computing overhead and communications delay may be even higher due to the encryption/decryption process.

- Due to the overhead of IP Security and the amount of manual configuration involved in implementing IP Security, we advise that it only be set up between hosts that absolutely require the authentication and guarantee of data integrity that it provides. As the standard evolves to create a secure means of automatic key management, the requirement for manual intervention will be lifted. At that time it will make implementation on an enterprise-wide scale more practical.

- Recently, a key exchange framework and session key protocol named Internet Security Association and Key Management Protocol (ISAKMP) & Oakley has been looked at by the IETF as a possible standard for key management regarding IPSec and Virtual Private Networks (VPN) which are based on the IP Security Architecture. To learn more about that framework, please take a look at the following URLs:

  `http://www.ietf.cnri.reston.va.us/ids.by.wg/ipsec.html`
  `http://www.cisco.com/public/library/isakmp.html`

For more information on IP Security, please refer to RFCs 1825 to 1829.

4.2 Implementing and Using IPv6

At the time of writing this publication, the Application Programming Interface (API) for writing applications that support IPv6 on a Windows platform has not yet been standardized. This means that there are a limited number of applications available that can take advantage of this new protocol. Traditional applications such as the Netscape Navigator cannot yet resolve IPv6 addresses correctly. If you are implementing an IPv6 network to take advantage of the extra features, you should be aware that this restriction currently applies.

If you are going to be using IPv6, we recommend that you also assign each interface an IPv4 address as well as the new IPv6 address. This will allow your core applications such as Netscape Navigator, and Personal Communications to function on each workstation. To do this, you simply enable IPv6 support, and supply an IPv4 address for the interface. IPv6 addresses are automatically assigned, and are based on the hardware address of the interface (IEEE 802 MAC address of the network card). You will need to select either advanced or automatic configuration before you can enable IPv6 support.

To get to the configuration panel shown in Figure 68 on page 148, you select **Settings** from the Start button, then select **Control Panel**. Once the Control Panel folder is open, double-click on the **Network** object. The configuration page will show a list of network components installed. From the list, click on **TCP/IP Stack. FTP Software, Inc. (FTPTCP96)** and then select **Properties**. Click on the tab marked **IP Configuration** and complete the details for this host.

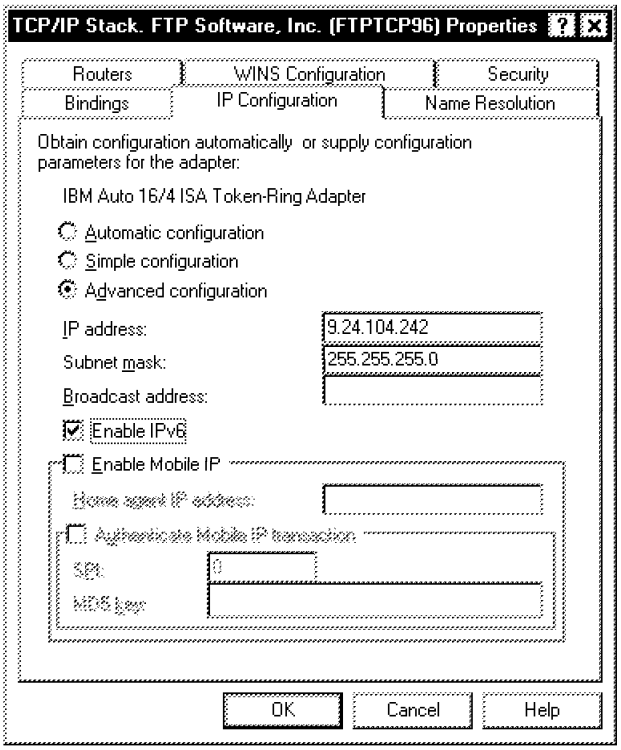


Figure 68. IP Configuration Using IPv6 and IPv4 Addressing

If you have the infrastructure to support an IPv6 environment, then IPv6 offers many advantages over IPv4. These advantages include the following enhancements and additions to the protocol.

4.2.1 Expanded Addressing Capabilities

The addressing structure for IPv6 has changed dramatically from IPv4. Most notable is the increase in the address size from a 32-bit to 128-bit identifier. IPv6 standards state that there are three type of addresses an interface can be assigned:

Unicast A unicast address is an address identifier that is usually assigned to a single interface. Packets with a destination of a unicast address will be delivered to that interface only. It should be noted that the address refers to the interface, and not the host. It is possible for a host to have multiple interfaces that would have separate address identifiers.

Anycast An anycast address is an identifier that can be associated with multiple interfaces across multiple hosts or multiple interfaces on the same host. A packet destined for an anycast address will be

delivered to the closest interface with that anycast address. Closest in this respect does not necessarily mean the interface that is physically nearest to the origin of the packet, but is closest in terms of time taken to deliver the packet.

Multicast A multicast address is an identifier that is assigned to a set of interfaces. A packet that is destined for a multicast address is delivered to all interfaces with the same multicast address identifier.

Note: IPv6 does not include a specification for broadcast addresses. The expansion of the multicast address functionality has removed the need for broadcast addresses in IPv6.

The increase in size of the IPv6 address enables auto-configuration of globally unique addresses by simply using the existing hardware address to create the interface address. The simplest and most common example is of an interface that has a 48-bit MAC address. Incorporating that complete address into the IPv6 address still leaves 80 bits (128 - 48) of the address for the prefix and other address segments. As an example, IBM may be assigned a 40-bit subscriber prefix under which it can divide and allocate the IP address segment as needed. IBM being a global company with networks in many countries may decide to split the remaining 88 bits into an 8-bit country prefix, an 8-bit area prefix that could represent the state, or territory of the interface, the next 24 bits representing the department or other information, and the remaining 48 bits for the hardware address of the interface card.

This scenario would create the following enhancement:

- All interfaces in the same country would have at least the first 48 bits of the address the same.
- All interfaces in the same state or territory would have at least the first 56 bits identical.
- All interfaces in the same department in the same state or territory would have at least the first 80 bits in common with all other interfaces in that department.

It would be possible for your organization to randomly assign IPv6 addresses to interfaces without the internal hierarchy. However, the ability to do so is one of the main features of the new IPv6 addressing architecture.

As part of the change associated with the increase in addressing space are the new multicast routing options that replace the broadcast addresses in IPv4. Any interface can also have any number of multicast addresses associated with that interface. These multicast addresses are scalable

using a scope field. When sending packets to a multicast address, it is possible to supply a scope field limiting the reach of the packets to either the same node as the source, the same link, the same site or the entire internetwork environment.

4.2.2 Updated Addressing Model

The IPv6 addressing standard recognizes that the new IPv6 address, being four times the size of the previous 32-bit IPv4 address, are going to be more difficult to represent in text form. An IPv4 address is a 32-bit binary number. This is broken into four sections of 8 bits, called octets. Each octet is converted to its decimal equivalent, and leading zeros are discarded. The final representation is the four decimal octets separated by a period. For more information on IPv4 addressing, refer to 1.5.1, “Internet Protocol (IP)” on page 5. The following is a brief example:

```
IPv4 Address: 00001001101110010100110011110100
```

The address is broken into four octets:

```
00001001 10111001 01001100 11110100
```

The octets are converted into decimal numbers:

```
00001001  = 009
10111001  = 185
01001100  = 076
11110100  = 244
```

The address is represented as follows:

```
9.185.76.244
```

The IPv6 address is a 128-bit binary number. This number would be impossible to manage if represented in its binary form. To represent the address in a more easily manageable format the authors of the IPv6 addressing standard have decided to represent the address in eight groups of 16 bits (two octets). These groups are the hexadecimal values of the eight segments of 16 bits each. They are separated by a colon. Leading zeros in a pair of octets can be discarded. If a pair of octets contains all zeros then you must leave one zero in the field. Due to the nature in which groups of IP addresses will be assigned in IPv6 there will usually be long

strings of zero bits within an address. If this occurs, the string of zero bits can be replaced by using the special syntax of a double colon ::. The double colon can be used anywhere in the address, including the beginning or the end. However, the double colon can only be used once in an address. The following example demonstrates this:

```
IPv6 Address: 11111110 10000000 00000000 00000000
              00000000 00000000 00000000 00000000
              00000000 00000000 00000000 10001100
              11101001 01001100 01011010 11101001
```

Each octet is converted to hexadecimal, and then each two octets are separated by a colon:

```
FE80:0000:0000:0000:0000:008C:E94C:5AE9
```

Leading zeros can be discarded:

```
FE80:0:0:0:0:8C:E94C:5AE9
```

Contiguous groups of zeros can be removed and represented by a double colon:

```
FE80::8C:E94C:5AE9
```

The expansion in size of the IPv6 address from 32-bit to 128-bit allows for a much larger number of possible addresses. It enables a hierarchical addressing structure similar to the modern method of global telephone numbering. Such things as provider IDs, subscriber IDs and address prefixes are part of the new addressing structure. This enables simplification in routing tables.

The address type of an IPv6 address can be determined from the leading bits in the address. The leading bits in an address are called the Format Prefix (FP). This is a variable-length field. Table 6 on page 152 represents the initial allocation of the format prefixes.

Table 6. Initial IPv6 Format Prefix Allocation

Allocation	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Reserved for NSAP	0000 001	1/128
Reserved for IPX	0000 010	1/128
Provider-Based Unicast Addresses	010	1/8
Reserved for Geographic-Based Unicast Addresses	100	1/8
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

Note: Only 15% of the total address space is initially allocated. The remaining 85% is reserved for future use.

The addressing model is greatly expanded to make room for an increased functionality. The next few sections explain the definitions of the major new features included as part of the IPv6 addressing model.

4.2.2.1 Unicast Addresses

The unicast address is effectively the replacement of the IPv4 address. Generally each interface will be assigned at least one unicast address. The unicast address is contiguously bit-wise maskable. This means the subnet mask is similar to the method used in the IPv4 Class-less Interdomain Routing (see 1.9.3, "Classless Inter-Domain Routing (CIDR)" on page 32). The IPv6 address therefore consists of the variable length subnet prefix and the host address. The following example highlights this.

```
11111110 1110.. ..1110 01011010 01011100    Examples of two
11111110 1110.. ..1110 01010010 10101010    IPv6 Addresses.
|      Subnet Prefix      |  Host ID   |
```

The following groups of valid unicast addresses have been assigned to certain tasks or groups for allocation:

- The unspecified address indicates the absence of an address. It could possibly be used as the source address of a host before it has created its own unique address. The unspecified address must not be used as the destination address or in IPv6 routing headers.

  The unspecified address:

0:0:0:0:0:0:0:0 or ::

- The loopback address is used by a node to send a datagram back to itself. The loopback address is never assigned to an interface, and a datagram containing the loopback address as a source or destination must never leave the originating node.

  The loopback address:

  0:0:0:0:0:0:0:1 or ::1

- Embedded IPv4 addresses are IPv6 addresses that contain an IPv4 compatible address embedded within. This technique has been designed to enable the transition from IPv4 to IPv6. There are two types of IPv6 addresses with embedded IPv4 addresses. In both types the first 80 bits of the address are zeroed.

  The first type is for nodes that will be tunneling IPv6 packets over an existing IPv4 network. These nodes are assigned a special unicast address that contains an IPv4 address in the last 32 bits of the the IPv6 address. The first 80 bits of the address are zeroed, and in this type of address the next 16 bits are also zeroed. There is an alternative address representation also available for this type of address. Instead of the colon separated octets, the last four octets can be shown in the decimal format as in IPv4 with the period separator. The example that follows shows this clearly.

  IPv6 address with embedded IPv4 address:

  00..00 00000000 00000000 11110011 00010001 00001001 00000101

  0:0:0:0:0:0:243.17.9.5 or ::243.17.9.5

  The second type of IPv4-compatible address is the address used to represent a node that does not support IPv6. In this type of address the first 80 bits are zeroed and the next 16 bits are ones. The remaining 32 bits contain the IPv4 address of the node being represented.

  IPv4-mapped IPv6 address:

  00..00 11111111 11111111 11010011 00011001 00001101 00000111

  0:0:0:0:0:FFFF:243.17.9.5 or ::FFFF:211.25.13.7

The IPv4-mapped address type allows applications to exclusively use the IPv6 addressing scheme even when communicating with hosts that only support IPv4.

- NSAP and IPX addresses are for mapping of NSAP and IPX addresses into the IPv6 address space. This mapping is still being defined. The prefix that has been assigned to this mapping can be found in Table 6 on page 152.
- Provider-based global unicast addresses are the section of the IPv6 address space assigned to a registry that will manage the subnetting of the address space to providers. These providers will then allocate their segments to various subscribers, who are then free to further subnet their portion of the address as they need. Examples of subscribers are Internet Service Providers (ISPs) and enterprises with their own direct link to the Internet.
- Local-use IPv6 unicast addresses are designed mainly for the purposes of automatic address configuration. There are two types of local-use addresses.

  The link local-use addresses are designed to be used on a single link where there are no routers present. The link local-use address can be used by a host for auto address configuration. The interface would initialize with a link local-use address created by using the 10-bit link local-use prefix with the hardware interface ID. The remaining bits would be zeroed. In the example of an address created using the IEEE 802 MAC address, it would appear as in the following example.

  ```
  Link local-use prefix: 1111111010

  48-bit MAC address: 10111010 11110101 10010100 10101001
                      01001110 00101001

  IPv6 address: 11111110 100..000 10111010 11110101
                10010100 10101001 01001110 00101001
  ```

  Typically represented as:

  ```
  FE80:0:0:0:0:BAF5:94A9:4E29  or  FE80::BAF5:94A9:4E29
  ```

  The other type of local-use address is the site local-use address. These addresses can be used by an enterprise that is not on the Internet. Instead of having to use a reserved address range for their hosts, they can use a site local-use address. If the enterprise should eventually join the Internet, they need only change the prefix of the address to that assigned to them by the provider. Datagrams with a site local-use

address must not be routed outside the site in which they are being used.

4.2.2.2 Anycast Addresses

IPv6 anycast addresses are assigned from the same address space as unicast addresses and as such are not distinguishable from unicast addresses. Any interface that has an anycast address assigned to it must be configured to know that it is an anycast address. A datagram that has a destination address that is an anycast address will be delivered to the closest interface having that address. The definition of closest is left to the routing protocols' determination. It should be noted that this does not necessarily mean which interface is physically closest to the router.

The IPv6 addressing standard defines a required anycast address for routers. Each router must support an anycast address consisting of their subnet prefix with the remaining bits zeroed. This is called the subnet-router anycast address. If the router belongs to more than one subnet it must support a subnet-router address for each subnet.

4.2.2.3 Multicast Addresses

The IPv6 multicast address replaces the concept of broadcast addresses in IPv4. An IPv6 multicast address is an identifier associated with more than one node. Each node that is assigned a specific multicast address will receive the datagram that has that multicast address as a destination address. Multicast addresses are of a particular format, as shown in this example.

```
First 8-bits:        11111111
Next 4-bits:         flags
Next 4-bits:         scope
Remaining 112-bits:  group ID

Example: FF12::56
```

Flags is a set of four flags. The first three are reserved and should always be initialized to zero. The fourth flag should be set as zero if it is a permanently assigned multicast address assigned by the Internet numbering authority, for instance the address FF02::1 identifies all systems on a link. The fourth flag should be set as one if it is a transient address, for instance an address established by a video conferencing application which is only required for the duration of the conference.

Scope is a 4-bit value used to limit the scope of the multicast group. This value determines the reach of the multicast datagram. The possible values are:

1 node-local
2 link-local
5 site-local
8 organization-local
E global

There are some predefined multicast addresses that are either reserved or must be assigned to an interface if it satisfies the requirements. These are listed here in this example.

Reserved multicast addresses:

```
FF00::   FF01::   FF02::    FF03::
FF04::   FF05::   FF06::    FF07::   These multicast addresses
FF08::   FF09::   FF0A::    FF0B::   shall never be assigned.
FF0C::   FF0D::   FF0E::    FF0F::
```

All nodes address:

```
FF01::1    These multicast addresses represent all nodes
FF02::1    within scope 1 (node-local) or 2 (link-local).
```

All routers address:

```
FF01::2    These multicast addresses represent all routers
FF02::2    within scope 1 (node-local) or 2 (link-local).
```

DHCP server/relay-agent:

```
FF02::C    This multicast address will identify all IPv6
           DHCP servers within scope 2 (link-local).
```

The other type of multicast address that a node must be assigned is known as the solicited-node address. This address is computed by taking the last 32 bits of an address and appending it to the prefix FF02:0:0:0:0:1, as in the following example.

Unicast or anycast address:

```
3823::4:800:200E:8C6C
```

Append low-order 32-bits with FF02::1 to create the solicited-node address:

```
FF02::1:200E:8C6C
```

The purpose of this multicast address is to enable addresses that may differ in only the high-order bits, perhaps due to different providers, to map to the same solicited node address. This will reduce the number of multicast addresses a node needs to join.

4.2.3 Simplified Header Format

Many of the previous IPv4 header fields have been removed or made optional. The time taken to process a packet is reduced if there are fewer header fields to be read and processed. The IPv6 header format is shown in Figure 69 on page 158.

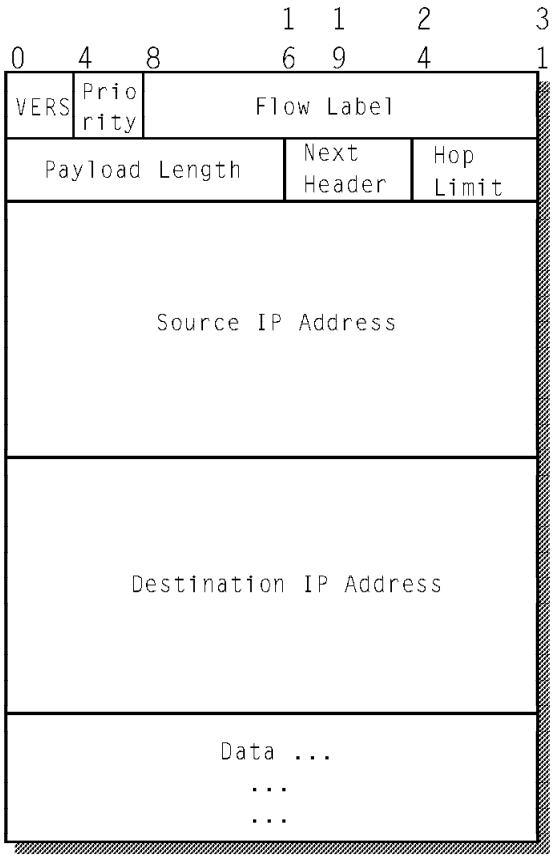


Figure 69. IPv6 Header Format

Version This 4-bit field contains the version level of the Internet Protocol. For an IPv6 packet, this will always be 6.

Priority This 4-bit field is the priority of the packet. For more information refer to 4.2.4, “Priority Handling” on page 159.

Flow Label The 24-bit flow label goes in this field. For more information refer to 4.2.5, “Flow Handling” on page 159.

Payload Length 16-bit unsigned integer that provides the length of the payload in octets. This should mean that the payload is limited to a maximum size of 65,535 octets. A method exists for sending packets longer than this. The method is known as jumbo payloads. For more information on

jumbo payloads, refer to RFC 1883, ″Internet Protocol, Version 6 (IPv6) Specification″.

Next Header The next header field refers to the type of header that follows the IPv6 header. The values are the same as used in the IPv4 protocol field. For more information on these values refer to RFC 1700, ″Assigned Numbers″.

Hop Limit This 8-bit number is decremented by one each time a node forwards the packet. When the hop limit reaches zero the packet is discarded.

Source Address The 128-bit address of the packet's origin.

Destination Address The 128-bit address of the packet's destination.

4.2.4 Priority Handling

The addition of a priority field in an IPv6 header enables the application to determine the relative importance of a packet. A router that can properly process the priority field can determine if a packet should be held during times of congestion, or forwarded despite other packets of lower priority still being held in cache.

It is also possible to define packets that can be discarded if required due to conditions of congestion. The priority field allows you to set the relative importance of packets, and which types should be discarded first. As an example, you may have a teleconference link between two sites. One stream of packets contains the video information and another stream of packets contains the audio. The audio stream is more important than the video stream for this example. If the link should become congested, the router will know from the values in the priority field to discard the packets containing the video stream in preference to the audio.

4.2.5 Flow Handling

Those packets that require special handling by IPv6 routers can be given a flow label to distinguish multiple active flows from a particular source to a destination. In the same example as 4.2.4, “Priority Handling,” the audio stream would be assigned a particular flow label and the video stream another. The router would associate the flow label with the assigned priority and cache that information. Then each time there was network congestion the router could discard the video stream packets based on that cached information without having to process each packet.

4.2.6 A Very Basic IPv6 Scenario

We have set up a small scenario to explore some of the basic features of IPv6, such as auto-configuration and subnet prefix advertisement. In particular, we used the following environment:

System A Windows 95 system running the FTP Software TCP/IP protocol stack with IPv6 support enabled and using TNVTPlus to connect to the other systems,

System B Sun Solaris system running a prototype of an IPv6 stack capable of prefix advertising, IPv6 routing, and IPv6 name serving.

System C AIX system running a prototype of an IPv6 stack capable of autoconfiguration.

Network Ethernet 10baseT LAN. Figure 70 illustrates the scenario and gives the IPv4, IPv6 link-local and IPv6 site-local (subnet) addresses of all systems.

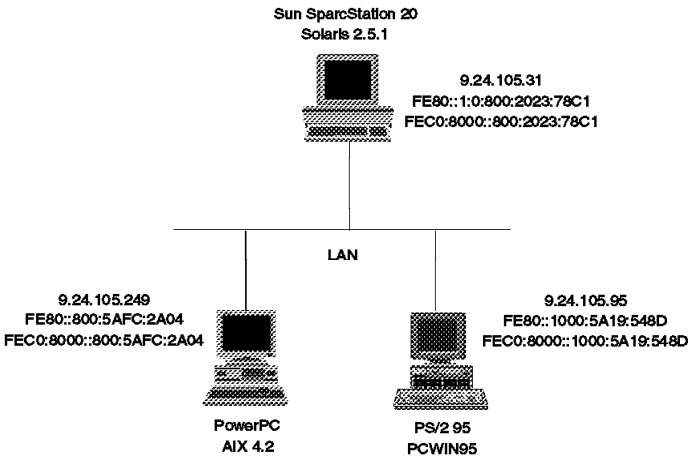


Figure 70. Basic IPv6 Scenario

Applications The following applications were used in this scenario:

1. Running Telnet from the PC to the unix systems. Figure 71 on page 161 shows a Telnet session to the Solaris system displaying the IPv6 configuration of that system:

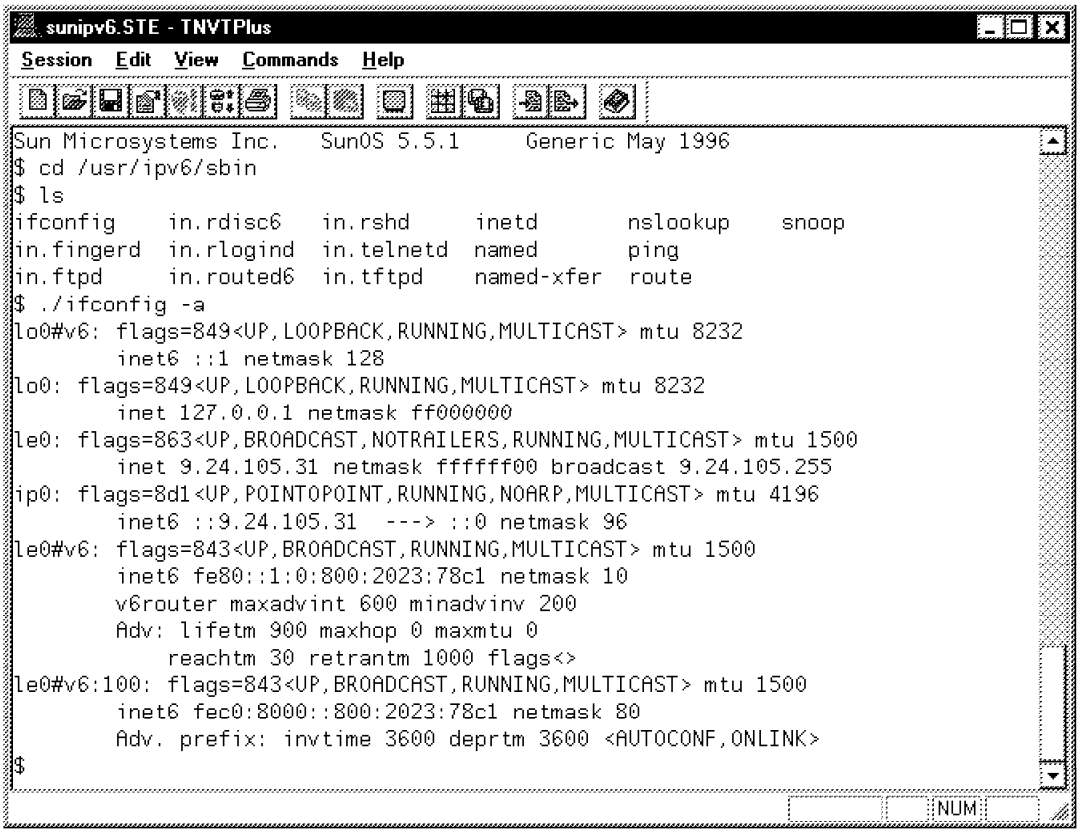


Figure 71. Telnet over IPv6

2. Displaying the local IPv6 configuration with Statistics.
   Figure 72 on page 162 shows the Interface, TCP, and Routing information windows displayed within the Statistics application window:

   - The Interface windows displays all local IP addresses.
   - The TCP window displays all TCP connections. In our case, a running Telnet session to the Solaris system, and a terminated Telnet session to the AIX system.
   - The Routing window displays routing information for both IPv4 and IPv6. For the IPv6 links, the Solaris system is listed as the default router.

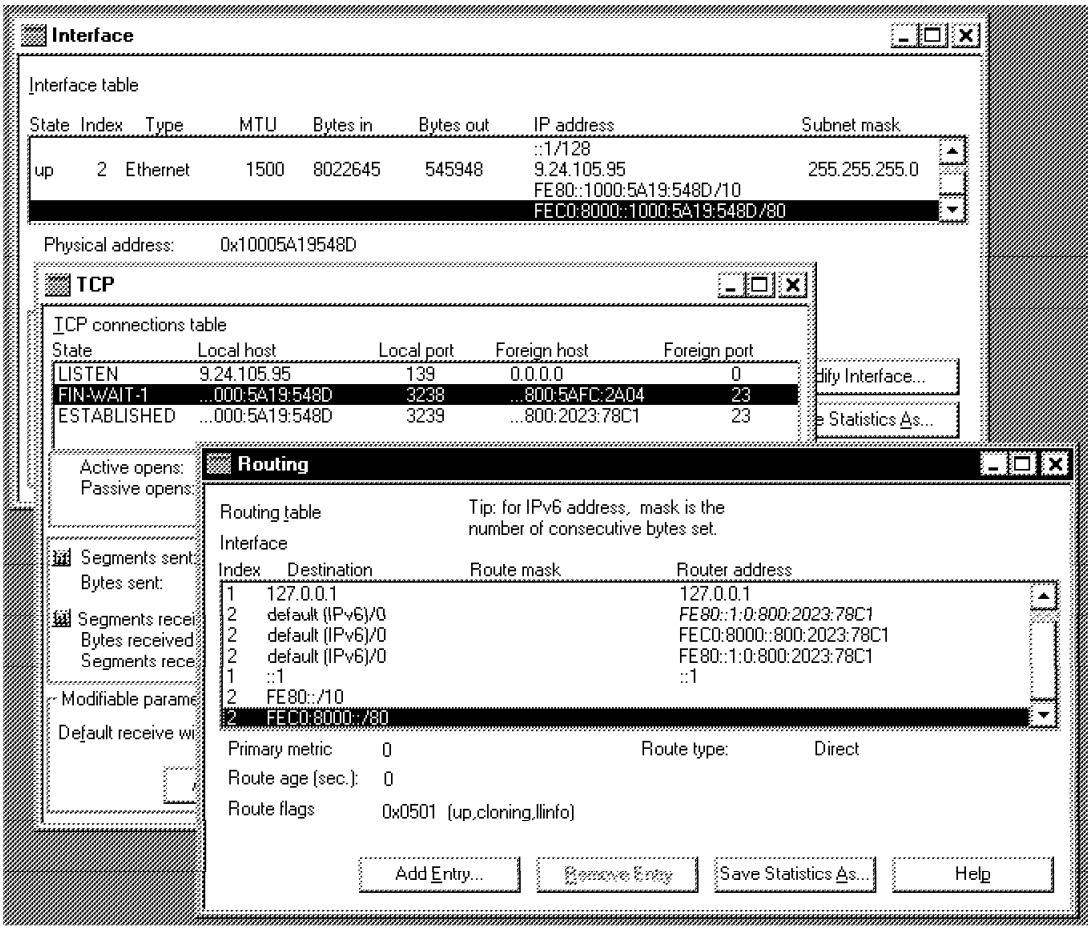


Figure 72. Displaying the Local IPv6 Configuration

3. Verifying the use of IPv6 with IPTrace.

4.3 Mobile IP

Mobile IP allows you to connect your IP host to a subnet other than your home subnet without having to reconfigure TCP/IP. Agents running on your usual subnet (home agent) and on the subnet you connect to (foreign agent) will establish a connection between each other and forward your IP traffic to the subnet you are connected to. Systems on your original (home) subnet will continue to perceive your system as being locally attached because the home agent will take over ARP requests on your behalf. A simple scenario for Mobile IP is shown in Figure 73 on page 163.

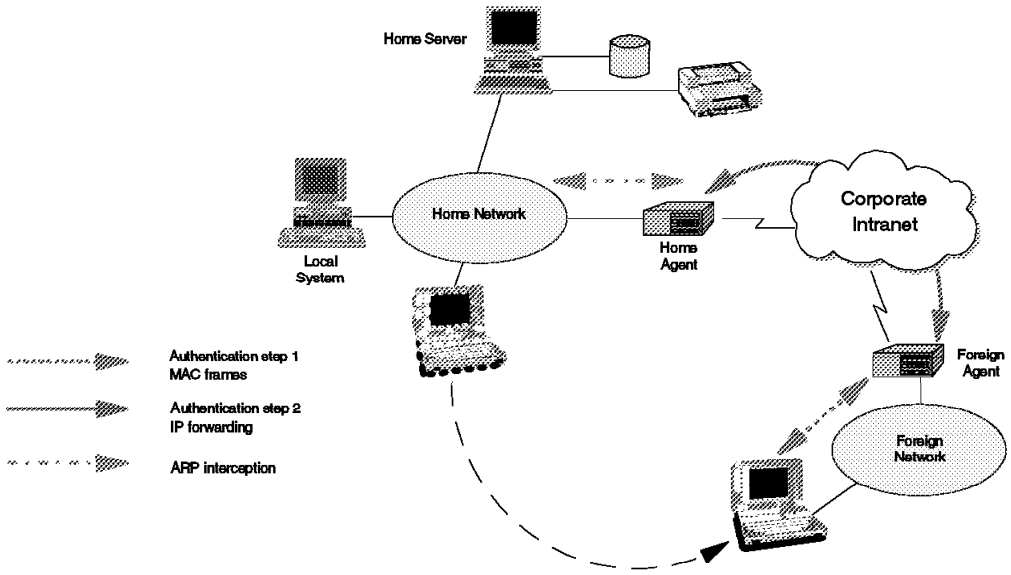


Figure 73. Mobile IP Scenario

This method of keeping the same IP address in different subnets has advantages over reconfiguring different IP addresses manually or using DHCP. Having to reconfigure an IP number for each different subnet is time consuming and prone to errors. Having a different IP address assigned each time you connect is also a problem if your IP address needs to be static. For example, you may have set up security associations with other hosts.

4.3.1 Configuring Mobile IP

The FTP Software TCP/IP protocol stack supports Mobile IP and Mobile IP authentication. To configure Mobile IP, you will need to

1. Click on the **Start** button in Windows 95, then select **Settings** and **Control Panel**.
2. From the Control Panel folder, double-click on the **Network** object to start the Network Configuration panel.
3. From the list of network components installed choose **TCP/IP Stack. FTP Software, Inc. (FTPTCP96)**, then click on **Properties**.
4. Select the configuration panel called **IP Configuration**.
5. To use mobile IP you will need to have enabled automatic or advanced configuration for your interface. Check the box next to **Enable Mobile IP** and also **Authenticate Mobile IP transaction** if you wish the registration

messages between your remote node and the home server to be authenticated.

Note: Only the registration messages between the remote node and the home server are authenticated by enabling Authenticate Mobile IP transaction. This does not enable authentication for other packets between those two hosts, or any others.

6. In the Home Agent IP address field, place the IP address of the agent on your home server that will act as your home IP traffic server. If you have enabled authentication you will need a Security Parameters Index (SPI) and a Message Digest 5 (MD5) key. These details are used to generate the security key for validation of your mobile host to the home server. The administrator of the home server will supply these details if they are required.

Once complete you should have a configuration similar to Figure 74.

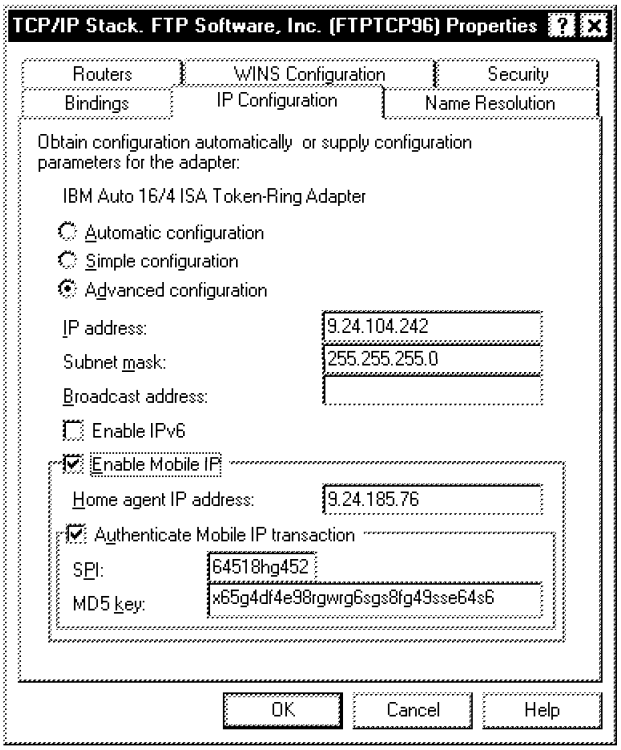


Figure 74. Mobile IP with Authentication Enabled

4.4 Using SOCKS

The FTP Software TCP/IP protocol stack implements a SOCKS V4 client that enables applications to use a SOCKS server (firewall) to access outside and non-secure IP networks, such as the Internet. The firewall controls access to the outside based on the TCP header, including source and destination IP addresses and port numbers. The firewall also hides the systems on the inside from anyone on the outside. SOCKS V4 only supports TCP-based applications and does not provide authentication.

In order to use a SOCKS firewall, a system must run a SOCKS client, called a socksified TCP/IP stack. In order to operate across a SOCKS firewall, an application must be relinked to a special set of libraries that contain SOCKS specific code. Such applications are referred to as socksified applications, and all of the FTP Software TCP/IP applications are of that kind.

Normally, only Web browsers implement SOCKS client functions to be able to access the Internet across a firewall. But in some cases, it may be desirable to use other applications across firewalls as well. To enable SOCKS with the FTP Software TCP/IP protocol stack, perform the following steps:

1. Click on the **Start** button in Windows 95, then select **Settings** and **Control Panel**.
2. From the Control Panel folder, double-click on the **Network** object to start the Network Configuration panel.
3. From the list of network components installed choose **TCP/IP Stack. FTP Software, Inc. (FTPTCP96)**, then click on **Properties**.
4. Select the configuration panel called **Security** and check the box next to **Enable SOCKS security**, as shown in the figure below:

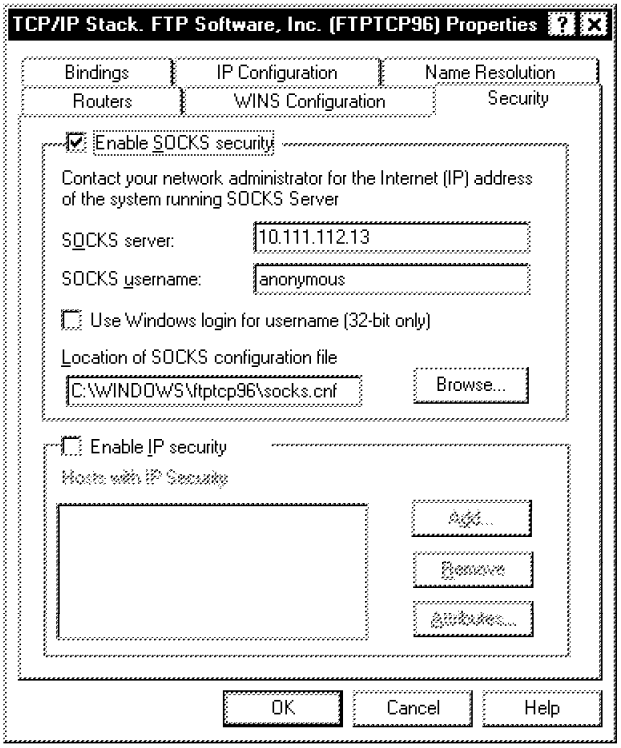


Figure 75. Configuring SOCKS

5. Enter the IP address of your SOCKS server (firewall) and your user name at that firewall in the appropriate fields. Optionally, you can use your Windows 95 logon ID as a SOCKS user name.
6. Enter the path and file name of the SOCKS configuration file (usually SOCKS.CNF). That file contains information about which applications should be configured to operate across the firewall, and which server should be contacted outside the firewall. An example of a SOCKS.CFG file is provided with the FTP Software TCP/IP protocol stack in the Windowsftptcp96SOCKS.TXT file.

   Note: According to our experience, it is always necessary to contact your system adminstrator for information required to setup SOCKS correctly.

More information about SOCKS can be found on the following URL:

`http://www.socks.nec.com`

Chapter 5. Scenario A - Multi-Platform TCP/IP Environment

In this chapter, we develop a corporate scenario based on a multi-platform TCP/IP network, and describe how to implement and use the eNetwork Communications Suite in that environment. This scenario assumes the following:

- Multiple connected IP networks in different locations
- UNIX servers
- Internet access
- The following eNetwork Communications Suite components are used:
  - FTP Software TCP/IP protocol stack and FTP Software TCP/IP applications
  - Netscape Navigator

5.1 Environment Overview

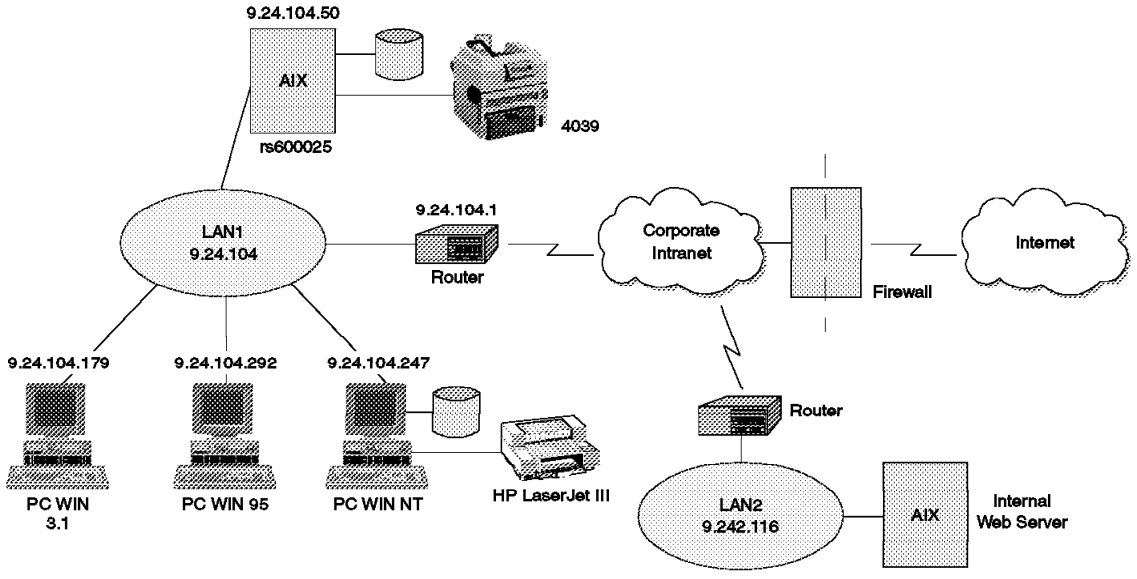


Figure 76. Scenario A - The Environment

Our environment is shown on Figure 76. At our newly established site, a small token-ring network has been installed (LAN1). In order to reduce the complexity of network management and cut the costs, a decision has been

made to deploy only one networking protocol. The selection of this protocol was based on the following considerations:

- The users will need access to corporate and Internet Web sites.
- The business-critical applications run on AIX systems.

These givens imply using TCP/IP. Because the users do not need access to legacy applications running on SNA-attached hosts and because all resource sharing requirements can be met by using TCP/IP, there is no need for any other networking protocol.

The connection to the corporate Intranet is made by an IBM 2210 router. A set of machines on site need access to the corporate WWW server. This server is an AIX system running the IBM Internet Connection Secure Server (ICSS) and is located on a separate token-ring network (LAN2), which is also a separate TCP/IP subnet.

Some users need to access the Internet. Their machines connect to the corporate firewall, which is an AIX system running the IBM Secure Network Gateway. The firewall is basically a SOCKS server. It manages the connections to the hosts on the Internet on behalf of the internal clients. The internal network structure is hidden in this way from the outside.

In their daily work, the users take advantage of the shared resources on the local network. The department server, which is an AIX system, runs the NFS subsystem for file sharing, and the LPD subsystem for printer sharing. This server also runs the business-critical applications. The users of these applications connect to the server with Telnet sessions.

All users exchange e-mail using Netscape Mail. There is a corporate POP3 server which provides the e-mail services.

An additional server provides access to a set of less used common files and to a second workgroup printer. This machine is an IBM PS/2 Model 95 running Windows NT Server 4.0.

The client workstations span over a wide performance range. The most basic users, who are using only the business-critical applications on the department server for data entry tasks, are equipped with older computers, capable of running Windows 3.x and the FTP Software TCP/IP protocol stack and applications. Another group of employees are using office productivity tools to process and print shared files. Their systems run Windows 95. The power users who run many applications concurrently and need to access all the networked resources are using fast PCs running Windows NT Workstation.

5.2 Setting Up the Environment

In this section we describe in detail how to configure the components of the eNetwork Communications Suite in case of the network in Scenario A. The detailed installation instructions can be found in Chapter 3, “Installation and Configuration” on page 61.

5.2.1 Information Needed

Before beginning the installation and configuration, make sure that you gathered the following information regarding your network:

1. Availability of DHCP and/or DDNS server(s). In case your organization uses Dynamic IP, you will not need all the information below, because it will be provided by these servers automatically. See your network administrator for details.
2. IP address range and network mask. Arrange with the enterprise network administration to allocate a range of usable addresses and a corresponding network mask to form a separate IP subnet.
3. The address of the default router. Make sure that routing entries are added for your newly formed subnet. Usually this is the task of the central network administration.
4. The address(es) of your name server(s).
5. The address of the firewall you will use to access the Internet. Find out whether it is a SOCKS or a proxy server and which ports it uses. SOCKS servers usually use port number 1080, while proxy servers use port number 80 or 8080.
6. The URL of the corporate home page, and the URLs of other Web pages on the Intranet and on the Internet that you will probably access.

After all information is available and you do not use Dynamic IP, assign hostanames to the machines. Use expressive, ″talking″ names. Avoid hostnames derived from user names, they will cause confusion when the users change systems. If there is a naming convention already in use, stick to that convention. Send all hostnames and the corresponding IP addresses to the network administration for name server update.

Notes:

1. Depending on your enterprise’s TCP/IP policy, your hostnames might be preassigned by central network administration.
2. Depending on how strict your enterprise network security policy is, you might have to register the hosts accessing the Internet at the corporate firewall.

5.3 Setting Up the FTP Server

The FTP server is available on all the Windows platforms. However, it is best used on the Windows NT Server. We do not recommend using it on the other Windows platforms, except for a very small anticipated workload.

Tip

For better performance and tighter access control, use the NTFS file system on the machine running the FTP server.

Before the actual setup, consider the following:

- What files in which structure do you want to put on the server?
- Who are the users? Are there logical user grouping criteria?
- What permissions should be granted to the users/groups? For example, who needs write access on the server?
- Is an anonymous account needed?

The FTP server can be configured and controlled from the Start menu. Select **Programs/Network Access Suite/FTP Server** to access the Properties panel. On the pages where it make sense, there is a possibility to restore the defaults (Restore Defaults button).

The first page of this panel is shown on Figure 77 on page 171. This is the page where you can start and stop the server, set the autostart option and specify some other general options.

Note: Under Windows NT and Windows 95, the FTP server is a service, therefore, you can start and stop it at the Services (Windows NT) or at the Network (Windows 95) dialog accessible through the Control Panel. This allows you to start the FTP server at system startup, and also to have the server running while no user is logged on.

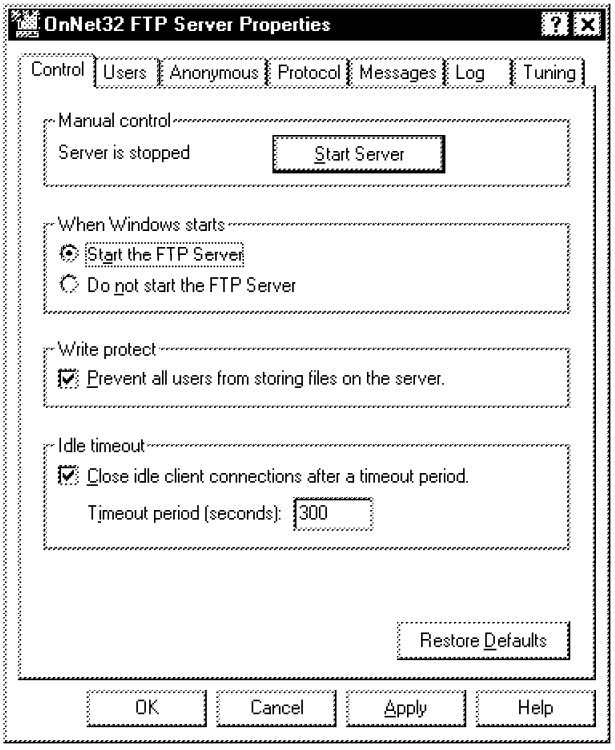


Figure 77. FTP Server Properties - Control

Note: By default, the users are not granted write access to the files on the server. Deselect the Prevent all users from storing files on the server check box to grant write access. Later you can allow read-only access on a per user basis.

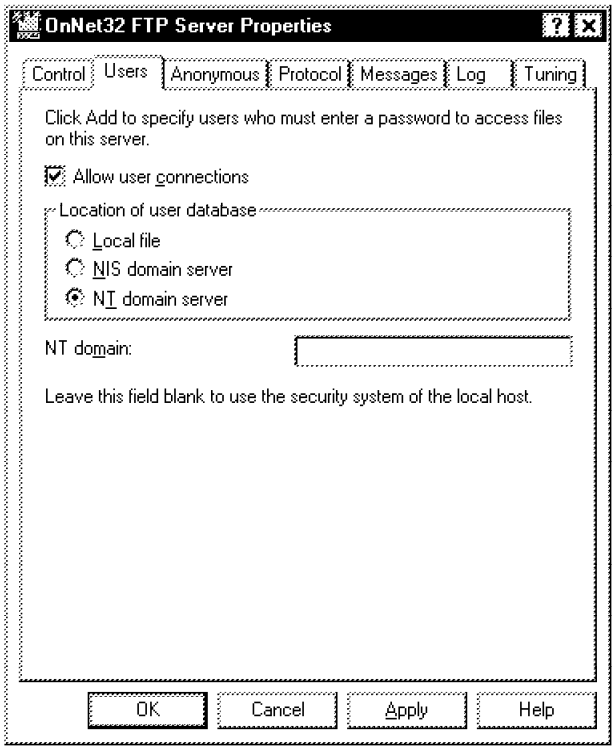


Figure 78. FTP Server Properties - Users

The user management functions are available on the Users page, as shown in Figure 78. You can set the following options on this page:

- Location of the user database: local, NIS or NT domain server. In our scenario the best choice is NT domain server. In this way you do not have to maintain a separate user list for the FTP server and you can fine-tune the access rights down to the file level, using the NT server user management functions (in case of an NTFS file system).

  Note: Choosing the Network Information System (NIS) domain server would make sense if you used NIS as the naming and user management service.

- Allow user connections: if you deselect this check box and then click on **Apply**, no more logins will be accepted, until you tick the check box and apply the change again. This is useful to limit the number of concurrent users if the server has become too busy, or to update the shared files without having to close the FTP server.

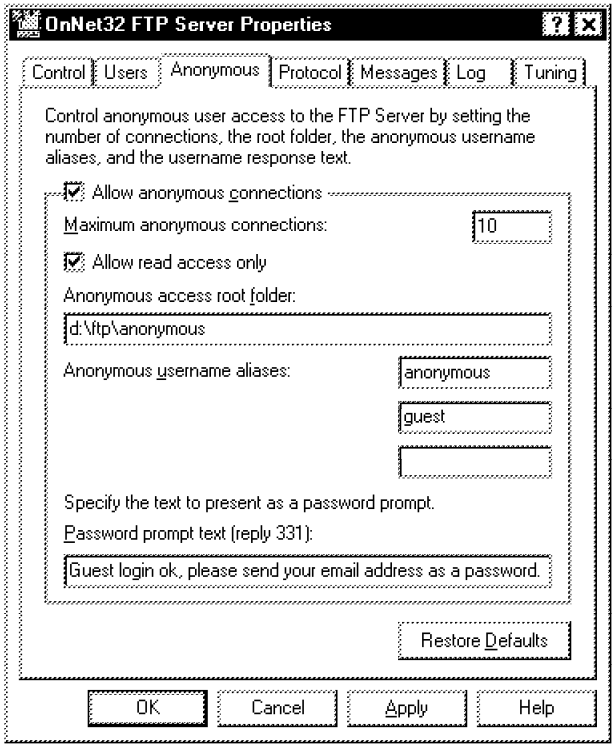


Figure 79. FTP Server Properties - Anonymous

At the Anonymous page (See Figure 79), you can allow the anonymous login to your FTP server and you can set up the parameters of this login type. We suggest limiting the maximum number of anonymous connections to a smaller number than the default 50. The range 10..30 is more appropriate for this scenario.

Note: Keep the access rights of the anonymous user under strict control. It is a good practice not to allow write access at all.

The settings on the other pages do not need to be modified in most cases. If you have to change those settings, consult the online documentation for descriptions and suggestions.

5.4 Using the FTP Client

The eNetwork Communications Suite has an FTP client on all Windows platforms. However, there are some user interface differences between the Windows 3.x and the other Windows platforms. The functionality of the client practically remains the same over all platforms. The Windows 95 and

Windows NT versions realize a better integration with the operating system′s user interface.

5.4.1 Using the FTP Client under Windows 95 and Windows NT

Invoke the FTP client from the Start menu. Select **Programs/Network Access Suite/File Transfer (FTP)**. The application′s main window is shown on Figure 80. Note the similarity to the Windows Explorer. If you are familiar with the Explorer, you will find using the FTP client very easy. You can regard this application as a special explorer, with the capability of exploring FTP servers.

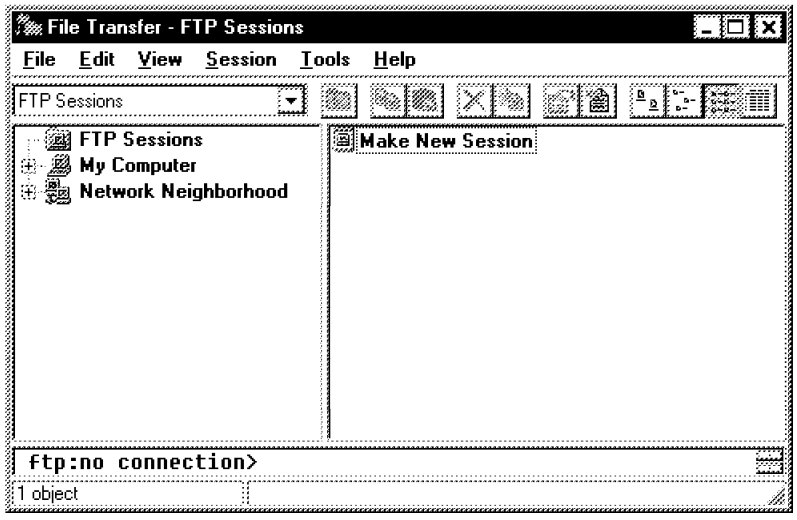


Figure 80. FTP Client Application Window

To connect to an FTP server, double-click on **Make New Session**. At the dialog box shown on Figure 81 on page 175, enter the hostname or IP address of the server, your user ID and password. If you wish to connect as anonymous, tick the **Anonymous FTP** check box.

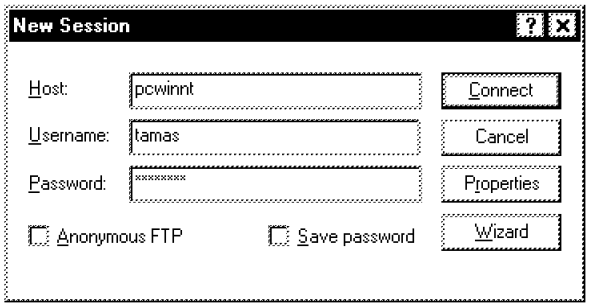


Figure 81. FTP Client - New Session

Click on **Connect** to initiate the connection. If you click on **Save Password** and you save your session, the next time you connect to the same host, you will not be prompted for the password. This is convenient, but there is a security risk associated; though the password is stored in encrypted form, one could copy your session file and use it on another computer.

For advanced options, click on **Properties**. At the corresponding dialog box you can set options such as account, port number, initial folder, server type, and firewall settings, in case you connect to an external FTP server through a firewall. These settings do not need to be altered in most situations. However, if you connect to an FTP server running under VM of MVS, you might have to specify account information. If you have to use a firewall, see your network administrator for details on parameter settings.

Once connected to the FTP server, you can browse its contents as you do with the Windows Explorer. Similarly, file transfers can be done by selecting and dragging items from the source to the destination folder. You can double-click on a remote file to automatically make a local copy and invoke the registered application to process it.

Advanced users, who prefer the power of the command line operation mode, can display a command window by selecting **View/Command Line** from the menu bar.

Note: You can connect to more than one host at the same time and perform file transfers directly between them. To do this, simply open another FTP session. The server's directory structure will be added to the tree view pane of the main application window.

Tip

Create a folder with shortcuts to the most commonly used FTP sessions. Double-click on a session shortcut to invoke the FTP Client and connect to the server.

5.4.2 Using the FTP Clients under Windows 3.x

Double-click on the **FTP** icon in the OnNet16 2.5 WinApps program group to start the FTP client. Its main window is shown on Figure 82.

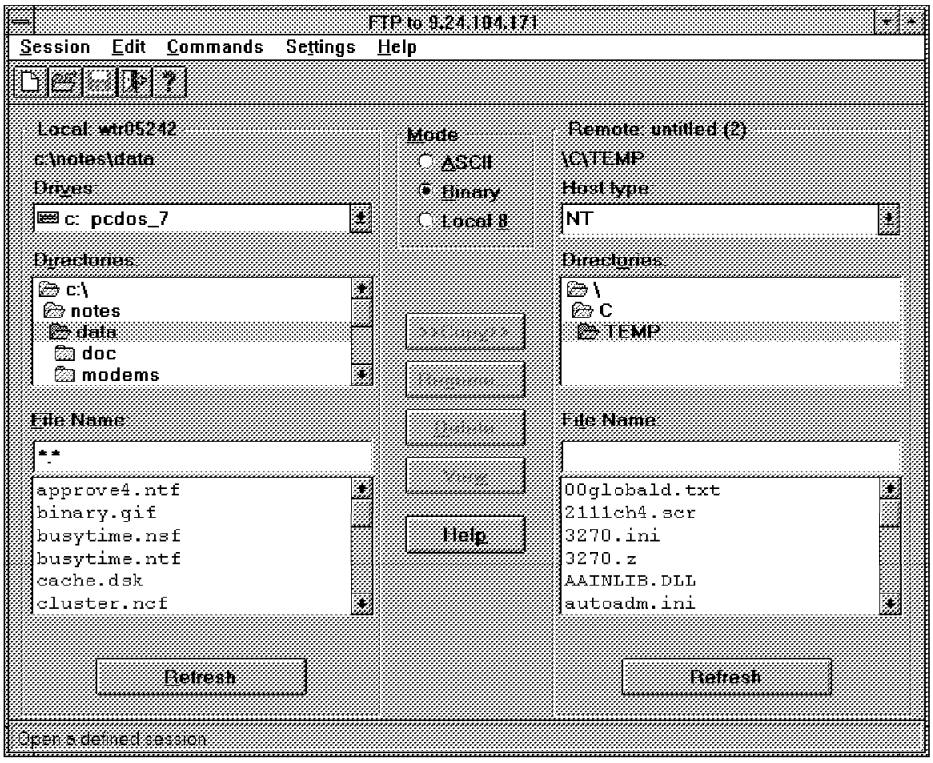


Figure 82. FTP Client - Main Window

If you have not saved any sessions yet, the New Session dialog box will be displayed, as shown in Figure 83 on page 177. Fill in the necessary information and click on **Connect** to initiate the connection to the FTP server. You can save your session, along with your password. Be aware of the security risk involved when saving passwords. One could copy the session file and use it on another computer to access the files on the FTP server.

If you connect to an external FTP server through a firewall, tick the **Use firewall** check box and click on **Modify** to set the firewall attributes. See your network administrator for details.

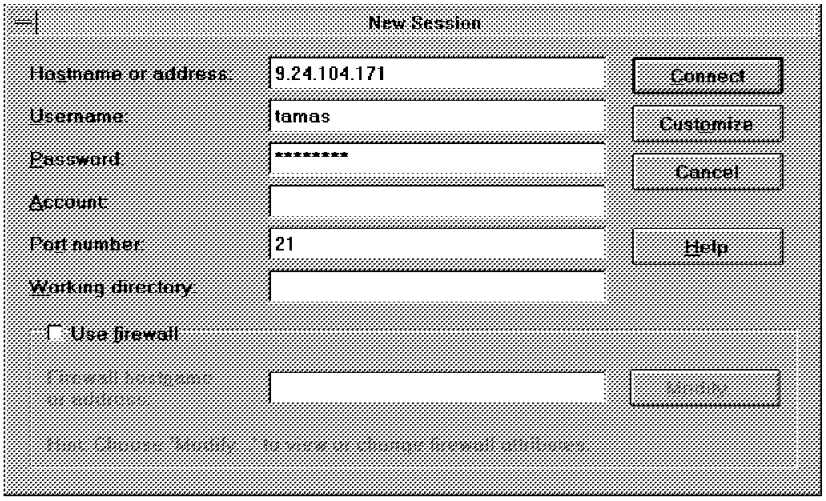


Figure 83. FTP Client - New Session

If the connection succeeds, the directory tree of the FTP server and the files in the selected directory will be displayed on the right panel.

You can transfer files in this way:

1. Select the files you wish to transfer at one panel (Remote or Local).
2. At the other panel select the destination directory.
3. Click on **Copy** to perform the operation. You can also drag the selected files to the file name list of the destination directory.

Notes:

1. You can connect to two FTP servers at the same time and make file transfers directly between them.
2. To view the selected files with KEYview, click on **View**. A temporary local copy of the files will be made and KEYview will be invoked for those files.
3. You have no access to an FTP client command prompt. You can only display a protocol window to monitor the conversation between your client and the server. To do this, select **Settings/Protocol Window**.

5.4.3 Using FTP Command Files

For automating routine tasks, you can create a command file, also called a take file. The FTP clients support command files on all Windows platforms.

Use a plain text editor, such as Notepad to create command files. Set the file extension to .TAK.

For example, you might want to get every morning a set of Lotus 1-2-3 files from the server. Here is the command file that does that:

```
# This is an FTP command file.  Enter comments after the '#'sign.
# Change the local drive and directory:
drive d
lcd \work\reports

# Change remote directory to the daily reports:
cd \reports\daily

# Set transfer mode to binary:
binary

# Get the files:
mget dept*.wk4

# End the session and exit from FTP:
bye
```

5.4.3.1 Environment Specifics for Windows 95 and Windows NT

In a Windows NT or Windows 95 environment, do the following:

- Run this command file after you have connected to the FTP server. Open the command window and type in the following:

  ```
  take
  command_file
  ```

  Where command_file is the full path name of the command file.

- For further automation, create a a shortcut to the WFTP.EXE program, usually located in the C:Program FilesFTP SoftwareNetSuite folder. The command line should be:

  ```
  "C:Program FilesFTP
  Software\NetSuite\wftp.exe" -s "session_name" take
  "command_file"
  ```

  where session_name is a full path name of a previously saved session to the FTP server, and command_file is the full pathname of the command file.

5.4.3.2 Environment Specifics for Windows 3.x

In a Windows 3.x environment, do the following:

- Run this command file by selecting **Commands/Run Command File...** from the menu bar and selecting the corresponding file name.

  Tip

  Open the protocol window to monitor the execution of the command file. You can get useful debugging information from there.

- For further automation, you may consider creating a program item and eventually adding it to your StartUp program group. When creating the program item, at the Program Item Properties dialog box, enter the following for the Command Line parameter:

  ```
  wftp.exe -s "session_name" take command_file
  ```

  where session_name is a full path name of a previously saved session to the FTP server, and command_file is the name of the command file.

  Note: Either enter the full path name of the command file, or specify its directory at the Working Directory parameter.

5.5 Using NFS File Servers

You can mount and access NFS file systems using the InterDrive Client, which is part of the FTP Software TCP/IP applications. This client also provides support for remote printing on LPD printers.

Note: The eNetwork Communications Suite does not provide an NFS server. This service is available by default on the AIX platform. It can be purchased separately from third-party vendors for the Windows NT platform, such as InterDrive NT Server from FTP Software.

5.5.1 General Considerations

Three issues must be addressed when discussing NFS-mounted drives with the InterDrive Client: access permissions, case sensitivity and file locking.

5.5.1.1 Access Permissions

NFS itself does not provide for access permissions for files or directories. NFS can only restrict access to an exported directory to a list of clients, and it can allow for read-only or for write access. Any further detailed access protection scheme is up to the underlying operating system or file system.

When an NFS client attaches to a server, the client hostname will first be checked against the export list. If the names match, users at the client

system have to identify themselves, and based on this information, access to the exported file or directory may be restricted further.

Note: The identification service for PC-based NFS clients is handled by the rpc.pcnfsd daemon on the NFS server. Make sure that this daemon runs on the server prior to attempt mounting NFS drives. Let's consider the following:

Example: In case of a UNIX NFS server, the client system pcwin95a may be listed for read access in the export list, and that is all that NFS cares about.

```
# export list for sample NFS server
# directory    NFS permissions    Export list

/home/joe         rw               pcwin95a pcwinnt pcwin31
```

If user Bill at that client authenticates himself properly to UNIX (not to NFS!), he will be able to mount the requested directory.

```
user:      bill
password:  ******
UNIX user ID:   102
UNIX group ID:  201
UNIX group:     clerks
```

But what that user can actually do to that resource is limited to the permissions he has within the UNIX file system, which is totally outside the control of NFS.

```
-rwxr-x---   1 joe      janitors    1853 Sep 22 18:17 Mwm
-rw-rw----   1 joe      janitors      47 Sep 22 18:17 Xant
-rw-rw----   1 joe      janitors   16387 Sep 22 18:17 Xmh
-rw-r-----   1 joe      janitors    1940 Sep 22 18:24 smit.log
-rw-r-----   1 joe      janitors       0 Sep 22 18:23 smit.script
```

In this case, user Bill would not be able to do anything on /home/joe because he is not the owner of the resource, nor his group nor anyone else is allowed access.

5.5.1.2 Case Sensitivity

Since many NFS servers actually run on UNIX or UNIX-like systems, there may be problems with file names in upper, lower or mixed case. The UNIX file system, and probably others as well, will treat any file name spelled in different cases as different files, as shown in the following example:

```
FileName
FILENAME
filename
```

Since the different Windows file systems are not case-sensitive to file names, the names in the above example would result in one and the same file, no matter how they are spelled. The name actually used for a file would be the first one ever given to it. The FAT file system only uses uppercase file names that comply with the 8.3 convention (eight character file name, separation period, three character extension).

This leads to the question of how clients that use the InterDrive Client will be able to differentiate between files at the NFS server which have the same name, but are spelled in different ways. The answer is simple: they cannot. Therefore avoid file names with the same names spelled in different ways.

5.5.1.3 File Locking

An NFS server does not provide for file locking, as strange as that is in a file sharing environment. This duty is left to the NFS clients. The InterDrive Client supports file locking. For file locking to be reliable, the host running the NFS server must also support locking. Many servers have a separate component, or daemon, that manages file locking. On UNIX systems, this component is the rpc.lockd daemon. The program that you are using must support file locking. All users who share the same files must have locking enabled. If one user in your work group disables file locking, the user can overwrite any network files for which that user has write permission, even if other users have locked those files.

Verify that all users have enabled file locking, both in InterDrive Client and in any program that they are using to open files.

5.5.2 Configuring the InterDrive Client

On the Windows NT and Windows 95 platforms, you can set the parameters globally for the InterDrive client using its Properties panel. Double-click on the **Network** icon found in the Control Panel. Select from the list box the **InterDrive Client from FTP Software, Inc.** item and click on **Properties**. A multi-page panel similar to Figure 84 on page 182 shows up.

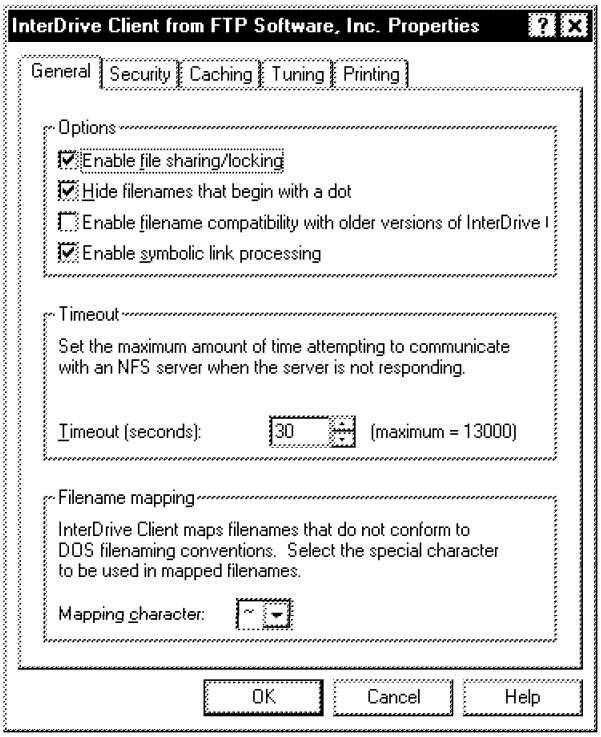


Figure 84. InterDrive Client Properties - Windows NT and Windows 95

The most important parameters are the following:

- General page:
  - Enable file sharing/locking. Select this option to enable file locking globally.
  - Hide filenames that begin with a dot. We recommend selecting this option, because those files are not for access by the general user and an accidental deletion or modification can cause problems.
  - Enable symbolic link processing. Select this option if you plan to access files by their symbolic link. A symbolic link is a file that points to the path name of another file or directory on the host. For example, certain directories or files can have such links for shortening their path names.
  - Timeout. You may consider setting a shorter timeout than the default 30 seconds.
- Security page:

- Use a central authentication server. If your organization uses such a server and you are registered on it, select this option. Ask your system administrator the name of this server.
- Default permissions. Select the permissions that a file created on an NFS-mounted drive should have. You may consider disabling the write permission for the group. If you are handling sensitive information through NFS, consider disabling any access for the Other category.

The other options generally do not need to be modified, their default values will work in most cases.

To configure the InterDrive Client for a selected resource (server or alias), use the Drive Options tab, available through the Properties menu item for the resource.

On the Windows 3.x platform the InterDrive Client parameters are settable in two ways:

1. From the Network Control window, shown on Figure 99 on page 196, click on the **InterDrive** icon to access the options dialog, shown in Figure 85.

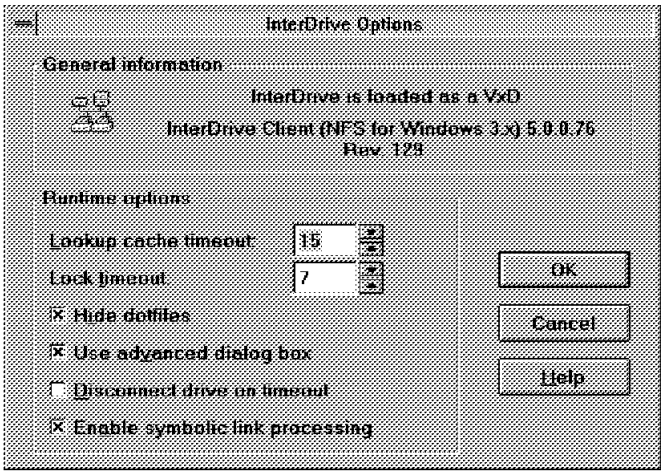


Figure 85. InterDrive Options - Windows 3.x

Note: Modifications to these settings will be effective only as long as the client is running.

2. From the configuration tool. Double-click on the **Configure** icon in the OnNet16 2.5 WinApps program group, select **InterDrive** from the list and

click on **Modify** to access the settings of the client. The modifications you make here will be permanent.

Note: The vast majority of the options do not need to be modified. Do not modify them unless you are sure what are you doing.

5.5.3 Using NFS from Windows 95 and Windows NT Clients

As in the case of LPD printers, accessing NFS-shared files is an easy task on these platforms. There are two ways to accomplish this:

- Using the Universal Naming Convention (UNC) method. You simply type in the name of the shared file you want to access. You can assign aliases to shared directories (or even printers) to simplify your work. You can browse the Network Neighborhood or use the Windows Explorer to find shared resources on your network.
- Mapping the shared directory to a local drive letter. In this way you can use applications that do not support the UNC to process the shared files.

5.5.3.1 Using the UNC Method

There are several ways to use this method:

1. In the application that supports the UNC, type in the path to the file you want to process.

   For example, in a word processor, you may enter the following at the open file dialog box:

   ```
   rs600025tamasAnnualReport.Doc
   ```

2. Browse the Network Neighborhood:

   a. Open the **Network Neighborhood** folder. Double-click on the **Entire Network** object (when using Windows NT, click on the **InterDriveNT** object in the upcoming folder) and find the NFS Servers I Have Configured object. From its context menu (right mousebutton click), select **Properties**. A dialog box similar to Figure 86 on page 185 will appear.

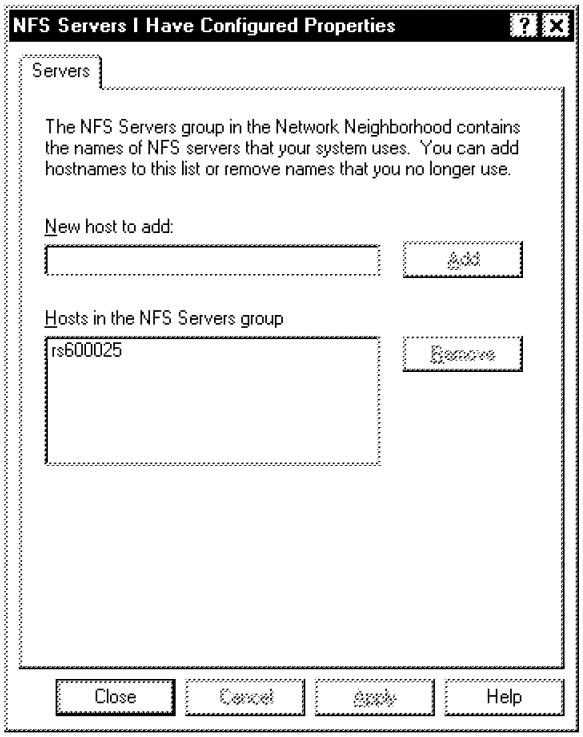


Figure 86. Add NFS Server

b. Type in the hostname or the IP address of the NFS server you want to access, then click on **Add**. Repeat this step for all the NFS servers you want to access. When finished, click on **Close**.

c. Double-click on the **NFS Servers I Have Configured** object. You will find in the folder that opens the list of the servers you have added in the previous step. You can browse them in the usual way: double-click a server name to see the folders and printers available on that server. In our scenario, for example, the exported resources of the rs600025 server look like this:

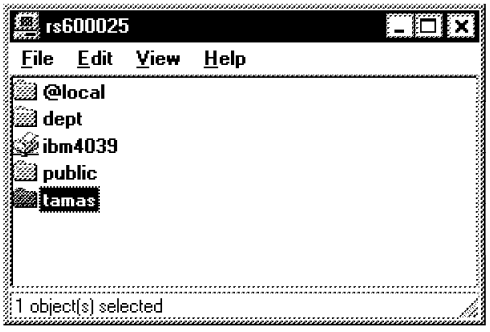


Figure 87. Contents of the NFS Server

d. Double-click a folder to see and use its contents, or double-click a printer to configure printing to it.

   Note: You have to have appropriate access rights to perform these operations.

3. Use the Windows Explorer as an alternative way to browse the Network Neighborhood.

5.5.3.2 Using Aliases

You can use aliases in order to make the NFS server access easier. Define aliases following this procedure:

1. Open the **Network NeighborhoodEntire NetworkNFS Servers I Have Configured** folder and double-click on the server name on which you want to define aliases. The contents of that server will be shown.

   Tip

   Create a shortcut of this folder on your desktop for easier operation.

2. Access the context menu of the shared resource you want to alias by clicking on it with the right mouse button. Select **Rename Alias...** from the menu. A dialog box shown in Figure 88 on page 187 will pop up. Enter your chosen alias name and click on **OK**.

   Notes:

   a. The InterDrive Client creates an alias, which is the directory name, by default.

   b. There can be only one alias defined for one resource at any time.

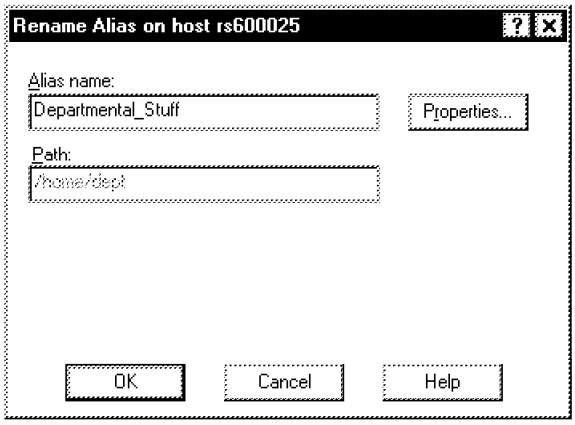


Figure 88. Definig/Renaming an Alias

The alias mechanism is especially useful in case of long path names. Of course, you can still use the fully qualified UNC name for accessing the resources.

5.5.3.3 Mapping Shared Directories to Drive Letters

Use this method if your applications do not support the Universal Naming Convention, or if you simply feel more comfortable with the classic drive letters.

From the Network Neighborhood object's context menu, select **Map Network Drive...** At the dialog box select the drive letter you want to map and type in the path to the shared directory using the Universal Naming Convention (see Figure 89).

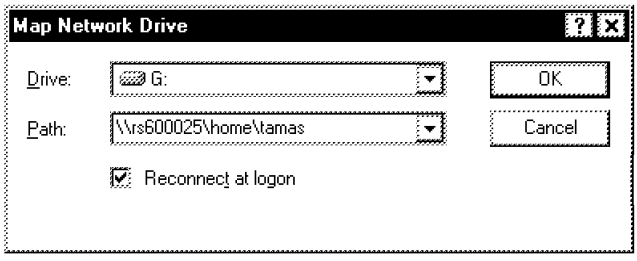


Figure 89. Mapping a Network Drive

As an alternative (for example, if you have forgotten the path name), browse the NFS Servers I Have Configured folder, select the directory, and perform the mapping from its context menu.

5.5.4 Using NFS from the Windows 3.x Clients

In the Windows 3.x environments you must map an NFS directory to a drive letter before accessing its content. As in the case of the shared printers, start with the Network Control application, shown in Figure 99 on page 196.

Click on **Drives**. The dialog box shown in Figure 90 will pop up. Select the drive letter you want to map. At the **Network Resource or Alias** input filed type in the name or the IP address of the NFS server and press Enter. In the box below you will see all the shared directories available on that server. Select one and click on **Connect**. If successful, the connection will be listed in the Current Connections list box. Click on **Done** to close the dialog box.

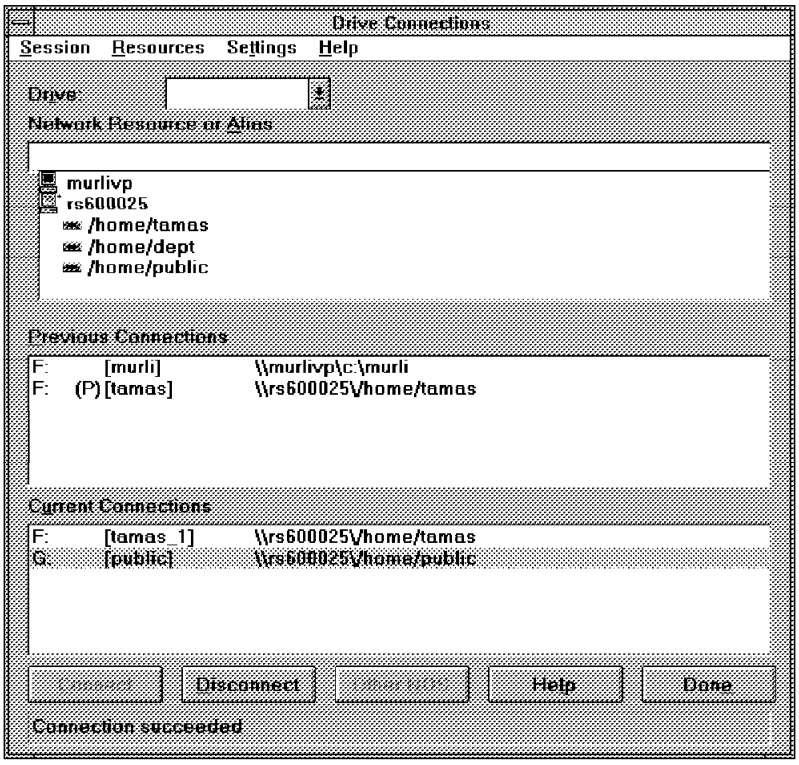


Figure 90. Printer Connections

You are ready to use the shared directory now as if it were a local drive.

You can make the drive connection permanent, that is, the shared directory will be reconnected automatically at system startup. For this, select the connection you want to make permanent from the Current Connections list box, then select **Settings/Make Connection Permanent** from the menu bar.

The InterDrive Client inserts a menu point to the File Manager's menu bar. When you open an NFS-mounted drive, you can access the following functions from this menu:

- NFS Attributes: to view the read-write-execute permissions and the owner of the selected file or directory.
- Drive Options: to see and to modify some of the connection's settings.
- Quota: to retrieve disk quota information for the specific drive.

5.6 Setting Up the IBM Printer Server

The IBM Printer Server is an LPD server, part of the FTP Software TCP/IP applications , and it is available on all of the Windows platforms. However, we strongly recommend using it on Windows NT Server, because of stability and performance considerations.

Set up this server on Windows NT Server 4.0 in the following way:

1. Install the locally attached printer, following the normal printer installation steps.
2. Select **Programs/Network Access Suite/Print Server** from the Start menu. The Print Server will display the Add New Printer dialog box, shown on Figure 91.

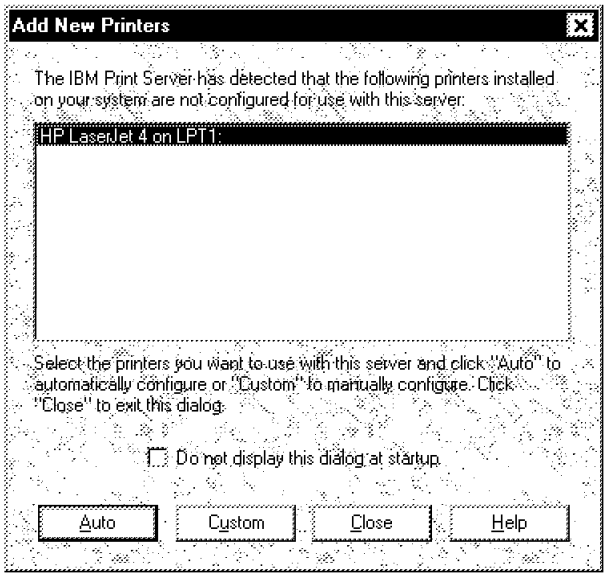


Figure 91. IBM Printer Server - Add New Printer Dialog Box

3. Select the printer installed at the previous step. Click on **Custom** to continue. You will see the New Printer dialog box, as shown in Figure 92 on page 190.

   Note: As a quick alternative, you can click on **Auto** and the configuration is done by the server. However, the print queue name in this case will be anything but descriptive.

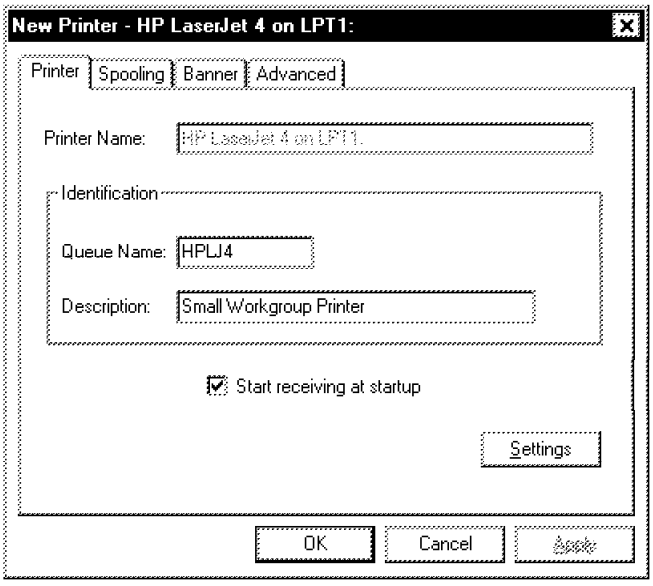


Figure 92. IBM Printer Server - New Printer Dialog Box

4. Type in a descriptive name for the print queue and a short description. Click on **OK** to finish the setup of this printer.

Now your print server is ready to use. You can send print jobs to it from any TCP/IP host that is capable of remote printing. Repeat these installation steps for any other printer you wish to share using this server.

After receiving several print jobs, the IBM Print Server window looks similar to Figure 93 on page 191. Note that you can control the printers either individually or globally. You can also control the documents in the print queues (cancel, alter processing order) either individually or by group selection.

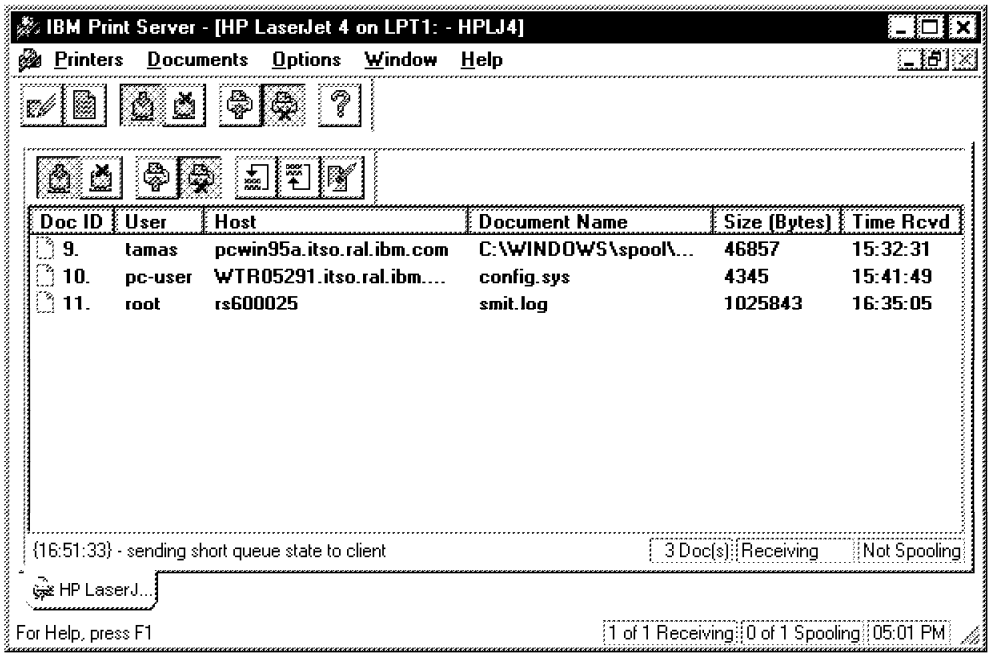


Figure 93. IBM Print Server - Main Window

Notes:

1. You can always modify the settings of the server, without the need of a restart.
2. There are more printer options you can set up, such as spool directory, spool delay, banner printing mode, and others. Consult the online help for a detailed description.

5.7 Printing to the Shared Printers

Once you have configured and started the print servers, you can use the shared printer resources from all the client platforms. However, there are some differences between the Windows platforms.

There are several ways to connect to print servers, depending upon the type of server that the printers are attached to:

1. Print servers running LPD
2. Print servers running NFS

In the first case, you need an LPR, LPRMON or LPRPORT client. In the latter case, you can use the InterDrive Client from FTP Software TCP/IP

applications. That will also allow you to select shared printers from the Network Neighborhood browser.

The setup of printers for either of those server types is slightly different on each of the Windows platforms and is described in the following sections.

5.7.1 Printing from Windows 95 Clients

It is very simple to print to the shared printers from these clients. Basically you have to install a network printer and specify the queue name associated with the specific shared printer you want to print to. Here is how to do it:

1. From the Control Panel, open the **Printers** folder. Double-click on the **Add Printer** object. At the Add Printer Wizard dialog box, click on **Next** to continue.
2. At the next dialog box, select **Network printer**. Click on **Next** to continue.

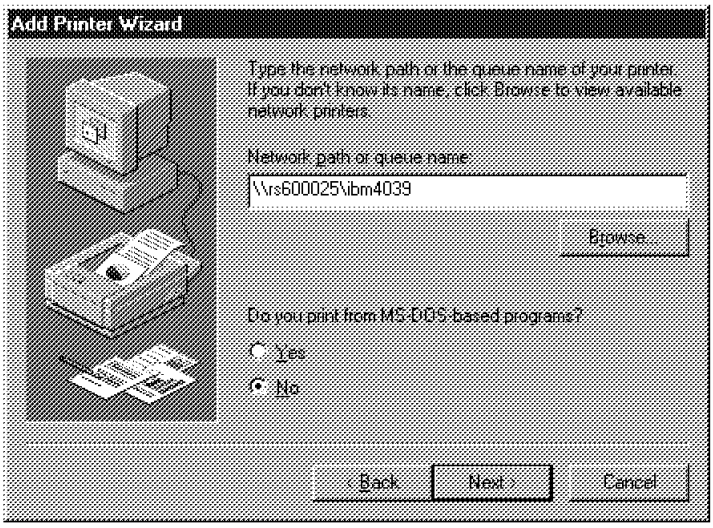


Figure 94. Specifying the Queue Name

3. At the dialog box shown in Figure 94, type in the queue name you want to send print jobs to, using the Universal Naming Convention (UNC) method.

   For example, rs600025ibm4039.

   Note: If you know that the printer is attached to an NFS server, you can optionally click on **Browse** and connect to the resource from the Network Neighborhood. This procedure is described in detail in 2 on page 184. This method is not possible for LPD servers, such as the IBM Print Server.

If you plan to print from MS-DOS based programs also, tick the **Yes** radio button. Click on **Next** to continue.

4. Follow the instructions of the wizard to complete the installation. We recommend that you print a test page, in order to verify the connectivity.

The printer installation is complete. A new printer object has been added to your Printers folder. You can use it as you use any other printer.

You have the possibility to query the print queue associated to the shared printer and eventually remove jobs from it. To do this, select **LPR Query/Delete** from the printer object's context menu. The response from the server will be shown in a window similar to Figure 95. Click on **Remove Jobs...**, enter a comma-delimited list of job numbers you wish to delete, then click on **OK** to finish the operation.

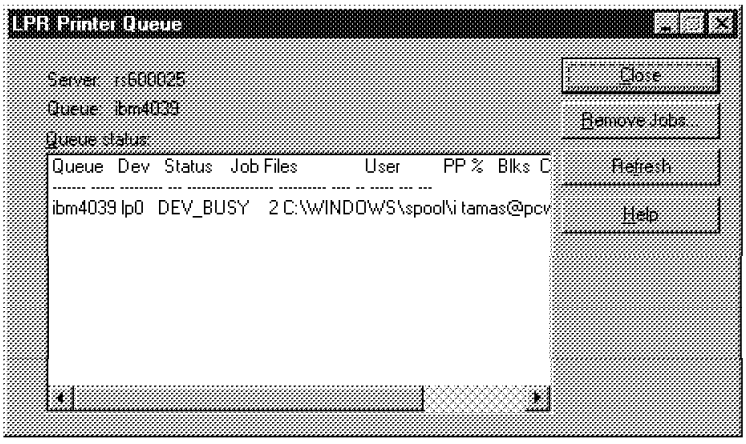


Figure 95. LPR Query Results Window

Another way to print to the shared printers is to use the Print Client application from the Network Access Suite. You can start it from the Start Menu/Programs/Network Access Suite menu. The Print Client is intended for general file printing, from outside any application. The main window is shown on Figure 96 on page 194.

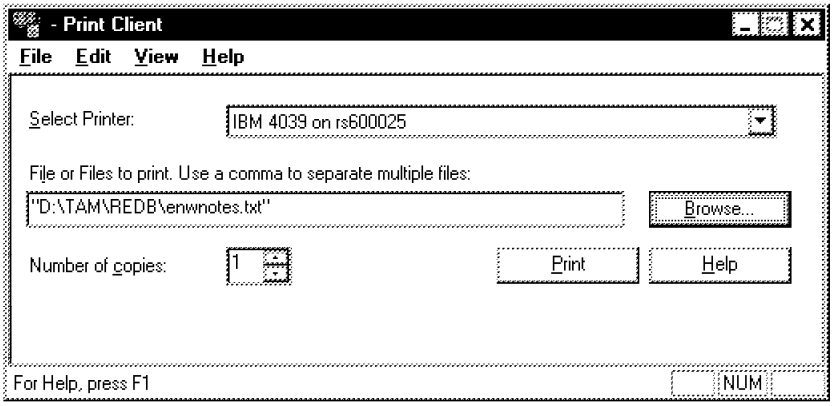


Figure 96. Print Client

Note that you can print multiple files, you can set the number of copies and you can use any printer installed on your system, not just the shared ones.

5.7.2 Printing from Windows NT Clients

On Windows NT, you can connect to printers that are attached to NFS servers using the InterDrive NT Client from FTP Software TCP/IP applications and the Network Neighborhood. This procedure is described in detail in 2 on page 184.

To connect to a printer that is attached to an LPD server, you have two options:

1. Use the LPR command
2. Configure a local printer and use the LPR Port

Important

In both cases, you have to install the Microsoft TCP/IP Printing service before you can continue.

To send a file to an LPD printer using the LPR command, simply enter the following command in an MS DOS command window:

```
lpr -s wtr05192 -p q1 test.txt
```

where wtr05192 is the name of the print (LPD) server and q1 is the name of the printer or print queue on that server.

If you want to print to an LPD server from applications such as Lotus Freelance, you might want to set up a local printer and connect it to an LPR port.

1. Open the **Start/Settings/Printers** folder and double-click on the **Add Printer** object.
2. Select **My computer** (local printer) and click **Next**.
3. Click on **Add Port** and select **LPR Port** from the menu shown in the figure below:

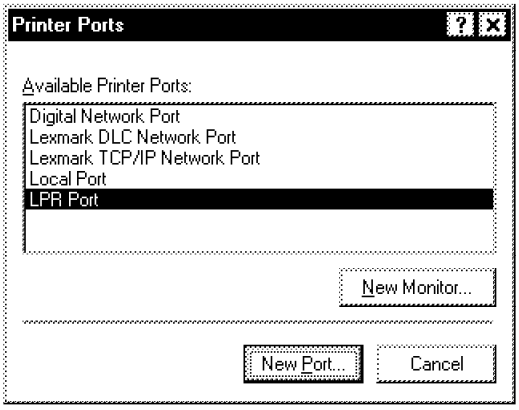


Figure 97. Add Printer Port on Windows NT

4. Click on **New Port**. In the dialog shown in the figure below enter the hostname or IP address of the LPD server and the name of the printer or printer queue, then click on **OK**.

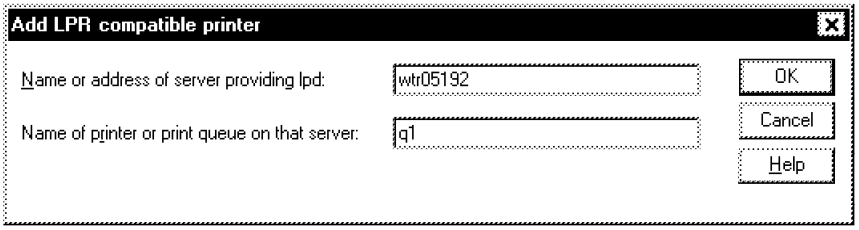


Figure 98. Add LPR Compatible Printer on Windows NT

5. Select this port for the printer and click **Next**.
6. Select a printer driver, then click **Next**.

   Note: This is different from defining a network printer or using the Network Neighborhood browser to connect to a shared printer. In that case, the appropriate driver for the network printer would be selected by the system. For LPD printers, you need to know which driver to use. If in doubt, ask your system administrator.

7. Decide if this should be the default printer, then click **Next**.

8. Decide if this printer should be shared, then click **Next**.
9. Decide if you want to print a test page, then click on **Finish**.

5.7.3 Printing from Windows 3.x Clients

In the Windows 3.x environment the remote printing is not as straightforward as in the Windows 95 and Windows NT environments. First you have to install the printer in the usual way, on a printer port that you do not use for locally attached printers. Then use the Network Control, which is part of the FTP Software TCP/IP applications, to redirect that printer port to a specific print queue on the network.

The detailed procedure is the following:

1. Install the printer driver following the usual procedure in Windows 3.x. Connect it to a port that is not used.
2. Double-click on the **Network Control** icon found in the OnNet16 2.5 WinApps program group. You will see a window similar to Figure 99. Click on **Printer** to access the Printer Connections dialog box.

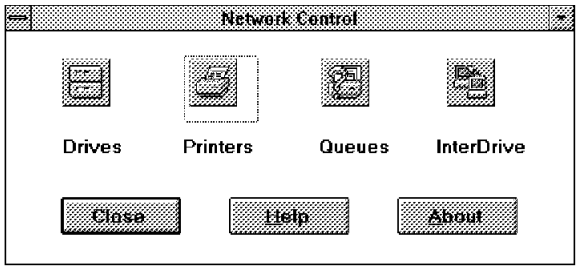


Figure 99. Network Control Window

3. At the dialog box shown in Figure 100 on page 197, select the printer port you want to redirect. At the Printer or Alias input field type in the name or the IP address of the print server and press Enter. In the field below you will see all the available print queues on that server. Select one and click on **Connect**. If successful, the connection will be listed in the Current Connections list box. Click on **Done** to close the dialog box.

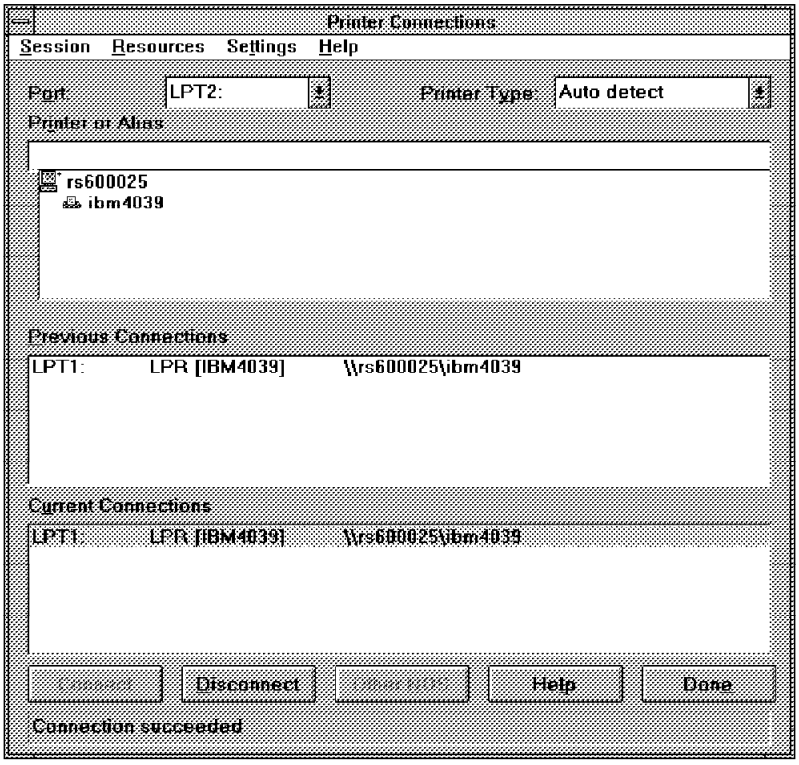


Figure 100. Printer Connections

You are ready to use the shared printer now as if it were a local printer.

You can make the printer connection permanent, that is, the shared printer will be reconnected automatically at system startup. For this, select the connection you want to make permanent from the Current Connections list box, then select **Settings/Make Connection Permanent** from the menu bar.

You can also query the status of the print queue. Click on the **Queues** icon on the Network Control window shown in Figure 99 on page 196. The Print Queues dialog box will be displayed, as shown in Figure 101 on page 198. Select a known queue or type in an other queue name, then click on **Refresh**. You will see the results in the text box at the bottom.

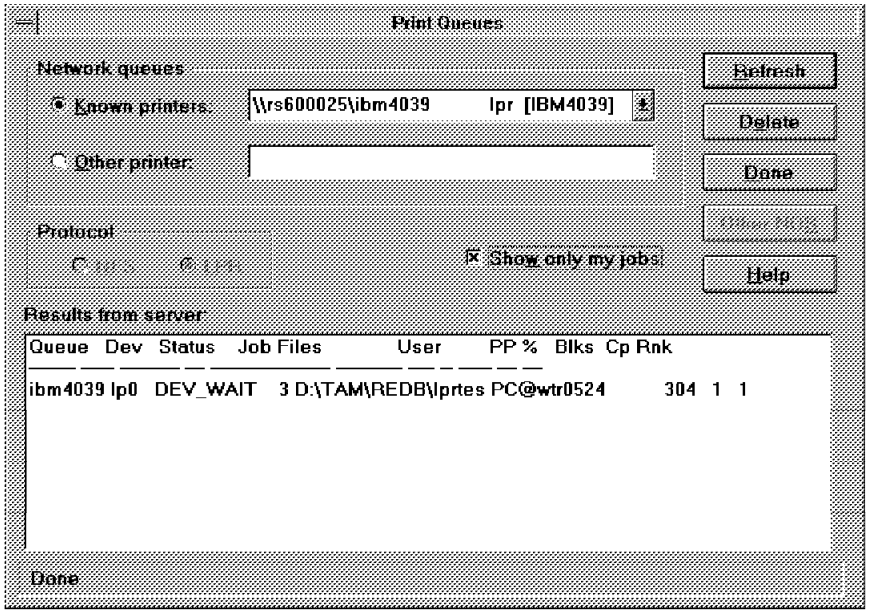


Figure 101. Querying a Print Queue

An alternative way to print on the shared printers is to use the Print Client of the FTP Software TCP/IP applications. To do this, double-click on the **Print Client** icon in the OnNet16 2.5 WinApps program group. The application's window will be displayed, similar to Figure 102.

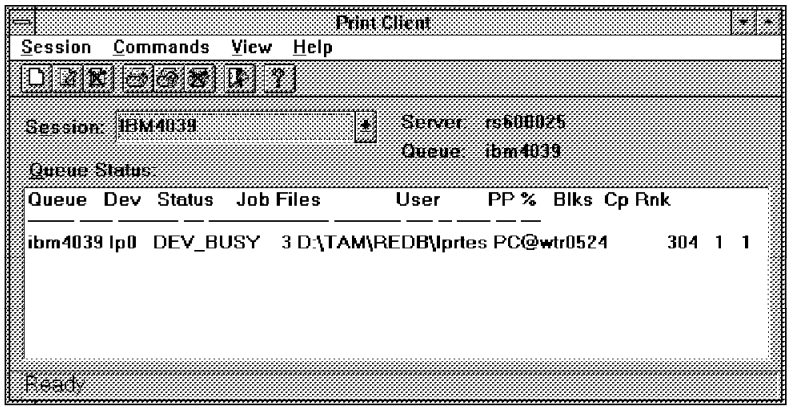


Figure 102. Print Client Window

Continue with defining a new session by selecting **Session/New...** from the menu bar. Fill in the fields of the dialog box with the appropriate information, then click on **OK** (see Figure 103 on page 199).

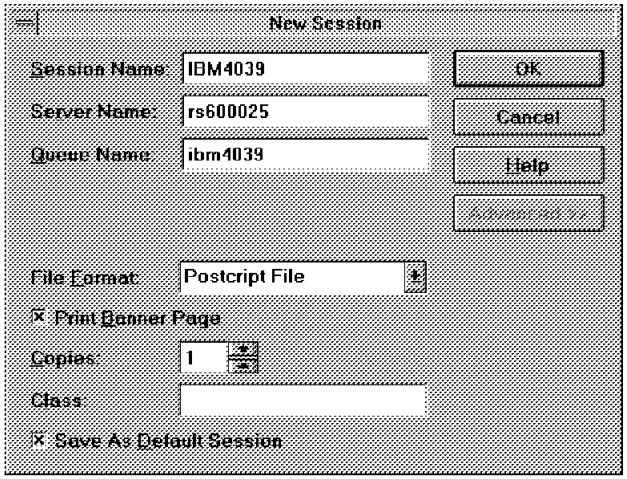


Figure 103. Definig a New Session

Now you can send print jobs to the queue, you can eventually delete jobs or query the status of the queue. Use either the tool bar buttons or the menu items to accomplish these tasks.

5.8 Connecting to Remote Hosts with TNVTPlus

The TNVTPlus terminal emulation program of the FTP Software TCP/IP applications enables you to connect your PC to a network host, that is, establish Telnet sessions. In our scenario it is used to work with the business applications on the AIX host.

5.8.1 Using TNVTPlus in Windows 95 and Windows NT Environments

Start the program by selecting **Programs/Network Access Suite/TNVTPlus** from the Start menu. The main application window will be shown, similar to Figure 105 on page 200, along with the New Session dialog box.

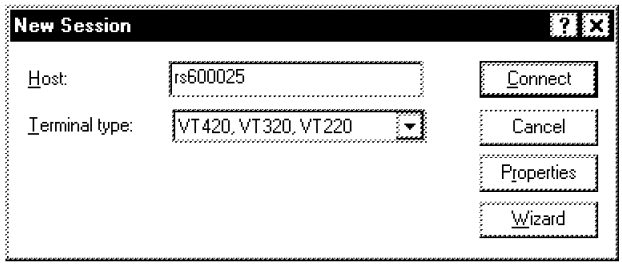


Figure 104. New Session Dialog Box

Enter the host name or IP address of the machine you want to connect to in the Host: field of the dialog box and select the terminal type from the list box, as shown in Figure 104. The default VT420, VT320, VT220 is the most commonly used and it is correct for our scenario.

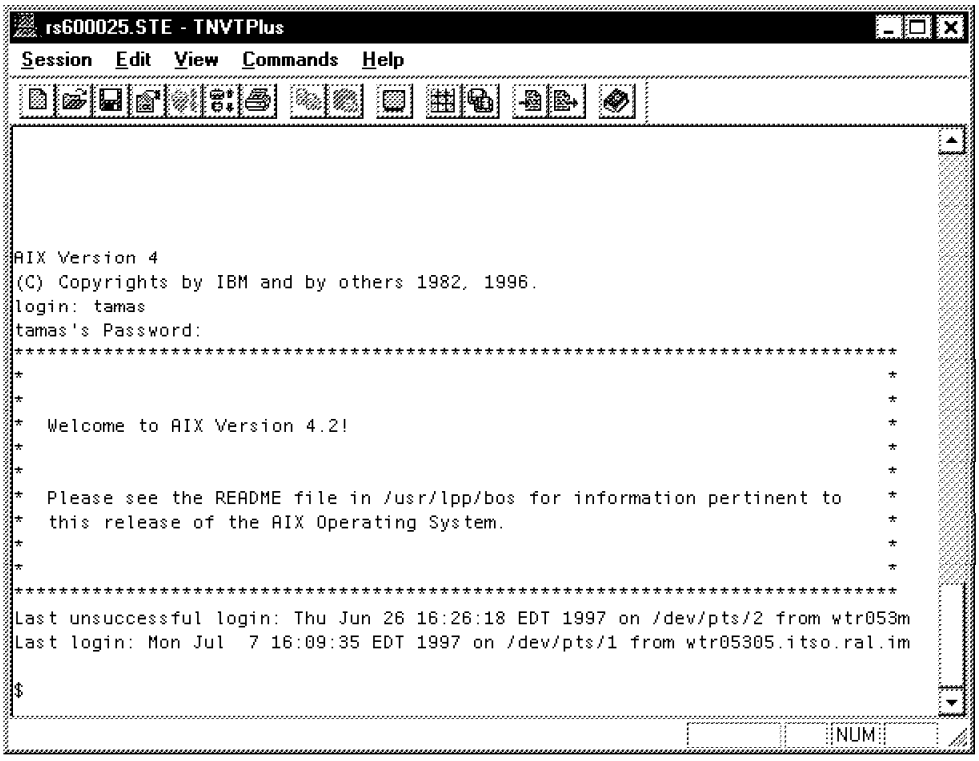


Figure 105. TNVTPlus Main Window

Depending on the target system and the application running on that system, you might have to use a different terminal type. Ask your system administrator for details.

5.8.1.1 Setting Up a Session

There are a large number of parameters which affect a Telnet session. You can set these parameters at the Telnet Connection Properties window, accessible by clicking on **Properties** at the New Session dialog box, or selecting the **Properties** from the Session menu of the menu bar. There is a button on the task bar which can be used also. You can modify most of the settings on-the-fly.

Let's take a brief look at the most important settings.

At the General page, shown in Figure 106 on page 201, besides the host and the terminal type, you can set the automatic login parameters. Specify your user name and password. If the target system's user name and password prompt differ from the default login: and password:, you have to specify those prompts at the corresponding fields. If you select the **Save password** check box, the login procedure will be fully automated; you will not be asked for a password. Use this feature with caution, becuse it implies a security risk. One could copy your session definition file and use it to log on fraudulently to the host.

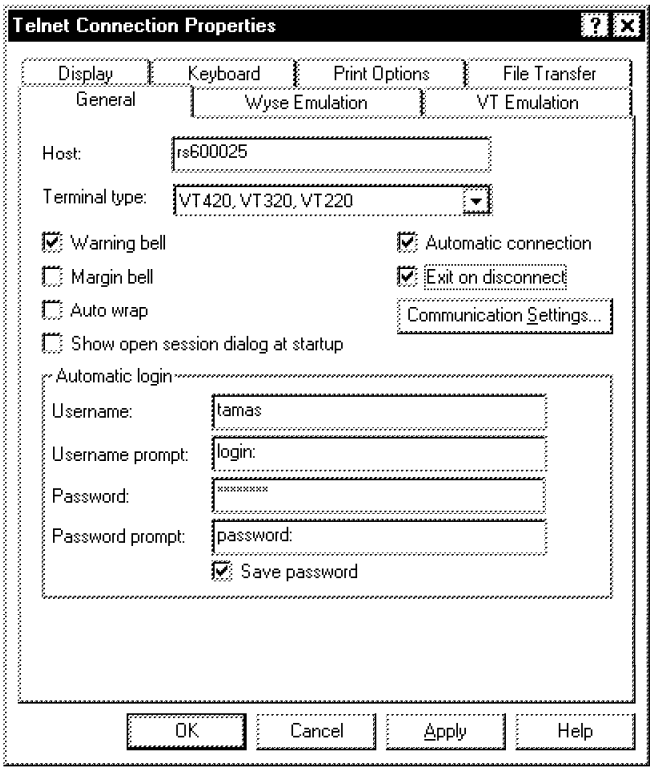


Figure 106. Telnet Connection Properties - General

Tip

If you defined and saved the sessions you want to use, select the **Show open session dialog at startup** check box. The next time you start TNVTPlus, you will be presented with the list of your saved sessions. Double-click on the session name to start that session.

You can modify your communication settings by clicking on **Communication Settings...**. Settable parameters include port number (if different from the standard Telnet port, which is 23), terminal negotiation options, window size, local echo option and others. Seldom these parameters have to be modified.

At the Display page you can customize the followings:

- The colors and the font used. Access the dialogs associated to these tasks by clicking on the **Change Colors...** and **Change Font...** For example, you can select Greek or Turkish font. If you want the displayed font size to remain constant when resizing the emulation window, deselect the **Scale font to window** check box.
- Display remapping. You can specify what character is to be displayed when receiving a certain character from the host. You can save your definitions to a file and assign this mapping file to any session. The online help contains step-by-step instructions on how to do this.
- Number of columns to display. The default is 80. Optionally you can select 132 for a wider display.
- Number of lines to display. Depending on the terminal type and the page memory selected, the valid range is between 24 and 48.
- Page memory. You can specify how many pages and lines the TNVTPlus screen has.
- Scrolling options. You can set the size of the buffer which holds the lines scrolled beyond the border of the terminal window, and the scroll rate.

5.8.1.2 Customizing the Keyboard

Another important page of the Telnet Connection Properties is the Keyboard page, at which you can customize your keyboard behavior, including keyboard remapping. The required settings are highly dependent on the host and the application running on the host.

Keyboard remapping might be needed for example when the application uses VT420 keys that are not on your keyboard, such as F15. You can map Alt-F5 to F15. You can also define useful keyboard macros. For example you can assign the smit<Enter> sequence to Alt-F1 and have the AIX system management tool ″smit″ launched by a keystroke. To do this, click on **Change...**. A window with your current keyboard layout will appear, as shown in Figure 107 on page 203.

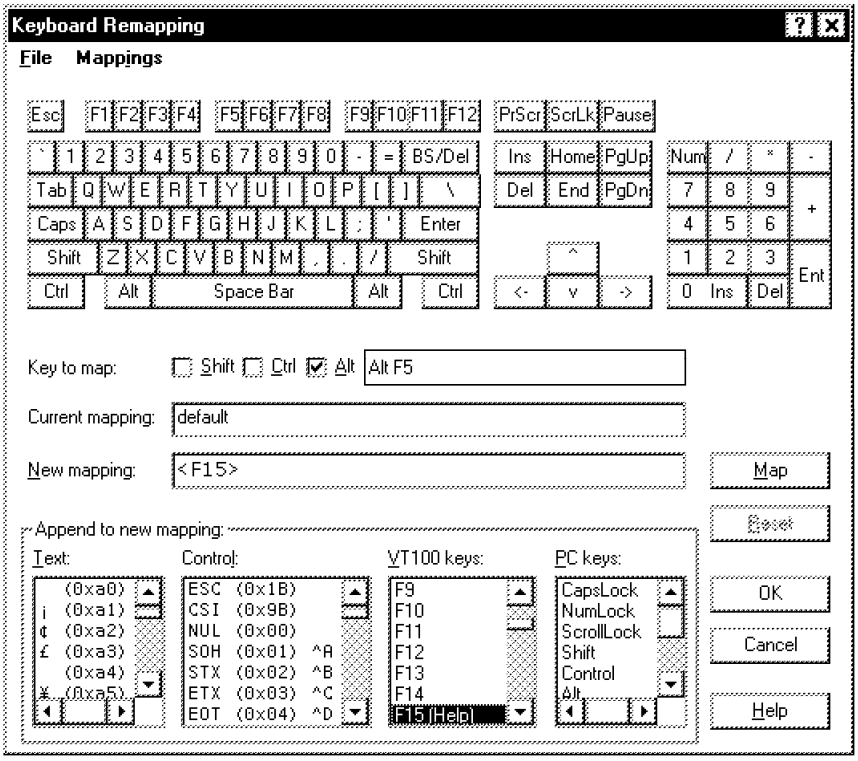


Figure 107. Keyboard Remapping

Click on the key you want to remap, select the corresponding modifier (Shift, Ctrl or Alt) if any, then select from the lists at the bottom of the window the new mapping. You can also enter text in the New mapping field. After you are ready, click on **Map**. Click **Yes** at the confirmation request dialog, then click **OK**. If you want to keep the remapping for future use, click on **Yes** at the save dialog and specify a file name. You can also use the saved file for other sessions.

5.8.1.3 Printing from a Session

Set up the print options at the Print Options page of the Telnet Connection Properties window (see Figure 108 on page 204).

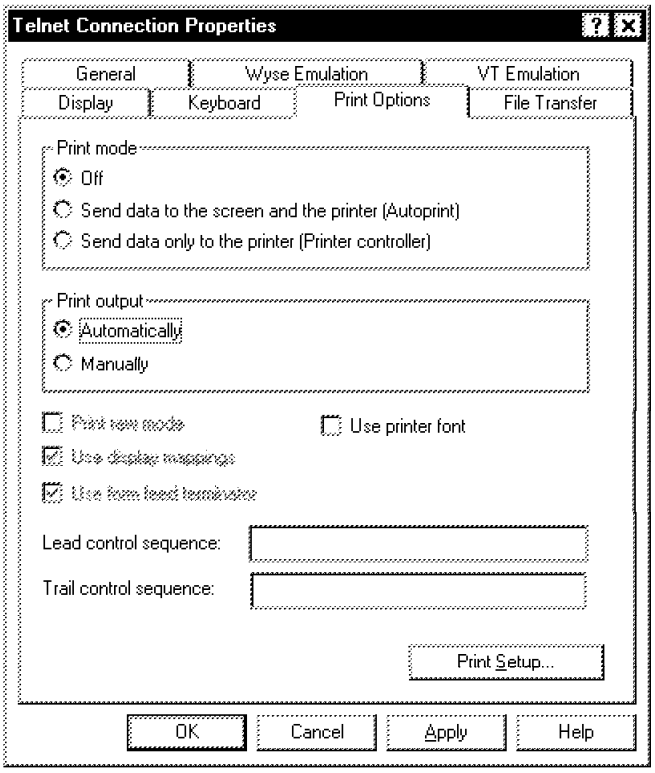


Figure 108. Telnet Connection Properties - Print Options

At the Print mode selection you have three choices:

- Off. This is the normal print mode. TNVTPlus displays the information from the host, but does not send it to the printer.
- Autoprint. Besides displaying the information from the host, the program sends the same information to the printer. That is, you will have a hardcopy of your session.
- Printer Controller. The information from the host is sent only to the printer, it will not be displayed on the screen. This option is useful for example to generate hardcopy from script-automated sessions.

At the Print output selection you can choose between Automatic to send the print job to the printer right after it has ended, or Manually to have multiple outputs spooled into a single spool file, which has to be sent manually to the printer. The default is Automatic. These options are valid with Print mode set to Autoprint or Printer controller.

Other options available include:

- Print raw mode. Select this check box to send untranslated (raw) data to the printer, for example a data stream that contains control sequences. Use this option in conjunction with the Printer Controller mode.
- Use display mappings. Use this option with the Printer Controller mode if you want to send display remapped characters to the printer.
- Use form feed terminator. This option adds a form feed character at the end of each print job in case you use the Print raw mode.
- Use printer font. If you select this option, the print job will be printed using a built-in font of the printer. This will result in faster processing, but the output format may not match the screen.
- Lead control sequence. You can specify in this input field a control sequence which will be sent to the printer at the beginning of the print job. This option is available only in Printer controller mode with Print raw mode selected.
- Trail control sequence. You can specify in this input field a control sequence which will be sent to the printer at the end of the print job. This option is available only in Printer controller mode with Print raw mode selected.

5.8.1.4 Transferring Files

If your host has support installed for any of the KERMIT, XMODEM, YMODEM or ZMODEM file transfer protocols, you can transfer files between your PC and the host.

Note: The current release of eNetwork Communications Suite does not provide direct access to a COM port for TNVTPlus to access, for instance, a BBS. This is planned for future versions.

You can set up the file transfer parameters at the File Transfer page of the Telnet Connection Properties window. You can select the protocol to use, the receiving directory, and some protocol-specific settings.

To perform a file transfer, first start the file transfer program at the host. Then select **Send File...** or **Receive File...** from the Commands menu point of the main window′s menu bar. Alternatively, you can use the corresponding buttons on the tool bar. At the dialog box similar to Figure 109 on page 206, fill in the file name subject to transfer, select the protocol to use, then click on **OK** to initiate the transfer.

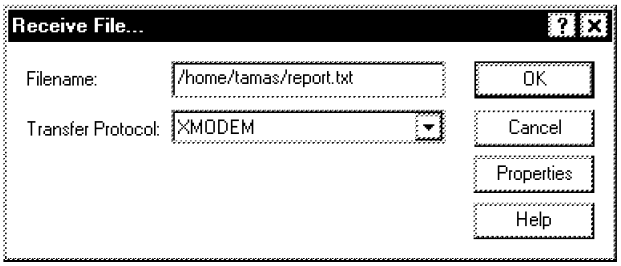


Figure 109. Receive File Dialog

This file transfer possibility is useful in case you need to exchange files with hosts not running an FTP or NFS server.

5.8.2 Using TNVTPlus in Windows 3.x Environments

TNVTPlus in these environments is almost identical to the Windows 95 or Windows NT versions. Minor differences exist in the user interface and some of the options.

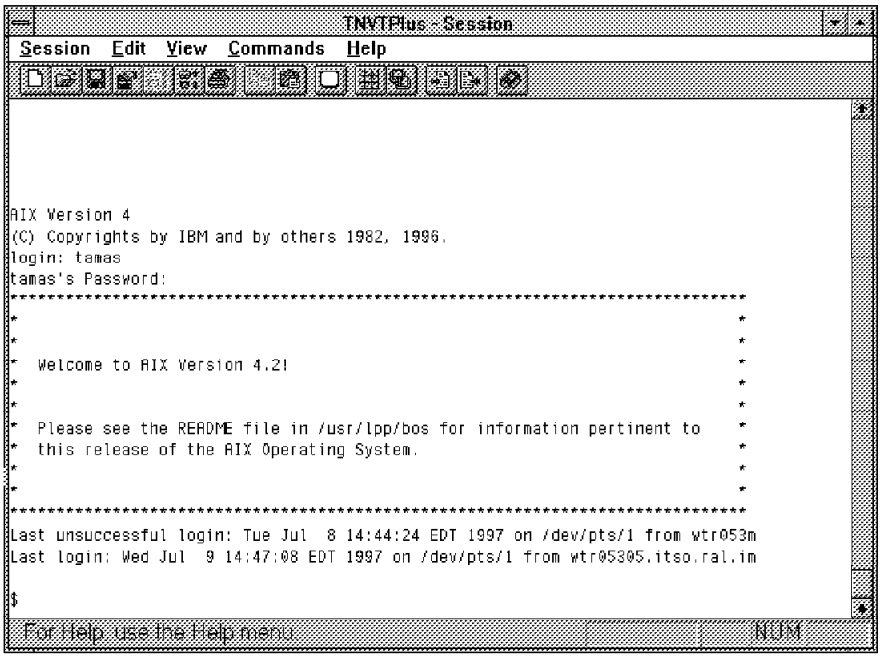


Figure 110. TNVTPlus Main Window

Start the program by clicking on the **TNVTPlus** icon in the OnNet16 2.5 WinApps program group. The main application window will be shown, similar to Figure 110, along with the Open File dialog box. If you have not

saved any session files yet, click on **Cancel**, then select **Session/New** from the menu bar to configure a new session. A dialog box shown in Figure 111 on page 207 will pop up. Type in the host name or IP address at the **Host** input field, select the connection type and the terminal type. The default terminal type VT420, VT320, VT220 is the most commonly used and it is correct for our scenario. Click on **Connect** to initiate a the session.

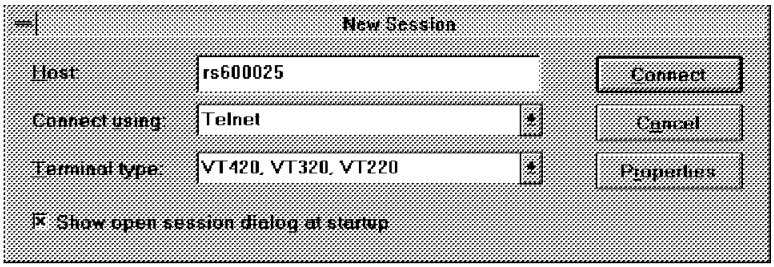


Figure 111. New Session Dialog Box

Depending on the target system and the application running on that system, you might have to use a different terminal type. Ask your system administrator for details.

5.8.2.1 Setting Up a Session

There are a large number of parameters which affect a Telnet session. You can set these parameters at the Telnet Connection Properties window, accessible by clicking on **Properties** at the New Session dialog box, or selecting the **Properties** from the **Session** menu point of the menu bar. There is a button on the task bar that can also be used. You can modify most of the settings on-the-fly.

Let′s take a brief look on the most important settings. At the General page, shown in Figure 112 on page 208, besides the host and the terminal type, you can set the automatic login parameters. Specify your user name and password. If the target system′s user name and password prompt differ from the default login: and password:, you have to specify those prompts at the corresponding fields. If you select the **Save password** check box, the login procedure will be fully automated; you will not be asked for a password. Use this feature with caution, because it implies a security risk. One could copy your session definition file and use it to log on fraudulently to the host.

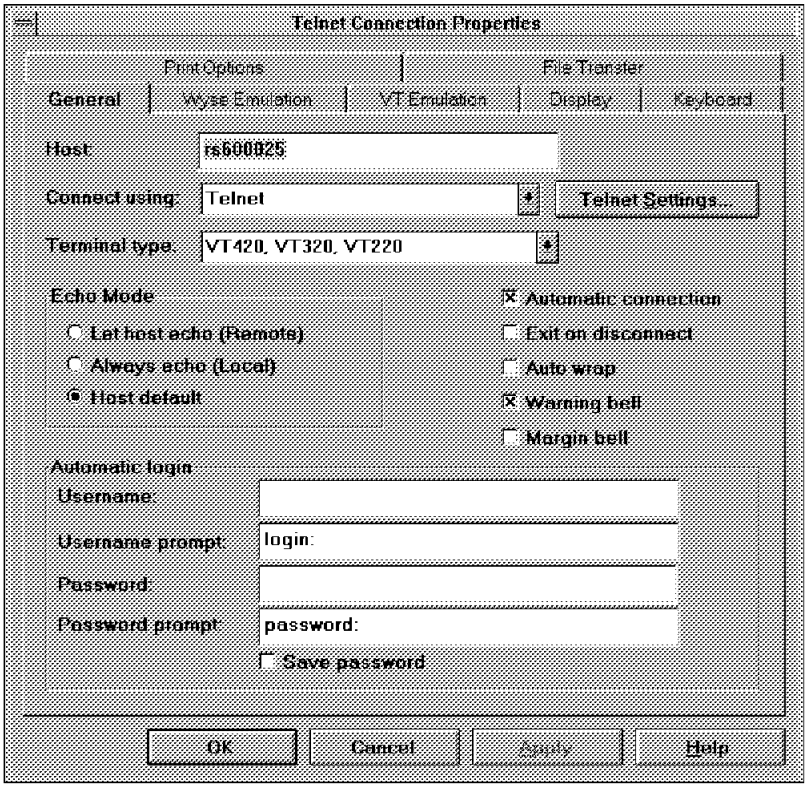


Figure 112. Telnet Connection Properties - General

You can modify your communication settings by clicking on **Telnet Settings...**. Settable parameters include port number (if different from the standard Telnet port, which is 23), terminal negotiation options, window size and local echo option and others. Seldom these parameters have to be modified.

At the Display page you can customize the following:

- The colors and the font used. Access the dialogs associated to these tasks by clicking on the **Change Colors...** and **Change Font...**. For example, you can select Greek, Hebrew or Turkish font. If you want the displayed font size to remain constant when resizing the emulation window, deselect the **Scale font to window** check box.
- Display remapping. You can specify what character is to be displayed when receiving a certain character from the host. You can save your definitions to a file and assign this mapping file to any session. The online help contains step-by-step instructions on how to do this.

- Number of columns to display. The default is 80. Optionally you can select 132 or 180 for a wider display.
- Number of lines to display. Depending on the terminal type and the page memory selected, the valid range is between 24 and 48.
- Page memory. You can specify how many pages and lines the TNVTPlus screen has.
- Scrolling options. You can set the size of the buffer that holds the lines scrolled beyond the border of the terminal window, and the scroll rate.

5.8.2.2 Customizing the Keyboard

Another important page of the Telnet Connection Properties is the Keyboard page, at which you can customize your keyboard behavior, including keyboard remapping. The required settings are highly dependent on the host and the application running on the host.

Keyboard remapping might be needed for example when the application uses VT420 keys that are not on your keyboard, such as F15. You can map Alt-F5 to F15. You can also define useful keyboard macros. For example you can assign the smit<Enter> sequence to Alt-F1 and have the AIX system management interface tool ″smit″ launched by a keystroke. To do this, click on **Change...**. A window with you current keyboard layout will appear, as shown in Figure 113 on page 210.

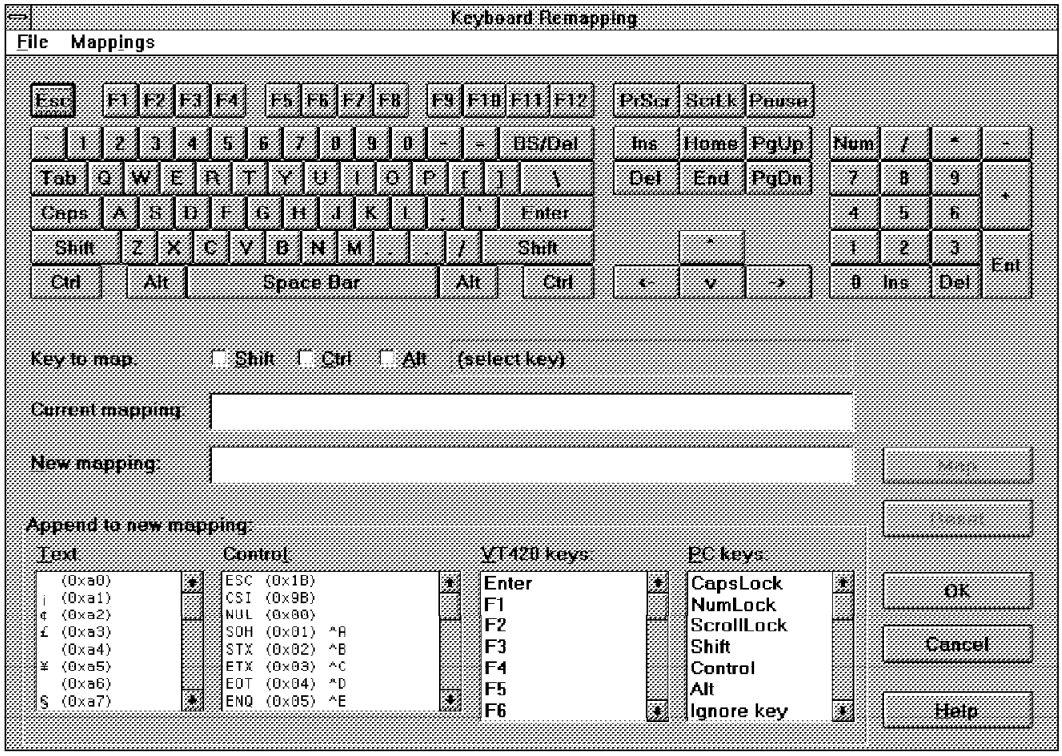


Figure 113. Keyboard Remapping

Click on the key you want to remap, select the corresponding modifier (Shift, Ctrl or Alt) if any, then select from the lists at the bottom of the window the new mapping. You can also enter text in the **New mapping** field. After you are ready, click on **Map**. Click **Yes** at the confirmation request dialog, then click **OK**. If you want to keep the remapping for future use, click on **Yes**, and specify a file name at the save dialog. You can also use the saved file for other sessions.

5.8.2.3 Printing from a Session

Set up the print options at the Print Options page of the Telnet Connection Properties window (see Figure 114 on page 211).

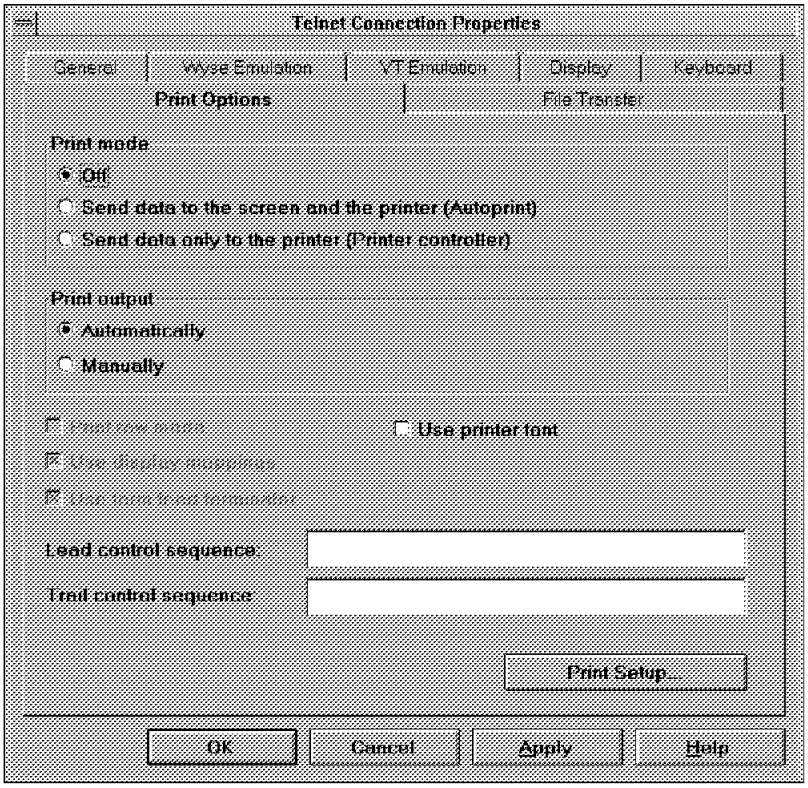


Figure 114. Telnet Connection Properties - Print Options

At the Print mode selection you have three choices:

- Off. This is the normal print mode. TNVTPlus displays the information from the host, but does not send it to the printer.
- Autoprint. Besides displaying the information from the host, the program sends the same information to the printer. That is, you will have a hardcopy of you session.
- Printer Controller. The information from the host is sent only to the printer; it will not be displayed on the screen. This option is useful for example to generate hardcopy from script-automated sessions.

At the Print output selection you can choose between Automatic to send the print job to the printer right after it has ended, or Manually to have multiple outputs spooled into a single spool file, which has to be sent manually to the printer. The default is Automatic. These options are valid with Print mode set to Autoprint or Printer controller.

Other options available include:

- Print raw mode. Select this check box to send untranslated (raw) data to the printer, for example data stream that contains control sequences. Use this option in conjunction with the Printer Controller mode.
- Use display mappings. Use this option with the Printer Controller mode if you want to send display remapped characters to the printer.
- Use form feed terminator. This option adds a form feed character at the end of each print job in case you use the Print raw mode.
- Use printer font. If you select this option, the print job will be printed using a built-in font of the printer. This will result in faster processing, but the output format may not match the screen.
- Lead control sequence. You can specify in this input field a control sequence which will be sent to the printer at the beginning of the print job. This option is available only in Printer controller mode with Print raw mode selected.
- Trail control sequence. You can specify in this input field a control sequence which will be sent to the printer at the end of the print job. This option is available only in Printer controller mode with Print raw mode selected.

5.8.2.4 Transferring Files

If your host has support installed for any of the KERMIT, XMODEM, YMODEM or ZMODEM file transfer protocols, you can transfer files between your PC and the host.

Note: The current release of eNetwork Communications Suite does not provide direct access to a COM port for TNVTPlus to access, for instance, a BBS. This is planned for future versions.

You can set up the file transfer parameters at the File Transfer page of the Telnet Connection Properties window. You can select the protocol to use, the receiving directory, and some protocol-specific settings.

To perform a file transfer, first start the file transfer program at the host. Then select **Send File...** or **Receive File...** from the Commands menu point of the main window's menu bar. Alternatively, you can use the corresponding buttons on the tool bar. At the dialog box similar to Figure 115 on page 213, fill in the file name subject to transfer, select the protocol to use then click on **OK** to initiate the transfer.

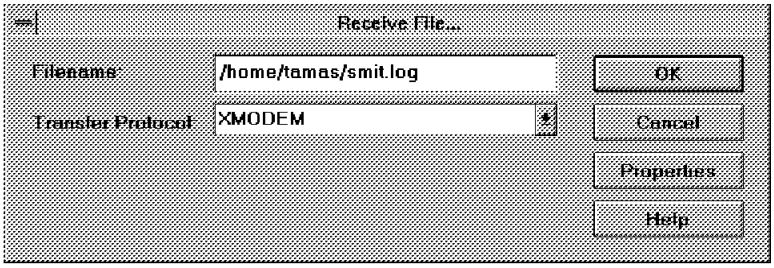


Figure 115. Receive File Dialog

This file transfer possibility is useful in case you need to exchange files with hosts not running an FTP or NFS server.

5.9 Using the Remote Utilities

In some cases your work on network hosts is limited to a single command or it consists of launching some batch jobs, for example, end-of-day processing, report printing, etc. Rather than establish a telnet session, you can use the Remote Command part of the Remote Utilities, which is very well suited for these kind of tasks.

It also happens that you occasionally need to exchange files with a host that does not run an FTP or an NFS server, or you cannot use them. In this case, you can use the Remote Copy part of the Remote Utilities.

Note: The rshd subsystem has to be active on the remote system and the proper authorizations set up in order to be able to use the Remote Utilities.

5.9.1 Using the Remote Utilities under Windows 95 and Windows NT

There are a couple of options that influence the behavior of Remote Utilities. Access the Remote Utility Options dialog box by selecting **Options** from the View menu point of the menu bar. Among others, you can customize the font used for normal and error output, you can select to be prompted before local files are overwritten and can save the passwords associated to sessions. Be aware of the security exposure when using the save password option.

5.9.1.1 Excuting Remote Commands

Start the Remote Utilities from the Start Menu by selecting **Programs/Network Access Suite/Remote Utilities**. The application window shown in Figure 116 on page 214 will appear. Click on the **Remote Command** tab. Fill in the input fields with the necessary command, host, user name and password information. Select the **Convert from UNIX style text** check box if the output is in text format, otherwise deselect it. Click on

Start to initiate the remote command execution. The results of the command will be shown in the text box at the bottom of the window.

For example, if you want to know whether your colleague is still logged on to the host, you can fill in the fields similar to Figure 116

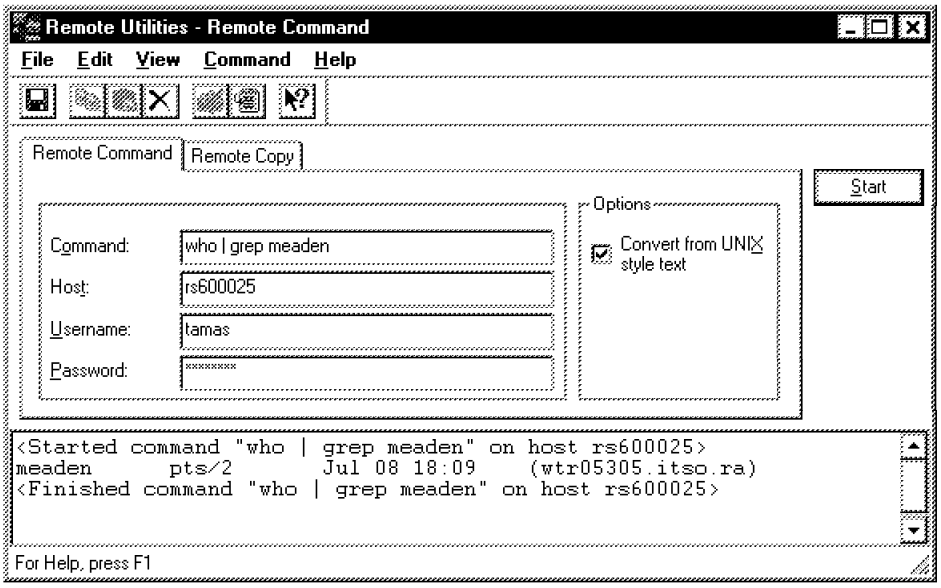


Figure 116. Remote Command

You can save your sessions by selecting **Save Session As...** from the File menu point of the menu bar.

Tip

Save the most common remote command sessions and create a separate folder with shortcuts to them. If you use the Save password feature, a remote command execution procedure will be simplified to a double-click.

5.9.1.2 Exchanging Files

The second part of the Remote Utilities allows you to exchange files between you PC and the host. Assuming that the Remote Utilities are started, click on the **Remote Copy** tab. You will see a page similar to Figure 117 on page 215. Select the direction of the copy procedure by clicking the corresponding **Local** or **Remote** button at the From input field

group. The icons at the From and To input field groups will change to show the direction selected.

To perform a remote copy operation, fill in the input fields in both the From and To groups with appropriate file, host, username and password information, set the options if needed and click on **Start**. See Figure 117 for an example.

Note: You can use wildcards to copy multiple files.

The results of the operation will be shown in the text box at the bottom of the application window.

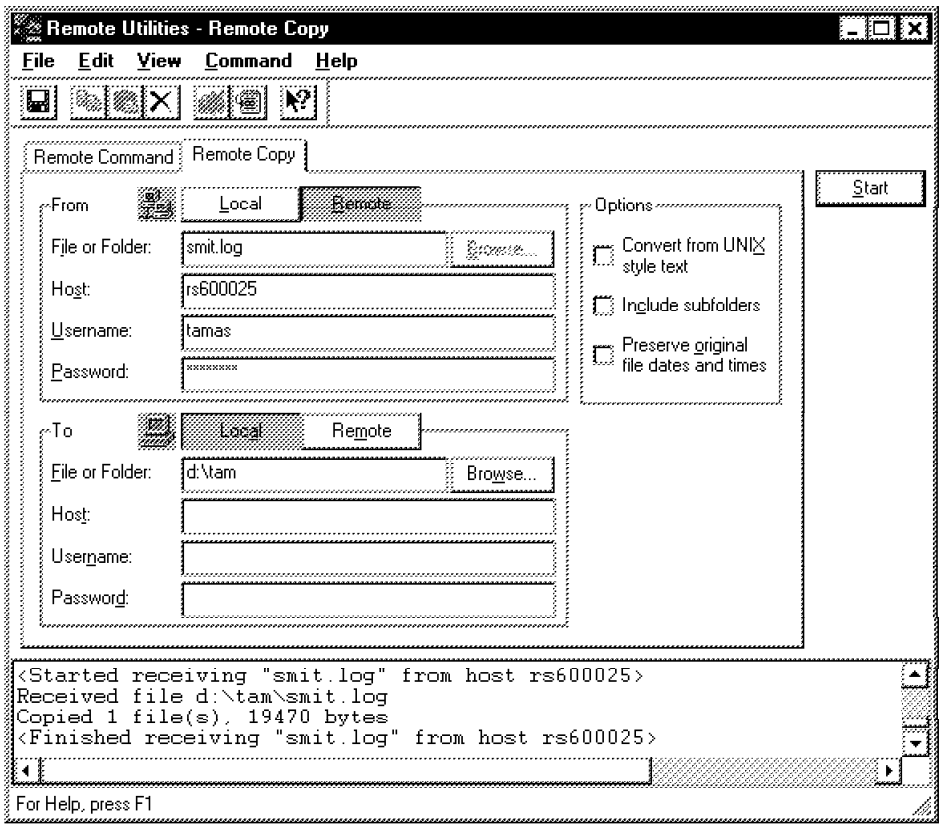


Figure 117. Remote Copy Window

You can save your sessions by selecting **Save Session As...** from the File menu point of the menu bar.

Tip

Save the most common remote copy sessions and create a separate folder with shortcuts to them. If you use the Save password feature, a remote copy operation will be simplified to a double-click.

5.9.2 Using the Remote Utilities under Windows 3.x

The remote utilities are accessible from the OnNet16 2.5 WinApps program group, by double-clicking on either the Remote Command or Remote Copy icon, depending on the task to be performed.

5.9.2.1 Excuting Remote Commands

Start the Remote Command application by double-clicking on the **Remote Command** icon in the OnNet16 2.5 WinApps program group. The application window shown in Figure 118 on page 217 will appear. Fill in the input fields with the necessary command, host, user name and password information. Select **Settings/Ouput is binary** from the menu bar if the output is in binary format, otherwise deselect this option. Click on **Start** to initiate the remote command execution. The results of the command will be shown in the **Output** text box. If you want to see details on the connection and command execution, select **Settings/Show Progress Details** from the menu bar. An additional text box with the details will be displayed at the bottom of the application window.

You can choose the authentication method to use. The options are available in the Authentication menu and the tool bar. They are the following:

- Do Not Request a Password. The program will use the rsh protocol to execute the command. The authentication is based on a list of hosts that is maintained at the remote host. If your computer is listed, you can execute the command.
- Request a Password. The program will use the rexec protocol. The authentication is based on a list of users and passwords that is maintained at the remote host.
- Use Default Authentication Order. The program will try the rsh protocol first. If that does not work, it will try the rexec protocol.

For example, if you want to know whether your colleague is still logged on to the host, you can fill in the fields similar to Figure 118 on page 217.

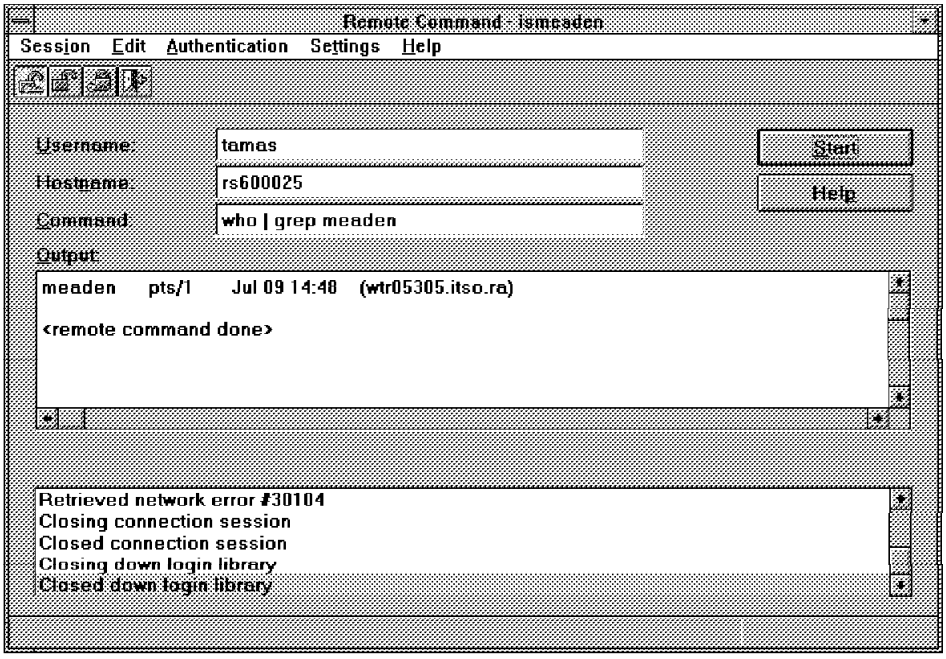


Figure 118. Remote Command Window

You can save your sessions by selecting **Session/Save...** from the menu bar.

Note: If you specified your password before saving the session, it will also be saved. This implies a security risk.

Tip

To automate the remote command execution, save your session and create a program icon with the following command line setting:

```
wrsh -s session_name
```

where session_name is the name of the previously saved session.

5.9.2.2 Exchanging Files

The Remote Copy component of the remote utilities allow you to exchange files between you PC and the host. Start the Remote Copy application by double-clicking on the **Remote Copy** icon in the OnNet16 2.5 WinApps program group. The application window shown in Figure 119 on page 218 will appear. Set the direction of the copy procedure by selecting the corresponding **Local** or **Remote** radio button.

To perform a remote copy operation, fill in the input fields with appropriate file, host, username and password information, set the options if needed and click on **Start**. See Figure 119 on page 218 for an example.

Note: You can use wildcards to copy multiple files.

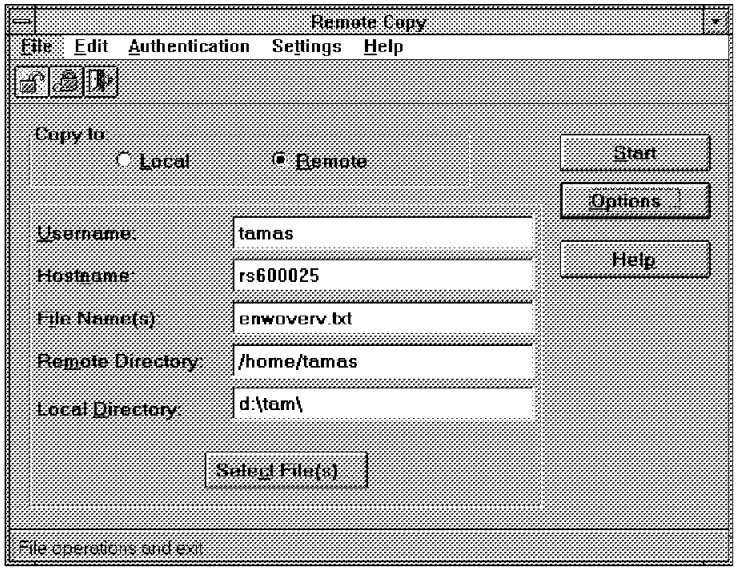


Figure 119. Remote Copy Window

The options you can set are the following:

- Type of Transfer. This can be ASCII or binary.
- UMASK. This is an octal value used to set the default permissions for new files that you transfer from the PC to the host. The default will allow full access for the owner (you) and no access for the group and others. Consult the online help for other values.

As in case of the Remote Copy, you can select the protocol to be used for the transfer:

- Do Not Request a Password. The program will use the rsh protocol. The authentication is based on a list of hosts that is maintained at the remote host. If your computer is listed, you can execute the command.
- Request a Password. The program will use the rexec protocol. The authentication is based on a list of users and passwords that is maintained at the remote host.

5.10 Setting Up Netscape Navigator

The setup of the Netscape browser for this scenario is simple and it is identical on all platforms. In order to access the Internet, you must specify the firewall's hostname or IP address at the Netscape preferences. Since the firewall in this case is a SOCKS server, you must enter its name or IP address in the SOCKS Host field of the Manual Proxy Configuration page.

To access the internal Web server, you do not need to go through the firewall. In most cases the firewall is set up in a way that it will refuse the connection attempts to internal hosts. Therefore you have to list the hostname or IP address of the Web server in the No Proxy for field, as shown in Figure 120.

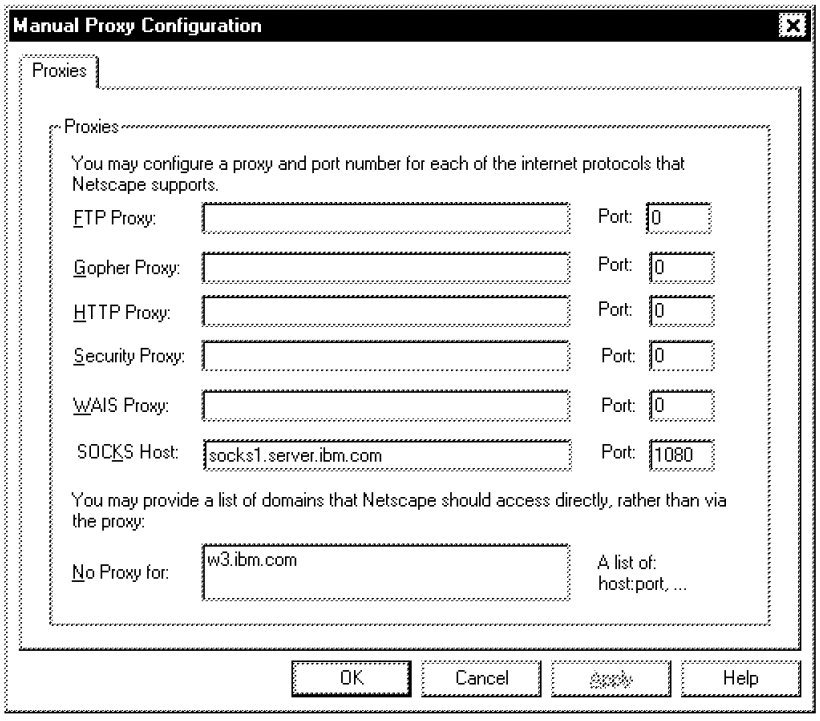


Figure 120. Netscape Preferences - Manual Proxy Configuration

5.10.1 Using Netscape Mail

In order to be able to use Netscape Mail, set it up via the Netscape preferences as described in 3.2.5, "Installing Netscape Navigator for Windows 95" on page 95. You have to have a user ID at an accessible POP3 mail server.

After you have set up Netscape Mail, display the application by selecting **Window/Netscape Mail** from the menu bar. You will see a window similar to Figure 121 on page 220.

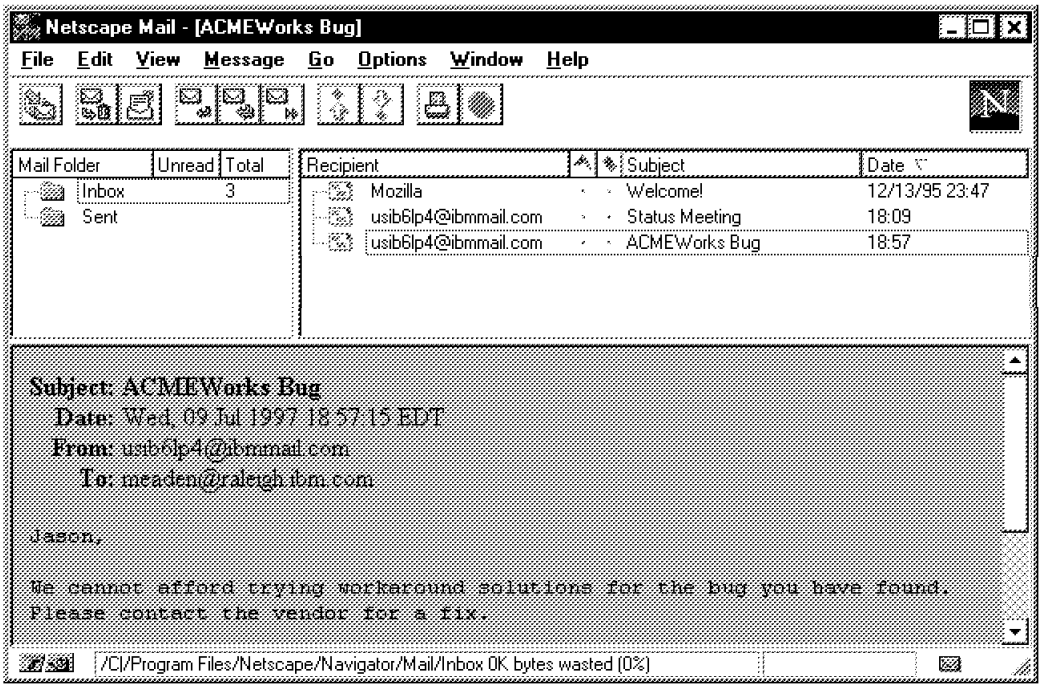


Figure 121. Netscape Mail

At the Mail Folder pane you can select a folder. Its content will be shown in the upper-right pane. Click on the mail item you want to see. It will be shown in the bottom pane. The context menu of the mail items allow for reply, reply to all, forward, forward quoted and delete operations.

To write a new mail item, select **File/New Mail Message** or click on the corresponding button on the tool bar. You will be presented with a window shown in Figure 122 on page 221.

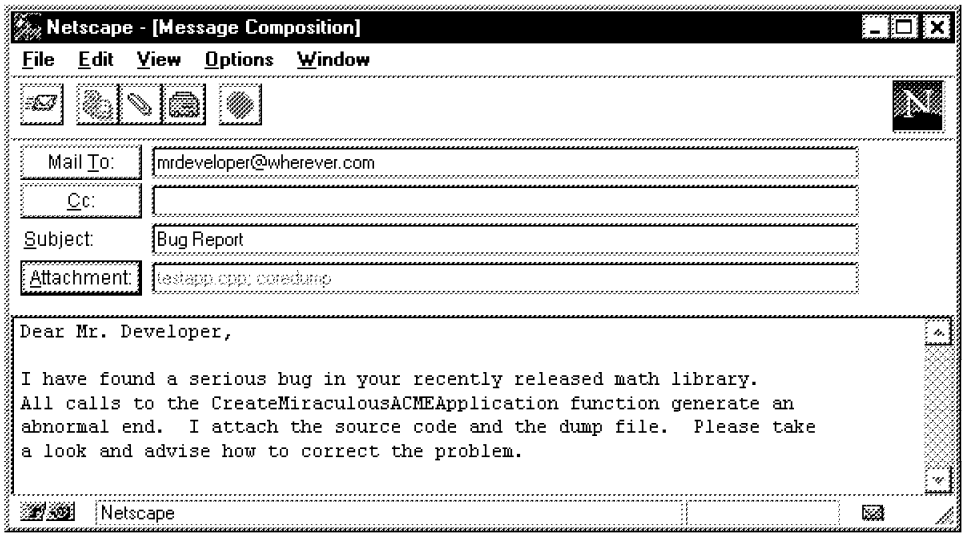


Figure 122. Netscape Mail - Message Composition

Fill in the Mail To field, and optionally the Cc and the Subject fields. Then compose you mail at the text box at the bottom of the window.

If you want to send attachments, click on **Attachment** and select the attachment type: URL or file. Then either specify the URL or select a file at the Enter file to attach dialog box, shown in Figure 123.

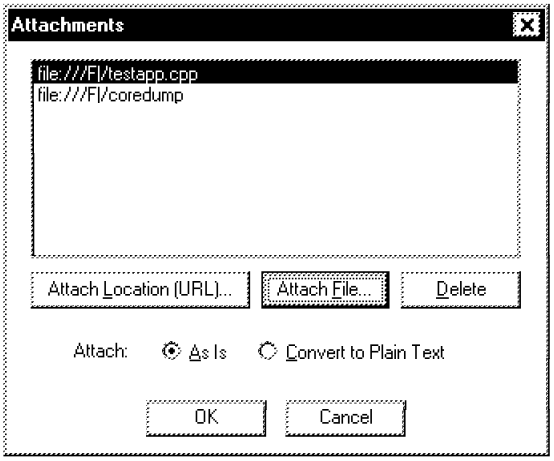


Figure 123. Netscape Mail - Attachments

When you are finished, select **File/Send Now** or click on the corresponding button on the tool bar to send you mail to the recipient(s).

Notes:

1. For details on installing and configuring Netscape Navigator, see 3.2.5, “Installing Netscape Navigator for Windows 95” on page 95.
2. For a detailed description of the Netscape Navigator features, consult the online help.

5.10.2 Using Netscape News

Netscape News provides a graphical interface to access news servers on the Internet, to browse through and subscribe to news groups, and to read and post articles to news groups. For more information on Internet news, please read 1.10.1, “Network News” on page 34.

There are many news servers available on the Internet. Access to some servers may be restricted to users within certain domains, or posting may not be allowed for certain news groups. We recommend that you consult with your network administrator for names or IP addresses of news servers. For suggestions on how to use IBM internal news servers, please refer to the following URL:

`http://w3.raleigh.ibm.com/Guides/IBMnews.html`

To start Netscape News, select **Window/Netscape News** from the menu bar of the browser. You can also have Netscape News started automatically whenever the browser starts by ticking the Netscape News check box on the Appearance tab of the General Preferences item of the Options menu.

Once Netscape News is started, you will see a window similar to the one shown in Figure 124 on page 223 that is devided into three panes:

1. In the News Server pane, you see a list of available news servers. You can add and remove servers and expand server entries to display the newsgroups available on a particular server.
2. In the upper right pane you see the discussion threads that make up a news group.
3. In the bottom pane you see the selected article, one at a time.

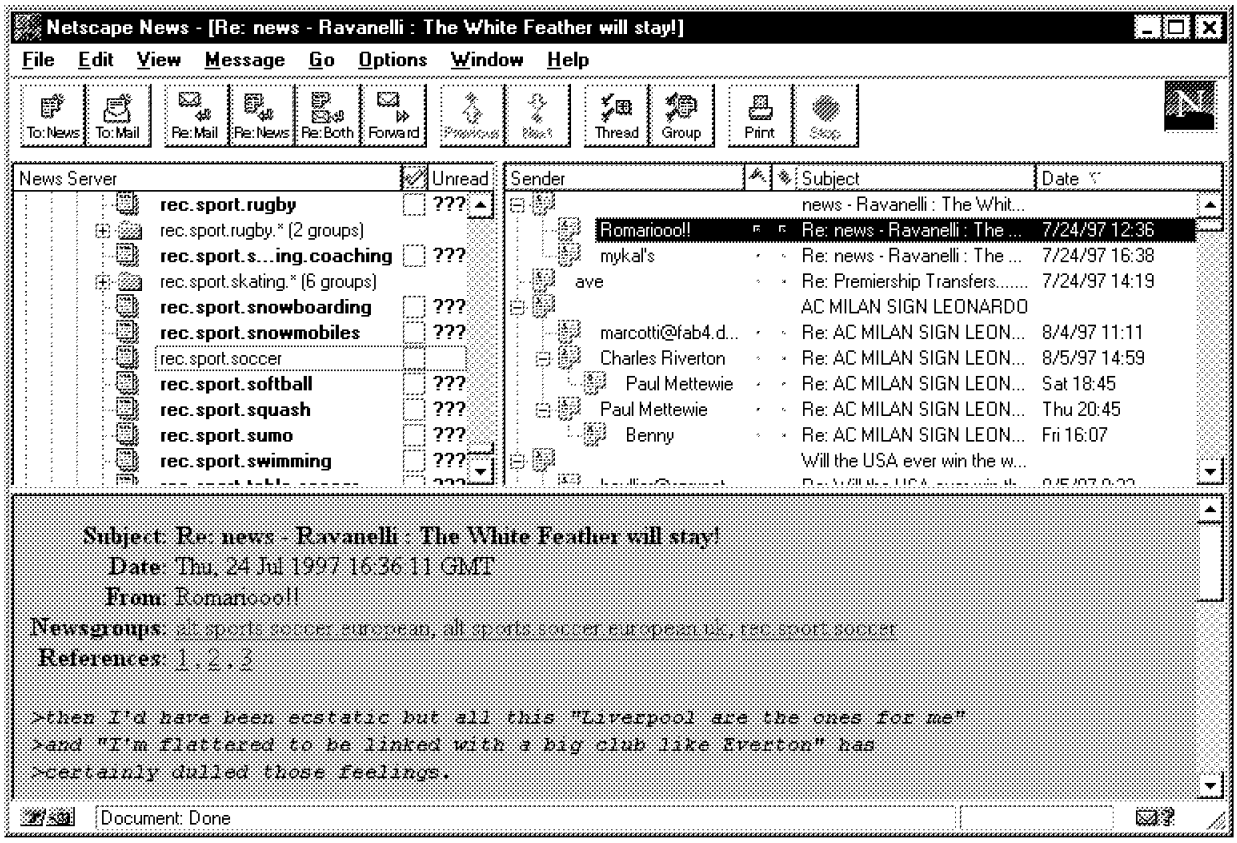


Figure 124. Netscape News

Use the menu items or the icons from the icon bar to post or mail articles and walk your way through discussion threads and news groups.

Chapter 6. Scenario B - Multiplatform, Multiprotocol Environment

In this chapter, we develop a corporate scenario based on a multiplatform, multiprotocol network, and describe how to implement and use the eNetwork Communications Suite in that environment. This scenario assumes the following:

- Multiple routed and bridged networks in different locations running TCP/IP, SNA and NetBIOS protocols
- MVS host or AS/400 with SNA and TCP/IP attachments
- UNIX, Windows NT, and OS/2 Warp Server
- Lotus Notes mail
- Internet access
- The following eNetwork Communications Suite components are used:
  - FTP Software TCP/IP protocol stack and FTP Software TCP/IP applications
  - Personal Communications over SNA
  - Netscape Navigator
  - Lotus Notes Mail Client
- The following eNetwork products are also used:
  - Communications Server
  - Host On-Demand

6.1 Environment Overview

In this scenario, our hypothetical enterprise has a number of networks that have been developed over time using different protocols such as SNA, NetBIOS and TCP/IP. A decision has been made that the corporation will now use TCP/IP on various Windows platforms. The router that connects this LAN segment to the corporate Intranet only routes TCP/IP packets. However these systems need access to the legacy networks which are still using other protocols. For this reason the servers running protocols other than TCP/IP have been configured to use TCP/IP as the transport for their own protocols. For example the Warp Server system is using NetBIOS over TCP/IP and the S/390 has been configured to use SNA over TCP/IP.

- Lotus Notes Domino Server

  This server provides access to Lotus Notes mail and databases over the network. The Notes Server is available across the entire enterprise and

is the main e-mail server for the organization. The server is configured to use TCP/IP and NetBIOS.

- S/390 Host

  The S/390 is using SNA to communicate with the network. It is also configured to provide SNA over TCP/IP so that it can be reached via the corporate Intranet using solely TCP/IP. This host is also running an NFS server that can be reached via the corporate Intranet.

- OS/2 LAN Server Network

  The LAN Server network has a number of workstations that contain some legacy data and files that need to be shared on this new network. The LAN Server network is using NetBIOS over TCP/IP to communicate across the LAN.

This corporate scenario could represent the branch office of a large enterprise with a centrally managed LAN containing the organizations major information resources, such as Lotus Notes, Internet access, S/390 Host and Warp Server systems. The branch office needs to be able to access these resources but without the complexity of multiple protocols on their LAN.

Since the majority of the connectivity issues are explained in Chapter 5, “Scenario A - Multi-Platform TCP/IP Environment” on page 167, only those portions which are new to this scenario are explained in this chapter. A graphical representation of this environment is shown in Figure 125 on page 227.

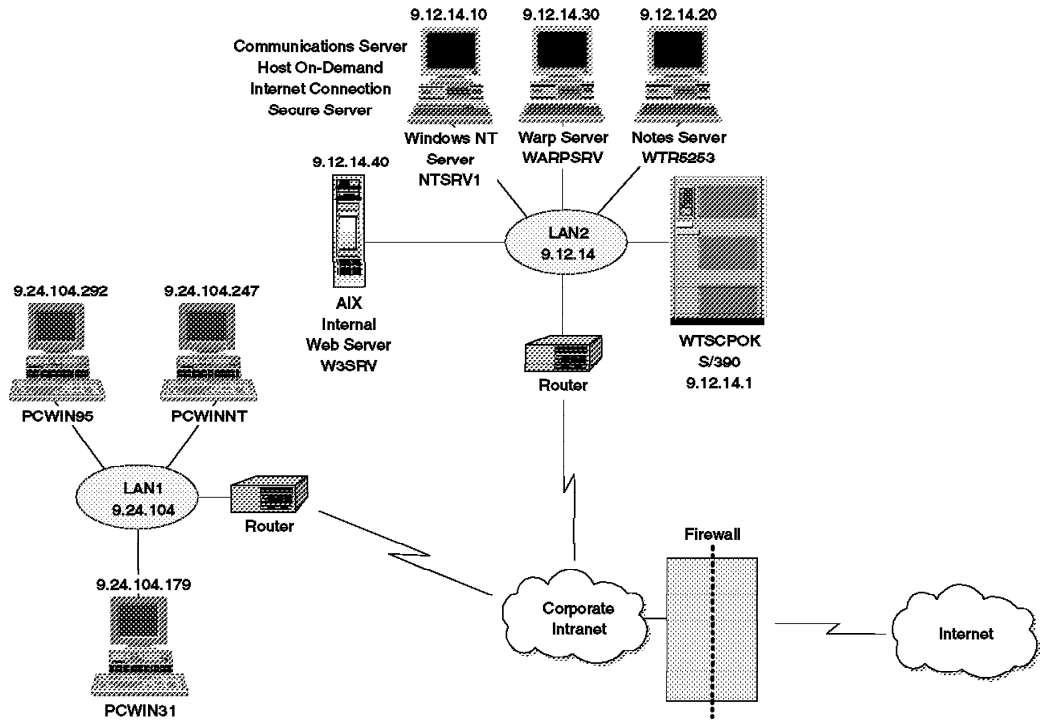


Figure 125. Scenario B - The Environment

6.2 Setting Up the Environment

In this section we describe in detail how to configure the components of the eNetwork Communications Suite to suit the network environment of Scenario B. Detailed installation instructions can be found in Chapter 3, “Installation and Configuration” on page 61.

6.2.1 Information Needed

Before beginning the installation and configuration, make sure that you have the following information about your network:

1. Lotus Notes address and a valid user ID file.. To install the Lotus Notes Mail Client you will need a valid user ID file created by the administrator of the Lotus Notes server. Ensure that when the administrator created your user ID file, that the license type specified for your client was Lotus Notes Mail, and not one of the other Lotus applications.

   To open Lotus Notes databases, you will need to know the address of the server that they reside on. Ask your Notes administrator for this information.

2. Personal Communications configuration. For this type of connection, there is quite a large amount of configuration information required. Your details will depend on the connection type being used in your environment. Many examples are presented in this scenario. Refer to 6.4, “Using Personal Communications over TCP/IP” on page 235 for more information.

3. OS/2 Warp Server NetBIOS names. If you are using shared resources on a Warp Server domain, you will need to know the name of the server that the resource resides on. You will also need the resource name. If the shared resource has access controls that prevent guest user access, then you will need to have a valid user ID on the Warp Server domain for authentication. Your network administrator can supply this information.

6.3 Setting Up the Lotus Notes Mail Client

For this scenario, it is assumed that you have a properly configured Lotus Notes Domino server available on your TCP/IP network, and that your Notes administrator has supplied you with a valid user ID file.

In this example the screen captures are from a Windows NT installation, however the installation and operation of the Lotus Notes Mail Client is virtually identical across all Windows platforms.

Install the Lotus Notes Mail Client as described in Chapter 3, “Installation and Configuration” on page 61. Start the Lotus Notes Mail Client by clicking on the **Start** button, then select **Programs**, **Lotus Applications**, and **Lotus Notes**.

The first time you start the mail client it will ask for the user ID file you wish to use. Select the location and user ID file you are going to use from the file open dialog box similar to Figure 126 on page 229. Your system administrator may have supplied the file to you on diskette or it may be on your hard disk or a network drive.

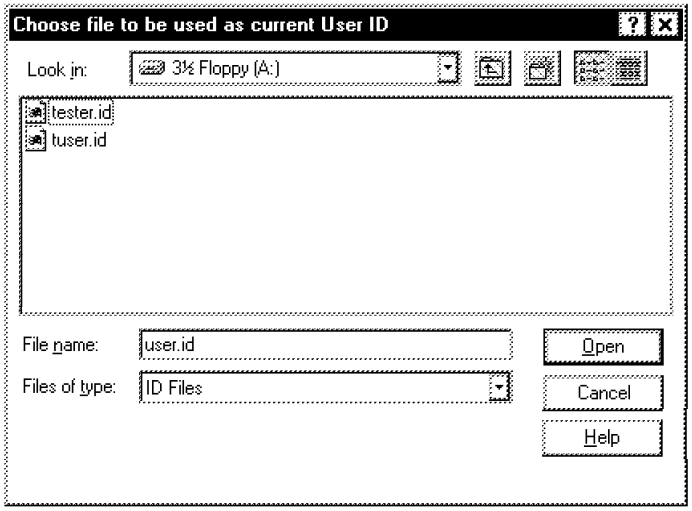


Figure 126. File Open Dialog Box - Select User ID

Your Notes administrator will have assigned an initial password when your user ID file was created. Lotus Notes will now prompt for that password for this client. The password is case-sensitive and should be entered exactly as supplied. The password dialog box looks like Figure 127. When you enter the password it will not appear on the screen, instead one or more X characters will appear instead.

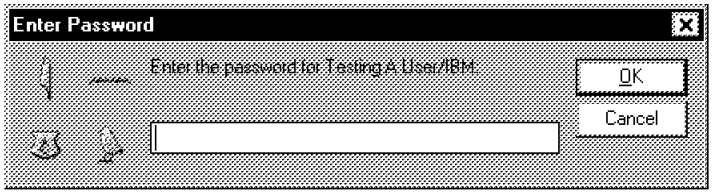


Figure 127. Password Prompt

The Lotus Notes Mail Client will now check for the connection to the server using your TCP/IP network. Once it has found the server and verified your user ID it will present you with the initial Lotus Notes workspace similar to Figure 128 on page 230.

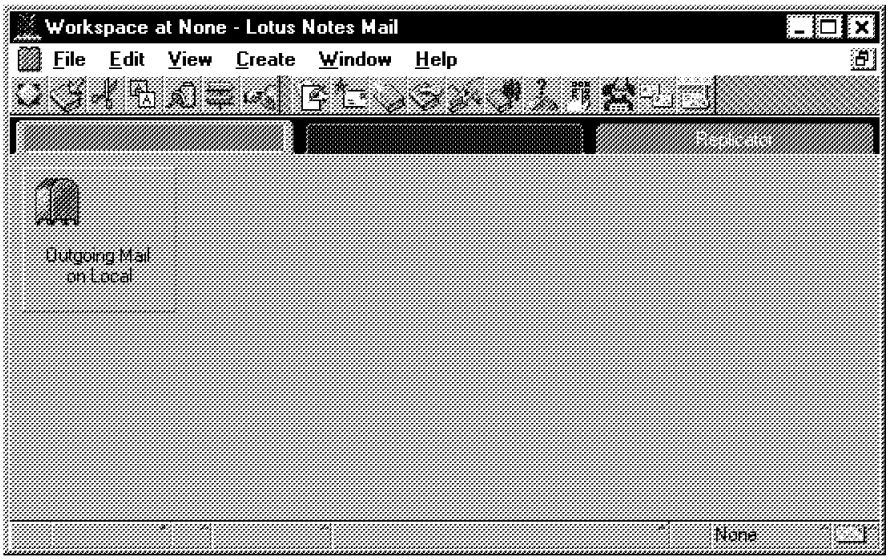


Figure 128. Lotus Notes Mail Client Initial Workspace

You can add databases to the desktop by clicking **File** from the Lotus Notes menu. From the drop-down menu select **Database** and then **Open**. In the Server field type the name of your domino server then select **Open**. After finding the server on the network, Lotus Notes will show a list of the databases that are available on that server. The list will look similar to Figure 129.

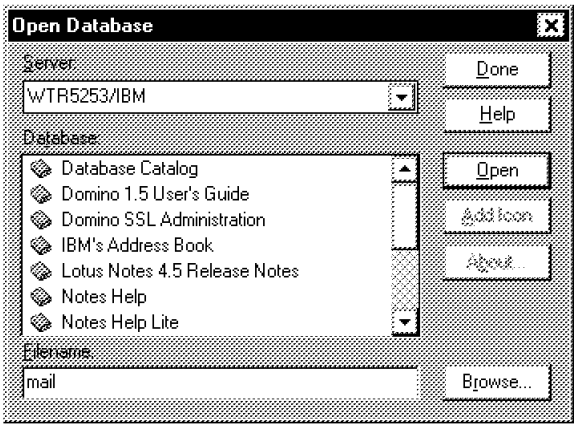


Figure 129. Open Database Dialog Box

The most important database is for your Lotus Notes e-mail. From the list of databases select the directory called Mail. From that directory select the mail database for your user ID then click on **Add Icon** then **Done**.

This will add a database shortcut for your e-mail onto your Lotus Notes workspace. To open this database, double-click on the shortcut. The first time you open the database, it will present you with an introduction to the e-mail template. Read this information then press Escape to open the database. Initially you will probably not have any mail or other items to view. Your e-mail database will look similar to Figure 130.

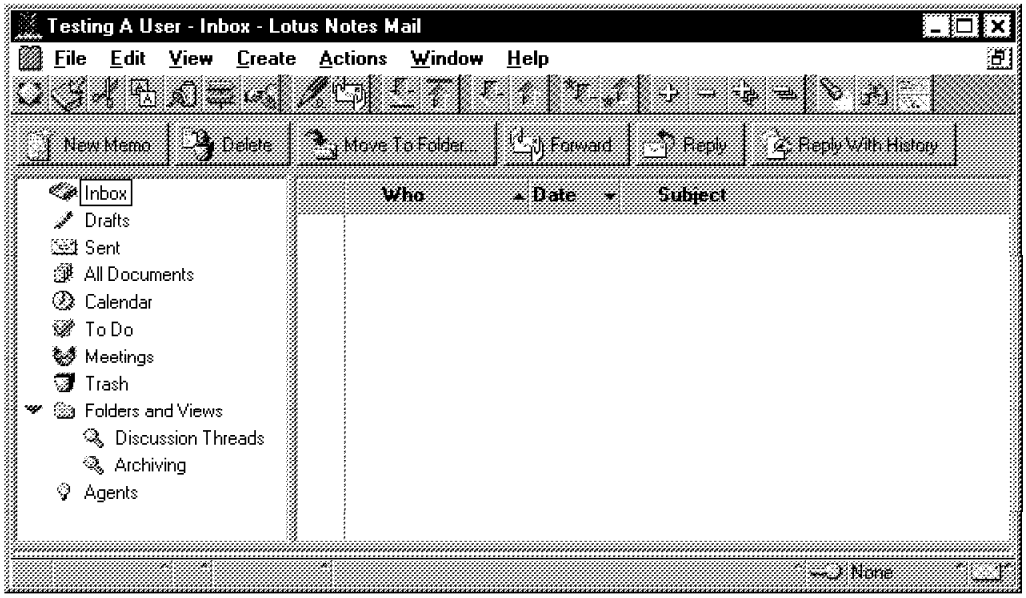


Figure 130. Lotus Notes Mail Database

To create a new e-mail message in the Lotus Notes Mail Client, click on **New Memo** while in the e-mail database. In the To: field type the name of the intended recipient. Press the Tab button until you get to the subject field and type in a subject for the message. Press the Tab button to get to the body of the message, and type in the text of your e-mail. Before sending, check that your message looks similar to Figure 131 on page 232 then click on **Send**.

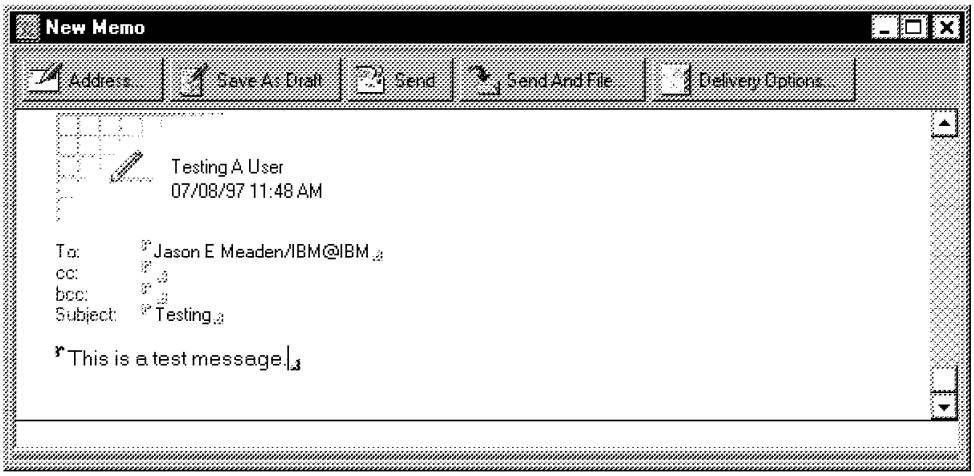


Figure 131. Sending a New Message

To check if you have unread mail waiting for you to read, ensure you are back at the Lotus Notes workspace. You can do this from anywhere in the Lotus Notes Mail Client by pressing the escape button repeatedly until you reach the main workspace. From the main menu, select **View** then **Refresh Unread Count**. If your e-mail database shows a number larger than zero, then you have unread mail.

To read this mail, double-click on the e-mail database to open it. From the folder views on the left-hand side of the workspace, select **Inbox**. Any unread mail will appear on the right-hand side. Double-click on the item to open it for viewing. An example message is shown in Figure 132 on page 233.

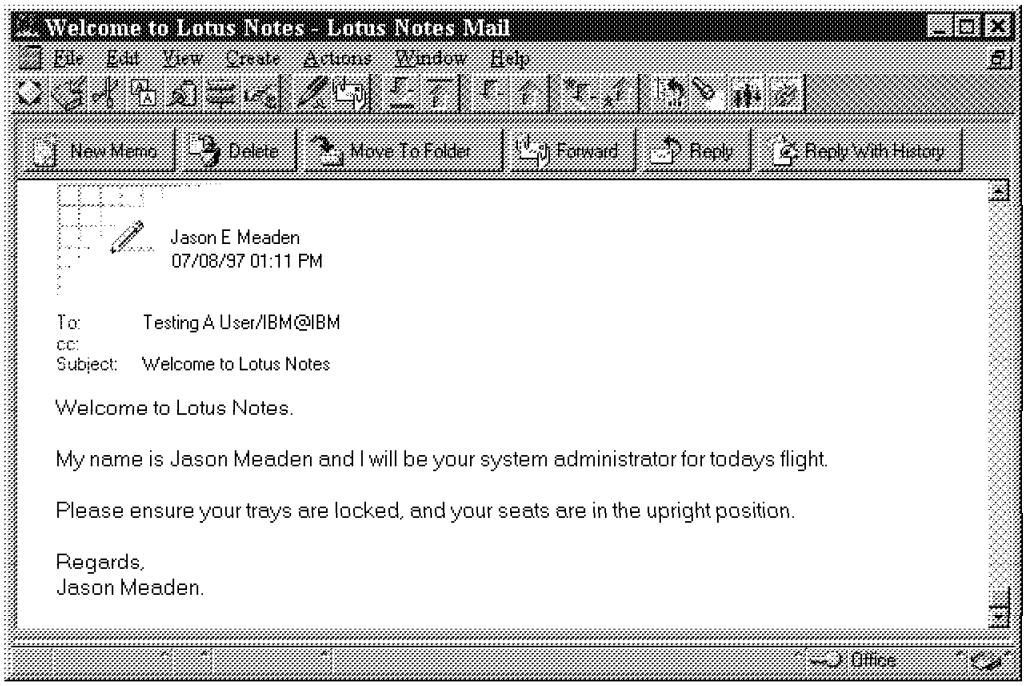


Figure 132. Reading a New Message

6.3.1 Browsing the Web with Lotus Notes Mail Client

The Lotus Notes Mail Client gives you the capability of browsing the World Wide Web in addition to using Lotus Notes databases. This feature is called the Personal Web Navigator. It allows you to access Web sites directly or via an InterNotes server, and it gives you the additional capability to store Web pages you have accessed into a Lotus Notes database.

In the personal address book on your Notes desktop you will find a location document for your Lotus Notes server. Edit that document to contain the following information:

- Web proxy and/or SOCKS server address
- Type of Internet browser; select **Notes**.
- Retrieve/open pages; select **from workstation** to create a local database with Web pages you've accessed.
- Web Navigator database; local database where you want your Web pages stored.
- Java Security.

To access Web pages, select **Open URL** from the File drop-down list on the menu bar, and enter the URL into the appearing dialog box. The figure below shows an example of a corporate home page accessed through Personal Web Navigator:

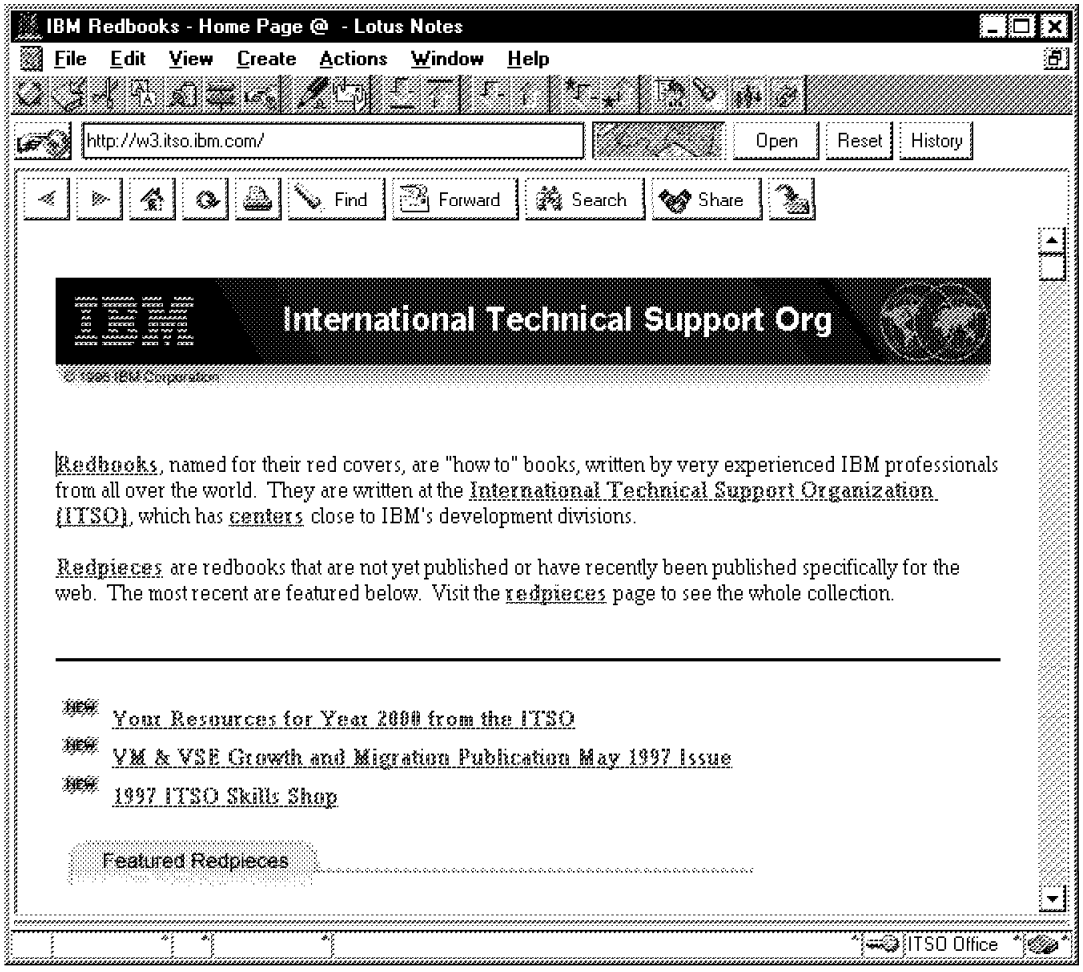


Figure 133. Lotus Notes Personal Web Navigator

You can quickly browse through pages on the Internet in that way to save access time. Later, you can turn to the Notes database where those Web pages have been stored to read through them in detail. Select **Database** from the File drop-down list on the menu bar, then select **Open**. From the list of databases (shown in Figure 129 on page 230) double-click on **Personal Web Navigator**.

Note: The current version, 4.5, of Notes Personal Web Navigator does not support frames and JavaScript.

6.4 Using Personal Communications over TCP/IP

There are several ways to connect Personal Communications to a mainframe over a TCP/IP connection, among them the following:

1. Using a direct TCP/IP connection and TCP/IP application protocols:
   - Telnet3270 (to MVS and VM)
   - Telnet5250 (to AS/400)
2. Using a TCP/IP connection to a SNA gateway running a Telnet3270E server:
   - Telnet3270 (Communications Server for NT, OS/2 or AIX to MVS)
3. Using a direct TCP/IP connection and SNA application protocols:
   - Dependent LU Requester (DLUR) over AnyNet SNA over TCP/IP (to MVS)
   - 5250 over AnyNet APPC over TCP/IP (to AS/400)
4. Using a TCP/IP connection to a SNA gateway running AnyNet SNA over TCP/IP gateway:
   - Dependent LU over AnyNet SNA over TCP/IP (to MVS)

Depending on the application (dependent and/or independent LUs) and network (TCP/IP or mixed) environment, you may want to choose one or the other connection possibility. Our scenario is mainly focussed on terminal emulation (dependent LUs), therefore we choose either Telnet3270 or DLUR over AnyNet SNA over TCP/IP.

6.4.1 Configuring Personal Communications Using Telnet3270

Once you have installed Personal Communications for your chosen platform, you can begin the configuration of the first communication session by following these steps:

1. From Windows NT or Windows 95 select **Start** then **Programs**. Then select **IBM Personal Communications** and then **Start or Configure Session**.

   Note: The installation described in this scenario is based on a Windows NT or Windows 95 installation, and includes screen captures from those platforms. However the basic configuration procedure is the same for a Windows 3.x installation. To start the configuration if you are using Windows 3.x, open the Personal

Communications folder from Program Manager and double-click on the icon **Start or Configure Session**.

2. Personal Communications will load and present you with a dialog box reminding you that you need to configure this session before you can connect to the host system. Read this dialog box, then dismiss it by selecting **OK**.

3. You will now be presented with the Customize Communication dialog box as shown in Figure 134.

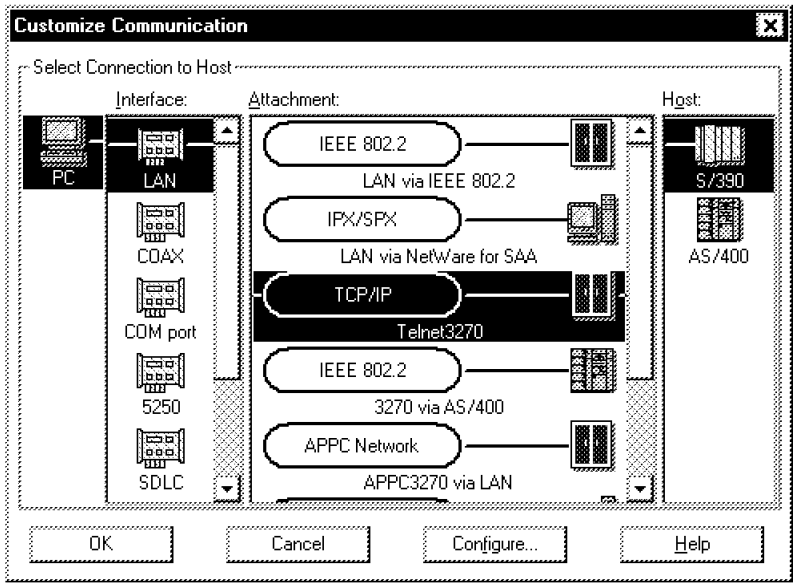


Figure 134. Customize Communication

From this dialog box you need to select the interface type, the attachment method, and the host type. In this scenario we are using a LAN adapter with TCP/IP to an S/390. Choose those options and then click **Configure**.

4. In this next dialog box you can select the screen size, code page, and if you wish to have host graphics enabled. Once you have done this select **Configure Link**.

5. In the field marked Host Name or IP Address type in the TCP/IP address of the host. You can use either the hostname or the IP address.

   In Figure 135 on page 237 we have used the fully qualified hostname. This is recommended as the host may change its IP address from time to time, or may have configured several interfaces with the same hostname and direct incoming connections to the interface with the

lightest load. The advanced section allows you to specify a TCP/IP port other than the default of 23. Do not do this unless your system administrator has advised you to do so. You can also specify an LU name if one has been assigned to you.

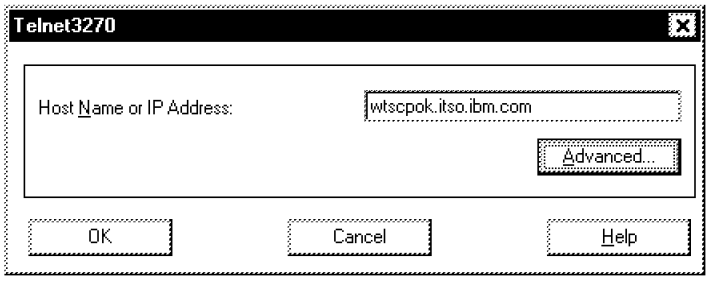


Figure 135. TN3270 Hostname or IP Address

6. Click on **OK** in the Customize Communications - 3270 Host window.
7. Click on **OK** in the Customize Communications window. Your 3270 terminal emulation session should start successfully.

6.4.2 Configuring Personal Communications Using DLUR over AnyNet

This section describes how to set up Personal Communications to connect to an MVS host over a TCP/IP network but using native SNA application protocols in contrast to using Telnet3270 data stream. We implement a simple scenario where a PC attaches directly to the host without intermediate AnyNet SNA over TCP/IP gateways.

Note: The versions of Personal Communications contained in Version 1.0 of the eNetwork Communications Suite support DLUR over AnyNet SNA over TCP/IP only on the Windows NT and Windows 3.x platforms. Support for these functions on Windows 95 is planned for future versions of Personal Communications and eNetwork Communications Suite.

For the following explanations, we assume that you are basically familiar with Personal Communications, SNA DLUR/DLUS and AnyNet SNA over TCP/IP concepts. You should already have Personal Communications installed with the 3270 Emulation and the Communications API components selected.

Note: We explain our configuration for this scenario which is an AnyNet environment. It is meant to help you understand this scenario and as a general guidance to other installations. There are many other configurations possible, and your SNA environment may be different. Please check with your system administrator about that.

For details on the installation and configuration of Personal Communications, please refer to Chapter 3, “Installation and Configuration” on page 61 or to the product documentation.

Figure 136 shows a diagram of the scenario that we are about to describe:

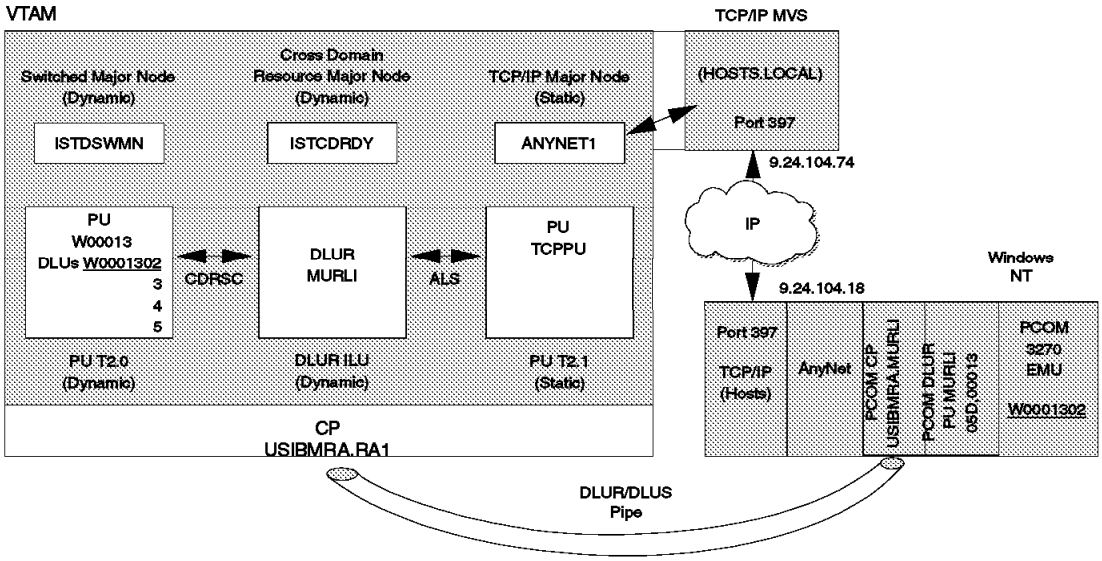


Figure 136. DLUR over AnyNet SNA over TCP/IP Scenario

Note: You can, of course, use IBM Communications Server for Windows NT or the Client Access Feature thereof, to set up your SNA connections via AnyNet and DLUR, but they are not part of the eNetwork Communications Suite.

Follow the instructions below to create a 3270 emulator definition with Personal Communications:

Note: **n** numbers indicate matching parameters and related configurations between Personal Communications and host definitions.

1. From the IBM Personal Communications folder, start the **Start or Configure Session** program.
2. Click on **OK** to start configuration. The Customize Communications window is displayed which is shown below:

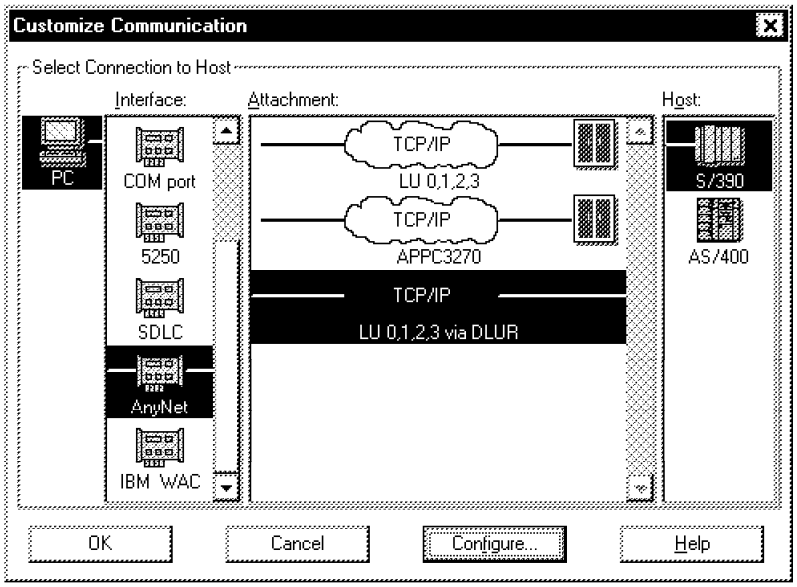


Figure 137. Customize Communication Window

3. Select **AnyNet** from the Interface list and **TCP/IP LU 0,1,2,3 via DLUR** from the Attachment list, then click on **Configure...**. Make the appropriate selections for your 3270 terminal emulation session. Our configuration is shown below:

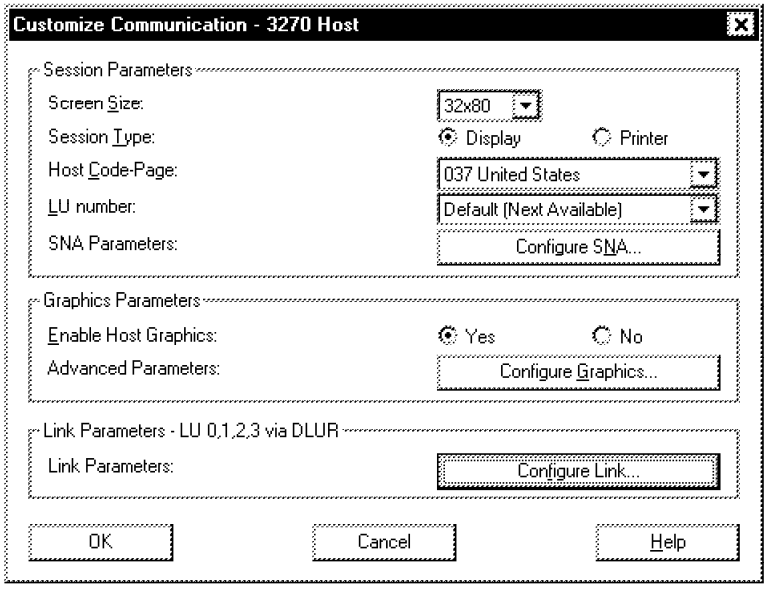


Figure 138. Customize 3270 Terminal Session

4. Click on **Configure Link...**. The Configure Local System window is displayed which is shown in Figure 139 on page 241. The active configuration file, if one exists, is shown in the SNA Node Configuration File box. Select **New** if you want to create a new configuration file, otherwise you are going to add new definitions to the existing configuration.

   Enter the configuration parameters for your workstation. Our configuration is shown in the figure below:

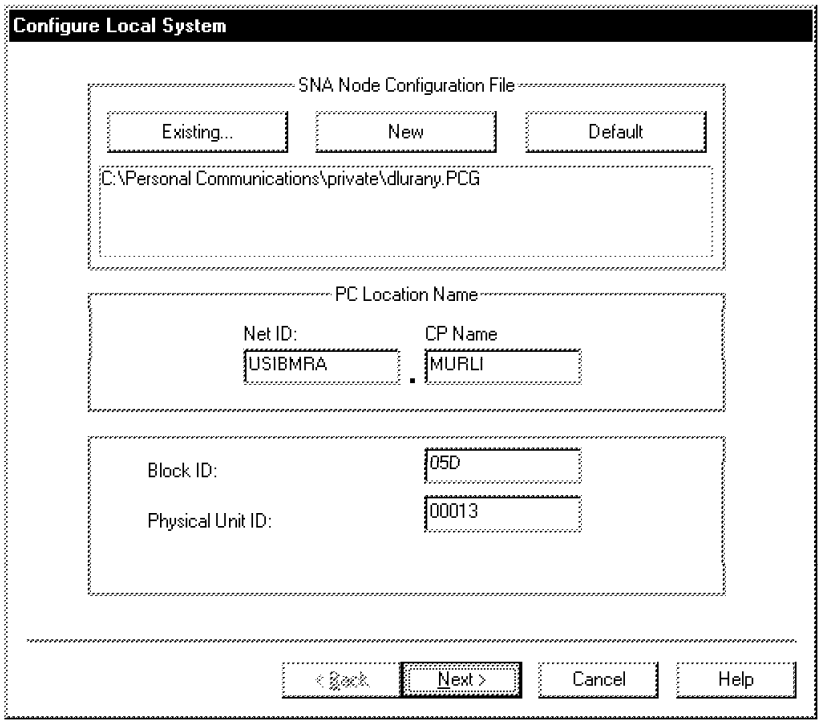


Figure 139. Configure Local System

a. The fully qualified CP name consists of a NETID portion (**1**) (matches that parameter in VTAM start options as shown in Figure 142 on page 246 and Figure 143 on page 247) and the CPNAME (**2**), which is used as the DLUR name and also as an independent LU 6.2, as shown in Figure 147 on page 252.

b. The Block ID (IDBLK) and Physical Unit ID (IDNUM) are used by VTAM to dynamically define a PU (**3**), as explained in 6.4.3.2, “Dynamic Definition of Switched PUs and Dependent LUs” on page 248 and shown in Figure 144 on page 249.

5. Click on **Next**.

6. On the Configure DLUR page, enter information about the dependent LU server and the AnyNet link. Our configuration is shown in the figure below:

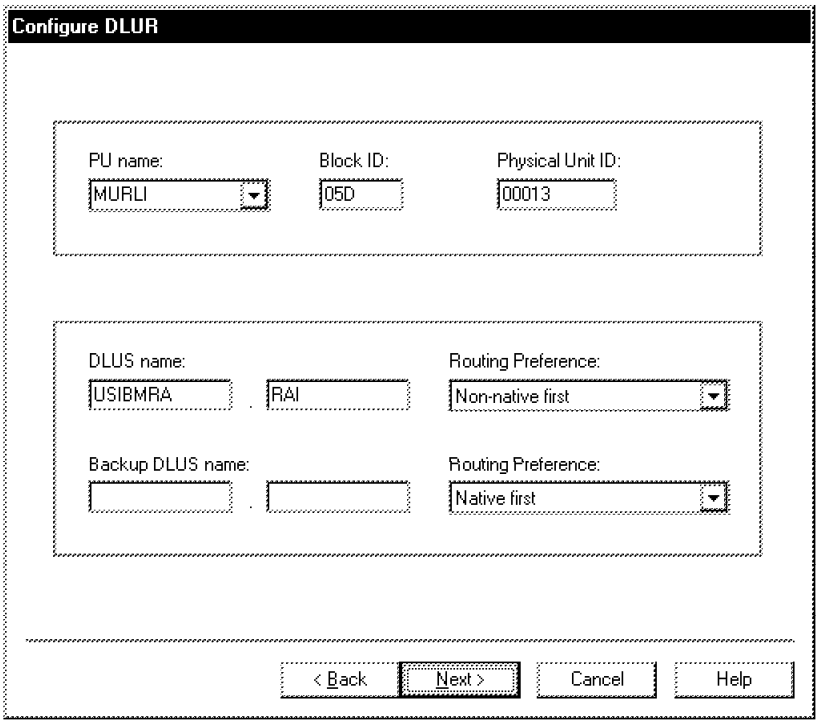


Figure 140. Configure DLUR

a. PU name has to be the same as the CP Name on the previous page and will be used as the DLUR name as shown in Figure 147 on page 252 (**8**).

b. USIBMRA matches the NETID parameter in VTAM start options, as shown in Figure 143 on page 247 (**1**).

c. RAI matches the SSCPNAME parameter in VTAM start options as shown in Figure 143 on page 247 (**4**). This is also the name of the dependent LU server (DLUS).

d. In the Routing Preference field, specify which transport Personal Communications should try first to establish the DLUR (LU 6.2) session:

   1) Native first: Try SNA transport first, than TCP/IP.
   2) Non-native first: Try TCP/IP first, than SNA.
   3) Native only: Only use SNA transport.
   4) Non-native only: Only use TCP/IP transport.

   For this scenario, use either Non-native only or Non-native first.

7. Click on **Next**.

8. On the Configure AnyNet Connection page, enter the SNA domain name suffix. We used the default, which is SNA.IBM.COM.
9. Switch to a command prompt and change to the winntsystem32driversetc directory.
10. Edit the HOSTS file to include the following line:

    ```
    <ip_address_of_mvs>     <LU_name.NETID.SNA_suffix>
    ```

    For instance:

    ```
    9.24.104.74     rai.usibmra.sna.ibm.com
    ```

11. Save the file, exit from the command session and return to Personal Communications configuration.

    Note: It is necessary to provide an IP address for every SNA LU that you want to connect to over AnyNet. As defined in the Multiprotocol Transport Network (MPTN) architecture, AnyNet will try to find an address for the transport provider (TCP/IP) that is mapped to the address of the application protocol (SNA). In our case, the SNA fully qualified CP name USIBMRA.RAI is mapped to the IP address 9.24.104.74 in the following way:

    a. Swap NetID.CPname to CPname.NetID and add a dot.
    b. Take the defined SNA suffix and append to the previous.

    The resulting string is a fully qualified TCP/IP domain name and can be resolved using either a local hosts file or a domain name server.

    See 6.4.3.6, “MVS TCP/IP Configuration for Name Resolution” on page 254 for corresponding definitions on MVS.

12. Click on **Next**, then click on **Finish**.
13. Enter a name for the configuration file in the Save As window, for instance `dlurany`, then click on **Save**.
14. Click on **OK** in the Customize Communications - 3270 Host window.
15. Click on **OK** in the Customize Communications window. Your 3270 terminal emulation session should start successfully.

6.4.2.1 Verifying the Connection

If your emulator doesn′t connect to the host, or if you are not using 3270 terminal emulation but other SNA applications that use dependent LUs, you can check the connection as follows:

1. From the IBM Personal Communications folder, open the **Administrative and PD Aids** folder, then start **SNA Node Operations**.

> **Tip**
>
> If you frequently use SNA Node Operations, create a shortcut to this program on the Desktop or in the IBM Personal Communications folder.

2. From the menu bar, select **Start Node...** and use the configuration file you have set up.
3. In the Select SNA Resources window, select **Connections** to check if your system has successfully connected to the host. If the state of $ANYNET$ does not show active, call your system administrator to verify that all of the following is true:
   - All of your configuration parameters are valid and correct.
   - The network is operational and you can ping the mainframe.
   - Your system is connected to the network and can communicate over TCP/IP.
   - VTAM and TCP/IP are up and also the network interface of TCP/IP.
   - All VTAM and TCP/IP definitions are correct and the required resources are active.
4. Select **LU 6.2 Sessions** in the Select SNA Resources window to display a list of active LU 6.2 sessions. The DLUR sessions should be listed, using the CPSVRMGR mode name, similar to the figure below:

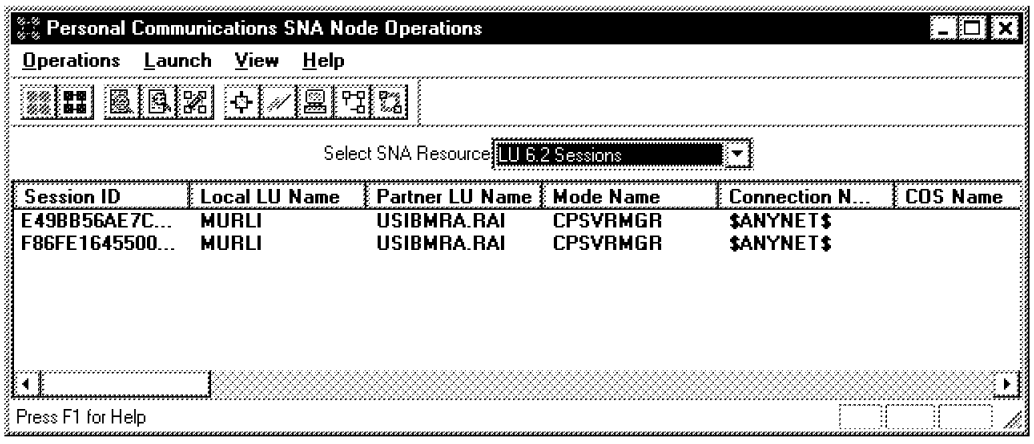


Figure 141. Active DLUR Sessions

Note: The DLUR/DLUS pipe is made up of two LU 6.2 sessions.

6.4.3 VTAM and MVS TCP/IP Definitions

In this section, we show the definitions of VTAM and TCP/IP on the mainframe as they relate to our scenario.

The following products are required on the host to facilitate a scenario like this:

1. MVS environment:
   - MVS
   - VTAM V4R2 or later
   - TCP/IP V3R1 or later
2. OS/390 environment:
   - OS/390 (includes VTAM and TCP/IP)

In our case, VTAM was set up for automatic configuration, so no static switched major node and cross domain resource definitions are required for PUs and independent LUs. Therefore, we include displays from NetView NCCF to show the active configuration parameters of the used resources.

Tip

Dynamic definitions in VTAM can help reduce the amount of static definitions dramatically, but they can be counter-productive in some environments. For a scenario like this, static definitions of switched major nodes, PUs, and DLURs would be better because of the requirement to map all LU names to TCP/IP addresses which is not a dynamic process. (See 6.4.3.6, “MVS TCP/IP Configuration for Name Resolution” on page 254 for details.)

6.4.3.1 VTAM Start Options

Figure 142 on page 246 and Figure 143 on page 247 show the start options for VTAM subarea 18.

```
IST1188I  ACF/VTAM V4R4   STARTED AT 06:36:30 ON 05/15/97
IST1349I  COMPONENT ID IS 5695-11701-401
IST1348I  VTAM STARTED AS INTERCHANGE NODE
IST1189I  ALSREQ   = NO                  APPNCOS  = NONE
IST1189I  ASIRFMSG = OLUSSCP             ASYDE    = TERM
IST1189I  AUTHLEN  = YES                 AUTORTRY = AUTOCAP
IST1189I  AUTOTI   = 0                   BN       = NO
IST1189I  BNDYN    = ***NA***            BNORD    = ***NA***
IST1189I  BSCMDRS  = (STATS,INOPS)       BSCTMOUT = 286
IST1189I  CACHETI  = 8                   CDRDYN   = YES   5
IST1189I  CDRSCTI  = 480S                CDSERVR  = NO
IST1189I  CDSREFER = 1                   CINDXSIZ = 8176
IST1189I  CMPMIPS  = 100                 CMPVTAM  = 0
IST1189I  CNMTAB   = ISTMGC00            COLD     = YES
IST1189I  CONFIG   = IO                  CONNTYPE = APPN
IST1189I  CPCDRSC  = NO                  CPCP     = YES
IST1189I  CSALIMIT = NOLIMIT             CSA24    = NOLIMIT
IST1189I  DATEFORM = MDY                 DIRSIZE  = 0
IST1189I  DIRTIME  = 691200S             DISCNTIM = (15,0)
IST1189I  DLRTCB   = 32                  DSPLYDEF = 100
IST1189I  DSPLYMAX = 65535               DSPLYWLD = FULLWILD
IST1189I  DYNADJCP = YES                 DYNASSCP = YES
IST1189I  DYNDLGMD = NONE                DYNLU    = YES   5
IST1189I  DYNMODTB = NONE                ENCRPREF = NONE
IST1189I  ENCRYPTN = NO                  ENHADDR  = NO
IST1189I  ESIRFMSG = ALLSSCP             FLDTAB   = ISTMSFLD
IST1189I  FSIRFMSG = OLUSSCP             GWSSCP   = YES
IST1189I  HNTSIZE  = 4080                HOSTPU   = ISTPUS18
IST1189I  HOSTSA   = 18    6             HOTIOTRM = 0
```

Figure 142. VTAM Options for SA18, Part 1

```
IST1189I  HPR      = (RTP,ANR)           HPRPST   = LOW          480S
IST1189I  HPRPST   = MEDIUM       240S   HPRPST   = HIGH         120S
IST1189I  HPRPST   = NETWRK        60S   HSRTSIZE = 9973
IST1189I  INITDB   = ALL                 INOPDUMP = OFF
IST1189I  IOINT    = 0                   IOMSGLIM = 2147483647
IST1189I  IOPURGE  = 300S                IRNSTRGE = 0
IST1189I  ISTCOSDF = INDLU               LIMINTCP = ***NA***
IST1189I  LIST     = IO                  MAINTLVL = *BLANKS*
IST1189I  MAXLOCAT = 5000                MAXLURU  = 6144
IST1189I  MAXSSCPS = 10                  MAXSUBA  = 15
IST1189I  MIHTMOUT = 1800                MSGLEVEL = BASE
IST1189I  MSGMOD   = NO                  MXSAWBUF = 10000
IST1189I  MXSSCPRU = 4096                MXSUBNUM = 511
IST1189I  NCPBUFSZ = 512                 NETID    = USIBMRA    1
IST1189I  NMVTLOG  = NPDA                NODELST  = *BLANKS*
IST1189I  NODETYPE = NN     6            NQNMODE  = NAME
IST1189I  NSRTSIZE = *BLANKS*            NUMTREES = 100
IST1189I  OSIEVENT = PATTERNS            OSIMGMT  = YES
IST1189I  OSITOPO  = LLINES              OSITOPO  = ILUCDRSC
IST1189I  OSRTSIZE = 43                  PDTRCBUF = 2
IST1189I  PIUMAXDS = 200                 PLUALMSG = NOSUPP
IST1189I  PPOLOG   = YES                 PSSTRACE = NORB
IST1189I  RESUSAGE = 100                 ROUTERES = 128
IST1189I  SAWMAXDS = 100                 SAWMXQPK = 0
IST1189I  SDLCMDRS = (STATS,INOPS)       SECLVLCP = ***NA***
IST1189I  SIRFMSG  = ALLSSCP             SLUALMSG = NOSUPP
IST1189I  SMEAUTH  = DISCARD             SNAPREQ  = 1000
IST1189I  SORDER   = APPN                SRCHRED  = OFF
IST1189I  SRCOUNT  = 10                  SRTIMER  = 30S
IST1189I  SSCPDYN  = YES                 SSCPID   = 18
IST1189I  SSCPNAME = RAI    4            SSCPORD  = PRIORITY
IST1189I  SSDTMOUT = 30                  SSEARCH  = YES
IST1189I  STRGR    = ***NA***            STRMNPS  = ***NA***
IST1189I  SUPP     = NOSUP               SWNORDER = CPNAME
IST1189I  TNSTAT   = CNSL,TIME=60        TRANSLAT = (0,1,2,3,4,5,6,7)
IST1189I  UPDDELAY = 60S                 USSTAB   = *BLANKS*
IST1189I  VERIFYCP = NONE                VFYRED   = YES
IST1189I  VFYREDTI = OFF                 VRTG     = YES
IST1189I  VRTGCPCP = YES                 VTAMEAS  = 32001
IST1189I  WARM     = NO                  XCFINIT  = ***NA***
IST1189I  XNETALS  = YES
IST314I  END
```

Figure 143. VTAM Options for SA18, Part 2

The following is an explanation to the points highlighted in the example above:

4 In VTAM, the SSCPNAME is also used as the APPN CP name and the name of the DLUS.

5 DYNLU=YES and CDRDYN=YES allow dynamic definition of independent LUs.

6 The combination of HOSTSA and NODETYPE=NN defines this VTAM as an interchange node, providing both subarea and APPN functions. The NODETYPE=NN parameter also enables VTAM to act as a dependent LU server (DLUS).

6.4.3.2 Dynamic Definition of Switched PUs and Dependent LUs

A device coming in to VTAM over a LAN is considered to be a switched device and must have a switched major node to define the PU and dependent LUs associated with it. VTAM provides a configuration services XID exit, ISTEXCCS, which among other things allows dynamic definition of switched devices. The sample exit shipped with VTAM will intercept the XID from an incoming switched device and based on the IDBLK and IDNUM or CPNAME generate a dynamic PU definition. The name generated in our example is done by the name generation table in the exit and bases the definition on a predefined model PU.

For example, in our scenario, the workstation uses an IDBLK of 05D. Based on definitions coded in the exit for an ′05D′ IDBLK, the exit uses a PU model called PUMOD05D, an LU model called LUMOD05D, and uses the letter ″W″ as a name prefix to build a PU definition. The model PU and LU definitions are defined in a VTAM by activating a model major node (Figure 144 on page 249 and Figure 145 on page 250). The PU name is defined using the prefix ″W″ and the IDNUM.

```
************************************************************************ 00950000
* MODEL FOR IDBLK X'05D' - PC 3270 EMULATION    3                     * 01050000
************************************************************************ 01150000
SWMODEL VBUILD TYPE=MODEL
PUMOD05D PU    ADDR=13,                                                 X
               DISCNT=NO,                                               X
               CONNTYPE=APPN,                                           X
               MAXDATA=1033,                                            X
               PUTYPE=2
*
LU6205D  LU    LOCADDR=0,DLOGMOD=DSIL6MOD
LUMOD05D LU    LOCADDR=2,                                               X
               PACING=0,                                                X
               DLOGMOD=D4C32XX3,                                        X
               MODETAB=ISTINCLM,                                        X
               USSTAB=US327X,                                           X
               VPACING=0
************************************************************************ 00950000
* MODEL FOR IDBLK X'017' - PC 3270 EMULATION                          * 01050000
************************************************************************ 01150000
PUMOD017 PU    ADDR=C1,                                                X01200000
               ANS=CONT,                                               X01250000
               PUTYPE=2                                                 01300000
LUMOD017 LU    LOCADDR=2,                                              X01350000
               MODETAB=ISTINCLM,                                       X01400000
               USSTAB=ISTINCDT,                                        X01450000
               PACING=1                                                 01500000
************************************************************************ 01550000
* MODEL FOR IDBLK X'056' - AS/400                                     * 01650000
************************************************************************ 01750000
PUMOD056 PU    ADDR=01,                                                X01800000
               ANS=CONT,                                               X01850000
               PUTYPE=2                                                 01900000
LUMOD056 LU    LOCADDR=2,                                              X01950000
               MODETAB=ISTINCLM,                                       X02000000
               USSTAB=ISTINCDT,                                        X02050000
               PACING=7                                                 02100000
LUMODP56 LU  LOCADDR=2,DLOGMOD=M2SDLCQ,MODETAB=AMODETAB
*
```

Figure 144. Models VTAMLST Entry, Part 1

```
************************************************************************ 01550000
* MODEL FOR IDBLK X'012' - DEC                                         * 01650000
************************************************************************ 01750000
PUMOD012 PU    ADDR=C1,                                                 +
               MAXDATA=521,                                             +
               MAXOUT=7,PASSLIM=7,                                      +
               PUTYPE=2
LUMODA12 LU  LOCADDR=0,DLOGMOD=SNASVCMG,MODETAB=MTAPPC
LUMODB12 LU  LOCADDR=0,DLOGMOD=SNASVCMG,MODETAB=MTAPPC
LUMODC12 LU  LOCADDR=2,DLOGMOD=M2SDLCQ,MODETAB=AMODETAB
LUMODC13 LU  LOCADDR=3,DLOGMOD=M2SDLCQ,MODETAB=AMODETAB
LUMODC14 LU  LOCADDR=4,DLOGMOD=M2SDLCQ,MODETAB=AMODETAB
************************************************************************ 00950000
*                                                                      * 01000000
* MODEL FOR IDBLK X'061' - PC 3270 EMULATION                           * 01050000
*                                                                      * 01100000
************************************************************************ 01150000
PUMOD061 PU    ADDR=C1,                                                X01200000
               ANS=CONT,                                               X01250000
               PUTYPE=2                                                 01300000
LUMOD061 LU    LOCADDR=2,                                              X01350000
               MODETAB=ISTINCLM,                                       X01400000
               USSTAB=ISTINCDT,                                        X01450000
               PACING=1                                                 01500000
```

Figure 145. Models VTAMLST Entry, Part 2

6.4.3.3 PU Configuration for the Windows NT System

In our scenario the workstation uses an IDNUM of 00013 so the PU name is W00013. This is configured on the workstation as shown in Figure 139 on page 241. The following screen shows the active SNA PU configuration for our NT system:

```
NCCF                     N E T V I E W    RAIAN MURLI    07/15/97 10:42:00 A
C RAIAN    DISPLAY NET,ID=W00013,SCOPE=ALL
  RAIAN    IST097I  DISPLAY  ACCEPTED
' RAIAN
IST075I  NAME = W00013           , TYPE = PU_T2    3
IST486I  STATUS= ACTIV---X-, DESIRED STATE= ACTIV
IST1043I  CP NAME = ***NA***, CP NETID = USIBMRA , DYNAMIC LU = YES
IST1589I  XNETALS = YES
IST1354I  DLUR NAME = MURLI    8         MAJNODE = ISTDSWMN
IST136I  SWITCHED SNA MAJOR NODE = ISTDSWMN
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I  STATE TRACE = OFF
IST355I  LOGICAL UNITS:
IST080I  W0001302 ACT/S---X- W0001303 ACTIV---X- W0001304 ACTIV---X-
IST080I  W0001305 ACTIV---X-
IST314I  END
```

Figure 146. Display of PU W00013 from VTAM

More information on the VTAM configuration services XID exit can be found in *VTAM V4R4 Customization*, LY43-0075.

6.4.3.4 Dependent LU Server (DLUS) Requester (DLUR) Configuration

Dependent LU server and requester (DLUS/DLUR) allow you to establish a special LU 6.2 session (pipe) between a control point and VTAM over which dependent LU traffic will flow. This mechanism was originally designed to route dependent LU traffic over APPN networks, but it is equally suitable for AnyNet SNA over TCP/IP.

The DLUS is VTAM itself, and the DLUR is an independent LU that represents the CP name of our Personal Communications workstation, MURLI. Independent LUs (ILUs) attaching to VTAM through a type 2.1 PU can be dynamically defined as cross-domain resources (CDRSCs). The PU becomes the adjacent link station (ALS) for the ILU. Dynamic CDRSCs are put in the VTAM major node ISTCDRDY (**7**).

In the VTAM start options we have coded DYNLU=YES and CDRDYN=YES to allow dynamic CDRSC definitions to be created for independent LUs. Adjacent CPs are independent LUs and are defined in the same way. See Figure 142 on page 246 and Figure 143 on page 247 for a complete listing of the VTAM options for this scenario.

Normally, our workstation PU, W00013, would be the adjacent link station for our independent LU, MURLI (**8**). But because we are using AnyNet to attach to the host, and because we are also using DLUR, things are getting a little bit more complicated:

1. As indicated by the DLUR NAME=MURLI parameter, the dynamically created PU W00013 belongs to that dependent LU requester. That also explains why W00013 is only a PU type 2.0 since DLUR only supports that type.

   On the workstation, this is configured as shown in Figure 140 on page 242.

   The following screen shows the active DLUR configuration for our Personal Communications on NT:

```
NCCF                     N E T V I E W    RAIAN MURLI    07/15/97 15:36:21 A
C RAIAN    DISPLAY NET,ID=MURLI,SCOPE=ALL
  RAIAN    IST097I  DISPLAY  ACCEPTED
' RAIAN
IST075I  NAME = USIBMRA.MURLI    , TYPE = CDRSC    8
IST486I  STATUS= ACT/S----Y, DESIRED STATE= ACTIV
IST1447I  REGISTRATION TYPE = NO
IST977I  MDLTAB=***NA*** ASLTAB=***NA***
IST1333I  ADJLIST = ***NA***
IST861I  MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I  DLOGMOD=CPSVRMGR USS LANGTAB=***NA***
IST597I  CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I  CDRSC    MAJOR NODE = ISTCDRDY           7
IST1044I  ALSLIST = TCPPU
IST082I  DEVTYPE = INDEPENDENT LU / CDRSC         2
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I  STATE TRACE = OFF
IST171I  ACTIVE SESSIONS = 0000000002, SESSION REQUESTS = 0000000000
IST206I  SESSIONS:
IST1081I  ADJACENT LINK STATION = TCPPU           9
IST634I  NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I  RAI      ACTIV/DL-S E49BB56AE7EC9CE2 000E 0000       USIBMRA
IST635I  RAI      ACTIV/DL-P F86FE1645500B001 0000 000C       USIBMRA
IST1355I  PHYSICAL UNITS SUPPORTED BY DLUR USIBMRA.MURLI
IST089I  W00013   TYPE = PU_T2            , ACTIV---X-    3
IST314I  END
```

Figure 147. Display of MURLI from VTAM

The following screen shows the active CDRSC major node for dynamically defined CDRSCs. Our Personal Communications on NT is represented by the MURLI entry:

```
NCCF                     N E T V I E W    RAIAN MURLI    07/15/97 15:40:44 A
* RAIAN    DISPLAY NET,ID=ISTCDRDY,SCOPE=ALL
  RAIAN    IST097I  DISPLAY  ACCEPTED
' RAIAN
IST075I  NAME = ISTCDRDY         , TYPE = CDRSC SEGMENT    7
IST486I  STATUS= ACTIV     , DESIRED STATE= ACTIV
IST478I  CDRSCS:
IST483I  RAKAA    ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAKTX016 ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  MURLI    ACT/S----Y, CDRM = ***NA***, NETID = USIBMRA    8
IST483I  RAKTX047 ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  A2217    ACT/S----Y, CDRM = ***NA***, NETID = USIBMRA
IST483I  RAKAP    ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  RAKTX060 ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  RAKTX059 ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  RAPANLUC ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAKANLUC ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAPANJE  ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RALVSMV6 ACT/S----Y, CDRM = RAK     , NETID = USIBMRA
IST483I  RA39     ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAP      ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAK      ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST483I  RAB      ACT/S----Y, CDRM = RAI     , NETID = USIBMRA
IST1500I  STATE TRACE = OFF
IST314I  END
```

Figure 148. ISTCDRDY Display

2. Since we are connecting to VTAM via AnyNet SNA over TCP/IP, this is where the dynamic ends. We need to define a PU that acts as an adjacent link station (ALS) to the independent LU of the DLUR as mentioned earlier. This PU is shown as TCPPU. It is listed below:

```
NCCF                     N E T V I E W    RAIAN MURLI    07/15/97 15:58:53 A
C RAIAN    DISPLAY NET,ID=TCPPU,SCOPE=ALL
  RAIAN    IST097I  DISPLAY  ACCEPTED
' RAIAN
IST075I  NAME = TCPPU            , TYPE = PU_T2.1    9
IST486I  STATUS= ACTIV--L--, DESIRED STATE= ACTIV
IST1043I  CP NAME = ***NA***, CP NETID = USIBMRA , DYNAMIC LU = YES
IST1589I  XNETALS = YES
IST081I  LINE NAME = TCPLN    , LINE GROUP = TCPGR   , MAJNOD = ANYNET1    10
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST1500I  STATE TRACE = OFF
IST355I  LOGICAL UNITS:
IST080I  MURLI    ACT/S----Y W0001302 ACT/S---X-     8
IST314I  END
```

Figure 149. TCPPU Display

6.4.3.5 TCP/IP Major Node

The PU TCPPU belongs to the ANYNET1 major node which is a TCP/IP major node, indicating to VTAM that AnyNet is being used to find a transport

provider for connections to this PU. The following screen shows the TCP/IP major node for AnyNet/MVS on subarea 18:

```
NCCF                      N E T V I E W    RAIAN MURLI    07/15/97 16:00:25 A
C RAIAN    DISPLAY NET,ID=ANYNET1,SCOPE=ALL
  RAIAN    IST097I  DISPLAY  ACCEPTED
' RAIAN
IST075I  NAME = ANYNET1          , TYPE = TCP/IP MAJOR NODE    10
IST486I  STATUS= ACTIV     , DESIRED STATE= ACTIV
IST1342I  DNSUFX = SNA.IBM.COM
IST1344I  TCPIPJOB = T18NTCP   TCB = 10  TCP PORT =   397
IST1400I  DGTIMER  =    30  EXTIMER =     3
IST1406I  CONTIMER =    30  IATIMER =   120
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST170I  LINES:
IST232I  TCPLN    ACTIV
IST314I  END
```

Figure 150. ANYNET1 Major Node Display

The following screen shows the configuration parameters for the ANYNET1 major node:

```
ANYNET1  VBUILD TYPE=TCP,DNSUFX=(SNA.IBM.COM),TCPIPJOB=T18NTCP
TCPGR    GROUP
TCPLN    LINE
TCPPU    PU
```

Figure 151. ANYNET1 Major Node Configuration

In order to make VTAM use AnyNet SNA over TCP/IP, a DD statement similar to the one shown in the example below has to be added to the PROCLIB that defines VTAM to the MVS operating system, in our case ITSC.PROCLIB(NET18):

```
//SYSTCPD  DD DSN=TCPIP.T18N.TCPPARMS(TCPDATA),DISP=SHR
```

6.4.3.6 MVS TCP/IP Configuration for Name Resolution

As mentioned earlier regarding the mapping from fully qualified SNA CP and LU names to fully qualified TCP/IP domain names on the NT system, the same is required on the MVS system to find the way back to Personal Communications over TCP/IP.

Notes:

1. On the Personal Communications side, you only need one mapping, between the CP name of your NT system and the IP address of the mainframe, because all dependent LUs will communicate over the DLUR/DLUS pipe.

   On the MVS side, however, you need to map the CP name as well as all dependent LUs associated with a particular DLUR to the IP address of the NT system.

   Shown below is an example of a HOSTS.LOCAL file that was used in our scenario:

   ```
   HOST : 9.24.104.18: MURLI.USIBMRA.SNA.IBM.COM ::::
   HOST : 9.24.104.18: WO001302.USIBMRA.SNA.IBM.COM ::::
   ```

   Don't forget to run the makesite utility on MVS to produce the HOSTS.SITEINFO and HOSTS.ADDRINFO files from the changed HOSTS.LOCAL file.

2. Dynamic switched major node definitions in VTAM make it hard to follow suite with the corresponding address mappings in either a HOSTS.LOCAL file or a domain name server (DNS) database, so static VTAM definitions would be better for a scenario like this.

3. Session establishment from MVS to Personal Communications using AnyNet SNA over TCP/IP and a HOSTS.LOCAL file on MVS can take a while because TCP/IP for MVS will always look up a DNS before using the HOSTS.LOCAL file for address mappings. This usually implies a 60 second timeout.

6.5 Using IBM Host On-Demand

IBM Host On-Demand is not included as part of the eNetwork Communications Suite, however it is part of the IBM eNetwork Family, as an added function to the current versions of IBM Communications Server. Host On-Demand is a Java-based application that allows any Java-enabled platform to connect to an S/390 SNA host over the corporate Intranet or over the Internet. The Host On-Demand emulator is not as full featured as the Personal Communications platform and is suitable for clients who only need occasional access to host systems and only have TCP/IP.

One example of a Java-enabled platform is the Netscape Navigator included in the IBM eNetwork Communications Suite. The Host On-Demand application requires an HTTP server capable of serving Java applets. In this scenario we have used the IBM Internet Connection Secure Server for Windows NT. This server is configured to provide the connection to an IBM

Communications Server for Windows NT installation that is acting as a gateway to the S/390 in our scenario.

To connect to Host On-Demand, you simply specify the address of the TCP/IP host which is serving the Host On-Demand application in your Netscape Navigator's URL locator. In this scenario, the address is:

```
http://9.12.14.10/hod/he3270en.htm
```

Load this HTML document to start the Java applet on your client. Within the Netscape client window will appear the Host On-Demand banner and the connection settings as shown in Figure 152.

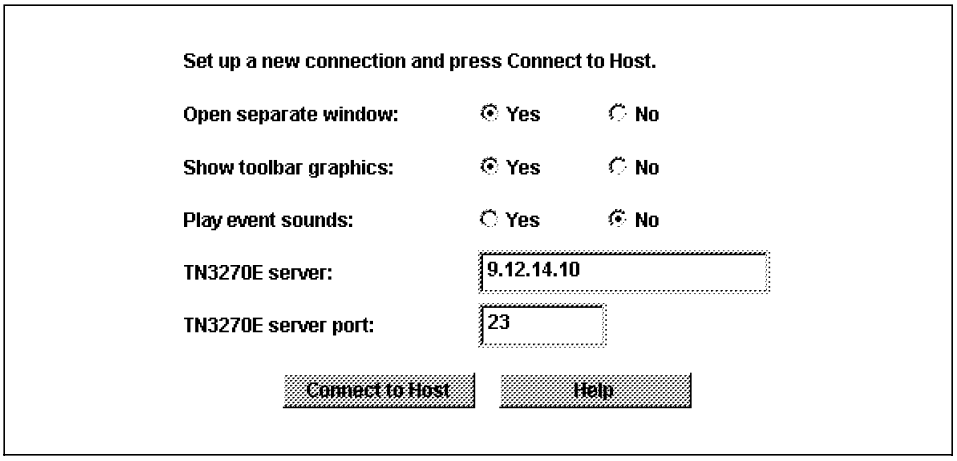


Figure 152. Host On-Demand Connection Settings

Within this page you can specify if the session should start in a separate window, if the graphical tool bar should be displayed, and if the session sounds should be enabled. You can also change the default connection port from 23. The address of the server cannot be changed as it points to the address of the machine you have loaded the Java applet from. Once those settings have been configured, you can select **Connect to Host**. The Host On-Demand application will establish the connection and display the output in the Netscape client frame. In this way you can interact with your host to run applications, or access information it contains. An example screen shot from our scenario is Figure 153 on page 257.

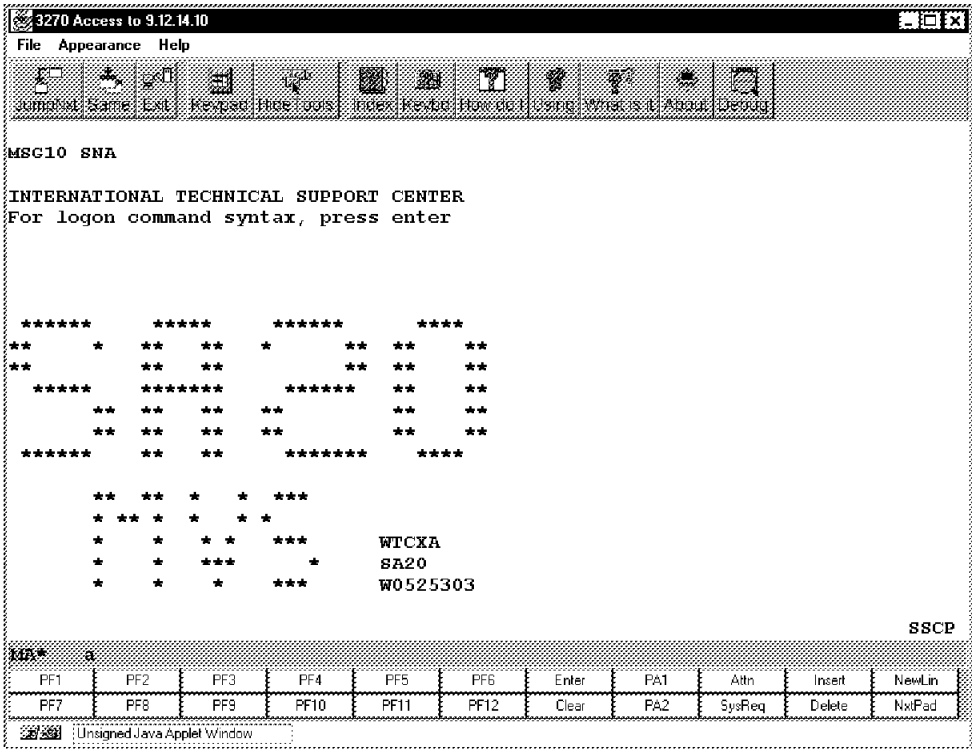


Figure 153. Host On-Demand Session

6.6 NetBIOS Support

In local area networks (LANs), NetBIOS is still a popular protocol and many organizations are still utilizing it in their networks topology. In this scenario we are using NetBIOS over TCP/IP. In this way the network uses only one protocol. It is possible to install NetBIOS to work alongside TCP/IP on the same LAN. While taking advantage of the features offered by the IBM eNetwork Communications Suite you can still use the file and printer sharing capabilities of NetBIOS. All the usual methods of accessing your NetBIOS resources are still available. A full discussion of the installation and setup of NetBIOS support on any Windows platform is beyond the scope of this document. It is described briefly to show that it does work with the eNetwork Communications Suite.

To set up NetBIOS over TCP/IP in a Windows NT or Windows 95 environment you will need to enable WINS resolution. To do this in Windows NT:

1. Select the **Start** button, then click on **Control Panel**.
2. Double-click on the **Network** applet to start the network configuration application.
3. Select **Protocols** from the available tabs.
4. Click on **TCP/IP Protocol** then **Properties**.
5. Select **WINS Address** from the tabs.
6. In the field marked Primary WINS Server, type in the IP address of the WINS server on your network.
7. Click on **OK** then reboot the machine as suggested by Windows NT.

If you are using Windows 95, then you will need to configure the FTP Software TCP/IP protocol stack To do this:

1. Click on the **Start** button, then select **Control Panel** and then double-click on the network applet to start the configuration.
2. Select **TCP/IP Stack. FTP Software, Inc. (FTPTCP96)** from the list of installed components and then select **Properties**.
3. Select the tab called **WINS Configuration**, check the radio button marked **Enable WINS Resolution** and then type in the IP address of your network WINS server in the field marked WINS Server then click on **Add**. Your configuration should look like Figure 154 on page 259.

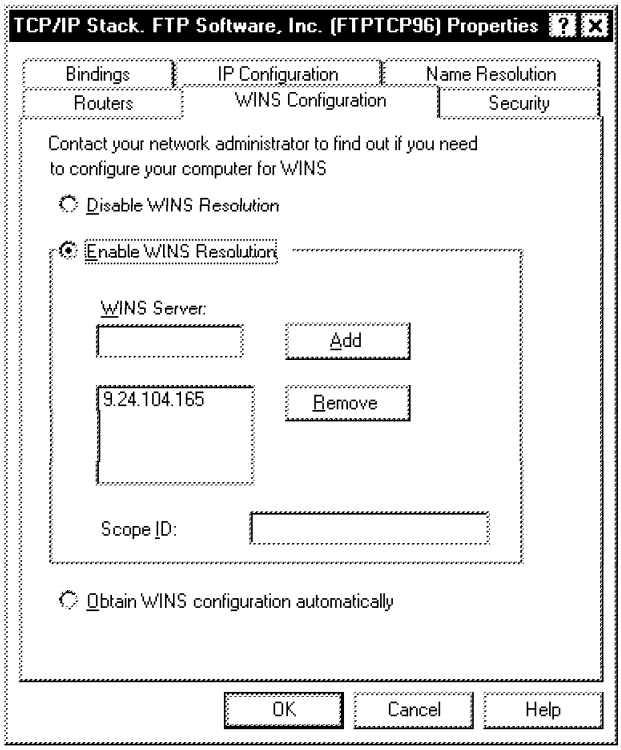


Figure 154. WINS Configuration

4. Click on **OK** and then reboot the machine when prompted.

In this scenario, there is a shared directory on the WARPSRV machine in the OS2LAN domain. This shared resource is called GRAPHICS. It could be accessed from the command line as in Figure 155 on page 260.

```
C:>net view WARPSRV
Shared resources at \\WARPSRV

Share name   Type         Used as  Comment
-------------------------------------------------------
GRAPHICS     Disk                  Shared Graphic Images

The command completed successfully.

C:\>net use T: \\WARPSRV\GRAPHICS
The command completed successfully.

C:\>net view \\WARPSRV
Shared resources at \\WARPSRV

Share name   Type         Used as  Comment
-------------------------------------------------------
GRAPHICS     Disk         T:       Shared Graphic Images
The command completed successfully.
```

Figure 155. Example NetBIOS Command Line Usage

Windows 95 and Windows NT users can also use the network neighborhood method to connect to NetBIOS resources. Open the network neighborhood from your desktop, then select the name of server the resource is located on. In this scenario it is WARPSRV. Click on the resource you wish to map to a local drive letter with the right mouse button. In this scenario the resource is called GRAPHICS and your screen should look similar to Figure 156.

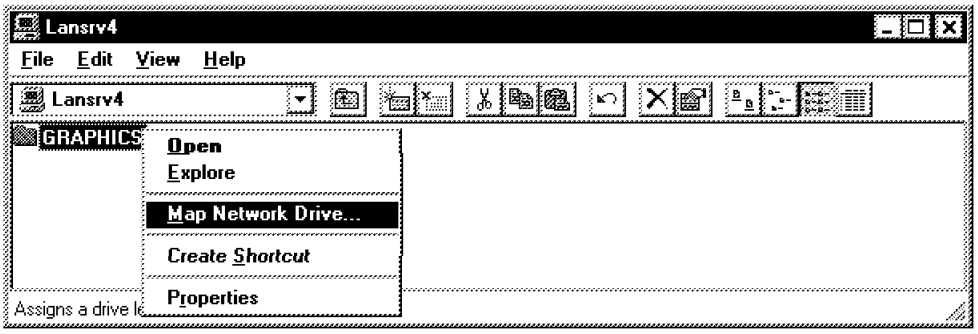


Figure 156. Network Neighborhood

Click on **Map Network Drive** and you will see a dialog box similar to Figure 157 on page 261. From this dialog box select the drive letter you wish to map the network drive to locally. Once completed select **OK**.

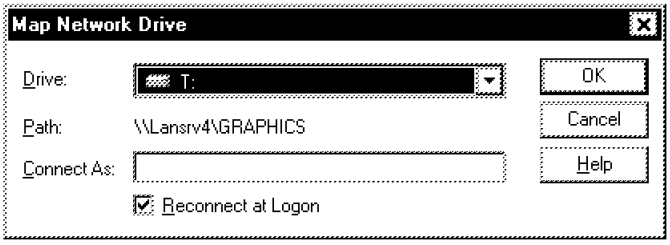


Figure 157. Map Network Drive

Tip

To connect to an OS/2 Warp Server from Windows NT or Windows 95, use the Warp Server clients for those platforms. The Windows 95 requester is shipped with Warp Server; the Windows NT requester is available from the following URL:

`http://www.software.ibm.com/os/warp-server`

Windows 3.x users should note that every protocol they load will reduce the amount of conventional memory available to applications. For more information on the installation of multiple protocols on a Windows 3.x platform, refer to 3.3.6, “Multiple Protocol Support” on page 128.

Chapter 7. Scenario C - Remote Access Environment

In this chapter, we develop a corporate scenario based on a central office with multiple dial-in connections, and describe how to implement and use the eNetwork Communications Suite in that environment. This scenario assumes the following:

- Central LAN with remote access server
- AS/400 host with SNA and TCP/IP attachment
- Windows NT servers
- Lotus Notes server
- Internet access
- The following eNetwork Communications Suite components will be used:
  - FTP Software TCP/IP protocol stack and FTP Software TCP/IP applications
  - Personal Communications over SNA and dial-in
  - Netscape Navigator
  - Lotus Notes Mail Client
- The following other eNetwork products will be used:
  - Communications Server

7.1 Environment Overview

In today's fast evolving business environment there is a big demand for information availability and processing capability from anywhere at anytime. Mobile computing addresses this demand. In this scenario we show how the eNetwork Communications Suite, together with other eNetwork products, supports mobile users.

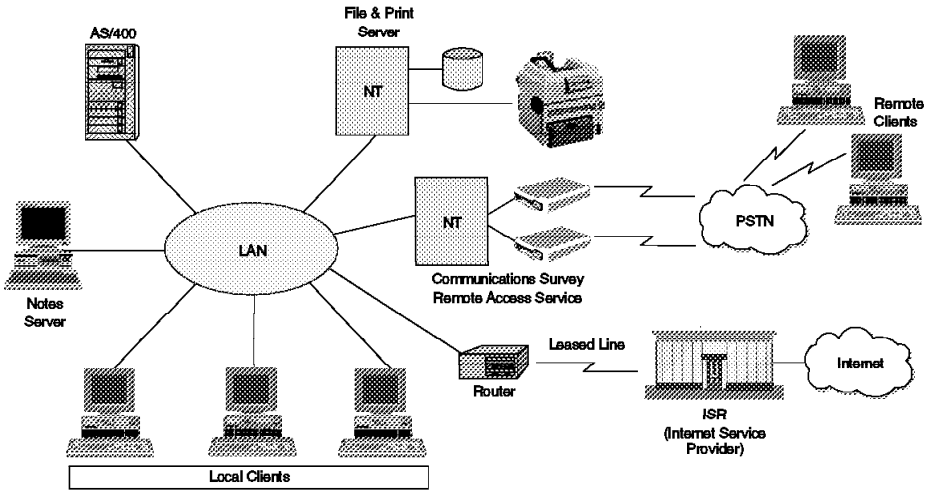


Figure 158. The Environment - Scenario C

The scenario in Figure 158, shows a plausible IT infrastructure of a small to medium sized company. This company relies on an AS/400 midsize business computer for running its mission-critical applications. This choice is based on the wide application portfolio, the small administration overhead, the cost effectiveness and the very robust security features of this platform.

The resource sharing is done by a Windows NT server. It provides shared files and a workgroup printer, accessible over NetBIOS.

The local users connect to the AS/400 over the IEEE 802.2 protocol. This type of connection allows them to fully exploit the SNA networking features of the AS/400. Printer sessions can be defined to have the AS/400 application output printed to their local printer. Also, the APPC and CPI-C programming interfaces are available.

From the mobile computing point of view, the key component of this environment is the dial-in gateway, which is implemented using the Windows NT Remote Access Service (RAS). The system running NT Server is an IBM PS/2 Model 95. There are IBM 7855 modems attached to the serial ports of the server. The modems connect to the public switched telephone network. In its initial configuration, this system allows for two concurrent dial-in sessions. As the demand for remote access grows, you can meet it in several ways:

- Add more serial ports to your RAS systems, for example using an ARTIC Multiport adapter.
- Increase the number of RAS systems.

- Use a dedicated remote access hardware server, for example the IBM 8235.

For more than three or four concurrent users, in an organization where reliable remote access is a must, the most comprehensive solution is a dedicated hardware server, for these reasons:

- Optimized for remote access
- Easy to use
- Highly scalable and manageable

The remote users dial in to the network using any kind of asynchronous modem that is compatible with the local Public Switched Telephone Network (PSTN). Once connected, they access the resources of the LAN over the TCP/IP and NetBIOS over TCP/IP protocols.

Note: At present the FTP Software Dialer does not support NetBEUI. This does not limit your capability to access shared resources either on Microsoft networks or on OS/2 Warp Server networks. However, you cannot browse the Network Neighborhood unless you use WINS. Instead, specify the fully qualified name of the resource you want to access using the UNC method.

The connection to the Remote Access Server (RAS) is made over Point-to-Point Protocol (PPP). RAS is configured to allow access to the entire network. Optionally, access can be restricted to the system running RAS. For example, if the remote users are not supposed to use the shared resources other than those on the RAS system itself, it makes sense to disable the access to the entire LAN.

7.2 Setting Up the Environment

At the RAS system, the administrator must configure and start this service. The modems must be installed and configured and the users have to be granted remote access rights. For a detailed description of these tasks, refer to your NT Server documentation.

7.2.1 Information Needed

In order to dial in to the network, you have to know the following:

- The phone number to be used to dial the RAS machine.
- The serial protocol. RAS uses PPP.
- Whether your IP address is permanently assigned or it will be obtained from the RAS.
- Name server configuration. Will this be obtained automatically or do you have to specify it? In the latter case, make sure you know the following:

- Your machine's hostname (optional)
- The TCP/IP domain name (required)
- The type of name server: DNS or NIS
- The DNS name server address(es)

• Authentication method: login or PPP authentication. RAS uses the latter. You will have to use your user ID and password that you would normally use to log on to the NT server.

7.2.2 Setting up the Remote Clients

The component that manages the dial-in connections at the clients depends on the Windows platform in use:

• Under Windows NT it is the Microsoft dialer, which comes with the operating system.
• Under Windows 95 and Windows 3.x it is the FTP Software Dialer, part of the FTP Software TCP/IP protocol stack.

Note: Make sure that the FTP Software Dialer is installed on the dial-in clients.

7.2.2.1 Using the Microsoft Dialer with Windows NT

Make sure that the following prerequisites are met when trying to dial in to the network:

1. A modem or another RAS capable device is installed (for example ISDN card).
2. The Remote Access Service is installed.

If not already installed, follow the standard Windows NT installation procedures to install the above components.

To be able to use the dialer you first have to create a phonebook entry for the remote server. The New Phonebook Entry Wizard will show up when you start the dialer for the first time and will guide you through the steps of creating that entry. Start the dialer by double-clicking the **Dial-up Networking** object found in the My Computer folder.

1. At the dialog shown in Figure 159 on page 267, enter a name for the connection. Then click on **Next** to continue.

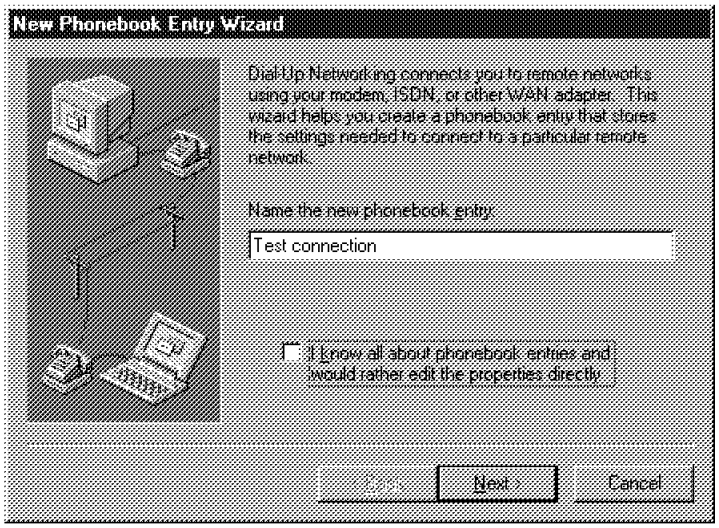


Figure 159. New Phonebook Entry Wizard

2. At the Server dialog check the **I am calling the Internet** check box. This will enable the TCP/IP protocol for this connection. Click on **Next** to continue.
3. At the Phone Number dialog enter the phone number to be called. Optionally you can specify alternate phone numbers by clicking **Alternates...**. Click on **Next** to continue.
4. At the Serial Line Protocol dialog select **PPP**. Click on **Next** to continue.

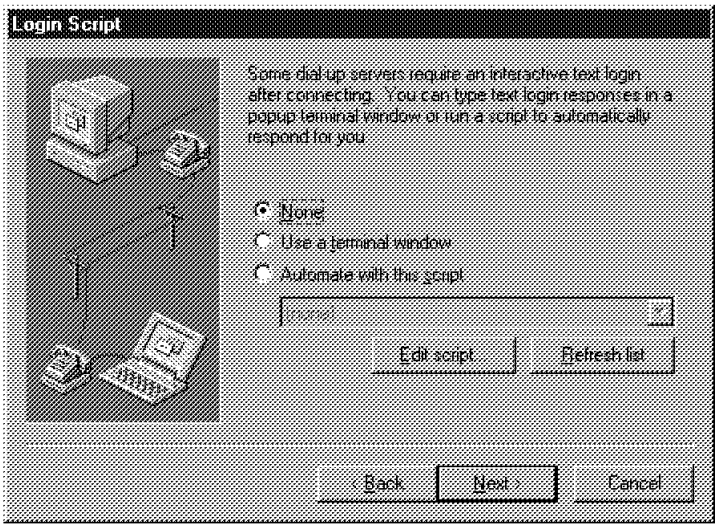


Figure 160. New Phonebook Entry - Login Script

5. At the Login Script dialog shown in Figure 160 select **None** and click on **Next** to continue.
6. At the IP Address dialog, enter the IP address if there is one permanently assigned to your computer. If there is not, leave the input field at its default 0.0.0.0 value. Click on **Next** to continue.
7. At the Name Server Addresses dialog, enter the IP address of a DNS and/or WINS server. If these addresses will be obtained automatically, leave the input fields at their default values. Click on **Next** to continue.
8. Click on **Finish** to save the connection.

The new connection definition is complete. The Dial-Up Networking dialog will be shown, similar to Figure 161 on page 269, with the entries completed with data from the newly defined connection.

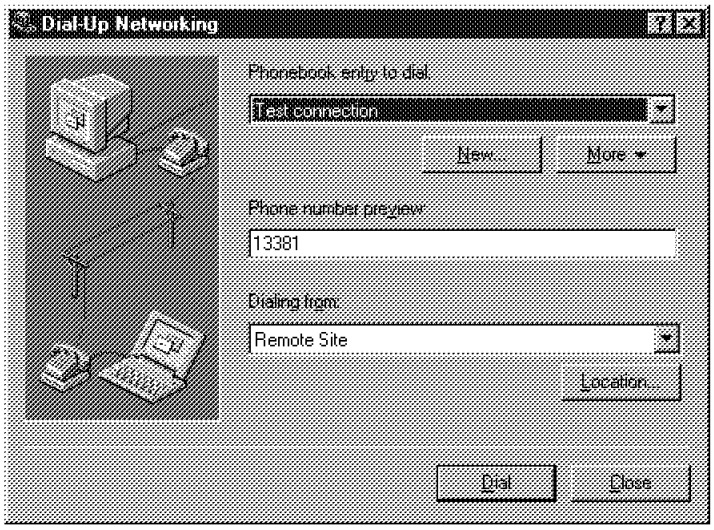


Figure 161. Dial-Up Networking Start Window

Click on **Dial** to initiate the connection. Specify your user ID and password, the NT domain you want to log on at the dialog box that pops up. You can also save your password. Be aware of the security exposure when saving passwords. Click on **OK** to continue. Monitor the progress of the connection at the dialer′s information box.

If the connection has succeeded, you become part of the remote LAN. You may use the resources on the LAN as if you were directly attached to that LAN.

You can also dial in to the network when you log on to Windows NT. At the Logon Information dialog box, fill in your user ID and password. Check the **Logon using Dial-up Networking** check box. Click on **OK**. The dialer window pops up as shown in Figure 161. Select your connection and dial it. You will be connected to the remote LAN.

7.2.2.2 Using the FTP Software Dialer with Windows 95

Start the dialer by selecting **Secure Client/Dialer**. If you have not added an adapter for the dialer yet, for example, at the product installation, you will be asked whether you want to proceed with the adapter installation. Select **Yes** and follow the wizard′s instructions to install the correct adapter. You will have to restart your computer for the changes to take effect. See 3.2, “Installing on Windows 95” on page 78 for details on installation.

The adapter you have installed for the dialer is listed at the Configuration page of the Network object found in the Control Panel. Besides the LAN

adapter the FTP Software TCP/IP protocol stack also binds to the dial-in adapter. Therefore it will be listed twice in the network components list box, as shown in Figure 162 on page 270.

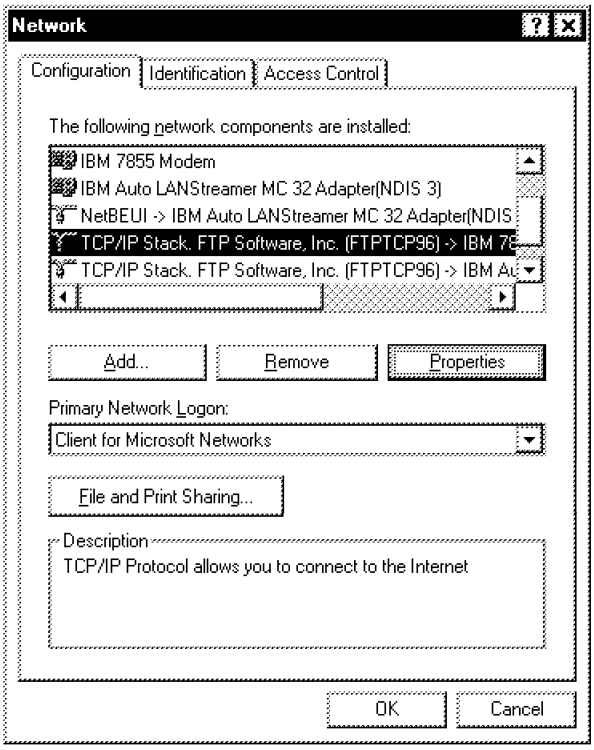


Figure 162. Network Configuration

If you take a look at the Bindings page of the Properties panel of the FTP Software TCP/IP protocol stack instance bound to the dial-in adapter (in our case an IBM 7855 modem), you will see that it has the following bindings:

- Client for Microsoft Networks

  This binding represents the NetBIOS over TCP/IP capability of the protocol stack. If you want to access resources shared by Windows or OS/2 systems, this binding must be selected.

- File and printer sharing for Microsoft Networks

  The binding to this service also represents the NetBIOS over TCP/IP capability. Select this binding if you want to share the resources of your computer.

- InterDrive Client

This binding makes possible the access to NFS drives and LPD or NFS printers.

Creating Connections: After the reboot, start the dialer again. The Dialer Connection Wizard will appear and will guide you through the steps of creating a connection:

1. The first step is to name the connection and associate an adapter with it, as shown in Figure 163.

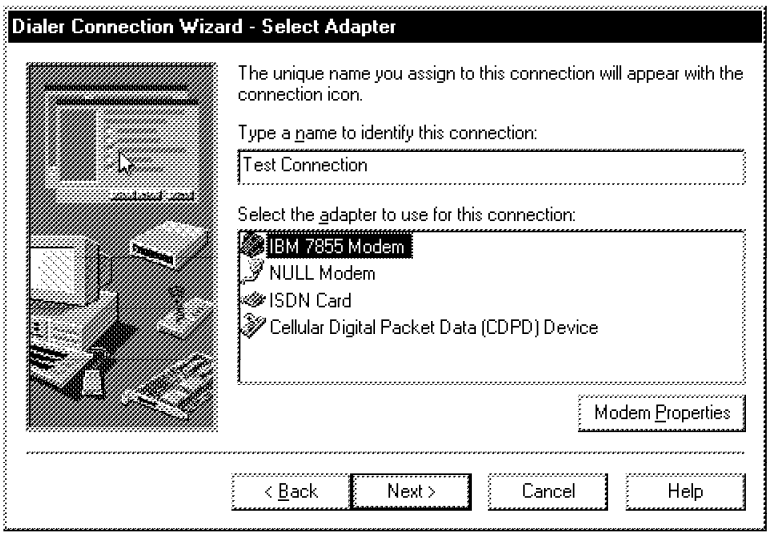


Figure 163. Adapter Selection

   If you want to customize the modem, for example COM port setting, maximum speed, serial connection parameters or call preferences, you can do so by clicking on **Modem Properties**.

   After you have finished with the modem setup, click on **Next** to continue.

2. At the Select Server Type dialog, choose the protocol and the authentication method to be used with this connection. To connect to the RAS system, select **PPP** for the protocol and **PPP authentication** for the authentication method. Click on **Next** to continue.
3. At the Configure PPP Authentication dialog provide the authentication information needed:
   - Identity or user ID
   - Secret or password

You can opt to have your user ID and/or password permanently stored. Although this feature is very convenient, for security reasons we suggest not selecting this option for the password.

Click on **Next** to continue.

4. At the dialog shown in Figure 164 specify the phone number to dial. You can select to use the Dialing Properties, that is, select from a list the country you are dialing from and specify the area code and phone number separately. The second option lets you specify the whole number directly. The third option will let you specify the number later at connection establishment time.

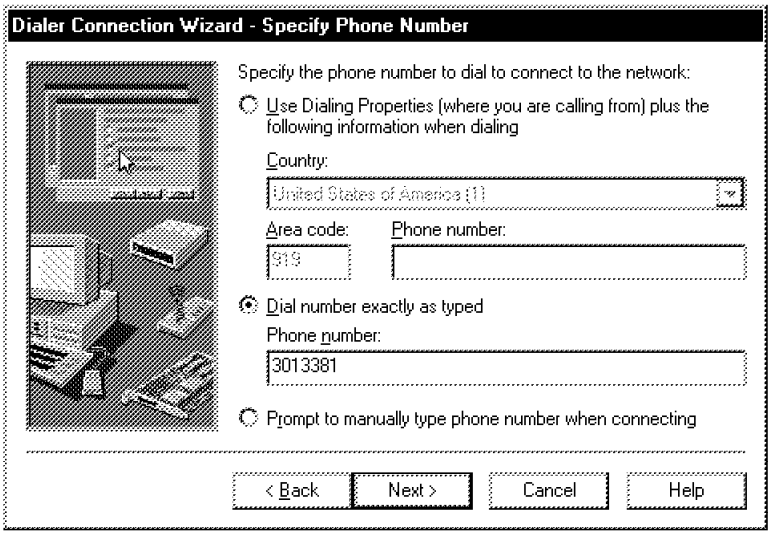


Figure 164. Specify Phone Number

Click on **Next** to continue.

5. Select whether you want to be connected automatically when network access is required (Dial-on-Demand feature) or you want to establish the connection manually. Click on **Next** to continue.

6. Select the inactivity timeout options: the inactivity timer settings and the automatic disconnect warning. Click on **Next** to continue.

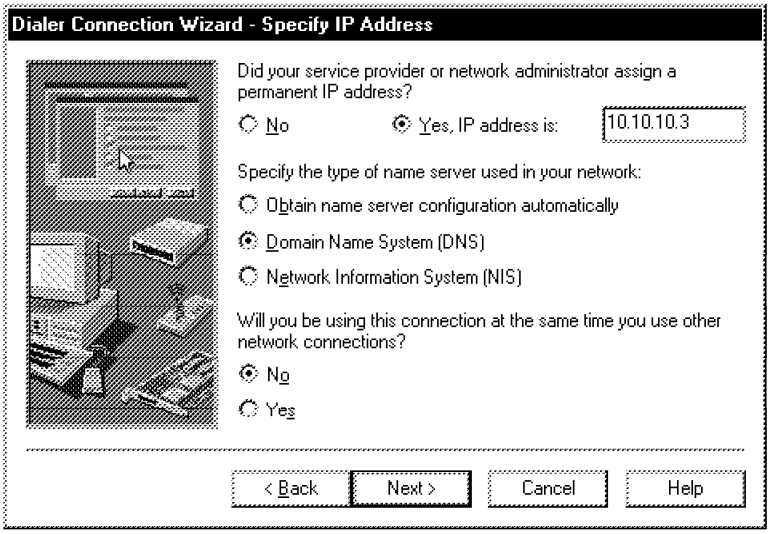


Figure 165. Specify IP Address

7. At the Specify IP Address dialog shown in Figure 165, specify the following:

   - Whether your IP address is assigned permanently (then type it in) or not. In the latter case the address will be obtained from the RAS system.
   - The name server type used. If it is DNS or NIS, you will have to specify additional parameters at the next step.
   - Whether you will be using this connection at the same time as other network connections (for example, a Telnet connection over a LAN).

   Click on **Next** to continue.

8. If you specified in the previous step that you will obtain the name server configuration automatically, go to step 9 on page 274. Otherwise configure the DNS or NIS service, depending on your selection in the previous. step. In our scenario DNS is used. The configuration is shown in Figure 166 on page 274.

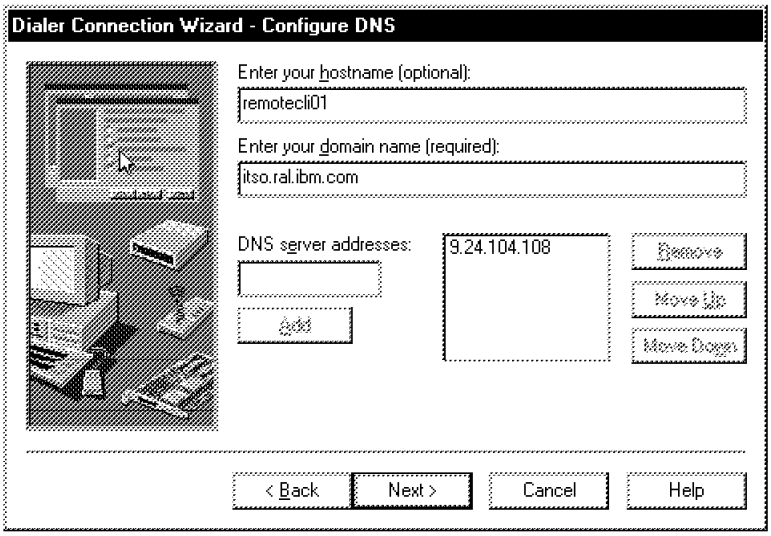


Figure 166. DNS Configuration

9. If you specified in step 7 on page 273 that you will use this connection at the same time as other network connections, you have to configure the routes at this step. Specify if you want to use this connection as the default router and also specify, if any, a list of hosts or networks that you explicitly want to access through this connection. This option is useful when you have multiple connections to the same host or network and you want to force the system to use this connection rather than another. For example, if you have a LAN connection in addition to the dial-up one, and your LAN provides a specific route to a network that is also accessible via the dial-up connection, that network will be accessed via the LAN unless you list it at this dialog.
10. The connection definition is complete by now. Select whether you want a shortcut for this connection on your desktop and whether you want to connect now. After making the selections, click on **Finish**.

Dialing in to the Network: Launch the FTP Software Dialer. The application main window will pop up, as shown in Figure 167 on page 275. All defined connections will be displayed.

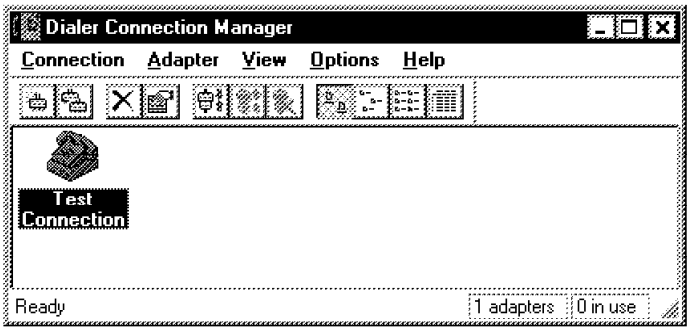


Figure 167. Dialer Connection Manager

Double-click on a connection to activate it. Depending on how you set up the authentication, a dialog box prompting for user ID and/or password will pop up. Fill in the necessary information and click on **OK** to initiate the connection. A details window will be shown where you can see the progress of the connection establishment. If the connection is established reliably, you might not want to see the details every time. To do this, select the **Do not show connection progress in the future** check box at the pop-up dialog box.

The functions of the Dialer Connection Manager are accessible from the menu bar or from the tool bar, and are the following:

- Create, delete, rename and duplicate connections.
- Create new adapters. For example, you may install an ISDN card.
- Connect to and disconnect from the network using the selected connection.
- Shut down the adapter associated with the selected connection.
- Show the detailed status window for the selected adapter.

Functions that are related to an existing connection can also be accessed from the context menu of that connection.

An icon is displayed on the task bar showing the status of the connection, as long as the associated adapter is active.

Once you are connected, you become part of the remote LAN. If your access is not restricted to the RAS system, you can access all resources available to you, in the way you normally can when you are directly connected to the LAN.

7.2.2.3 Using the FTP Software Dialer with Windows 3.x

The Windows 3.x dialer is not available unless you specified that you want to use a serial connection at installation time. To install the dialer after you have installed the FTP Software TCP/IP protocol stack without serial connection support, follow these steps:

1. Insert the eNetwork Communications Suite product CD-ROM disk into the CD-ROM driver and start the SETUP.EXE program found in the root directory of the CD-ROM disk. At eNetwork Communications Suite setup panel shown in Figure 45 on page 105 click on **Install FTP Software TCP/IP applications and Protocol Stack** to launch the setup. Click on **Continue** on the Welcome window.
2. At the Reinstallation window select **Add**, then click on **Continue**.
3. At the Installation Options panel select the location of the online books; either they will be copied to your hard drive or will be left on the CD-ROM. Click on **Continue**.
4. At the Components panel shown in Figure 46 on page 107, optionally select additional components you may want to use. After you are done with the selections, click on **Continue**.
5. At the Network Interface Summary panel shown in Figure 168 on page 277, click on **Add...**. At the Found Existing Driver dialog box that pops up, select **Install a new driver** and click on **OK** to continue.

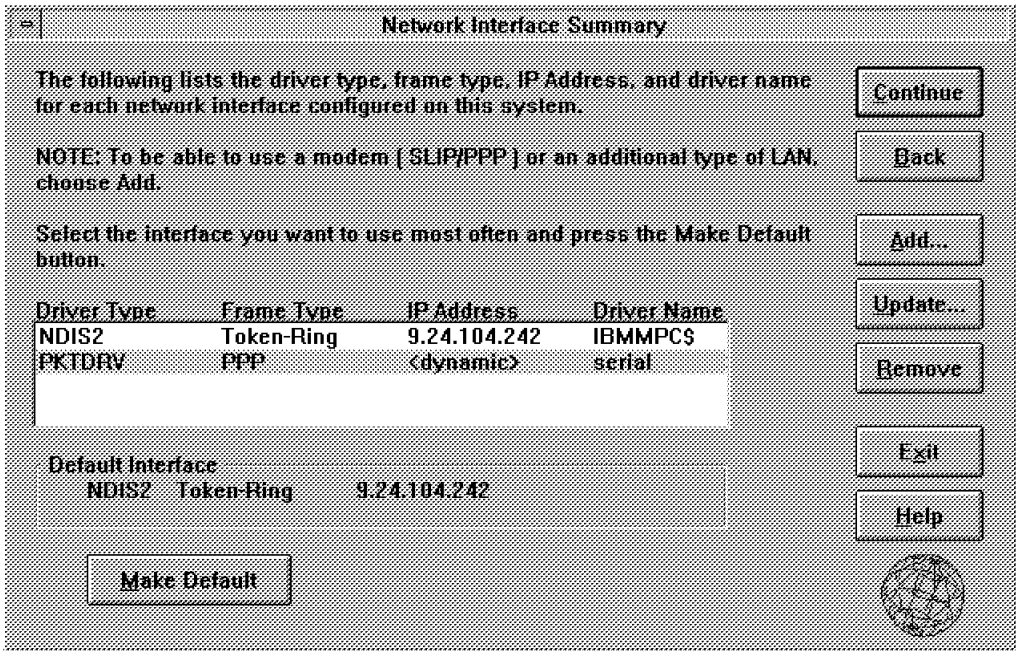


Figure 168. FTP Software Dialer Installation - Network Interface Summary

6. At the Network Card panel shown in Figure 47 on page 108 select **Serial Port Using SLIP or PPP** and click on **OK** to continue.
7. At the Serial Protocol dialog box select either PPP or SLIP as the protocol to be used for the network connection. You are able to change this setting later using the dialer, if needed. To connect to a RAS system, select **PPP**. Click on **OK** and you are returned to the Network Interface Summary panel, where the list box has been updated with the new driver (see Figure 168). Click on **Continue**.
8. At the WINS (NetBIOS) Configuration panel shown in Figure 49 on page 110, change the parameters for this service, if needed. See step 10 on page 110 for details. After you have finished, click on **Continue**.
9. At the Copy Files dialog box click on **Continue** to start copying the product files.
10. At the Setup Complete dialog box read the information and click **OK**.
11. At the Restart System dialog box click on **Restart System**.

The dialer has been installed and its icon has been added to the OnNet16 2.5 WinApps window.

Defining Connections: The dialer has two modes of operation: simple and advanced. It always starts in simple mode, which is intended for nontechnical users and is sufficient in most cases.

When you start the dialer for the first time, its main window is similar to Figure 169. Click on **Define a New Connection** to have the Dialer Connection Wizard guide you through the steps of creating a new connection.

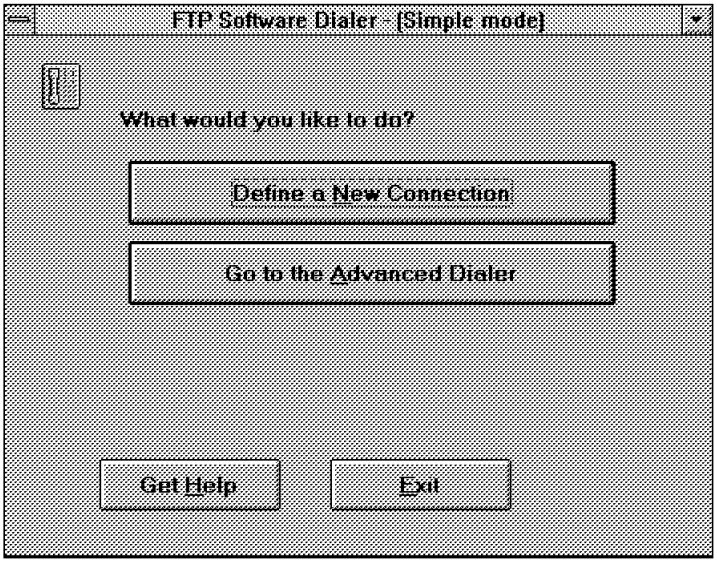


Figure 169. FTP Software Dialer - Simple Mode

1. At the Name New Connection Icon panel give a name to your connection and select what the dialer should do after completing the connection: remain active, exit or minimize. Click on **Next** to continue.
2. At the Determine Connection Type panel select **Modem** as the connection type, then click on **Next** to continue.

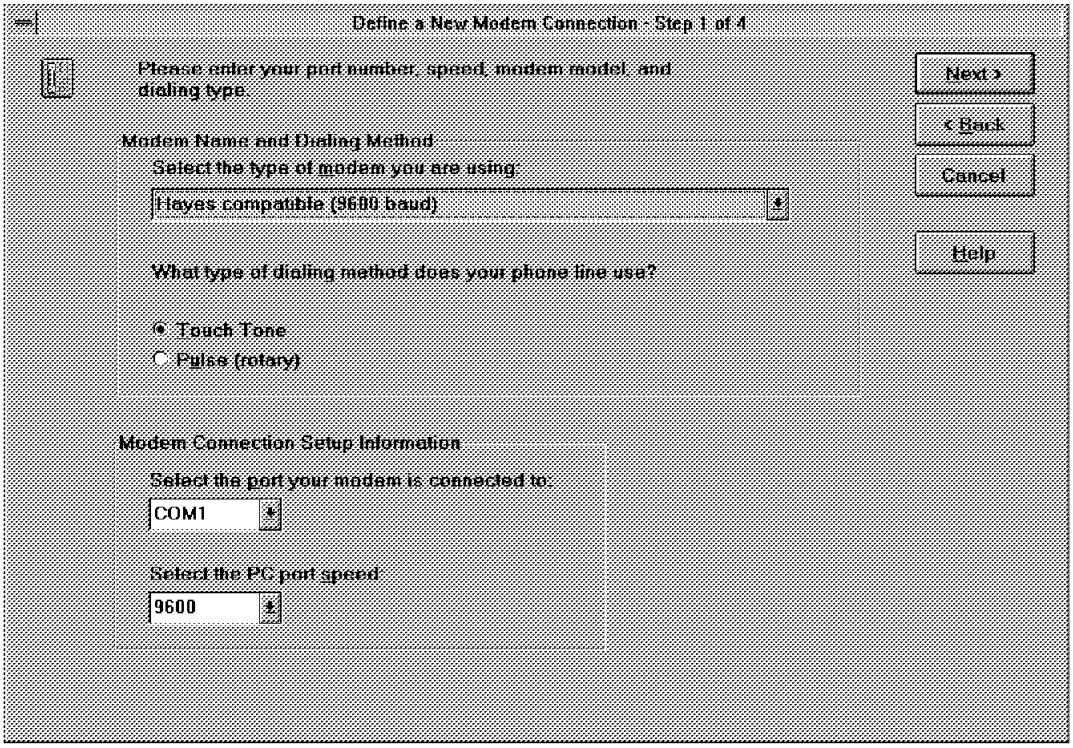


Figure 170. FTP Software Dialer - Determine Connection Type

3. At the panel shown in Figure 170 set the modem type and modem connection parameters, then click on **Next** to continue.
4. Enter the phone number to dial. Set the disconnect timeout interval and the disconnect warning time. Select the **Automatic Connection Enabled** check box to have the connection activated whenever the FTP Software applications need to communicate with remote hosts (Dial-on-Demand feature.)

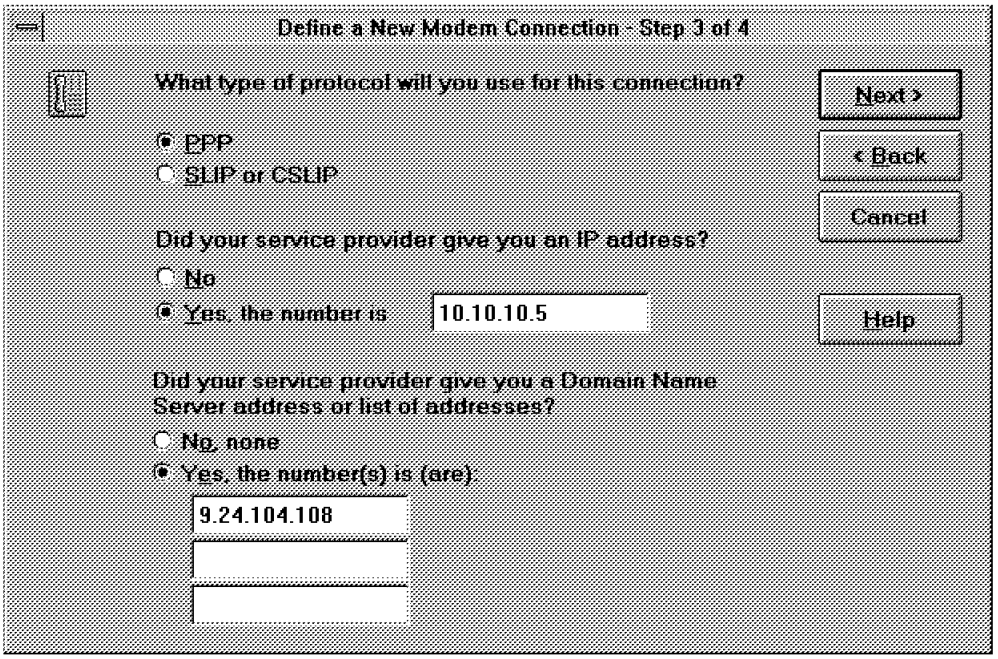


Figure 171. FTP Software Dialer - Protocol Selection

5. At the panel shown in Figure 171 choose either the PPP or SLIP protocols. In our scenario PPP is used. If there is an IP address permanently assigned to your machine, type it in at the corresponding input field. Also type in the address(es) of the name server(s), if any. Then click on **Next** to continue.
6. Type in the user name and password information. In our scenario, choose **No** for the question ″Will your service provider require you to type anything when you dial in?″. Choose **Yes** for the question ″Does your service provider support CHAP or PAP?″ and specify your user ID and password. Then click on **Next** to complete the connection definition.
7. As a last step, select whether you want to connect now using this connection, then click on **OK**.

Dialing into the Network: The dialer has created a program group named Dialer Connections which contains an icon representing your newly defined connection.

Double-click on the icon to use that connection.

Once you are connected, you become part of the remote LAN. If your access is not restricted to the RAS system, you can access all resources

available to you, in the way you normally can when you are directly connected to the LAN.

You may want to use the Advanced Mode of the dialer, which lets you customize connections with Scripting LANGuage (SLANG) scripts. A default script is created for every connection, but in simple mode you do not have access to these scripts. The advanced mode is also useful when you want to bypass the Dialer Connection Wizard. To use advanced mode, choose **Go to the Advanced Dialer** at the Dialer main window.

Note: For more information on SLANG scripts, see the FTP Software home page at http://www.ftp.com.

7.2.2.4 Using the FTP Software Dialer to Access the IBM Global Network

To access IBM Global Network (IGN), you may need a list of access numbers which is included in the IGN dialer software that comes with Internet Connection for Windows or OS/2 Warp. You can get an up-to-date list of those numbers from the following URL:

`http://www.ibm.net/phoneint.html`

7.3 Using Personal Communications to Access the AS/400

As a remote client connected to the LAN over TCP/IP, you can use 5250 terminal emulation and can transfer files using FTP. There are several ways to connect Personal Communications to an AS/400 over a TCP/IP connection, among them the following:

1. Using a direct TCP/IP connection and TCP/IP application protocols:
   - Telnet5250
2. Using a direct TCP/IP connection and SNA application protocols:
   - 5250 over AnyNet APPC over TCP/IP (to AS/400)

We use the Telnet5250 connection for this scenario. It is assumed that Personal Communications has already been installed with the 5250 features necessary to connect to an AS/400. Please refer to 3.1.4, “Installing Personal Communications for Windows NT” on page 65, 3.2.4, “Installing Personal Communications for Windows 95” on page 89 and 3.3.3, “Installing Personal Communications for Windows 3.x” on page 111 for more information on Personal Communications installation.

7.3.1 Configuring a Terminal Emulation

To set up a 5250 terminal emulator, follow these steps:

1. For the Windows 95 and Windows NT environments, select **Programs/IBM Personal Communications/Start or Configure Session** from the Start menu. For the Windows 3.x environments, double-click on the **Start or Configure . Session** icon.
2. Personal Communications will load and present you with a dialog box reminding you that you need to configure this session before you can connect to the host system. Read this dialog box, then dismiss it by selecting **OK**.
3. You will now be presented with the Customize Communication dialog box, shown in Figure 172.

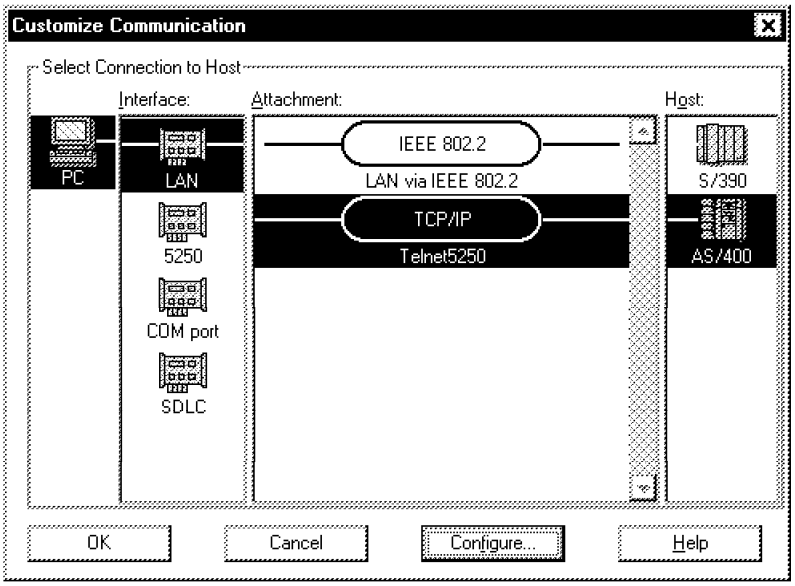


Figure 172. Customize Communication Window

From this dialog box select the **AS/400** host and the **Telnet5250** attachment. Leave the interface at its default (LAN). Click on **Configure** to continue.

4. At the Customize Communication - 5250 Host dialog box you can select the screen size and host code page. Once you have done this, click on **Configure Link...**.
5. In the field marked Host Name or IP Address type in the TCP/IP address of the AS/400 host. You can use either the hostname or the IP address. In Figure 173 on page 283 we have used the fully qualified hostname.

This is recommended as the host may change its IP address from time to time, or may have configured several interfaces with the same hostname and direct incoming connections to the interface with the lightest load.

The advanced section allows you to specify a TCP/IP port other than the default of 23. Do not do this unless your system administrator has advised you to do so. If you wish to be automatically reconnected in case your session has been accidentally disconnected, check the **Auto-reconnect** check box.

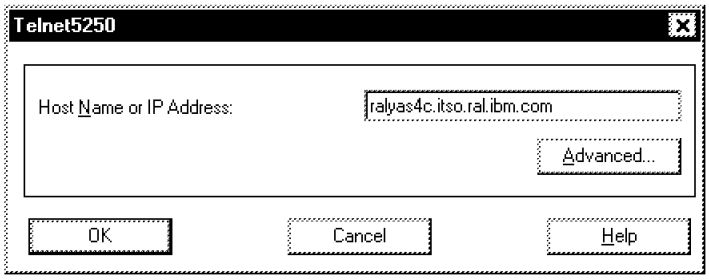


Figure 173. Telnet5250 Host Name or IP Address Dialog

6. Click on **OK** on the open dialog boxes until all of them are closed. If your settings are correct, after a few seconds you will see the AS/400 sign-on screen in your emulator window.

7.3.2 Using FTP to the AS/400

You set up an FTP session to the AS/400 FTP server in the same way as you do it for any other host. See 5.4, “Using the FTP Client” on page 173 for details on this procedure.

Once connected, depending on the FTP server settings, you will see or of more libraries of the AS/400 as folders. The objects of type *FILE are listed, along with their members. For example, the file member FIRST in file QDDSSRC in library TAMLIB is accessible with the FTP client as file QDDSSRC.FIRST in folder TAMLIB. Accordingly, a PC file named TEST.TXT is sent to the host as member TXT in file TEST in the selected library.

Notes:

1. Bear in mind the file naming conventions on the AS/400 when transferring files. For example, file names can not start with a number and the name length is limited to ten characters.
2. You can access files (that is, objects of type *FILE) on the AS/400 even in libraries that do not appear in the directory pane of the FTP client window. To do this, use the command line interface.

Chapter 8. Troubleshooting the eNetwork Communications Suite

In this chapter, we concentrate on aspects of troubleshooting in an environment where eNetwork Communications Suite components are being used, in particular the FTP Software TCP/IP protocol stack and FTP Software TCP/IP applications. The following problem areas are addressed:

- Installation
- Configuration
- Network failure
- Application failure

Referring to the scenarios developed in the previous chapters, we take a look at the major applications of the eNetwork Communications Suite, provide related problem determination checklists and procedures, and take a look at available tools.

8.1 Using Available Tools and Getting Support

The following applications included in the FTP Software TCP/IP protocol stack are useful tools for problem determination:

Ping
To check if you can actually send anything to a remote system.

Traceroute
To check the path from your system to the system you want to connect to. You may find out about any routers on the way causing problems.

Statistics
To obtain information about the current configuration and state of the FTP Software TCP/IP protocol stack, such as:

- Active interfaces and IP addresses used by them
- Active IP routing table
- Protocol connections
- Protocol transmission errors that may indicate network errors
- Active ARP table

Query
To get information from a domain name server and to map IP addresses to host names and vice versa.

IPTrace
To analyze IP traffic originating from and/or destined to your system.

Retrieve

To obtain current system configuration such as:

- Hardware configuration (processor, disk size, etc.)
- Operating system type and level
- Operating system environment variables
- Registry information about FTP Software components
- Name of system user, problem description and recreation steps. This has to be filled in by the user experiencing the problem, as is shown in the figure below:

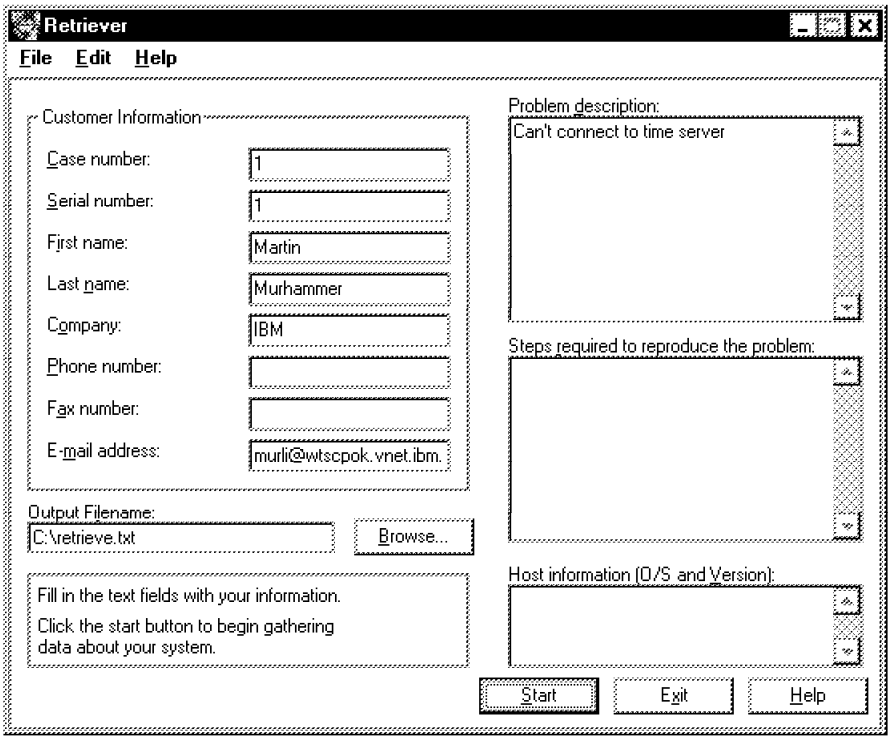


Figure 174. Using Retrieve for Problem Reporting

- Once everything has been filled out, press the **Start** button. A text file will be generated that contains all the gathered information. Retrieve can optionally send this file as an e-mail to a help desk for investigation.

OpenScript and OpenTools

To generate automated scripts that can employ the aforementioned applications to collect system information and submit it to a central management system without interaction from the local user.

For general support issues, you can contact the eNetwork Communications Suite forum at the following URL:

http://www.networking.ibm.com/ecs/forum/ecsforum.html

For hotline, on-site or defect support, please call you local IBM Service Center or your IBM Business Partner.

8.2 General Connectivity Problems

Use the following checklist to track down and solve problems related to general connectivity and installation issues. Ensure that the following statements are true:

- The network cable is connected to the adapter.
- The adapter card is functioning (diagnostics).
- The proper driver for the adapter card is installed and functioning.
- The TCP/IP stack is bound to the adapter card driver.
- Your TCP/IP configuration is correct:
  - IP address
  - Subnet mask
  - Default router
  - Domain name server
  - Domain name
  - Hostname
- If you are using DHCP, ask your system administrator to check the DHCP server records that apply to your workstation. Especially, the values supplied for IP subnets, IP routers and domain name servers should be checked thoroughly.
- If you are connecting via an Internet Service Provider (ISP), verify your account and connection information with the ISP.
- The installation log files to not list errors related to the setup of any eNetwork Communications Suite component. The following installation log files are provided:

  FTP Software TCP/IP applications: Program FilesFTP SoftwareNetSuiteINSTALL.LOG

  FTP Software TCP/IP protocol stack: Program FilesFTP SoftwareOnNet32INSTALL.LOG
- The configuration of the components is correct. Refer to your system administrator for actual configuration parameters, and also check out

chapters 3 to 7 of this book as well as related product documentation for configuration information and examples.

8.3 File Transfer Problems

Use the following checklist to track down and solve problems related to file transfer issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The FTP server is running on the remote system.
- You are defined as a user on the FTP server, or else the FTP server allows anonymous connections.
- You used the correct password.
- You have the appropriate access permissions on the target directory.
- The type of the FTP server's operating system is configured properly in the FTP client session profile.

8.4 File Sharing Problems

Use the following checklist to track down and solve problems related to file sharing issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The NFS server is running on the remote system, and also the PCNFSD server.
- The Sun Lock Manager server is running on the remote system if file locking is required. (Remember that is is actually performed by the NFS client.)
- Your host has been added to the export list of the directory you try to mount.
- You are defined as a user to the NFS server (validated via PCNFSD.)
- You have correctly configured the NFS server to the InterDrive client.
- You used the correct password.
- You have the appropriate access permissions on the target directory.
- The drive letter you try to use for the remote drive is not already in use.
- You are spelling file names correctly if the NFS server system is case-sensitive.

8.5 Printing Problems

Use the following checklist to track down and solve problems related to printing issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The remote printer is online and not out of paper.
- The remote printer is connected to the print server system.
- The print server is running at the remote system.
- The print queue you want to print to actually exists and is active.
- You are defined as a user to the print server.
- You used the correct password.
- You have the appropriate access permissions on the target print queue.
- You use a printer driver that is compatible with the remote printer and/or the printer driver that the server is using.
- You used a data stream that is understood by the remote printer.
- You defined a paper size that matches the paper that the remote printer is currently loaded with.

8.6 Terminal Emulation Problems

Use the following checklist to track down and solve problems related to terminal emulation issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The terminal server is running at the remote system.
- You are using the correct terminal type, code page and keyboard mapping for the remote applications.
- You are defined as a user to the terminal server.
- You used the correct password.
- You have the appropriate access permissions on the target applications.
- When using Personal Communications, all SNA configuration parameters are entered correctly.
- When using Personal Communications, the SNA path to the application is available.

8.7 E-mail Problems

Use the following checklist to track down and solve problems related to e-mail issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The mail server is running at the remote system.
- Any mail gateways, mail routers or pass-through servers between your system and the mail server are also running.
- The domain name server is up and correctly resolves host names and mail exchange records.
- You have a user account at the mail server.
- You have specified the name of the Lotus Notes server correctly.
- The information in the Lotus Notes location document for the mail server is correct.
- Your mail file and/or directory is set up at the mail server.
- You used the correct password.
- You use the appropriate protocol to connect to the mail server (SMTP, POP, Lotus Notes, MIME, etc.).

8.8 Web Browsing Problems

Use the following checklist to track down and solve problems related to Web browsing issues. Ensure that the following statements are true:

- The FTP Software TCP/IP applications are installed and functioning properly.
- The Web server is running at the remote system.
- Any proxy or SOCKS servers (firewalls) you need to use to connect to external Web sites are running.
- You have enough free disk space to accommodate the cache files for the Web browser.
- The browser is capable of, and enabled for using SSL, Java and JavaScript, and to accept cookies and self-signed certificates.
- The required browser plug-ins are installed and functioning properly.
- Your system is capable of, and configured for handling features such as playing audio files and displaying video clips.

8.9 Security Problems

Use the following checklist to track down and solve problems related to security issues. Ensure that the following statements are true:

- When using IPSec, the secret key and encryption algorithm information is exchanged and configured properly for both systems.
- When using SOCKS, you are defined to the firewall and your SOCKS configuration is correct.
- When using SSL, this protocol is enabled in the Web browser (Netscape Navigator or Lotus Notes Mail Client), and the browser supports self-signed certificates if required.
- When using a Lotus Domino Server, check that the SSL configuration has been performed at the server.
- The remote system as well as proxy servers and/or firewalls are running and reachable. Use the Ping and Traceroute applications to verify that.

Appendix A. TCP/IP Reference

In this chapter, we provide an reference listing of the relevant RFC documents for the FTP Software TCP/IP protocol stack, FTP Software TCP/IP applications, and Netscape Navigator components of the eNetwork Communications Suite, and we also list URLs for further information on the Internet.

A.1 List of RFCs for More Information

In this section, we provide a list of RFCs and IDs relating to TCP/IP and Internet protocols and applications that are either contained in the eNetwork Communications Suite or discussed in this redbook.

Table 7 (Page 1 of 2). List of RFC and Internet Draft Documents

Topic	**RFC(s)**
Official Protocol Standards	2000
Internet Assigned Numbers	1700
IP	791, 950, 919, 922
ICMP	792
UDP	768
TCP	793
ARP	826
IPv6	1883-1886
IPSec	1825-1829
PPP	1661, 1662, 1717
SLIP	1055
DNS	1034, 1035
DHCP	1541
DDNS	2136, 2137
SNMP	1155, 1157, 1212, 1213
MIB-II	1213
NTP	958
CIDR	1518-1520
RIP	1058
RIP 2	1722-1724

Table 7 (Page 2 of 2). List of RFC and Internet Draft Documents	
Topic	**RFC(s)**
OSPF	1583
NetBIOS	1001, 1002
FTP	959
Telnet	854, 855
Telnet3270E	1647
RPC	1831
XDR	1832
NFS	1094, 1813, 2054, 2055
SMTP	821, 822, 974, 1869, 1870
POP3	1725
MIME	2045-2049
Printing	1179
HTTP	2068
NNTP	977
Gopher	1436

A.2 List of Web Sites (URLs) for More Information

In this section, we provide a list of Web sites and URLs to turn to for more information on topics related to this redbook.

IBM Corp. home page:

`http://www.ibm.com`

eNetwork Communications Suite home page:

`http://www.networking.ibm.com/ecs/ecshome.htm`

ITSO home page:

`http://www.redbooks.ibm.com/`

FTP Software, Inc. home page:

`http://www.ftp.com`

Lotus Corp. home page:

`http://www.lotus.com`

Netscape Communications Company home page:

`http://www.netscape.com`

List of RFCs:

http://ds.internic.net/ds/dspg0intdoc.html

IPv6 information:

http://www-6bone.lbl.gov/6bone/
http://playground.sun.com/pub/ipng/html/ipng-main.html

Internet history:

http://www.isoc.org/internet-history/

Internet growth:

http://info.isoc.org/guest/zakon/Internet/History/HIT.html#Growth
http://www.nw.com/zone/WWW/dist-bynum.html

InterNIC registration information:

http://rs.internic.net/about-rs.html

WWW growth:

http://www.mit.edu/people/mkgray/net/web-growth-summary.html

WWW information, HTML and HTTP:

http://www.w3.org/pub/WWW/

Java information:

http://ncc.hursley.ibm.com/javainfo/
http://java.sun.com/

Information about SSL:

http://home.netscape.com/assist/security/ssl/index.html

Information about firewalls and SOCKS:

http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com

Information about ISAKMP/Oakley key management framework:

http://www.ietf.cnri.reston.va.us/ids.by.wg/ipsec.html
http://www.cisco.com/public/library/isakmp.html

Appendix B. Special Notices

This publication is intended to help system administrators and networking engineers to plan for and implement the IBM eNetwork Communications Suite in a corporate network.

The information in this publication is not intended as the specification of any programming interfaces that are provided by the eNetwork Communications Suite or any of its components.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (″vendor″) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each

item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

Advanced Peer-to-Peer Networking	AIX
AnyNet	APPN
ARTour	AS/400
Cryptolope	eNetwork
IBM	OfficeVision
OS/2	OS/390
PROFS	PS/2
S/390	

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Adobe, Adobe Acrobat, PostScript	Adobe Systems, Inc.
FistFloor, SmartBookmarks	FirstFloor, Inc.
FTP Software, InterDrive, OnNet, KEYView	FTP Software, Inc.
IPX, Novell	Novell, Inc.
Lotus, Notes, Domino	Lotus Development Corp.
Netscape	Netscape Communications Corp.
Network File System, NFS, Solaris	Sun Microsystems, Inc.
RSA	RSA Data Security, Inc.
VT52, VT100	Digital Equipment Corp.
Wyse	Wyse Technology, Inc.
X Window System	Massachusetts Institute of Technology

Appendix C. Related Publications

C.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 303.

- *Personal Communications Version 4.1 for Windows 95 and Windows NT*, SG24-4689-00
- *PCOMM 4.X Interoperability and Problem Determination Guide*, GG24-4457-00
- *TCP/IP Tutorial and Technical Overview*, GG24-3376-04

C.2 Product Documentation

- *eNetwork Communications Suite for Windows - Installation Guide*, GC31-8528-00
- *PCOMM 4.1 Windows 95 Up and Running*, SC31-8205-00
- *PCOMM 4.1 Windows 95 Reference*, SC31-8206-00
- *PCOMM 4.1 Windows Up and Running*, SC31-8261-00
- *Personal Communications AS/400 and 3270 for Windows NT Reference*, SC31-8315-00
- *Personal Communications AS/400 and 3270 for Windows NT System Management*, SC31-8318-00
- *VTAM V4R4 Customization*, LY43-0075 (licensed customers only)

Also refer to the online documentation for FTP Software TCP/IP protocol stack, FTP Software TCP/IP applications and Lotus Notes Mail Client that comes with eNetwork Communications Suite

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

C.3 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
Application Development Redbooks Collection	SBOF-7290	SK2T-8037
Personal Systems Redbooks Collection	SBOF-7250	SK2T-8042

C.4 Other Publications

These publications are also relevant as further information sources:

- *Intranet Bible*, SR23-7780-00
- *Migration to IBM eNetwork Personal Communications and Communications Server*, G325-3711-00
- *The Computing Advantage for a Networking World*, G520-9402-02
- *10 Minute Guide to Lotus Notes Mail 4.5*, Que Corp., 1996, by Jane Calabria; ISBN 0-7879-0974-0.
- *Internetworking with TCP/IP, Volume I, Principles, Protocols and Architecture* third edition, Prentice-Hall, Inc., 1995, by Douglas E. Comer; ISBN 0-13-216987-8.
- *Applied Cryprography*, second edition, John Wiley & Sons, Inc., 1996, by Bruce Schneier; ISBN 0-471-11709-9.
- *IPng and the TCP/IP Protocols*, John Wiley & Sons, Inc., 1996, by Stephen A. Thomas; ISBN 0-471-13088-5.
- *Communications for Cooperating Systems - OSI, SNA and TCP/IP*, Addison-Wesley, Publishing Company, Inc., 1992, by R. J. Cypser; ISBN 0-201-50775-7.
- *The Request For Comments (RFCs)*

  There are more than 2000 RFCs today. For those readers who want to keep up-to-date with the latest advances and research activities in TCP/IP, the ever-increasing number of RFCs and Internet Drafts (ID) is the best source of this information. (See 1.3, “Internet Standards and Request for Comments (RFC)” on page 3 for more details on RFCs.)

  RFCs can be viewed or obtained online from the Internet Engineering Taskforce (IETF) Web page using the following URL:

  `http://ds.internic.net/ds/dspg0intdoc.html`

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO: type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Web Site on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1)001-408-256-5422 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet e-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an e-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number
- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

List of Abbreviations

AH	Authentication Header
AIX	Advanced Interactive Executive
API	Application Programming Interface
APPC	Advanced Program-to-Program Communication
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
AS/400	Application System/400
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CDRSC	Cross Domain Resource
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Interdomain Routing
CP	Control Point
CPI-C	Common Programming Interface for Communications
CPU	Central Processing Unit
DDE	Dynamic Data Exchange
DDNS	Dynamic Domain Name System
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLUR	Dependent LU Requester
DLUS	Dependent LU Server
DMZ	De-Militarized Zone
DNS	Domain Name System
DOS	Disk Operating System
EBCDIC	Extended Binary Communication Data Interchange Code
EHLLAPI	Enhanced High-level Language API
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IAB	Internet Activities Board
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
ICSS	Internet Connection Secure Server
IDBLK	Identification Block
IDEA	International Data Encryption Algorithm
IDNUM	Identification Number

IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGN	IBM Global Network
ILU	Independent Logical Unit
IP	Internet Protocol
IPC	Interprocess Communication
IPSec	IP Security Architecture
IPX	Internetwork Packet Exchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITSO	International Technical Support Organization
LAN	Local Area Network
LLC	Logical Link Layer
LPD	Line Printer Daemon
LPR	Line Printer Requester
LSP	LAN Support Program
LU	Logical Unit
MAC	Media Access Control
MD2	RSA Message Digest 2 Algorithm
MD5	RSA Message Digest 5 Algorithm
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MPTN	Multiprotocol Transport Network
MVS	Multiple Virtual Storage Operating System
NDIS	Network Device Interface Specification
NETID	SNA Network Identifier
NFS	Network File System
NIC	Network Information Center
NIS	Network Information Systems
NNTP	Network News Transfer Protocol
NSAP	Network Service Access Point
NTP	Network Time Protocol
NVT	Network Virtual Terminal
ODI	Open Data Link Interface
OSPF	Open Shortest Path First
OS/2	Operating System/2
PAP	Password Authentication Protocol
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
PU	Physical Unit
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Server
RC4	RSA Rivest Cipher 4 Algorithm
RFC	Request for Comments
RIP	Routing Information Protocol
ROM	Read-only Memory

RPC	Remote Procedure Call
RSH	Remote Shell
SDLC	Synchronous Data Link Control
S-HTTP	Secure Hypertext Transfer Protocol
SLIP	Serial Line Internet Protocol
SMIT	System Management Interface Tool
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SRPI	Server-Requester Programming Interface
SSCP	System Service Control Point
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UNC	Universal Naming Convention
URL	Uniform Resource Locator
VM	Virtual Machine Operating System
VTAM	Virtual Telecommunications Access Method
WINS	Windows Internet Name Server
WWW	World Wide Web
XDR	Extended Data Representation
XID	Exchange Identifier

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

O

P

R

S

T

X

Y

Z

ITSO Redbook Evaluation

Exploring the IBM eNetwork Communications Suite
SG24-2111-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@vnet.ibm.com

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes____ No____

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____

_____

_____

_____

_____

Printed in U.S.A.