Personal Communications for Windows, Version 5.5

Access Feature

SC31-8684-02

Personal Communications for Windows, Version 5.5

Access Feature

SC31-8684-02

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix F. Notices" on page 115.

Third Edition (September 2001)

This edition applies to Version 5.5 of Personal Communications and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About This Book

This book describes how to install, configure, and start IBM Personal Communications Access Feature for Windows, Version 5.5. After you get Personal Communications Access Feature up and running and begin to perform various tasks, use the online help whenever you need additional information. See "Where to Find More Information" for information about online help, the Personal Communications library, and related publications. Refer to the IBM® Glossary of Computing Terms at the following URL for definitions of technical terms used throughout this book:

http://www.networking.ibm.com/nsg/nsgmain.htm

The screens in this book are representative of ones that you might see while working with Personal Communications. Minor variations could occur between what you see on your display and what is in the book.

In this book, *Windows*® refers to Windows 95, Windows 98, Windows NT, Windows Me, and Windows 2000. When information is applicable only to a specific operating system, this will be indicated in the text.

What's in the Package

The Personal Communications Access Feature Version 5.5 CD-ROM also contains the following:

- Adobe Acrobat reader to enable you to read softcopy books (.PDF) available on the CD-ROM
- Book files in .PDF format, which allow you to view the books shipped with the products

Notes:

1. There are also separate CD-ROMs, depending on:

   National Languages
   There is a multiple-language version that supports up to nineteen languages at the same time. There are also single language versions for
   - Traditional Chinese
   - Simplified Chinese
   - Korean

   Security Levels
   Personal Communications Access Feature is shipped at the 168-bit encryption level.
2. There is a separate CD-ROM containing the DB2 Connect® product.

Where to Find More Information

The following sections discuss getting help when you are installing, configuring, or using Personal Communications Access Feature.

Online Help

The help facility describes how to install, configure, and use Personal Communications Access Feature. Online help is very extensive and includes information about every aspect of configuring and using Personal Communications Access Feature. You can use Personal Communications online help just as you use the online help for Windows.

Use help to obtain information about:

- Menu choices
- Operation procedures
- Operations in windows
- Meanings of the terms displayed in windows
- Causes of errors and the corresponding actions to take
- Mouse-based operations
- Operation without a mouse
- Detailed explanations of specific terms
- Further technical information about Personal Communications
- Detailed explanations of operator information area (OIA) messages

Related Publications

For information about local area networks (LANs), refer to the following publications:

- *IBM Local Area Network Technical Reference*
- *AS/400 Communications: Local Area Network (LAN) Guide Version 2*

For more information about NetWare, refer to the publications for the following products:

• For the client	*NetWare Client for Windows*
• For NetWare for SAA®	*NetWare for SAA*

Contacting IBM

This section lists ways you can reach IBM in case you encounter a problem or concern with Personal Communications. Depending on the nature of your problem or concern, we ask that you be prepared to provide the following information to allow us to serve you better.

- The environment in which the problem occurs:
  - Personal Communications Access Feature configuration
    - Personal Communications Access Feature version and CSD level
    - The name of the workstation profile
    - The name of the SNA Node Configuration file
  - Workstation configuration
    - The machine type and model, the system memory, the video adapter
    - The communication adapter you are using
    - Other adapters (especially communication adapters) installed
    - The printer type and model
    - Other devices installed, such as sound cards, modems, or fax machines
  - Software configuration
    - Windows version and level
    - Communication and device-driver version and level

    - Other communication programs (such as NetWare, Microsoft® SNA Server, or Microsoft Data Link Control) that are running and using resources
    - Printer driver version and level
  - Host configuration
    - The upstream host connection and configuration
- Problem analysis information
  - Symptoms
  - Type of problem
  - OIA messages or error messages (if any)
  - Key factors related to the problem

If you have a technical problem, take the time to review and carry out the actions suggested here. Use your local support personnel before contacting IBM. You can also check the Hints and Tips at the Personal Communications support Web page for more information. Only persons with in-depth knowledge of the problem should contact IBM; therefore, support personnel should act as the interface with IBM.

Support Options

If you determine that you need to contact IBM, you can do any of the following:

- Access the Personal Communications Web page at the following URL:

  http://www.ibm.com/software/network/pcomm
- To find the phone number for IBM Software Support, U.S. customers can call 1-800-IBM-4YOU. International customers that have access to the U.S. ″800″ toll free numbers can reach the International Support Center by calling 1-800-IBM-4YOU and asking to speak with the International Support Center (ISC) in Atlanta. International customers without access to the U.S. toll free numbers can call the ISC directly at 770-863-1234. The ISC's FAX number is 770-863-3030 and is available 24 hours a day.

Part 1. Introduction

Chapter 1. Welcome to Personal Communications Access Feature

A variety of SNA-based client application programming interfaces (APIs) are supported by Personal Communications Access Feature. You can create applications that use the peer-to-peer client APIs, which are based on LU 6.2 and provided by Personal Communications. These APIs let you simultaneously access and process information on peer workstations.

Personal Communications supports Advanced-Peer-to-Peer Networking (APPN) as an end node, and uses the advanced network features: high-performance routing (HPR) and dependent LU requester (DLUR).

AnyNet® SNA over TCP/IP is a feature of Personal Communications which allows emulator and client/server SNA applications to communicate over a TCP/IP network.

What’s New in IBM Personal Communications Access Feature Version 5.5

Personal Communications Access Feature Version 5.5 is based on the popular Personal Communications Access Feature Version 5.0. If you are familiar with Personal Communications Version 5.0, you might want to review some of the new functions and enhancements.

The following sections briefly describe the major new Personal Communications Access Feature functions.

Programming Enhancements

Windows 2000 Certification
Personal Communications 5.5 holds Microsoft Windows 2000 certification.

Installation/Configuration Enhancements

Use of Windows Installer
One specific installation enhancement is that the user can specify the default location of configuration files.

Corrective Service Distributions and Authorized Program Analysis Reports
Authorized users may use the WebUpdate tool in the **Administrative and PD Aids** menu to check for Personal Communications Corrective Service Distributions (CSDs) and Authorized Program Analysis Reports (APARs) via the Internet.

Tivoli® Support
Personal Communications Access Feature Version 5.5 is Tivoli-Ready certified. It is integrated with Tivoli Enterprise™ as a Desktop application, and provides a Plus module for its application management. The Plus module, called IBMPCOMM Plus, includes event management, software distribution, and administrative tasks. Support for problem determination is new. The Plus module includes tasks for remote operation of the Integrated Trace facility.

Other Enhancements

Defining the session view from a batch file

When starting a session from a batch file, you can define the view to be used with that session.

Convert Macro to XML

A macro may now be converted to XML, in addition to VBScript.

Windows 2000 Power Management

Personal Communications complies with Windows 2000 Power Management requirements for handling sleep events (stand by and hibernate). This support minimizes session interruptions due to network disconnections caused by sleep on Windows 2000 and subsequent versions.

Smart Card Support

Personal Communications supports Smart Cards and other cryptographic devices, which allows you to store a certificate in a dedicated security device.

Capture View

This function allows you to automatically add all open sessions (with the current session IDs) to a view and add that view to a batch file. You can add up to 26 sessions in one view; you can save as many as 8 views in a batch file.

Personal Communications Access Feature Program Icons

When you have installed Personal Communications, the main functions that you can use are displayed as icons. Icons are grouped in subfolders of the IBM Personal Communications program folder.

A brief explanation of each function follows:

SNA Node Configuration

Use this icon to configure an SNA node and associated resources or to change advanced configuration parameters.

IBM Software Registration

Use this icon if you want to be notified of any program updates provided by IBM.

Administrative and Problem Determination (PD) Aids

Display SNA Sense Data

Use this icon to display SNA sense data and associated explanations. Sense data is SNA error information located in internal SNA flows, error logs, error messages, and traces. Some Personal Communications error messages include sense data.

Information Bundler

Use this icon to gather system files and specific trace and log files, as well as registry information, such as the software installed or running on a machine.

Internet Service

Use this icon to send system and diagnostic data collected by the Information Bundler to an FTP server.

Log Viewer

Use this icon to view, merge, and sort the Personal Communications message and trace logs. Personal Communications logs errors and informational messages during initialization and operation.

Migration Utility

Use this icon to migrate your user-class and system-class files and desktop icons to Personal Communications Version 5.5.

Product Update Tool

Use this icon to access WebUpdate and check for Authorized Program Analysis Reports (APARs) and Corrective Service Distributions (CSDs).

SNA Node Configuration Verification

Use this icon to verify that the ASCII editing changes that you have manually made to the SNA node configuration data are valid.

SNA Node Operations

Use this icon to perform SNA node operations, such as starting or stopping resources or displaying resource information.

Trace Facility

Use this icon to turn trace functions on and off and to capture communication-protocol information that passes between your workstation and other host systems. You can use traces to resolve communication problems.

Product Information

The Personal Communications documentation is available on the installation CD-ROM. You can copy any of these PDF or HTML files to your workstation, for viewing at your convenience.

Readme-Please!

The Readme file includes recent updates to the documentation or other information that might be of special interest.

Manuals

Client/Server Communications Programming

This book describes support for the APPC and LUA application programming interfaces (APIs).

System Management Programming

This book describes how to use the Node Operations Facility (NOF) application programming interface (API).

Configuration File Reference

This book describes how to edit and verify configuration data using an ASCII editor.

Host Access Class Library for Java

This HTML document describes how to write an ActiveX/OLE 2.0–compliant application to use Personal Communications as an embedded object.

Host Access Beans for Java

This HTML document describes Personal Communications emulator functions delivered as a set of Java™ Beans.

Utilities

The APING and AFTP utilities are available in U.S. English only.

> **Note**
>
> THESE PROGRAMS ARE PROVIDED ON AN AS-IS BASIS WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WHICH ARE EXPRESSLY DISCLAIMED.

Certificate Management

Use this icon to enable Secure Sockets Layer (SSL) communication between your communication server and client. See “Using Certificate Management” on page 60 for details on how to use this utility.

Certificate Wizard

Use this icon to launch the Certificate Wizard which allows you to enable Secure Sockets Layer (SSL) communication between your communications server and client. See “Using Certificate Wizard” on page 60 for details on how to use this utility.

Check Connection APING

Use this sample CPI-C program to verify network connections. You can use APING to establish network connections, diagnose problems, and take simple performance measurements. APING exchanges data packets with a partner computer and measures how long the data transfer takes.

Convert Macro

Use this icon to convert an existing Personal Communications macro to an XML or VBScript file.

DOS EHLLAPI

Use this icon to enable or disable DOS-based EHLLAPI programs that communicate with the 32-bit Personal Communications emulator.

Menu-Bar Customization

Use this icon to customize the menu bar in the session window.

Multiple Sessions

Use this icon to create batch files (.BCH), which specify multiple emulator sessions (workstation profiles) or other supported Windows programs that you want to start concurrently. You can create an icon for each batch file and start the programs just by clicking the icon. By default, this utility is not installed automatically.

Transfer File AFTP

Use this program to provide a fast and efficient transfer of text and binary files.

Personal Communications Access Feature Sessions

The sessions that Personal Communications Access Feature provides are logical connections enabling communication between your workstation and a host system. The following session type is available:

Client/server session

Establish connections that allow peer communications using CPI-C and APPC (LU 6.2).

Personal Communications Access Feature Connections

Personal Communications Access Feature supports a variety of connections to the following host systems.

Client/Server (Peer) Connections

Personal Communications provides APPN® end node support for workstations, allowing them to communicate more flexibly with other systems in the network.

When your workstation is defined as an APPN end node, an APPN network node server provides the following directory and routing services for your workstation:

- Intermediate session routing
- Directory services
- Topology and route selection services

Using Personal Communications, you can establish client/server connections to a variety of computers and to workstations running OS/2®, Windows 95, Windows 98, Windows NT, Windows Me, or Windows 2000. Another option is to connect the computers to a workstation running Communications Server. Available SNA client/server connection types are:

- LAN via IEEE 802.2
- Synchronous Data Link Control
- SNA-over-Async
- AnyNet SNA over TCP/IP
- Hayes AutoSync
- IBM Global Network® – SNA over Async
- Twinaxial Data Link Control (APPC)
- X.25
- OEM Deep adapter
- WAC
- Enterprise Extender

APPN Networking

Advanced Peer-to-Peer Networking® (APPN) is the underlying networking protocol that routes APPC traffic through intermediate nodes in the network. For instance, when Program A uses APPC to talk to Program B, APPN finds the node where Program B is located and directs the APPC traffic through the network.

APPN includes several features that help reduce the amount of configuration required to set up and maintain a network. These features automate many tasks that are time consuming, complicated, and error prone. For example, if you're installing a new workstation that uses APPN, you don't have to set up configuration information for every workstation you want to communicate with. You simply provide the name of the computer and the address of the intermediate node that handles your traffic. APPN takes care of the rest of the information needed to route APPC traffic to and from your workstation.

If you connect to an APPN network, you simplify your own configuration and make it easier for other computers in the network to find you.

APPC

Advanced program-to-program communication (APPC), also known as LU 6.2, is software that enables high-speed communications between programs on different computers, from portables and workstations to midrange and host computers. APPC software is available for many different operating systems, either as part of the operating system or as a separate software package.

APPC is a communications protocol that enables programs on different computers to "talk to" each other. APPC provides the interface between the programs and the networking hardware and software and defines the rules that programs use to exchange information.

APPC serves as an interface between application programs and the network. When the communications application on your workstation passes information to the APPC software, APPC takes the information and sends it on to a network interface, such as a Token-Ring adapter card. The information travels across the network to another computer, where the APPC software receives the information from the network interface. APPC puts the information back into its original format and passes it to the corresponding communications application.

APPN Network

By participating in an APPN network, Personal Communications workstations can also take advantage of two additional functions:

- High-performance routing
- Dependent LU requester

High-Performance Routing (HPR): Personal Communications supports high-performance routing (HPR) over token-ring and Ethernet connections, which increases data routing performance and reliability. HPR supports the rapid transport protocol to provide nondisruptive rerouting around network outages, efficient selective retransmission, and end-to-end data integrity and congestion control.

Dependent LU Requester (DLUR): DLUR allows dependent LUs (LU 0, 1, 2, 3, and dependent LU 6.2) to benefit from an APPN network. It supports dynamic and multiple paths through the network and eliminates the need for dependent LUs (or their gateway) to be adjacent to the VTAM® host.

A DLUR is an APPN end node or network node that owns dependent LUs, but requests that a dependent LU server (DLUS) provide the system services control point (SSCP) for those dependent LUs. A DLUS controls conversion from a subarea environment to an APPN environment, allowing you to maintain central management of remote dependent LUs while benefiting from an APPN network.

Personal Communications uses the support in VTAM V4R2 for dependent LUs through APPN networks and combined subarea and APPN networks. The dependent LU server function (in VTAM) provides dependent secondarylogical unit (SLU) support by establishing an LU 6.2 session between a dependent LU requester node (DLUR), and a dependent LU server node (DLUS).

See “Appendix B. SNA Client/Server Concepts” on page 91 for more information.

AnyNet

AnyNet allows any application to communicate over any networking protocol and to extend the reach of applications over multiple networks. Using AnyNet function, you can reduce the number of installed network protocols and reduce operational complexity without modifying your existing applications or hardware. Personal Communications includes AnyNet SNA over TCP/IP support, which allows SNA emulator and client/server applications to communicate over a TCP/IP network.

Note: This function is not available for Windows 2000.

See “Appendix C. AnyNet SNA over TCP/IP” on page 99 for more information.

Enterprise Extender (HPR over IP)

Enterprise Extender allows you to extend the reach of SNA applications and data to include IP networks and IP-attached clients with similar levels of reliability, scalability, and control as SNA users. Enterprise Extender integration uses standard IP technology and does not require new hardware or software in the IP backbone.

Enterprise Extender is a simple set of extensions to the existing HPR technology, and provides the following:

- Non-disruptive backup from desktop to host
- SNA transport over native IP network
- End-to-end failure protection
- End-to-end data prioritization
- Scalable and cost-effective connectivity

ActiveX/OLE 2.0 Support

Personal Communications Version 5.5 sessions can now be included as part of a compound document. A compound document is a document that appears to be a single unit, but which is in fact made up of information from more than one program. For example, a compound document could include data that allows Personal Communications to execute within the context of the spreadsheet program.

When included as part of another program, Personal Communications is known as an embedded or linked object and the program is known as a container. Personal Communications supports ActiveX/OLE 2.0–compliant containers such as Lotus Notes®, Lotus® WordPro, and Microsoft Word. For most containers you can embed an object by using a menu sequence (for example, in Microsoft Word, use **Insert**, then **Object**), or by dragging and dropping a workstation profile into the document.

As an embedded object, Personal Communications can change its appearance to be part of the container program, providing the container program allows this change to occur. Or, Personal Communications can be started so that it runs in its own separate window utilizing its own profile and screen displays.

There is a variety of ways that Personal Communications can be activated as an embedded object. For example, Personal Communications can be shown as an icon within another program, and be activated by double-clicking. Another way Personal Communications can be activated is through a script; Visual Basic or LotusScript are examples of scripting languages supported by Personal Communications, but any ActiveX/OLE automation scripting language can be used.

The use of scripts allows Personal Communications to be activated as a part of an automation request. For example, a script can be written to automatically start Personal Communications every time the container object is started, or a script can be used to automatically put data on host entry screens.

The Personal Communications session ends when the container is closed or when you close the Personal Communications window. If Personal Communications was actuated as a linked object, it must be closed separately.

Object-Oriented API

Personal Communications provides a new language-independent object-oriented API. There are seven objects that can be used in conjunction with Visual Basic, Lotus Script, or any ActiveX/OLE automation scripting language to produce compound documents where Personal Communications is an embedded object within another program.

If you are interested in writing an application that includes Personal Communications as an object within your ActiveX/OLE 2.0 compliant program, refer to the *Host Access Class Library* (HACL) programming manual. This manual describes the objects that Personal Communications provides and describes what you need to do to access the Personal Communications data. Information is provided for programmers using Visual Basic scripts, Lotus scripts, and the C++ programming language. Samples of Visual Basic and Lotus scripts are provided on the Personal Communications CD-ROM.

Part 2. Planning for and Installing Personal Communications Access Feature

Chapter 2. Planning to Install Personal Communications Access Feature

This chapter describes the companion products provided with Personal Communications Access Feature and topics that should be considered before installing Personal Communications Access Feature Version 5.5.

Companion Products

The following companion products are included with Personal Communications Version 5.5.

Adobe Acrobat Reader

Acrobat Reader allows you to view, navigate, and print the online books in the Personal Communications library. If you choose to view the documentation, Adobe Acrobat Reader is automatically installed onto your system. You can view the documentation for Personal Communications directly from the CD-ROM or through the Install Manager welcome panel using Adobe Acrobat Reader.

Notes:

1. As appropriate and available, national language versions of the Adobe Acrobat Reader program are included.
2. The English-language version is also included; it can be used for those languages not directly supported by the national language versions. It is also used to display documents which are chosen for viewing during the install process.

DB2 Connect for Personal Communications

DB2 Connect for Personal Communications provides access to host databases in a cost-effective way by implementing a standard architecture for managing distributed data, known as Distributed Relational Database Architecture™ (DRDA®). Use of DRDA allows your applications to establish a fast connection to MVS/ESA™ and AS/400® databases without expensive host components or proprietary gateways. DB2 Connect for Personal Communications is a member of the DB2® family of products, which includes relational database systems, middleware, and application development tools.

IBM DB2 Connect for Personal Communications enables applications on your workstation to directly access host databases stored on:

- DB2 for MVS/ESA
- DB2 for AS/400

If you require ODBC support, it is available on the IBM DB2 Connect CD-ROM included with your Personal Communications Access Feature Version 5.5 package. For information on installing DB2 Connect see "Chapter 4. Installing DB2 Connect for Personal Communications" on page 29.

Considerations Before Installing

The following sections describe topics that should be taken into consideration prior to installation of IBM Personal Communications Access Feature for Windows, Version 5.5

Migration Considerations

Personal Communications Access Feature Version 5.5 offers several migration options. To ensure that your session profiles, batch files, and other configuration information are migrated so you can use them with Version 5.5, see "Custom Installation" on page 23 and the details on automatic migration options at "Automatic Migration Options" on page 26.

Multi-Boot Environment Installation

If you want to install Personal Communications Access Feature into a Personal Communications subdirectory that was originally installed under another operating system, you must remove the previous version first. Failure to do this may cause unpredictable results, including not being able to run Personal Communications from either operating system.

National Language Support (NLS) Considerations

The products available on this CD-ROM vary depending on the language and country:

- A multiple language version supports the installation of up to nineteen languages at the same time.
- Single language versions:
  - Simplified Chinese
  - Traditional Chinese
  - Korean

This book describes the CD-ROM for the multiple language support version. Single–language version CD-ROMs contain the same products and support, with the following exceptions:

- There is no multiple language support
- There are no CM Mouse utility programs

Additionally, each package is enabled for Triple DES (168-bit) encryption.

For information on multiple language support directories and language codes, see "Appendix E. National Language Support (NLS) Abbreviations and Language Codes" on page 113.

National Language Support Font Files

Personal Communications Version 5.5 automatically installs font files for the following additional languages: Arabic, Belorussian, Cyrillic languages, Estonian, Greek, Hebrew, Laotian, Latin-2 Languages, Latvian, Lithuanian, Thai, Turkish, Ukranian and Vietnamese. In releases prior to Version 5.0, you had to explicitly select which additional font file support you required.

Personal Communications Client Installation

Personal Communications supports the following SNA protocol stacks:

- IBM Communications Server
- IBM Communications Server Client
- NetWare for SAA
- Microsoft SNA

The installation process detects if any of the SNA protocol stacks listed above are installed on your system. If any of the listed SNA protocol stacks are detected, then Personal Communications installs the client version of these SNA protocol stacks.

If you plan to install the Communications Server, API client for NetWare for SAA, IBM Communications Server for Windows, or Microsoft SNA clients, install them prior to installing Personal Communications. If you already have Personal Communications installed on your machine and decide you want to install these products, you must first remove Personal Communications.

If you first install one of the listed SNA communications stacks, and then choose to uninstall any of them, Personal Communications will not work. In order for Personal Communications to work again, you must uninstall and reinstall Personal Communications.

Remote Installation Using Install Manager

If you plan to run Install Manager's setup.exe from a remote location, the location must be mapped to the network drive letter.

Windows 2000 Certification Considerations

In order to comply with Windows 2000 certification requirements, the following are included on the Personal Communications CD-ROM but are no longer automatically installed during installation of Personal Communications Version 5.5:

- Adobe Acrobat Reader (installed only through Install Manager)
- DB2 Connect (on a separate CD-ROM)
- Personal Communications documentation
- The hardware drivers listed in Table 1.

Table 1. Optionally Installed Hardware Drivers

IBM Adapter Names	**Windows 2000/NT Driver Names**
IBM 3270 Emulation adapters (PCI, ISA, PCMCIA, MicroChannel)	PCSCOAX.SYS
IBM 3270 Emulation adapters (ISA and MicroChannel only) used for 3174 Peer Communications (Lan-over-Coax)	XLNCOAX.SYS
IBM 5250 Emulation adapters (PCI, ISA, PCMCIA, MicroChannel)	PDLNATSN.SYS
IBM 5250 Emulation adapters (Asia-Pacific) (ISA, PCMCIA, MicroChannel)	PDLNATNM.SYS
IBM Wide Area Connector (WAC) adapters (ISA, MicroChannel)	PDLNAWAC.SYS
IBM Multiprotocol Adapters (PCI, ISA, MicroChannel) and IBM SDLC adapters (PCMCIA, ISA)	PDLNAMPA.SYS

Note: You are given the opportunity to install the hardware drivers from the Install Manager dialog. If you decide to install the drivers, you are notified that the driver you selected for installation is not certified for Windows 2000.

Chapter 3. Installing Personal Communications Access Feature

Personal Communications for Windows, Version 5.5 provides four installation options:

- Installation to a local hard drive, including installing to run from source, where source medium is a CD-ROM (see "Installing to a Local Hard Drive" on page 20)
- Administrative installation, including installing or running from source, where source medium is a network server (see "Chapter 5. Administrative Installation" on page 31)
- Remote installation using Microsoft Systems Management Server (SMS) (see "Chapter 8. Remote Installation of Personal Communications Access Feature" on page 41)
- Remote installation using Tivoli/Courier® or the IBMPCOMM Plus Module (for information about remote installation using Tivoli, refer to the *Administrator's Guide and Reference*).

Personal Communications also offers the ability to customize the installation procedure. For information on customizing with initialization file processing, including performing silent installations, see "Chapter 6. Customizing the Installation of Personal Communications Access Feature" on page 35.

This chapter describes the general installation procedure for all options and the specific procedure for installing to a local hard drive. Typical and custom setups are described in this chapter, as well as silent installation options. Additionally, this chapter provides an introduction to the Microsoft Windows Installer service.

Microsoft Windows Installer

Personal Communications utilizes the Windows Installer service, which is included with Windows 2000 and Windows Me. However, on Windows 95, Windows 98, and Windows NT® 4.0, you must install the Windows Installer service before installing Personal Communications. When the Personal Communications Access Feature CD-ROM is first run, it examines the target system and, if necessary, automatically installs the proper version of the Windows Installer service.

Setup.exe is the bootstrap loader that calls the Windows Installer service (msiexec.exe) and launches the installation dialogs. For a detailed description of the Microsoft Windows Installer service, refer to the Windows Installer SDK available online at http://www.msdn.microsoft.com. For more information on setup.exe, see "Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters" on page 109.

Note: The following should be taken into account when installing Personal Communications Access Feature:

- In some cases, installation of Windows Installer triggers a reboot of the system. If you are required to reboot, upon subsequent startup you are taken immediately back to Windows Installer to continue installation of Personal Communications.
- After Windows Installer has been successfully installed, if the installation of Personal Communications fails or is cancelled by the user, Windows

Installer rolls back all partially installed Personal Communications files and returns the system to its original state.

Note: Start menu icons from previous versions of Personal Communications are not rolled back if installation fails. If this occurs, Personal Communications start menu icons will no longer be available.

- You must be a member of the Administrator's group to perform these installations on Windows NT or Windows 2000.
- Before you begin installation, make sure all other applications are stopped. If you are reinstalling Personal Communications Access Feature or are upgrading Personal Communications Access Feature, make sure that Personal Communications is not running before you start setup.

Installing to a Local Hard Drive

To install Personal Communications Access Feature Version 5.5, begin by inserting the CD-ROM into your CD-ROM drive. If AutoPlay is on, inserting the CD-ROM automatically invokes the Install Manager welcome dialog.

Note: If AutoPlay is off, do the following:

1. Click **Run...** on the Windows **Start** menu.
2. Type

   ```
   E:\setup
   ```

   in the Command Line box (where E: is your CD-ROM drive).

From the Install Manager welcome dialog for Personal Communications, you can choose from the following options:

- **Install Product** invokes the Windows Installer service and begins the installation process.
- **View Documentation** allows you to view the books available in the Personal Communications Access Feature library and the Personal Communications Access Feature README file.
- **Visit Our Website** contains a link that takes you directly to the Personal Communications Web site.
- **Explore This CD** allows you to view the files contained on the CD-ROM.

To begin the installation of Personal Communications Access Feature select **Install Product** from the Install Manager welcome dialog.

After Install Manager determines your system configuration, the installation process begins.

1. The Windows Installer welcome dialog for Personal Communications Access Feature opens. Click **ReadMe** to open a window with the README text or click **Next** to continue.
2. The License Agreement dialog opens. Click the button to accept the terms of agreement. You can print the license agreement by clicking **Print**. If you decline the license agreement, the installation process terminates. Click **Next** to continue.
3. The Customer Information dialog opens. Type in your user name and organization information. Choose whether you want to install Personal

Communications Access Feature for use by all users that log on to the workstation or only for yourself. Click **Next** to continue.

4. The Setup Type dialog opens. You are given an option to choose a **Typical** or **Custom** installation. The following sections describe Typical and Custom installation choices.

Table 2. Application Data File Types

User Class		**System Class**	
Extension	**File Type**	**Extension**	**File Type**
.ws	Workstation Profile	.acg	SNA Configuration
.bch	Multiple Sessions	.mlg	Default Message Log
.ini	Session Size and Location	.trc	Unformatted Trace
.pmp	Popup-Keypad Configuration	.tlg	Formatted Trace
.kmp	Keyboard Configuration		
.srl	File Transfer List		
.ndc	AS/400 Connection Configuration		
.upr	AS/400 User Profile		
.tto	AS/400 Data Transfer Request (Receive)		
.tfr	AS/400 Data Transfer Request (Send)		
.bar	Toolbar Setup		
.mac	Macro		
.mmp	Mouse Setup		
.xlt	Translation Table		
.xld	DBCS Translation Table		
.cert	Certificate		
.sth	Password Stash		
.adu	Automatic Dial Utility		
.kdb	Certificate Management Database		
.der	Binary DER		

Typical Installation

Typical installation selects all default features for installation. Features are defined as the specific functions of a program. See "Feature Selection" on page 24 for a list of default features. You can customize Personal Communications Access Feature features by selecting the custom installation option (see "Custom Installation" on page 23).

By default, Typical is selected for installation. To proceed:

1. Click **Next**.
2. The Application Data Location dialog opens. Select from the following application data location options:

- User's application data folder ([UserProfile]\Application Data)
- All user's common application data folder (All Users\Application Data)
- Classic private directory

If the [UserProfile]\Application Data location is selected, the following profile paths are used:

Operating System	User Class Directory (Current User)	System Class Directory
Windows 95/98/Me	C:\Windows\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows 95/98/Me (user profiles enabled)	C:\Windows\Profiles\%USERNAME%\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows NT 4.0	C:\Winnt\Profiles\%USERNAME%\Application Data\IBM\Personal Communications	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications
Windows 2000	C:\Documents and Settings\%USERNAME%\Application Data\IBM\Personal Communications	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications

If the All Users\Application Data location is selected, the following profile paths are used:

Operating System	User Class Directory (Current User)	System Class Directory
Windows 95/98/Me	C:\Windows\All Users\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows 95/98/Me (user profiles enabled)	C:\Windows\All Users\Application Data\IBM\Personal Communications	C:\Windows\All Users\Application Data\IBM\Personal Communications
Windows NT 4.0	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications	C:\Winnt\Profiles\All Users\Application Data\IBM\Personal Communications
Windows 2000	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications	C:\Documents and Settings\All Users\Application Data\IBM\Personal Communications

Note: In Windows 95, 98 and Me, you have the option of enabling user profiles. A user profile is an account, maintained by the operating system, that keeps track of a particular user's files and system configuration. When a user logs on to the system, Windows is loaded with the logged-on user's files and system configuration settings in place.

In Windows NT, user profiles are always enabled.

If the classic Private directory location is selected, the following profile paths are used:

Operating System	User Class Directory (Current User)[1,2]	System Class Directory
Windows 95/98/Me	D:\Program Files\IBM\Personal Communications\Private	D:\Program Files\IBM\Personal Communications\Private
Windows 95/98/Me (user profiles enabled)	D:\Program Files\IBM\Personal Communications\Private	D:\Program Files\IBM\Personal Communications\Private
Windows NT 4.0	D:\Program Files\IBM\Personal Communications\Private	D:\Program Files\IBM\Personal Communications\Private
Windows 2000	D:\ Program Files\IBM\Personal Communications\Private	D:\ Program Files\IBM\Personal Communications\Private
[1]If the User Preference Manager (UPM) was set to a directory other than the default directory, Personal Communications will utilize that directory to store the user–class files. System–class files are always stored in the Private directory. [2]For the classic Private directory locations, D:\Program Files\IBM\ Personal Communications is the drive where Personal Communications is installed.		

After selecting your application data location, click **Next** to continue with the installation.

3. The Ready to Install the Program dialog opens. Click **Back** to change your previous settings, or click **Cancel** to terminate the installation process. Click **Install** to continue with installation.

The typical setup uses the following directory for program installation:

```
C:\Program Files\IBM\Personal Communications
```

Note: If there is not enough disk space on the C: drive, you are prompted to choose the custom installation setup type in order to choose an alternate installation destination.

After installation is complete, the Installation Complete dialog opens and you are given the opportunity to launch the registration tool. Click **Finish** to exit the installation process.

After installation is complete, you are prompted to reboot your computer. You must reboot your computer before configuration changes take effect and you can use Personal Communications.

Notes:

1. **Typical** installs the most common features for the applicable emulators.
2. **Typical** does not include CM Mouse or API sample programs.

Custom Installation

Though the default feature selection for a custom setup is the same as for a typical setup, a custom configuration allows you to modify feature selection for your system. To continue with the custom installation setup:

1. Click the button to choose **Custom** setup type. Click **Next** to continue.

2. The Custom setup dialog opens and asks you to select the program features that you want to install. Some features have subfeatures available. To view the subfeatures for a particular feature, click the plus sign (+) to the left of the feature name.

   Included in the Custom Setup window are **Feature Descriptions**. You can view the description of any feature by clicking on that feature and then reading the description section to the right of the feature selection tree. The feature description gives basic information about each feature, as well as the disk space required for installation. For more detailed information on disk space requirements for each feature, click the **Disk Space** button. For a description of available features, see "Feature Selection". For a description of feature installation options, see "Feature Installation Options" on page 25.
3. From the Custom Setup dialog, you can change the directory where Personal Communications is installed. Click the **Change** button to choose another installation directory.

   Note: If you have an earlier version of Personal Communications installed and you install Version 5.5 to a different directory, Personal Communications configuration files are moved to the new directory location upon reboot.
4. After making your feature selection choices and confirming your installation directory, click **Next** to continue with the installation.

   Note: If there is not enough space on the destination drive, you are prompted to choose another location.
5. The Application Data Location dialog opens. Select from the following application data location options:
   - User's application data folder ([UserProfile]\Application Data)
   - All user's common application data folder (All Users\Application Data)
   - Classic private directory

   See "Typical Installation" on page 21 for information on the profile paths used for each application data location. Click **Next** to continue.
6. The Automatic Migration Options dialog opens. By default, the **Automatic Migration of Profiles** box is checked. If you clear this check box, no migration occurs. The migration choices that are available to you are based on the information that you provided in the Application Data Location dialog. For information on the Application Data Location dialog, see "Installing to a Local Hard Drive" on page 20.

   By default, the highest level of migration available for your application data location is selected. This is the recommended level of migration for your configuration. You can proceed with the installation using the default migration option, or you can choose another level of migration. For a description of the different levels of migration available for each Application Data Location, see "Automatic Migration Options" on page 26.

   Click **Next** to continue with the installation.
7. The Ready to Install dialog opens. Click **Install** to complete the installation.

Feature Selection

The features and subfeatures available for Personal Communications Access Feature are described in Table 3 on page 25. This table also identifies which features are installed by default.

Note: In the custom setup window, if the icon to the left of the feature name is white, that feature and all of its subfeatures will be installed. If the icon appears grey, that feature or one or more of its subfeatures will not be installed.

Table 3. Feature Selection Tree Contents

Feature	Description	Subfeatures Available	Default
Secure Sockets Layer	Allows encryption and authentication customization.	**Certificate Management** **Certificate Wizard**	Yes
IBM SNA Protocols	This feature includes the APPC and CPI-C programming interfaces, and the device drivers that let you use SNA communications.	**AnyNet SNA over TCP/IP**	Yes
Languages	By default, the system default language locale and English are installed. You can select other languages for installation here. **Note:** By default, English is always installed and cannot be deselected.	See list of languages supported in "Appendix E. National Language Support (NLS) Abbreviations and Language Codes" on page 113.	Only the system default language locale and English are default.
Common Utilities	Optional product utilities that can be installed.	• **Convert Macro** • **DOS EHLLAPI** • **Multiple Sessions** • **Menu Bar Customization Utility**	All but **Multiple Sessions** are installed by default.

Note: If you want to make any of the following attachments, you must install **IBM SNA Protocols**. However, if another SNA protocol stack is already installed on your machine, this feature is hidden and not available for installation.

- LAN via IEEE 802.2
- APPC 3270
- 3270 via AS/400 (3270 Passthru)
- Microsoft SNA client over FMI
- SDLC
- SNA over Async
- IBM Global Network SNA-over-Async
- Hayes AutoSync
- AnyNet SNA over TCP/IP
- Dependent Logical Unit Requester (DLUR)
- Twinaxial Data Link Control (APPC)
- Twinaxial Data Link Control (Console)
- 3174 Peer Communication (LAN over Coax)

Feature Installation Options

Each feature and subfeature allows several installation options. To view the options available for each feature, click on the drop down icon to the left of the feature name. Select your desired installation type by clicking on it in the drop down menu. A description of each possible installation option follows:

- **This feature will be installed on local hard drive** selects this feature for installation to your local hard drive.
- **This feature, and all subfeatures, will be installed on local hard drive** selects the main feature and all of its associated subfeatures to be installed on the local hard drive.
- **This feature will be installed to run from CD** selects the feature to run from source where source medium is the CD-ROM at the local workstation. This installation option installs only the base files needed to run the feature.

  Note: If you are installing from a network, this option instead displays as, **This feature will be installed to run from network**. For more information on running from a network server, see "Installing to Run from Source, Where Source Medium Is a Network Server" on page 32.
- **This feature, and all subfeatures, will be installed to run from the CD** selects the main feature and all associated subfeatures to run from source where source medium is CD-ROM at the local workstation. This installation option installs only the base files needed to run the features.

  Note: If you are installing from a network, this option instead displays as, **This feature, and all subfeatures, will be installed to run from the network**. For more information on running from a network server, see "Installing to Run from Source, Where Source Medium Is a Network Server" on page 32.
- **This feature will be installed when required** places a shortcut on the Personal Communications menu allowing the feature to be installed when the shortcut is selected. This installation option is also called *advertisement*.

  Note: Advertisement is not available on Windows 95 and versions of Windows NT 4 that utilize a version of shell32.dll that is older than 4.72.3110.0.
- **This feature will not be available** deselects the feature for installation or advertisement.

Note: If no installation choice is made, features are installed to the local hard drive.

Automatic Migration Options

Personal Communications Access Feature Version 5.5 allows you to customize the automatic migration process when updating from previous versions of Personal Communications. All profile references are updated to the current path for profiles that are moved during automatic migration. There are three general levels of migration that are available to you:

- **Level 1** migrates desktop icons only.

  Note: Start menu icons from previous versions of Personal Communications are removed during the installation of Personal Communications Version 5.5. You can use the Start or Configure Sessions icon to start sessions. For more information on starting or configuring a session, refer to *Quick Beginnings*.
- **Level 2** migrates system-class profiles and desktop icons. Also migrates user-class profiles when migrating profiles to either All Users or the classic Private directory. System-class profiles have the following file extensions:

  - ACG
  - MLG
  - TLG
  - TRC

- **Level 3** migrates user-class profiles, system-class profiles, and desktop icons. User-class profiles have the following file extensions:
  - BAR
  - BCH
  - CAE
  - CERT
  - CLASS
  - DER
  - INI
  - KBD
  - KMP
  - MAC
  - MMP
  - NDC
  - PMP
  - SRL
  - STH
  - TTO
  - UPR
  - WS
  - XLD
  - XLT

Based on the information provided in the Application Data Location dialog, a Level 3 migration may not be available. The highest level of migration available, based on your application data location, is the recommended level of migration. A description of how the migration levels function for each data location is provided in the following sections.

Note: If an administrator performs a remote installation, some migration does not occur until users log on to the workstations.

Migration to [UserProfile]\Application Data Directory

If you have chosen to migrate your profiles from your previous profile directory to the [UserProfile]\Application Data directory, migration levels 1, 2, and 3 are available to you. The migration levels function as follows:

Level 1

Desktop icons are migrated. This is the lowest level of migration.

Level 2

- Desktop icons are migrated.
- System-class profiles are migrated from the previous profile directory to the All Users\Application Data directory.

Level 3 (Recommended)

- Desktop icons are migrated.
- System-class profiles are migrated.
- User-class profiles are migrated from the previous profile directory to the [UserProfile]\Application Data directory. As each new user logs on to the workstation, the user-class profiles associated with that user are migrated until all user-class profiles are copied into the [UserProfile] directory.

Migration to All Users\Application Data Directory

If you have chosen to migrate your profiles from your previous profile directory to the All Users\Application Data directory, migration levels 1 and 2 are available to you. The migration levels function as follows:

Level 1

Desktop icons are migrated. This is the lowest level of migration.

Level 2 (Recommended)

- Desktop icons are migrated.
- All system-class and user-class profiles are migrated from the previous profile directory to the All Users\Application Data directory. As each new user logs on to the workstation, the user-class profiles associated with that user are migrated into the All Users\Application Data directory.

Migration to Private Directory

If you have chosen to migrate your profiles from your previous profile directory to the private directory which under the installed directory, migration levels 1 and 2 are available to you. The migration levels function as follows:

Level 1

Desktop icons are migrated. This is the lowest level of migration.

Level 2 (Recommended)

- Desktop icons are migrated.
- All system-class and user-class profiles are migrated from the previous private profile directory to the private directory. As each new user logs on to the workstation, any user-class profiles associated with that user, set by the User Preference Manager, are migrated in place.

Silent Installation

Personal Communications Access Feature is installed silently by passing command-line parameters through setup.exe to the MSI (Windows Installer database) package. When running a silent installation, the user does not provide input via dialogs or see a progress bar during the installation process. Instead, installation occurs automatically using either a typical configuration or a custom configuration created during initialization file processing.

For details on initialization file processing, see “Initialization File Processing Using Windows Installer” on page 35. For information on performing a silent installation using setup.exe command-line parameters, see “Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters” on page 109.

Chapter 4. Installing DB2 Connect for Personal Communications

IBM DB2 Connect for Personal Communications enables applications on your workstation to directly access host databases stored on:

- DB2 for MVS/ESA
- DB2 for AS/400

To install DB2 Connect, insert the IBM DB2 Connect CD-ROM into your CD-ROM drive. If AutoPlay is on, inserting the CD-ROM automatically invokes the Install Manager welcome dialog.

Note: If AutoPlay is off, do the following:

1. Click **Run...** on the Windows **Start** menu.
2. Type

   ```
   E:\welcome.exe
   ```

   in the command-line box (where E: is your CD-ROM drive).

From the Install Manager welcome dialog for DB2 Connect, you can choose from the following options:

- **Quick Install DB2 Connect** begins the installation process.
- **Read Information** opens a ReadMe text document containing information about how DB2 Connect and Personal Communications Version 5.5 work together.
- **Visit Our Website** contains a link to take you directly to the Personal Communications Web site.
- **Explore the DB2 CD** allows you to view the files contained on the CD-ROM.

Note: Selecting Quick Install allows the user to choose a target destination for installation and then completes the installation without further user input.

Silent Installation of DB2 Connect

DB2 Connect allows users to perform silent installations using a generated response file. To complete a silent installation, begin by installing DB2 to your system hard drive using the **Quick Install DB2 Connect** function.

Once the initial installation is completed successfully, a response (.rsp) file containing the settings appropriate for your system is automatically saved in the Temp directory of your C: drive. This response file allows future installations to be completed without requiring user input through dialogs. To install DB2 Connect silently, type:

```
E:\DB2\Common\Wininst.exe /U C:\Windows\Temp\DB2conpe.rsp /i EN
```

at the command prompt where E: is your CD-ROM drive. The default response file, DB2conpe.rsp, silently installs a DB2 Connect Personal Edition configuration to your system. The /i parameter designates an English configuration.

For detailed information on performing distributed installations of DB2 Connect, including customizing response files for distribution, and information on performing installations using systems management software, refer to the *IBM DB2 Universal Database and DB2 Connect Installation and Configuration Supplement Version 7*. This document is available in the online library at http://www.ibm.com/software/data/db2/.

Chapter 5. Administrative Installation

An administrative installation copies a source image of Personal Communications Access Feature installation files onto a network drive. The resulting location of this source image is called the installation point. After you complete an administrative installation, any user connected to the network can install Personal Communications Access Feature to their own workstation by pointing to the installation point and running the setup. An administrative installation offers two installation choices to users:

- Installation directly to their system from the network server
- Installation to run from the network server

In order for you to take full advantage of an administrative installation, Personal Communications Access Feature is enabled to run from source. This permits administrators to leave only a minimal footprint on the users machine by allowing users to run program features directly from the network server.

Note: An administrative installation must be completed prior to installing and running Personal Communications Access Feature from source, where the source medium is a network server.

To begin an administrative installation, disable the AutoPlay function on your system or simply close the Personal Communications welcome window when it opens. With the CD-ROM in the CD-ROM drive:

1. Open your command prompt and switch to the Personal Communications installation directory by typing

   ```
   E:\install\pcomm
   ```

   at the command prompt (where E: is your CD-ROM drive).
2. From this directory, type

   ```
   setup.exe /a
   ```
3. The Windows Installer welcome dialog for Personal Communications Access Feature opens. Click **Next** to continue with the installation.
4. The License Agreement dialog opens. Click the button to accept the terms of agreement. You can print the license agreement by clicking **Print**. If you decline the license agreement, the installation process terminates. Click **Next** to continue.

   Note: Windows NT and Windows 2000 administrators have the option to accept the license agreement on behalf of all users. This allows users who install Personal Communications from the network server to skip the license agreement window during installation.
5. The Network Location dialog opens. You can type the desired network installation point in the command line or click **Change** to browse for a location.
6. Click **Install** to complete the installation process.

Note: To remove the source image of Personal Communications Access Feature from your network server you must manually delete the source image directory from the network location.

Installing from Network Server

After the administrative installation is complete, any user connected to the network can install Personal Communications Access Feature from the network server. To install from the network server:

1. Click **Run...** on the Windows **Start** menu.
2. Type

   ```
   X:\MyLocation\setup.exe
   ```

   in the command line (where X: is your network server and MyLocation is the installation point designated in the administrative installation) or click **Browse** to browse for the location on the network.
3. The Windows Installer welcome dialog opens. Proceed with the installation as described in "Installing to a Local Hard Drive" on page 20.

Installing to Run from Source, Where Source Medium Is a Network Server

After the administrative installation is complete, any user connected to the network can install Personal Communications Access Feature to their workstation and designate any available features to run from source, where source medium is a network server (see "Feature Selection" on page 24 for a description of available features). In this scenario, feature shortcuts are placed on the Personal Communications Access Feature menu but are not installed to the local hard drive. To install and run from the network server:

1. Click **Run...** on the Windows **Start** menu.
2. Type

   ```
   X:\MyLocation\setup.exe
   ```

   in the command line (where X: is your network server and MyLocation is the installation point designated in the administrative installation) or click **Browse** to browse for the location on the network.
3. The Windows Installer welcome dialog opens. Proceed with the installation as described in "Installing to a Local Hard Drive" on page 20, selecting **Custom** as your setup type.
4. In the Feature Selection dialog, click on the icon to the right of a desired feature to view its available installation options.
5. To select the feature to run from the network server, click on one of the following two options:
   - **This feature will be installed to run from network** to select a single feature to run from the network.
   - **This feature, and all subfeatures, will be installed to run from the network** to select the feature and all of its associated subfeatures to run from the network.
6. After making feature selection choices, proceed with the installation as described in "Custom Installation" on page 23.

Installing Patches

You can administratively install corrective patches to Personal Communications Access Feature for later distribution using Windows Installer command-line parameters. In some instances, it may be necessary to reinstall Personal Communications after the application of a patch. For more information on installing patches to Personal Communications, refer to the *Administrator's Guide and Reference*. For more information on using Windows Installer command-line parameters to install patches, refer to the Microsoft Windows Installer SDK at http://www.msdn.microsoft.com.

Chapter 6. Customizing the Installation of Personal Communications Access Feature

Personal Communications Access Feature provides two methods of customizing installation processes:

- Initialization file processing
- Transform file processing

Through customization, administrators determine what features and settings are available for users to install based on initialization files or transform files. Once customization has been completed, users silently install Personal Communications Access Feature on their workstations with the predetermined settings.

Note: Previous versions of Personal Communications Access Feature used response files for customization and silent installation. However, in Personal Communications Access Feature Version 5.5, the term *initialization file* is used to refer to the .ini files which are used for customization and silent installation procedures.

If you want to use transform files for customization, refer to http://www.msdn.microsoft.com for more information and specific usage examples.

Initialization File Processing Using Windows Installer

Personal Communications Access Feature provides an optional method of customization that allows property values and feature installation choices made during one installation to be automatically applied during subsequent installations. The initialization file (.ini) contains the properties and options for Windows Installer to use as initialization choices so that subsequent installations do not require users to provide installation input using dialogs. Then, future installations can be set to run silently using an initialization file.

Administrators create, save, and implement initialization files using command-line parameters. Personal Communications Access Feature provides four command-line parameters:

- SAVEINI
- ONLYINI
- USEINI
- REMOVEINI

Each parameter, with a corresponding usage description, is described in the following sections.

Two sample initialization files are included on the Personal Communications Access Feature CD-ROM. These sample initialization files can be used during your installation if your workstation configuration matches the definitions in the sample. Personal Communications Access Feature Version 5.5 includes the following sample .ini files:

- **typical.ini** installs a typical setup

- **custom.ini** installs a custom setup to a user-defined path and includes the installation of French in addition to English

The samples are defined for a first-time installation of Personal Communications. If you already have Personal Communications, AnyNet, Microsoft SNA Server, Communications Server for Windows NT, or NetWare for SAA previously installed, the samples will not work; you will need to create a unique initialization file to match your workstation.

Note: To ensure successful initialization file processing, use all syntax exactly as described.

Parameter Descriptions

SAVEINI

This parameter designates an initialization file to be created and installs Personal Communications. To create an initialization file without installing Personal Communications, see the description of the command-line parameter “ONLYINI” on page 37. The .ini file that is saved contains property values and feature installation choices that can be passed on to future installations of Personal Communications. By default, the .ini file is not removed when Personal Communications is uninstalled. The following command creates the .ini file and installs Personal Communications:

Syntax

```
E:\install\pcomm\setup.exe /v"SAVEINI=\"C:\Personal Communications\pcomm.ini""
```

where E: is your CD-ROM drive and your .ini is saved in the Personal Communications folder.

Note: Parameters are passed through setup.exe to the MSI (Windows Installer database) package using the /v command-line parameter. Within the /v″...″ argument, you can specify parameters such as SAVEINI, ONLYINI, and USEINI which all take a file path. If a path containing spaces is specified, it must be quoted and preceded by a backslash within the /v″...″ argument as indicated in “Syntax”. For more information on the /v command-line parameter, see “Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters” on page 109.

Usage Description

An administrator creates an initialization file by using the SAVEINI command-line parameter and running either a typical or custom Windows Installer service installation for Personal Communications (see “Installing to a Local Hard Drive” on page 20). Upon completion of the installation, the .ini file containing all of the property values and feature installation choices designated during the custom setup is saved in the directory specified in the SAVEINI parameter.

Note: Based on the information provided in the Customer Information dialog during setup, the default .ini is saved in either the All Users\Application Data or the [UserProfile]\Application Data directory. For more information on the Customer Information dialog, see “Installing to a Local Hard Drive” on page 20.

ONLYINI

This parameter designates that a .ini be created without installing Personal Communications. Upon completion of the custom setup, Windows Installer prompts you to exit the installation program without installing Personal Communications.

Syntax

```
E:\install\pcomm\setup.exe /v"SAVEINI=\"C:\Personal Communications\pcomm.ini" ONLYINI=1"
```

where E: is your CD-ROM drive and your .ini is saved in the Personal Communications folder.

Usage Description

An administrator can use this parameter to create several unique .ini files to meet the needs of different types of users without performing an installation each time an initialization file is created.

Note: The SAVEINI and ONLYINI parameters can be used to create a .ini file for either a custom or typical installation. If using ONLYINI, installation of Personal Communications is always suppressed after creating the .ini file regardless of installation choice.

USEINI

This parameter designates that a previously created .ini file be used to determine property values and feature installation choices for a current installation.

Syntax

```
E:\install\pcomm\setup.exe /v"USEINI=\"C:\Personal Communications\pcomm.ini""
```

where E: is your CD-ROM drive and pcomm.ini is the initialization file you wish to designate.

Usage Description

In order to apply the initialization file you created using SAVEINI, or one of the sample initialization files included with Personal Communications, you must use the USEINI command-line parameter. USEINI can be used to run either a typical or custom installation for Personal Communications (see “Custom Installation” on page 23). If you choose custom setup, all property values and feature installation options designated in the specified initialization file are selected for installation.

Note: Unless installation is set to run silently, users can override values designated in the .ini file by running either a custom or typical installation setup. Any changes made during setup will alter the .ini for future installations. See “Silent Installation Using Initialization File Processing” on page 38 for details on running a silent installation.

Though you can specify a particular initialization file to be applied with the USEINI parameter, use of initialization files is not required for remote installations. If no initialization file is specified during a remote installation, a typical installation results.

REMOVEINI

This parameter designates that the .ini be removed when Personal Communications is uninstalled from the system. If this parameter is not set or if any value other than that designated in the syntax is used, the initialization file remains on the system after Personal Communications has been removed.

Syntax

```
E:\install\pcomm\setup.exe /v"REMOVEINI=1"
```

where E: is your CD-ROM drive.

Usage Description

This parameter can be used at any time after you have created the .ini file. It removes the .ini when Personal Communications is uninstalled from the system. The .ini is only removed if the occurrence of Personal Communications that is being uninstalled was originally installed using the .ini that is designated for removal.

Silent Installation Using Initialization File Processing

In order to ensure that property values and feature installation options designated in the initialization file are not overridden by users or to enhance the ease of installation, you can apply initialization files during silent installations.

To perform a silent installation using initialization file processing, type the following command:

```
E:\install\pcomm\setup.exe /v"USEINI=\"C:\Personal Communications\pcomm.ini" /qn"
```

This process passes the silent installation command-line parameter (/qn) through setup.exe to the MSI package. For more information about setup.exe command-line parameters, see "Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters" on page 109.

Chapter 7. Maintenance Installation of Personal Communications Access Feature

After you have successfully installed Personal Communications on your system, users can perform maintenance installations to their Personal Communications program. The maintenance installation utility has three functions:

- **Modify** allows users to change their feature selection options. For details on changing feature tree selections, see "Feature Selection" on page 24.
- **Repair** analyzes the current configuration of Personal Communications and either repairs or reinstalls damaged features.
- **Remove** allows users to remove Personal Communications from their system.

  Notes:

  1. When removing Personal Communications from your system, you are given the option to save the current program configuration for future installations of Personal Communications. If you choose to save the current settings, when you reinstall Personal Communications you are asked if you would like to use the previous settings to reinstall the product.
  2. To remove a source image of Personal Communications created during an administrative installation, you must manually delete the source image directory from your network drive.

After Personal Communications is successfully installed on your system, you can access maintenance installation through **Add/Remove Programs** from the Windows **Control Panel**. Select **Personal Communications** from the list of installed programs and click **Change** (for Windows 2000 operating systems) or **Add/Remove** (for all other supported Windows operating systems) to begin maintenance installation.

When the **Program Maintenance** dialog opens, select **Modify**, **Repair**, or **Remove** and click **Next**.

Note: To successfully run maintenance installation, the Personal Communications installation image must be available on either the CD-ROM or on the network server. If you installed from a network server, the installation image must still be present at the original network location. If the installation image is not present, when you use the Modify or Remove utility to add features or to remove Personal Communications from your system, you may receive one of the following error messages:

- The feature you are trying to use is on a CD-ROM or other removable disk that is not available.
- The feature you are trying to use is on a network resource that is not available.

To continue with maintenance installation you must either insert the CD-ROM or browse the network to find the new location of the installation image.

Chapter 8. Remote Installation of Personal Communications Access Feature

Personal Communications Access Feature supports remote installation using either Tivoli/Courier or Microsoft Systems Management Server (SMS) 2.0 Service Pack 2, or higher. Remote installation and uninstallation can be performed in a normal mode (attended) or silent mode (unattended).

Remote Installation Using Tivoli/Courier

For details on installing Personal Communications using Tivoli/Courier, refer to the *Administrator's Guide and Reference*.

Remote Installation Using SMS

A remote installation using SMS consists of the following steps:

1. Perform an administrative installation to copy Personal Communications Access Feature installation files to the network (see "Chapter 5. Administrative Installation" on page 31).
2. Create an SMS package containing the Personal Communications Access Feature installation software.
3. Create an SMS job to distribute and install the software package.

Note: Personal Communications Access Feature provides a sample SMS file, IBM Personal Communications.sms, for use in creating the SMS package. You can also create your own SMS file. An SMS file is the same as a Package Definition File (PDF) used in previous versions of Microsoft SMS.

For detailed and up-to-date instructions on installing and deploying Personal Communications Access Feature using SMS, refer to the SMS product documentation provided at http://www.microsoft.com/smsmgmt.

Part 3. Using Personal Communications Access Feature

Chapter 9. Enabling Client/Server Applications

Personal Communications support for APPN end nodes lets you take advantage of APPN networks. An APPN network allows automatic locating of partner applications and dynamic, optimized route selection. These features allow workstations to communicate more flexibly with other systems in the network.

Personal Communications also provides support for 32-bit APPC and CPI-C application programming interfaces (APIs), which provide convenient ways for 32-bit client application programs on your workstation to communicate with those on other workstations.

Configuring a Node

Before you can take advantage of the client APIs and communicate with other application programs, you first need to configure Personal Communications as an SNA end node.

To configure the SNA node:

1. From the **Start** menu, click **Programs** → **IBM Personal Communications** → **SNA Node Configuration**.

   The Personal Communications SNA Node Configuration window appears.
2. Select the necessary Configuration Options in the order listed on the window.

   To select an option, click it and then click **New...**.

   For each option, enter the appropriate information on the property pages. Most required information is listed on the Basic page. Click **OK** to complete the option. Click **Help** for more information about the individual parameters.
3. Click **Save** or **Save As** from the File menu.
4. Type the file name and then click **Save**. Note that you can choose the file type and where to save this file. The default file type is .ACG and the default directory is the location specified in the User Preference Manager.
5. Click **Exit** from the File menu.

Tip

If you have more than one configuration file, you can apply additional configuration files to an active node. Refer to the help in the SNA Node Operations section of the product for details.

Starting the SNA Node

1. To start the SNA node, from the Start menu, click **Programs** → **IBM Personal Communications** → **SNA Node Configuration**.

   The Personal Communications SNA Node Operations window appears.
2. Click **Start Node...** from the Operations menu.

   The Select configuration file to use... window appears.
3. Double-click the configuration file (.ACG) that defines the node you want to start.

Note:

Another way to start the SNA node is to use the command line. The command to use is CSSTART. For the proper syntax see “Command-Line Utilities” on page 50.

Stopping the SNA Node

1. To stop the SNA node, from the Start menu, select:**Programs → IBM Personal Communications → Administrative and PD Aids → SNA Node Operations**.

   The Personal Communications SNA Node Operations window appears.
2. Click a resource in the Alias column.
3. Click **Stop Node...** from the Operations menu.

Note

Another way to stop the SNA node is to use the command line. The command to use is CSSTOP. For the proper syntax see “Command-Line Utilities” on page 50.

APING Requirements

If you wish to run the Check Connection (APING) utility provided with this package to an AS/400 running OS/400® V3R1, you must install PTF MF10808 on the AS/400 first. If this PTF is not installed, then errors with sense codes of 080F 6051 and 1008 201D will occur.

Chapter 10. SNA Node Operations

SNA Node Operations enable you to display information and manage the node for certain Personal Communications resources, which can be useful when operating the SNA node. The following tasks are supported:

- Starting and stopping resources
- Deleting resources
- Displaying resource information
- Changing session limits
- Initiating path switches

The configuration information for a SNA Node is stored in an ASCII file, with the extension .ACG. You can edit the file by launching SNA Node Configuration. To ensure that your new configuration is correct, use the Verification tool.

You can display information or take action on resources if you start 3270, 5250, or any client/server sessions with one of the following attachment types:

Client/Server Connections

LAN LAN via IEEE 802.2

Twinaxial
Twinaxial Data Link Control (APPC)

COM port
SNA-over-Async
Hayes AutoSync
X.25

SDLC Synchronous Data Link Control

IBM WAC
Synchronous Data Link Control
X.25

AnyNet SNA over TCP/IP
APPC

Enterprise Extender
HPR over IP

SNA resources that can be displayed or managed include the following:

Connection Networks
Allows APPN nodes in a LAN to have direct links with each other without requiring logical link definitions at each node.

Connections
Link stations to the adjacent nodes

CPI-C Side Information
Associate a set of parameters with a specified symbolic destination name.

Data Link Controls
How data is formatted for transmission on the physical connection.

Devices
Parts of the workstation hardware, such as adapters, that are used to transmit and receive data.

DLUR PUs
A dependent logical unit requester (DLUR) physical unit (PU) is a PU in

an APPN end node that owns dependent LUs, but requests that a dependent LU server provide the SSCP services for those dependent LUs.

Focal Points
A system that provides centralized network management services.

Local LU 0 to 3
A local logical unit (LU) type 0, 1, 2, or 3 is a dependent LU on the workstation that provides services for 3270 terminal and printer emulation applications.

Local LU 6.2
A local logical unit (LU) type 6.2 is an independent or dependent LU that provides APPC services.

LU 6.2 Sessions
Transports data between two partner LU 6.2s. Conversations between transaction programs use LU 6.2 sessions.

Mode The name used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length limits, sync point and cryptography options, and the class of service (COS) within the transport network.

Node The control point that manages the node and its associated resources. The local node provides APPN services.

Partner LU 6.2
A remote computer that communicates through an APPC session with local LU 6.2s.

RTP Connections
In high-performance routing (HPR), a rapid transport protocol (RTP) connection is the connection established between the endpoints of the route to transport session traffic.

Transaction Programs
A transaction program (TP) is a program that processes transactions in an SNA network. There are two kinds of TPs: application transaction programs and service transaction programs.

Starting Node Operations

To start Node Operations, click the **SNA Node Operations** icon in the Personal Communications folder.

Note: This utility can also be started using a command (see “Command-Line Utilities” on page 50).

Using the Menu Bar

From the menu bar of the SNA Node Operations utility, click one of the following:

Operations
To start or stop a SNA node.

To start a node, select the configuration file you want to use.

To change session limits (CNOS).

To apply a new configuration file, select the configuration file you want to use.

Launch
To launch to other Personal Communications programs, such as Log Viewer, Trace Facility, or SNA Node Configuration.

View To modify the layout of your Personal Communications window (Tool bar or Status bar).

To select resource attributes, which allows you to customize the display of SNA resource attributes.

To view frequently used resources, such as:
- Node
- Connections
- Local LU 0 to 3
- Partner LUs
- LU 6.2 sessions

Window
To modify the layout of your Personal Communications window.

Help To view the Personal Communications online help.

Displaying a Resource

To display a resource, select a resource from the pull-down list on the toolbar.

Starting a Resource

To start a resource:
1. Select a resource from the pull-down list on the toolbar.
2. Select the first column of the item, and right mouse click to display the pop-up menu.
3. Click **Start** to start the resource. A started (active) resource can be stopped, but not deleted.

Stopping a Resource

There are two ways of stopping a resource:

Normal Stop
Performs clean up and then stops the resource.

Abnormal Stop
Immediately stops the resource.

To stop a resource:
1. Select a resource from the pull-down list on the tool bar.
2. Select the first column of the item, and right mouse click to display the pop-up.
3. Select **Normal Stop** or **Abnormal Stop** to suspend the resource. If a resource is stopped (inactive), it can be deleted or redefined.

Deleting a Resource

To delete a resource:
1. Select a resource from the pull-down list on the tool bar.
2. Select the first column of the item, and right mouse click to display the pop-up.
3. Select **Delete** to delete the resource.

You should stop a resource (make it inactive) before redefining it. You do not need to delete the resource before redefining it.

Changing an HPR Path Switch

To perform a high performance routing (HPR) path switch:

1. Select **RTP connections** from the pull-down list on the tool bar.
2. Select the first column of the item, and right mouse click to display the pop-up.
3. Select **HPR path switch** to change the path for the data on this RTP connection.

Updating SNA Resources Dynamically

It is not necessary to delete an SNA resource before redefining it. A resource must be inactive, however, when you redefine it.

If a redefinition is rejected for a reason other than that the resource is active, a STATE_CHECK return code is returned as well as a specific secondary return code, as listed in the NOF specification. Most rejections are due to inconsistencies in the configuration, such as one of the following:

- Attempting to define an LS with the adjacent CP name set to the local CP name.
- Attempting to define two link stations on a non-switched port with the same destination address.

Such rejections occur regardless of whether you are defining a resource for the first time or redefining it.

Keep in mind the following when redefining resources:

- You may not change the ls_role of a port that has link stations defined on it. The link stations must be deleted before the port role can be changed (because an LS may default to the port ls_role).
- You may not change the type of a named DLC. The DLC definition must be deleted before the same name can be reused for a DLC of a different type.

Command-Line Utilities

Another way to perform SNA Node operations is to use the command line. Five command line programs are available to perform basic operations for the SNA Node.

CSSTART [-a | -d | -m | -h] [-p | -q] [cfgfile]

> Use the CSSTART command to start the SNA Node with a specified configuration. The -a flag enables automatic start up after rebooting the machine. The -d flag sets the default SNA node configuration file. The -m flag stands for manual start which disables automatic start up after rebooting the machine. If the -p flag is used, all messages are shown in a message box pop-up. Messages are written to stdout by default. The -q flag suppresses all output. The -h flag summons the help data for this command. The cfgfile parameter is the name of the configuration file you want to use to start the product. If no cfgfile parameter is specified, the default configuration file is used. If no default configuration file has been set, an error is reported. If the node is successfully started, CSSTART returns zero, otherwise a nonzero value is returned.

CSSTOP [-p | -q][-h]

Use the CSSTOP command to stop the SNA Node. The flags have the same meaning as for CSSTART. If the node is successfully stopped then CSSTOP returns zero, otherwise a nonzero value is returned.

CSQUERY [-p | -q][-h]

Use the CSQUERY command to query the status of the SNA Node. The flags have the same meaning as for CSSTART. Along with the status, the default and active configuration file names are shown. If the node is running, then CSQUERY returns zero; otherwise a nonzero value is returned.

CSDSPY {resource [object_id] [/D#]} | [-h]

Displays information about SNA node resources, where:

resource

One of the following:

AIL	AnyNet IP to LU mapping
CNT	Connection networks
CON	Connections
CPS	CPI-C side information
DLC	Data link controls
DEV	Devices
DPU	DLUR PUs
FPT	Focal Points
LU0	Local LU 0 to 3
L62	Local LU 6.2
L6S	LU 6.2 sessions
MOD	Modes
NOD	Nodes
PLU	Partner LU 6.2
RTP	RTP connections
TRP	Transaction programs

object_id

Specifies a case-sensitive value (for example, LU001 or LINK001) to search for. Only objects whose first attribute matches this value are displayed. The object_id must be spelled correctly, including case (upper and lower). An incorrect object_id will result in nothing being displayed.

/D# Specifies the level of detail to display. # is a number in the range 1 – 3, where 1 displays the least level of detail and 3 shows all information. The default is 2.

CSMODIFY {resource object_id action} | [-h]

Enables you to control SNA node resources, where:

resource

Is one of the following:

CON	Connections. You can start, stop, or delete this resource.

CPS CPI-C side information. You can delete this resource.

DLC Data link controls. You can start, stop, or delete this resource.

DEV Devices. You can start, stop, or delete this resource.

DPU DLUR DPUs. You can start or stop this resource.

LU0 Local LU 0 to 3. You can delete this resource unless the LU is in use.

L62 Local LU 6.2. You can delete this resource.

RTP RTP connections. You can switch the path of this resource.

object_id
Specifies a case-sensitive value (for example, LU001 or LINK001) to search for. Only objects whose first attribute matches this value are displayed. The object id must be spelled correctly, including case (upper and lower). An incorrect object id will result in an error being displayed.

action One of the following:

SN Normal stop

SI Immediate stop

ST Start

DL Delete

PS Path switch

[-h] This switch is used to summon help data for this command.

Chapter 11. Problem Analysis

This chapter describes the information that will help you analyze problems with Personal Communications Access Feature, and ways to report a problem to IBM.

For information about Personal Communications Access Feature and support, refer to the following Web sites:

- The Personal Communications home page provides access to general product information, and download services. To view this page, use an Internet browser and go to the following Internet address or Universal Resource Locator (URL):

  http://www.ibm.com/software/network/pcomm
- The Personal Communications support page provides links to code fixes, tips, newsgroups, support options, and services. To view this page or to submit a software defect report, use an Internet browser and go to the following Internet address:

  http://www.ibm.com/software/network/pcomm/support

Personal Communications provides several utilities to help you with problem analysis. They can be invoked by selecting their icons from the **Programs → IBM Personal Communications → Administrative and PD Aids** subfolder on the Windows **Start** menu.

The following sections describe these utilities and how to use them.

Log Viewer

The Personal Communications log viewer utility enables you to view, merge, sort, search, and filter information contained in message and trace logs. Use the log viewer during problem analysis to work with message and trace log entries. The default name of the message log output file is PCSMSG.MLG; its file extension must be .MLG. The file extension for trace logs must be .TLG.

To view message or trace logs:

1. From the Administrative and PD Aids subfolder, click **Log Viewer**.
2. From the list of logged messages, double-click a message to display the message text.

Trace Facility

The Personal Communications trace facility enables you to log trace information for certain Personal Communications functions.

To start a trace, perform the following steps:

1. From the **Administrative and PD Aids** folder, click **Trace Facility**. The trace status on the title bar displays the current state:

   Active Trace data is being collected by the trace facility.

   Inactive
   No trace data is being collected.
2. From the main dialog box, click **Set Up** to set the desired trace system parameters.

3. Click **OK** to return to the main trace dialog box.
4. From the main trace dialog box, select the type of data you want to trace from the **Function Name**, **Component Name**, and **Trace Option** list boxes.

   Function Name
   A specific set of Personal Communications features, such as 3270/5250 Emulator or User Services.

   Component Name
   The name of a specific part of a function, such as API data (for the 3270 Emulator function) or Node Initialization (for the User Services function).

   Trace Options
   The options associated with a particular component, such as EHLLAPI (for the API component) or API trace (for the Node Initialization component).
5. Start tracing data by clicking **Start**, or apply changes to the trace options by clicking **Apply**.
6. Run the operation that you want to trace.
7. Optionally, stop the trace by clicking **Stop**.
8. Save the trace data to your hard disk by clicking **Save**.
9. Click **Format** to specify a formatted trace file name and to format the trace data. The Information Bundler utility should be used immediately after the trace is complete to ensure that the correct information is gathered.

   Note: If you have changed the path for the formatted trace file, the Information Bundler will not find the trace information. Copy the trace files to the Personal Communications private subdirectory.
10. Click **OK**.
11. Click **Clear** to clear the trace buffer where you saved a trace.
12. Use the log viewer to view the formatted trace log.

Information Bundler

The Personal Communications Information Bundler utility gathers system files, trace and log files, and registry information and creates a self-extracting .EXE file. This .EXE file is sent to support personnel via FTP for problem resolution. This utility should be executed immediately after the trace is complete to ensure that the correct information is gathered. To use the information bundler utility:

1. From the **PD Aids** folder in the Personal Communications program group, double-click the **Information Bundler** icon.
2. A .EXE file containing system and Personal Communications information is created in the Personal Communications directory. By default this file is called 12345.EXE.

Internet Service

The Internet Service utility enables you to send the .EXE file containing diagnostic data collected by the Information Bundler to an FTP server. This utility will not work unless TCP/IP is configured and you have a direct connection to the internet. To use Internet Service:

1. Double-click the **Internet Service** icon located in the Personal Communications program group..

The Internet Service window contains four data fields that must have valid values before you can submit your problem report.

2. Verify that the FTP Address field contains the default address **testcase.software.ibm.com**. This is the service anonymous FTP server.
3. Type your e–mail address in the field provided.
4. In the Problem Determination Filename field, type the file name and path of the .EXE file created with the Information Bundler. This file is located in the Personal Communications installation directory.
5. In the PMR Number field, type the PMR number that you received as a result of contacting IBM support personnel.
6. When all fields in the window have been filled with valid values, click **Transmit** to submit your problem determination information.

Chapter 12. Configuring and Using SSL Security for Personal Communications

The purpose of basing communications on Secure Sockets Layer (SSL) is to provide privacy and integrity during communication over an unsecured TCP/IP connection between a client and a target server. This chapter briefly describes how to configure the Personal Communications client to use this mode.

Personal Communications provides several ways to manage certificates:

- "Using Certificate Wizard" on page 60
- "Using Certificate Management" on page 60
- "Using the Command-line Mode for Managing Certificates" on page 65

What is SSL?

SSL is an industry-standard protocol that provides X.509 certificate-based authentication and encryption for unsecured connections. Personal Communications supports client and server side certificate-issuer authentication and encryption of sessions in compliance with the SSL V3 standard. Server side certificate-issuer authentication means that the target server presents its X.509 certificate for the Personal Communications client to inspect for certificate-issuer authenticity before initiating an encrypted session.

SSL client authentication allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs. This confirmation might be important if the server, for example, is a bank sending confidential financial information to a customer; in that case it is important to check the recipient's identity.

Privacy and integrity are mediated by X.509 certificates, which act as electronic ID cards. Usually these are issued by external Certificate Authorities (CAs), whose business is the issuing of Internet certificates. Some of these CAs are widely-trusted because of their vetting protocols and performance records. That is, those CAs are thorough in verifying the identity of a certificate requester before issuing a commercial use certificate. Also, the operations of the CAs are secure enough to prevent theft of encryption keys and other materials that can be used to counterfeit their certificates.

Preparation for SSL Communication

There is a division of labor for SSL configuration tasks. The configurations of the client and the server are coordinated to achieve the required compatibility. The following sections describe the preparation tasks required for client configuration and server configuration.

Server and Related Client Configuration

The administrator of a target server must have completed at least one of the following:

- **Equip the server with an appropriate class X.509 certificate from a well-known Certificate Authority (CA).** The administrator will have created a public/private key pair, submitted a request to the CA for a certificate, and received and activated that server certificate. By definition a *well-known CA* is one whose root certificates are already stored in the Personal Communications PCommClientKeyDb.kdb database file—see “Configuring SSL for Connecting to a Server Using a Certificate from a Well-Known CA” on page 61 for a list of these.

  Note: You must also equip the client PCommClientKeyDb.kdb database file with an X.509 personal certificate from the same certificate authority (CA) to enable client authentication.
- **Equip the server with an appropriate class X.509 certificate from an unknown CA.** The procedure is the same as the step above with the added necessity of obtaining the root certificate from the *unknown* CA. Usually the administrator of the target server will distribute the appropriate root certificate which must then be added to the PCommClientKeyDb.kdb database file.

  Note: You must also equip the client PCommClientKeyDb.kdb database file with an X.509 personal certificate from the same certificate authority (CA) to enable client authentication.
- **Equip the server with a self-signed X.509 certificate.** The administrator of the target server can do this as an interim measure while waiting for a CA’s certificate. A copy of that certificate must be added to the client PCommClientKeyDb.kdb database file. The distribution must be done in a secure manner to guard the privacy and integrity offered by SSL.

  Notes:
  1. You must also equip the client PCommClientKeyDb.kdb database file with a X.509 self-signed personal certificate from the same certificate authority (CA) to enable client authentication.
  2. You must also add a copy of this certificate to the server’s key database.

Client Configuration

The following elements must be configured on the client side to enable SSL:

- **PCommClientKeyDb.kdb** is a certificate management database that is automatically created in the Personal Communications private subdirectory when Personal Communications is installed. It is password protected. The default password is *pcomm* and is generated when PCommClientKeyDb.kdb is initially created by Personal Communications. To assure the continued integrity of PCommClientKeyDb.kdb, change the default password to a password or passphrase that is not easily guessed. See “Changing the Password of a Client’s Key Database” on page 60 for instructions on changing the password. As installed, this database contains a list of well known CAs and their root certificates that will be sufficient for the majority of SSL client users for server-side authentication. If the target server uses a certificate from one of those well-known CAs, the client user does not need to modify the PCommClientKeyDb.kdb other than to change the default password for server-side authentication. See the notes in “Server and Related Client Configuration” on page 57.
- **PCommClientKeyDb.sth** is a password stash file that is automatically created when Personal Communications is installed. The password or passphrase used to protect PCommClientKeyDb.kdb is encrypted and stored in this stash file for use by Personal Communications. Every time the password is changed on

PCommClientKeyDb.kdb, this stash file must be regenerated. Otherwise, the SSL-mode will not operate. See “Changing the Password of a Client’s Key Database” on page 60 for instructions on changing the password.

Notes:

1. The use of a password stash file is strongly discouraged; the protection for these files is not strong.
2. **Using Password for ClientKeyDb.kdb instead of PCommClientKeyDb.sth**: Personal Communications allows the option to not use the PCommClientKeyDb.sth password stash file. To operate in this manner, erase the PCommClientKeyDb.sth file from the Personal Communications private subdirectory; then, during SSL session configuration, select the **Prompt for Password Once** radio button from the **Advanced Security Setup** property page.

- The **Enable Security** check box must be set in the telnet configuration of Personal Communications to operate in SSL mode. A client operating in SSL mode cannot establish a connection with a server that is operating in ordinary Telnet mode. Likewise, a client operating in ordinary Telnet mode cannot establish a connection with a server operating in SSL mode.
- Check the **Send Personal Certificate to Server if Requested** check box on the **Advanced Security Setup** property page for client authentication. If this field is not checked, only server-side authentication is performed. See “Opening a Key Database and Adding a Root Certificate” on page 62 for details.

Establishing an SSL-Based Session

Upon establishing a preliminary connection with a target server, the Personal Communications client is presented a certificate by that server; if you have enabled client certificate authentication, your certificate is likewise presented to the server. The digital signature of the CA is authenticated using a published *root* certificate of the issuing CA. The client automatically decrypts certain information on the presented certificate using a *public* key on the CAs root certificate. This step is successful only when the presented certificate was encrypted using a well-guarded, unique, and corresponding *private* key, known only to the CA. This process can detect (and reject) intentional alterations (forgeries) and the rare garbling that can occur over data circuits.

Personal Communications also allows users to use self-signed certificates for this purpose.

Once this certificate-issuer authentication step succeeds, the client and server negotiate to agree on an encryption key to be used during the ensuing data exchange session.

Secure Session Icon

When an SSL connection is established, a padlock icon is displayed in the Personal Communications status bar. Depending on the level of encryption, the icon is accompanied by a number (0, 40, 56, 128, 168). If the session is not SSL-based, the icon shows as unlocked.

You can display information about the security aspects of your session by clicking **Security → Client** from the **Communication** menu, or **Security → Server** from the **Communication** menu.

Pop-up Messages

During session establishment, your workstation may display pop-up messages in order to solicit from you:

- The password for accessing the PCommClientKeyDb.kdb database
- The location of the PCommClientKeyDb.kdb

If you chose to be prompted for personal client certificate information, the Select Client Personal Certificate Label Name screen is displayed at connection time, when the server requests the client personal certificate. The **Server Certificate Information** list box displays the information about the certificate issued to the server, as well as the issuer. Information includes common name, organization, locality and e-mail. This is provided for information purpose only; none of the information can be selected. The **Server Trusted Root List** list box displays the information about the trusted root supported by the server. This is also provided for information purpose only; none of the information can be selected. Click the **Select Personal Certificate Label Name** drop-down list and select the personal certificate to be sent to the server for client authentication. Click **OK** after selection.

If you chose to be prompted once for the key database password, the Enter Key Database Password screen is displayed at connection time, when the server requests the client personal certificate. Enter the key database password and click **OK**.

Changing the Password of a Client's Key Database

The key database file created when Personal Communications is installed has a default set of root certificates that will handle a majority of server certificates without modification to the file. This initial file is accessible using certificate management. The default password *pcomm*.

Certificates can be managed using Certificate Wizard, Certificate Manager, or using the command-line mode. For information on using the command-line mode, see "Using the Command-line Mode for Managing Certificates" on page 65.

Using Certificate Wizard

The wizard is provided to allow users to easily change a password or add a certificate to a key database file. To access the Certificate Wizard, do the following:

1. From the **Start → Programs → IBM Personal Communications → Utilities** menu, select **Certificate Wizard**.
2. Select the **Change the password to your key database** radio button on the Welcome to the Personal Communications Certificate Wizard panel, click **Next**, and proceed through the wizard following the instructions on each panel.

Using Certificate Management

To change the password using Certificate Management, do the following:

1. From the **Start → Programs → IBM Personal Communications → Utilities** menu, select **Certificate Management**.
2. From the **Key Database File** menu, select **Open**.
3. Select the PCommClientKeyDb.kdb file from the Personal Communications private subdirectory.
4. Click **Open**.
5. Type the current password for the file in the Password entry field.

6. From the **Key Database File** menu, select **Change Password**.

   Follow the guidelines issued by your network manager for selecting a password or passphrase that is not easily guessed.
7. Type the new password in the New Password entry field.
8. Type the new password again in the Confirm New Password entry field.
9. To set a password expiration time, click **Set expiration time** and enter the number of days until expiration.
10. Click **Stash the password** to *stash* the password of the current database encrypted.

    Note: Personal Communications cannot access the certificates in your file if this check box is not selected.
11. Click **OK**.

Configuring SSL for Connecting to a Server Using a Certificate from a Well-Known CA

The following CA signed root certificates are already stored in the key database and marked as trusted certificates:

- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 1 Public Primary CA

Following is a summary of the steps required for connecting to a server using a certificate issued by a well-known CA:

1. Confirm that the server you want to connect to has a certificate from a well-known CA.
2. Configure Personal Communications for SSL support.

Configuring SSL for Connecting to a Server Using a Certificate from an Unknown CA

The procedures in this section explain how to configure security for connecting to a server using a certificate issued by an unknown CA; that is, a CA that is not already defined in the PCommClientKeyDb.kdb file.

Following is a summary of the steps required:

1. Confirm that the server you want to connect with has a certificate from an unknown CA.
2. Request the root certificate for the unknown CA from your server administrator.
3. Open the PCommClientKeyDb.kdb file and add the root certificate to it.
4. For client authentication, obtain a personal certificate from this unknown CA and add it to the PCommClientKeyDb.kdb file.

Opening a Key Database and Adding a Root Certificate

When you get the root certificate file from your server administrator, make sure that it is in one of the following formats, based on the normal file extensions:

.ARM Base64-encoded ASCII data (armored 64 format)

.DER Binary DER data

Only a certificate in one of these formats can be added to the keyring database.

Note: In many cases, instead of providing a root certificate file, the server administrator may create the key database file and password stash file at the server. After adding the root certificate, the server administrator can copy the files to each client. If you do this, it is important that the names and location match as follows:

- Key database file: PCommClientKeyDb.kdb
- Password stash file: PCommClientKeyDb.sth

These files are located in the Personal Communications private subdirectory.

If the server administrator provided only a root certificate file, use the Certificate Wizard or Certificate Management utility to open the key database file and add the root certificate.

Certificates can be managed using Certificate Wizard, Certificate Management, or command-line mode. For information on using the command-line mode, see “Using the Command-line Mode for Managing Certificates” on page 65.

Using Certificate Wizard

The wizard is provided to allow users to easily change a password or add a certificate to a key database file. To use the certificate wizard, do the following:

1. From the **Start** → **Programs** → **IBM Personal Communications** → **Utilities** menu, select **Certificate Wizard**.
2. Select one of the following radio buttons on the Welcome to the Certificate Wizard panel:

   Import a certificate

   Create a self-signed certificate
3. Click **Next** and proceed through the wizard following the instructions on each panel.

Using Certificate Management

To use certificate management to open a key database and add a root certificate, do the following:

1. From the **Start** → **Programs** → **IBM Personal Communications** → **Utilities** menu, select **Certificate Management**.
2. From the **Key Database File** menu, click **Open**.
3. Select the PCommClientKeyDb.kdb file.
4. Click **Open**.
5. Type the password in the **Password** entry field and click **OK**.
6. Select **Signer Certificates** from the drop-down listbox.
7. Click **Add** to receive the certificate.

   The Add CA’s Certificate from a File panel appears.

8. Select the format dictated by your server administrator from the **Data Type** listbox.
9. Type the full path to the root certificate file in the **Certificate file name** entry field.
10. Click **Browse**, open the certificate file, and click **OK**.
11. Enter a label for the certificate and click **OK**.
12. Click **View/Edit**.
13. Activate the **Set the certificate as a trusted root**, and click **OK**.

Opening a Key Database and Adding a Personal Certificate

When you get the personal certificate file from your server administrator or a CA, make sure that it is in one of the following formats:

- PKCS12 file
- CMS key database file
- Keyring file
- Base64-encoded ASCII data (armored 64 format)
- Binary DER data

Only a certificate in one of these formats can be added to the keyring database.

Notes:

1. In many cases, instead of providing a personal certificate file, the server administrator may create the key database file and password stash file at the server. After adding the personal certificate, the server administrator can copy the files to each client. If you do this, it is important that the names and location match as follows:

   Key database file
      PCommClientKeyDb.kdb

   Password Stash file
      PCommClientKeyDb.sth

   These files are located in the Personal Communications private subdirectory.
2. If the server administrator provided only a personal certificate file, use the certificate management to open the key database file and add the root certificate.

Using Certificate Management

To use certificate management to open a key database and add a personal certificate, do the following:

1. From the **Start** → **Programs** → **IBM Personal Communications** → **Utilities** menu, select **Certificate Management**.
2. From the **Key Database File** menu, click **Open**.
3. Select the PCommClientKeyDb.kdb file.
4. Click **Open**.
5. Type the password in the **Password** entry field and click **OK**.
6. Select **Personal Certificates** from the drop-down listbox.
7. Click **Import for KDB, DYR and P12 format files** to import the certificate.

   The Import Key panel appears.
8. Select the format dictated by your server administrator from the **Key file Type** listbox.

9. Type the full path to the root certificate file in the **Certificate file name** entry field.
10. Click **Browse**, open the certificate file, and click **OK**.
11. Enter the **Key Label**, or accept the default, and click **OK**.
12. Click **Receive for ARM and DER format files**.

    The Add CA's Certificate from a File panel appears.
13. Select the format dictated by your server administrator from the **Data Type** listbox.
14. Type the full path to the root certificate file in the **Certificate file name** entry field.
15. Click **Browse**, open the certificate file, and click **OK**.
16. Enter a label for the certificate and click **OK**.

Using Certificate Wizard

The wizard is provided to allow users to easily change a password or add a certificate to a key database file. To use the certificate wizard, do the following:

1. From the **Start** → **Programs** → **IBM Personal Communications** → **Utilities** menu, select **Certificate Wizard**.
2. Select the **Import a certificate** radio button on the Welcome to the Personal Communications Certificate Wizard panel, click **Next**.
3. Select the **Import a client certificate** radio button on the Import Certificate panel, click **Next** and proceed through the wizard following the instructions on each panel.

Note: The certificate wizard only supports importing a PKCS12 file.

Obtaining a Personal ID Certificate from a Known Certificate Authority (CA)

A personal ID certificate uniquely identifies you, and can be obtained from known certificate authorities. One such certificate authority is VeriSign. To obtain a Personal ID certificate from VeriSign:

1. Open the VeriSign web page at http://digitalid.verisign.com/.
2. Select **Personal IDs** from the page.
3. Follow the instructions on the next web page to install a **Digital ID** (either **full-service** or **trial**) in your web browser.

After the certificate has been installed in your browser, you must store it in the key database:

1. From the browser, export the certificate into a new key file.
2. Open the Personal Communications client key database file.
3. Click on **Export/Import** to import the certificate. The **Export/Import Key** dialog appears.
4. Click the **Key** button.

   Note: The key file type must be PKCS12 file.
5. Enter the name of the file in the first field, the path to the file in the second field; click **OK**.
6. At the password prompt, enter your password and click **OK**.

Configuring SSL for Connecting to a Server Using a Self-Signed Certificate

Although using self-signed certificates is not recommended, a server administrator can use them while waiting on a purchased CA certificate. Once the CA certificate is available, the server and all clients should be reconfigured to switch from the self-signed certificate to the purchased one.

Following is a summary of the steps required:

1. Confirm that the server you want to connect with has a self-signed certificate.
2. Request from your server administrator the root certificate for the self-signed certificate.
3. Open the PCommClientKeyDb.kdb file and add the root certificate to it.

The steps required by a client in this scenario are the same as those for the Unknown CA scenario. See "Opening a Key Database and Adding a Root Certificate" on page 62 for the steps involved.

Using the Command-line Mode for Managing Certificates

The command-line mode for managing certificates allows users to create batch files to change a password or add a certificate for a large number of key database files.

Note: Before using the command-line mode, be sure to make backup copies of the following files:

PCommClientKeyDb.kdb
The key database

PCommClientKeyDb.sth
The stash file where the password is stashed

Pcsgsk.pro
A sample profile.

From the command prompt, the command-line mode has the following syntax:

```
pcsgsk [-h | -?] <filename>.pro | -e | -g
```

The options have the following significance:

-h or -?
Displays the command-line mode syntax.

<filename>.pro
Based on the information specified in <*filename*>.pro, change the password of a key database, add a certificate to the key database, or both.

The <*filename*>.pro must be a fully qualified path, or the name of a file that exists in the Personal Communications private subdirectory. A default profile PCSGSK.PRO has been provided in the \private subdirectory.

-e Displays a list of possible error codes and their associated messages.

-g Launches the Certificate Wizard instead of the command-line mode.

The following examples show the different ways to invoke the command-line mode:

pcsgsk -?
Displays the syntax.

pcsgsk pcsgsk.pro
Action performed depends on the keyword content of the text file pcsgsk.pro which resides in the Personal Communications private subdirectory. For example, if the file contains **NewPwd=**, then the password of a key database will be changed. If **CertFile=** or **CertLabel=** are included, these certificate files will be imported.

pcsgsk -e
Displays the possible error codes and the associated messages on the screen.

pcsgsk -g
Launches the Certificate Wizard.

A sample profile, PCSGSK.PRO, is provided in the Personal Communications private subdirectory.

The rules for specifying parameters in the profile are as follows:

1. The file must contain a `-----BEGIN PROFILE-----` line with 5 hyphens before and 5 hyphens after BEGIN PROFILE, and must also contain a succeeding `-----END PROFILE-----` line with 5 hyphens before and 5 hyphens after END PROFILE.

   Active parameter information must be between `-----BEGIN PROFILE-----` and `-----END PROFILE-----`. Everything prior to the BEGIN PROFILE line and after the END PROFILE line is ignored.

   Note: The BEGIN PROFILE line, all active parameters, and the END PROFILE line *must* be in English.

2. Each parameter must be specified on a separate line of the profile. A parameter line must have the following form:

   ```
   Keyword=String
   ```

   Valid keywords are:

   KdbFile=
   Used to specify the name of a key database. This parameter is required.

   KdbFilePwd=
   Used to specify the current password of the key database. This parameter is required.

   Note: As default behavior, leading and trailing spaces in a password string are not treated as part of the password. However, imbedded spaces are retained. For example,

   ```
   NewPwd= Multi-word password
   ```

   The password is: *Multi-word password.*

   To retain leading and trailing spaces, use the PwdSpaces= keyword.

   NewPwd=
   Used to specify the new password to be set.

Note: As default behavior, leading and trailing spaces in a password string are not treated as part of the password. However, imbedded spaces are retained. For example,

```
NewPwd= Multi-word password
```

The password is: *Multi-word password.*

To retain leading and trailing spaces, use the PwdSpaces= keyword.

PwdSpaces=
Set this parameter to **Yes** only if you want any leading or trailing spaces to be included in the passwords specified for KdbFilePwd= or NewPwd=. Normally, you will *not* want to set this parameter to **Yes**. For example:

```
NewPwd= Multi-word password
```

If PwdSpaces= is not set to Yes, the password is Multi-word password.

If PwdSpaces= is set to Yes, the password begins with the string *"Multi-word password"* with five leading spaces plus any trailing spaces.

Warning

Many ASCII editors can leave trailing spaces at the end of lines without giving any obvious indication.

CertFile=
Used to specify the fully qualified path of a certificate file to be added to the database. This must be a fully qualified path name.

CertLabel=
Used to provide a label to identify the certificate being added to the database.

3. One operation (changing the password or adding a certificate), or both, can be specified.

   If the **NewPwd=** parameter is specified, the password will be changed to the new password.

   If the **CertFile=** and the **CertLabel=** parameters are specified, the certificate is added to the key database.
4. A line is treated as a comment if it is not the first line or last line and if it is not a keyword line.
5. To preserve the security of passwords, both the new password and the old password is deleted from the profile during processing. This is true even if the attempted operation fails. For example, if the program cannot find the specified key database, and therefore cannot change the password, the old password and the new password *will* be deleted from the profile.
6. After processing, two lines is added to the end of the profile, after the `-----END PROFILE-----` line, that specify the results of the attempted operation. These lines are as follows:

   ResultPwd=nnnn
   Specifies the status of the change-password operation.

   ResultCert=nnnn
   Specifies the status of the add-certificate operation.

The values possible for *nnnn* can be found by invoking PCSGSK with the -e option, as previously described, which causes the possible error codes and the associated messages to be displayed on the screen.

Security References

Personal Communications supports server and client authentication. The following publications are available on the World Wide Web and provide more information:

- *SSL-Talk FAQ Version 1.0.3*

  http://www.consensus.com/security/ssl-talk-faq.html
- *Introduction to SSL*

  http://www.camb.opengroup.org/˜fjh/Papers/cook/ssl_intro.html
- *SSL Version 3.0 Specification*

  http://home.netscape.com/eng/ssl3/index.html

For an introduction to and a history of public key cryptography and privacy, refer to *Simson Garfinkel, PGP: Pretty Good Privacy, O'Reilly and Associates, 1995*; ISBN: 1565920988.

Problem Determination

Following is some information to help you avoid problems that might be related to SSL configuration.

- With server-side authentication, the common name in the sever's certificate is always compared to the name you type in the Host Name field on the client. These names must match exactly. You cannot:
  - Type the IP address in one place and the host name in the other
  - Type wrt05306 in one place and WTR5306 in the other
  - Type wtr05036 in one place and wtr05036.raleigh.ibm.com in the other

  Note: This information is available only from the target server administrator.
- Make sure that SSL is enabled in both the Personal Communications client and the SSL server.
- Makes sure that the port number in the Advanced configuration panel on the client matches the port number defined in the server.
- For each different server using a self-signed certificate, you must add a copy of each of the server certificates to your keyring.
- Be sure there is a root certificate of the proper class to correspond with the class and issuer of the certificate on the server.

Note: Notify your server administrator of any problems prior to contacting IBM Service.

Smart Card Support

Personal Communications Version 5.5 includes Smart Card support, which allows you to store a certificate in a dedicated security device. A Smart Card is a small electronic device that contains electronic memory and can be used to store a certificate. You can keep the certificate in a local or network accessed file, in Netscape PKCS#11 format. You can specify the location of the certificate in the session preferences, or prompt for the personal client certificate. You can control the timing of prompts for client certificates. You can choose to prompt each time a connection is made to the server, or only the first time after starting Personal Communications. In addition, if your client stores preferences locally, you can choose to be prompted once, and all subsequent connections will use information stored in the local preferences. You can also store the password for the certificate on your local client, if you store preferences on your local client. You can allow the client to access its certificate before connecting to the server, whether the server requests a certificate or not.

Table 4 displays the supported Smart Card drivers and their filename.

Table 4. Supported Netscape PKCS#11-compatible Smart Card Drivers

Smart Card Drivers	**File names**
IBM Secureway Smartcard	w32pk2ig.dll
GemPlus/GemSoft Smartcard	w32pk2ig.dll
IBM Netfinity® PSG Chip[1]	ibmpkcss.dll
Rainbow Ikey 1000	Cryptoki22.dll
Schlumberger Cryptoflex	acpkcs.dll *or* slbck.dll
SCW PKCS 3GI 3-G International	3gp11csp.dll
Data Key	Dkck232.dll
Fortezza Module	fort32.dll

[1] The system boards in some IBM systems are pre-configured with a Promise of Value (POV) card, a 256-bit encrypted security chip daughtercard attached to the motherboard. If an attempt is made to remove the POV card from the board and install it into another system, the cryptographic key material will be erased, rendering it unusable. This security feature is by design and prevents the cryptographic key migration from one system to another. Therefore, moving this security chip from one board to another is not a supported option. If an attempt is made to move the POV card from one system to another, it may hang on boot and display an error message referring to an invalid machine type and serial number.

Enabling Smart Card Support

Smart Card is only used for the personal certificate and can only hold one personal certificate and does not hold the signer certificates. The signer certificate or the root and any intermediate certificate of the personal certificate on the Smart Card should be added in the PCommClientKeyDb.kdb file.

Part 4. Appendixes

Appendix A. Attachment Considerations

This chapter describes factors you should consider when configuring Personal Communications for the following attachment types:

- “COAX Attachment”
- “LAN via IEEE 802.2 Attachment” on page 75
- “TCP/IP Connection” on page 75
- “SDLC MPA Attachment” on page 76
- “IBM Global Network - SNA over Async Attachment” on page 78
- “IBM Global Network Connection Attachment” on page 78
- “Home3270 Attachment” on page 79
- “IBM PC720 Modem Initialization (Japan Only)” on page 80
- “Twinax Attachments” on page 80
- “IBM SDLC PCMCIA Adapter and Modem (Japan Only)” on page 81
- “IBM PCI Multiprotocol Adapter” on page 82
- “WAC Attachments” on page 82
- “3174 Peer Communications Support (LAN over Coax)” on page 84
- “Twinaxial Console” on page 85
- “Asynchronous Console” on page 85

Note: Support for Windows 2000 Plug-and-Play may differ somewhat from that for Windows 95 and Windows 98.

COAX Attachment

This section describes factors you should consider when configuring Personal Communications with a coaxial attachment.

Note: The APPC and CPI-C APIs, provided with Personal Communications Access Feature, do not support coaxial connections.

Avoiding Machine Check 207

Patch the microcode of the 3174 control unit. The following list shows the relationship between 3174 control unit microcode levels and patch IDs:

Microcode Level	Patch ID
S0503	PCA53D1
S0504	PCA53D2
A0503	PCA53D3
A0504	PCA53D4
B0200	PCA53D5
B0401	PCA53D6
B0402	PCA53D8
C0101	PCA53D7

In addition, if you have a 3174 with Configuration Support B or higher, you can set the following parameters:

- 3174 customization **Q126 digit 2=1** to change the COAX timeout from 50 to 100 microseconds.
- 3174 customization **Q125 digit 4=1** to set command chaining off.

Polling Feature

Your workstation may have been configured so that an IBM coax adapter cannot acquire an interrupt request line (IRQ) that it needs in order to function. This situation occurs because other devices have been configured to use these IRQs, so that the IRQs are no longer available. This situation can occur in Windows 95, Windows 98, Windows NT, Windows Me, or Windows 2000.

In such a situation, the IBM coax adapter may or may not be able to use another available IRQ. The IBM 3278/79 Emulation Adapter (ISA bus) can use only IRQ 9. Other IBM coax adapters, such as the IBM 3270 Credit Card adapter, can use other IRQs than IRQ 9, but all these other usable IRQs may also have been reserved for other devices in the system.

If this happens, you can use the polling feature to enable the IBM coax adapter to function without using an IRQ. To activate the polling feature, add the **`Poll=Y`** parameter to the [CSDFT] or h[CNDFT] section of your workstation profile (*.WS) as follows:

- SNA/DFT attachment

  ```
  [CSDFT]
  Poll=Y        <-- add
  ```

- Non SNA/DFT attachment

  ```
  [CNDFT]
  Poll=Y        <-- add
  ```

For an IBM 3270 Credit Card adapter, the polling feature is automatically activated, without Poll=Y being added to the .WS file.

Restrictions

When your workstation is configured to use a DFT attachment, the following functions and capabilities of the IBM 3174 or 3274 Control Units are not supported:

- Programmed symbols on attached workstations
- Attachment to port 0 on attached workstations
- Database operations
- 3270 Diagnostic Reset Dump
- Patch facility

PCMCIA and PCI Configuration for a DFT Attachment

Using a Plug-and-Play Coax Adapter (PCMCIA or PCI)

If your workstation has an IBM 3270 Emulation Plug-and-Play Adapter (3270 PnP) installed, Personal Communications uses it in the same way as the IBM 3278/79 Emulation or 3270 Connection Adapter.

You cannot use multiple 3270 PnP adapters; nor can you use a 3270 PnP at the same time as a 3278/79 Emulation or 3270 Connection Adapter. Before you can use a PCMCIA or PCI adapter under Windows 95, Windows 98, or Windows 2000, you must first install drivers for it. See “Adapter Setup Hints and Tips” on page 85 for more information.

Coax Adapters and ROM Shadowing

Personal Communications maps the shared RAM of the 3270 connection adapter on the PC. The default values for the adapters as follows:

- Adapter #0 CE000h - CFFFFh
- Adapter #1 D0000h - D1FFFh
- Adapter #2 D2000h - D3FFFh
- Adapter #3 D4000h - D5FFFh

PCs that support ROM shadowing in BIOS may use these areas for ROM shadowing by default (IBM PC350 P100, for example). Check the ROM shadowing settings before installing an adapter and disable the range for the adapter you are going to install.

LAN via IEEE 802.2 Attachment

Following is a description of preinstallation considerations for installing Personal Communications for use on a LAN. For more detailed information, refer to the *IBM Local Area Network Technical Reference*.

PIU Size

This value is negotiated between your workstation and the host system, unless `XID=No` is defined on the PU, or the Adjacent CP type has been changed to `Host - XID0` in SNA Node Configuration. If this value is not negotiated, the `Maximum PIU Size` must match the `MAXDATA` value defined on the host system.

Receive Window Count

This value is negotiated between your workstation and the host system, unless `XID=No` is defined on the PU, or the Adjacent CP type has been changed to `Host - XID0` in SNA Node Configuration. If this value is not negotiated, the `Receive Window Count` must match the `MAXOUT` value defined on the host system.

Using a PCMCIA Token-Ring or Ethernet Card

PC/3270 supports the IBM Token-Ring and Ethernet credit card adapters in the same way as it does the full-size adapters.

TCP/IP Connection

This section provides information, considerations, and restrictions for Personal Communications TCP/IP connections.

TCP/IP Protocol Driver

You must set up your Windows environment for the TCP/IP network. To verify that the TCP/IP protocol is installed on your workstation, double-click **Network** in your Control Panel and see if `TCP/IP` appears in the list of network components. Double-click **TCP/IP** to specify your IP address and other TCP/IP properties.

Screen Size

The following four screen sizes are supported for TN3270:

24 x 80

32 x 80
43 x 80
27 x 132

The following two screen sizes are supported for TN5250:
24 x 80
27 x 132

Screen size 48X80, 62X160, and 24X132 are supported if your server/host supports the TN3270E protocol.

Other TCP/IP Functions

The following sections describe enhancements made to TCP/IP connections for Personal Communications Version 5.5.

Backup Server/Host with LU Name and Port Number

Personal Communications enables you to specify up to two backup host or server names to connect to. This provides easier connections when the primary host or server cannot be reached. You can also specify a specific LU name or port number unique to that server or host.

Service Location Protocol

Personal Communications enables connection to SLP servers that are RFC 2165 compliant. This function eliminates the need for users to know the name of a network host supporting a specific service. SLP implementation for a Personal Communications client allows load balancing and dynamic location of a specific LU or LU pool across a group of servers. Netware for SAA (IWSAA) 4.0 and IBM Communications Server (CS/NT) 6.1 currently support SLP. This support can be used in conjunction with SSL support.

Connect Timeout

Personal Communications uses non-blocking sockets when connecting to a remote system. Personal Communications waits three seconds, by default, to establish the socket connection. The default can be changed by adding the following line to the Telnet3270 or Telnet5250 section of the workstation profile:

```
InactiveTimeout=xx
```

where xx is the time in seconds.

SDLC MPA Attachment

This section describes factors you should consider when configuring Personal Communications with an SDLC attachment.

Line Speed

For the SDLC attachment, a line speed up to 28.8 Kbps is supported. However, actual line speed will vary depending on the carrier speed the modem supports.

V.25bis Autodial

Personal Communications only supports the bit-oriented protocol for V.25bis call control messages. Modems must support an ASCII-coded character set consisting of 7-bit coded ASCII characters with odd parity.

Personal Communications supports the following adapters:

- Multiprotocol (MPA) interface compatible adapters, for example:

  - IBM Multiprotocol Communications Adapter (73G7099)
  - IBM Multiprotocol Adapter/A (645114 or later)
  - IBM SDLC/Asynch Communications Adapter (ASCA) (42H4332)
- IBM SDLC PCMCIA adapter (Japanese only)
- IBM SDLC PCMCIA modem (Japanese only)
- IBM PCI Multiprotocol Adapter (12J2981)

Performance Considerations

If you use multiple sessions in a high-speed and high-load configuration with an SDLC attachment, the connection to the host might fail. In this case, set the host's timeout value to be greater than that of Personal Communications.

- To change the host timeout value, modify the following NCP parameters:

  REPLYTO
  The maximum duration in seconds that the host waits for a reply from the terminal. The default is 1 second.

  RETRIES=(m,t,n)
  The number of recovery attempts for errors occurring during transmission over the link. Repetitive retries are called a retry sequence. The maximum number of retries is specified as m, which can be from 0 to 128. NCP pause (the time between the retry sequences) is specified as *t* and can be from 1 to 255 seconds. The maximum number of retry sequences is specified by *n* and can be from 1 to 127. For example:

  ```
  REPLYTO=1, RETRIES=(3,4,5)
  (( 1(seconds) x 3(times) + 4(seconds)) x 5(times)
  = 35 (seconds)
  ```

  Note: In this example, the host waits 35 seconds for the terminal to reply.

  For more details, ask your system personnel.

- To change the Personal Communications timeout value, type a new value in the Inactivity timer field on the Performance page of the Connections property sheet in SNA Node Configuration.

  The value is in seconds and can be from 40 to 160. The default is 80.

PIU Size

This value is negotiated between your workstation and the host system, unless `XID=No` is defined on the PU, or the Adjacent CP type has been changed to `Host - XID0` in SNA Node Configuration. If this value is not negotiated, the `Maximum PIU Size` must match the `MAXDATA` value defined on the host system.

Receive Window Count

This value is negotiated between your workstation and the host system, unless `XID=No` is defined on the PU, or the Adjacent CP type has been changed to `Host - XID0` in SNA Node Configuration. If this value is not negotiated, the `Receive Window Count` must match the `MAXOUT` value defined on the host system.

Preventing Conflicts with Non-PCI MPA Adapters

The multiprotocol adapters use system resources that, in some cases, cannot be shared. Therefore, you must make sure there are no conflicts with the following resources:

- DMA level
- I/O addresses (MPA0 uses X'380'–X'38F' and MPA1 uses X'3A0'–X'3AF')

- IRQ level (ISA bus only)

The IBM Multiprotocol interface adapters use the following system resources:

- The AT-bus SDLC adapters require the use of IRQ3 and DMA channel 1 and only the MPA0 communication port is supported.
- The MPA for ISA can be supported using mode 4 (IRQ3 and DMA1 channel 1) or mode A (IRQ4 and DMA channel 1). IRQ level send/receive of 3 or 4 is supported. The ASCA can be supported using mode 4 (IDQ3 or IRQ5 or IRQ4 or IRQ7 and DMA channel 1) or mode A (IRQ4 or IRQ7 and DMA channel 1). IRQ level send/receive or 3, 4, 5, or 7 is supported. The interrupt level setting on the configuration panel in Personal Communications must match the value on the adapter card.

  Note: When the MPA is configured for mode 4, the device is not allowed to use the other IRQ even though only one interrupt is claimed.

  Personal Communications supports the MPA0 or MPA1 communication ports. Some sound cards use an I/O address within the range X'380'–X'38F'. MPA1 should be used to avoid a conflict.
- The MPA/A for a microchannel-bus workstation uses IRQ3, and the DMA level can be configured. Both the MPA0 and MPA1 communication ports can be active at the same time and the interrupt is claimed as sharable.

IBM Global Network - SNA over Async Attachment

IBM Global Network - SNA over Async is supported using 8-bit no parity; SNA session-level compression and decompression is not supported.

Line Speed

Line speeds up to 115.2 Kbps are supported. However, the maximum usable line speed depends on the speed of the processor or communication port. If communication stops or becomes exceedingly slow, reduce the line speed.

Updating Phone List

To update the phone number list for IBM Global Network SNA over Async, do the following:

1. Click the **Used Phone Book** button on the Define a Com Port Connection panel.
2. Click the **Download Phone Numbers** button.

   Personal Communications FTPs to the IGN server and downloads the phone number file and converts it to the correct format.

   Note: A Proxy must be configured in order for this procedure to work.

IBM Global Network Connection Attachment

Note: This attachment type is not available in Japan.

IBM Global Network Connection supports only a single communication port.

Line Speed

IBM Global Network Connection supports up to 115.2 kbps as the line speed. However, the maximum usable line speed depends on the speed of the processor or communication port. If communication stops or becomes exceedingly slow, reduce the line speed.

Updating Phone List

To update the phone number list for IBM Global Network SNA over Async, click the **Download Phone Numbers** button from the **Configuration** panel. When this button is selected, Personal Communications FTPs to the IGN server and downloads the phone number file and converts it to the correct format.

Note: A Proxy must be configured in order for this procedure to work.

Restrictions

You cannot use the following functions:
- Import/Export
- Host graphics
- Host print
- Server-Requester Programming Interface (SRPI)
- Concurrent multiple file transfers

Home3270 Attachment

Because Home3270 supports only a single COM port, only one session is available for use at a time.

Setting the Screen Colors in a Home3270 Session

Because protocol converters translate the 3270 (EBCDIC) data stream into an ASCII data stream, the original information about the 3270 fields is lost, and all the field attributes of the 3270 screen are treated as extended attributes. Because of this, you must select the **Extended Color** category in order to change the colors of characters on the screen. Changing base colors will have no effect.

For example, if you want to change the color of characters that appear in green on a black background, select **Extended Color - Green**, then click or drag-and-drop the color you want for the characters (and for the background if you wish). Do not change the appropriate **Base Color** because the change will have no effect.

Line Speed

Line speeds up to 115,200 bps are supported. However, characters might be lost on high-speed lines, depending on the processor speed. If communication stops or becomes exceedingly slow, reduce the line speed.

Unsupported Character Sequences

The following character sequences are valid for the Home3270 attachment. However, they perform no function.
- ESC P 1 (Block cursor command)
- ESC P 0 (Underline cursor command)
- DLE DC2 (Printer start command)
- DLE DC4 (Printer end command)

Conditions for Communication Check 50x

Home3270 requires both Data Set Ready (DSR) and Carrier Detect (CD) to determine the state of the attachment with the host system. If DSR is not recognized, communication check 501 appears in the operator information area. When DSR is recognized and CD is not recognized, communication check 504 appears in the operator information area.

When you select ROLMphone with DCM in the Home3270 configuration, communication check 504 does not appear.

Home3270 and OIA message COMM 504

If you run Home3270 sessions at a speed of 28.8 kbps or higher and the session disconnects with a COMM504 in the OIA, try lowering the port speed to equal the line speed of the Protocol Converter you are connecting to.

Note: DBCS is not available with this attachment.

Restrictions

The following functions are not available with this attachment:
- Host graphics
- Host print
- Server Requester Programming Interface

IBM PC720 Modem Initialization (Japan Only)

In the Japanese version of Personal Communications, if you use an IBM PC720 and connect it via a dial connection, the error message “`COMDIA15 Unable to initialize modem`” may appear at startup. To correct this condition, increase the value of **Retries** in **Initialization** to more than 1 by using the **Modem Information** panel.

Twinax Attachments

Twinax Adapter Types

Personal Communications classifies twinax adapters under five adapter types:

- IBM 5250 Plug-and-Play Adapters
  – IBM 5250 Emulation PCMCIA Adapter
  – IBM 5250 PCMCIA Adapter (DBCS-unique adapter)
  – IBM 5250 Emulation PCI Adapter
  – IBM 5250 Express ISA Adapter, *when the adapter’s Plug-and-Play BIOS is enabled*
  – IBM 5250 Express PC Card
  – IBM 5250 Express PCI Adapter
- IBM 5250 MicroChannel Adapters
  – IBM System36/38 Workstation Emulation Adapter /A (DBCS-unique adapter)
  – IBM 5250 Emulation Adapter /A
- IBM 5250 ISA Adapters
  – IBM Enhanced 5250 Display Station Emulation Adapter
  – IBM 5250 Express ISA Adapter, *when the adapter’s Plug-and-Play BIOS is disabled*
- IBM 5250 ISA Adapter (Asia-Pacific)
  – IBM AT-Bus Communication Adapter (DBCS-unique adapter)
- Other Twinax Adapter
  – OEM 5250 adapters

See “Using Twinax (5250) Adapters” on page 87 for details on these adapters.

Using IBM 5250 Plug-and-Play Adapters

Before you can use one of the IBM 5250 Plug-and-Play adapters under Windows 95, Windows 98, or Windows 2000, you must first install a driver for the adapter. See “Adapter Setup Hints and Tips” on page 85 for more information on configuring all the IBM 5250 adapters.

OEM Twinax Adapter Cards

Developers of software drivers for OEM twinax cards that are seeking to implement support for Personal Communications on an OEM twinax adapter, should obtain a copy of the document *Twinax OEM Interface Specification for Windows NT and Windows 95*, as well as associated program materials. You can download these at www.ibm.com/software/network/pcomm/about/api/twinax.html.

The documented interface is completely functional for Windows 98 and Windows 2000 Professional, as well as for Windows 95 and Windows NT. However, it does not support the Microsoft Windows Driver Model (WDM) for Windows 98 and Windows 2000.

IBM SDLC PCMCIA Adapter and Modem (Japan Only)

For Windows 95 and Windows 98: The support uses the Configuration Manager for Plug-and-Play support, which automatically configures IRQ number, I/O ports, and memory addresses as required. IBMSDLC.INF (installed in the Personal Communications installation directory) describes the SDLC PCMCIA cards to the operating system. When you insert the PCMCIA card, Windows 95 and Windows 98 prompt you for the adapter drivers. You must specify the Personal Communications installation directory and click **OK**. To verify that the adapter is functioning properly, select the appropriate PCMCIA adapter under **Other Devices** on the **Device Manager** property page of the **System** Windows control panel applet.

For Windows NT: Plug-and-Play is not supported. During installation the registry is updated, using default parameters. When the configuration is started and an incoming or outbound connection is enabled, the device attempts to load, using the stored parameters from the registry. If a card is found and a conflict is detected, the registry is updated with values that do not conflict and you are notified to restart the system.

Note: The system must be restarted for these values to take effect.

Only one SDLC PCMCIA card can be used at a time. Because a common driver supports both SDLC PCMCIA and MPA interface cards, an MPA cannot be used concurrently with SDLC PCMCIA.

IBM SDLC PCMCIA Adapter

The IBM SDLC PCMCIA adapter supports:

- Leased and switched connections
- Speeds up to 19.2 Kbps
- Switched and Constant Request To Send (RTS)
- NRZ and NRZI encoding schemes

The IRQ number on the device page’s adapter property sheet is ignored.

IBM SDLC PCMCIA Modem

The IBM SDLC PCMCIA modem supports:

- Switched V.26bis connections only
- Speeds up to 2400 baud
- Switched RTS only

The configured value on the constant RTS and IRQ level send/receive device page's adapter property sheet are ignored.

IBM PCI Multiprotocol Adapter

Refer to the *Quick Installation Guide* in the *PCI Multiprotocol Adapter User's Guide* for instructions on installing this adapter under Windows 95, Windows 98, and Windows NT.

Two IBM PCI Multiprotocol Adapters can operate concurrently. The configuration specifies one adapter with Communication Port MPA0 and the second adapter with Communication Port MPA1. When the link is activated, MPA0 is the first PCI Multiprotocol Adapter that the operating system finds and MPA1 is the second adapter found. If more than one PCI Multiprotocol adapter is installed on a machine and you are unsure which adapter the operating system will find first, you may want to perform an isolated test to determine which adapter is connected to which Communication Port. One suggestion is to disconnect the modems connected to the adapter from the telephone line and then try to start each link individually. By watching the modems, you should be able to determine which modem is connected to which Communication Port. Then the modems can be attached to the proper network. If a single PCI Multiprotocol Adapter is used, the configuration file must specify MPA0 as the Communication Port.

Note: If a Personal Communications configuration is using this adapter, and a PCI MPA adapter is added or removed from the system, Personal Communications may have to be reconfigured.

An ISA-bus MPA and IBM PCI Multiprotocol Adapter can be used concurrently, as long as the ISA-bus MPA adapter is configured as MPA1.

The IBM PCI Multiprotocol Adapter supports:

- Leased and switched connections
- Speeds up to 56 kbps
- Switched and Constant Request To Send (RTS)
- NRZ and NRZI encoding schemes

The IRQ number on the device page adapter property sheet is ignored.

WAC Attachments

This section describes factors you should consider when configuring Personal Communications to communicate through a Wide Area Connector (WAC) adapter.

EIB Support

All available Electrical Interface Boards (EIBs) are supported for the WAC adapter.

Supported Adapters

The IBM WAC adapters for bus types ISA and MCA are supported.

Note: At this time, the new IBM PCI bus WAC adapter is *not* supported by Personal Communications.

Potential Configuration Issues

When configuring both ports (upper and lower) on a single WAC adapter, you must create two logical devices, using the configuration utility. Be careful to configure the same Shared Ram Address for both devices, using the same adapter number. If you do not do this, the Shared Ram Address for the first device activated will be used for the second device.

For ISA systems, the adapter number is obtained from the interpretation of the on-board DIP switch settings. Switches 1-3 determine the Interrupt level, and switches 4-7 (read in reverse order) determine the adapter number. Please consult the adapter installation publication for additional information. Adapter numbers 0 and 1 are logically the same. This is also true for adapter numbers 8 and 9.

On some IBM ValuePoint systems, intermittent problems can occur. If you are using one of these systems and are having problems, ensure that the adapter's DIP switch settings are such that Interrupt Level 9 is being used.

If you intend to use the WAC adapter in a system and you also plan on using Hayes AutoSync function, then you might experience problems with your async connection. To find appropriate Shared Memory values, you should use the adapter diagnostic disk provided with the adapter.

For MCA systems, the adapter number is the slot number in which the adapter physically resides. You can easily obtain this number via the MCA Configuration utility that was provided with your system. For IBM systems, you can determine this number by looking at the back of the system unit and providing the number displayed for the selected slot.

System Resources

The Wide Area Connector adapter utilizes the following system resources per each adapter installed:

- 32 bytes of IO addresses (differs depending upon the adapter number used on ISA; see **Help** on the Configuration panel for additional information, or through MCA adapter configuration)
- Interrupt level (1 level can be used on MCA if all adapters share the same, ISA adapters must have unique interrupt numbers)
- 16 KB of shared memory

For ISA adapters, you should consult your WAC installation publication for information concerning the IRQ used and the adapter number configured, both of which are configured through the adapter's DIP switches.

3174 Peer Communications Support (LAN over Coax)

The LAN over Coax function provides peer-to-peer communication for workstations connected to an IBM 3174 Control Unit through an IBM 3270 communication adapter. It provides support for any NDIS protocol stack capable of utilizing the IEEE 802.5 (token-ring) frame format, such as IEEE 802.2 (SNA), NETBIOS, TCP/IP, or LLC2. This function is not supported for Windows 2000.

Installing LAN Over Coax

Under Windows 95 or Windows 98:

1. On the network Control Panel, choose to install a new adapter.
2. Select the **Have Disk** option when prompted.
3. Install the program in the XLNCOAX subdirectory in the Personal Communications installation directory.

For Windows 95 and Windows 98, the .INF file installs the new adapter support and binds the adapter to all valid protocol stacks. To utilize the new adapter, after installing and rebooting, configure Personal Communications to utilize a LAN adapter, and enter the adapter number that corresponds to the 3174 Peer Communications adapter number found under the LLC Protocol for this adapter. The 3174 Peer Communications RPQ is also required on the 3174.

Configuring LAN Over Coax

For Windows 95 and Windows 98, configure by using the Network Control Panel **Properties** button for the selected adapter.

Options

Network Address
Overrides the burned-in adapter address.

Queued Transmits
Number of queued transmit elements to support.

Slot Number
Required for MCA bus systems, not applicable to others; indicates the adapter to use in a specific MCA slot.

On Micro Channel® workstations, you can use up to 4 type-B 3270 Connection Adapters (but only 1 type A). When you configure Personal Communications, you must specify the physical slot in which each adapter is installed.

System Resources

On ISA Bus systems, the following system resources are used:

- Interrupt Level 2
- IO address 0x2d0 through 0x2df
- Shared memory address 0xce000

These resources are not changeable. On MCA systems, these resources are configured via the MCA adapter configuration, with the exception for the Interrupt number, which is Interrupt 2.

Multiple Adapter Coexistence

If you use type-B adapters, you can use one or more for DFT connections concurrently with 3174 Peer Communications. If you want to do this, the Peer

Communications adapters must be in higher-numbered slots than the DFT adapters because DFT connections will, by design, use the first adapters they find, searching from slot 1.

Twinaxial Console

You can configure Personal Communications to act as the console for an AS/400. If you want to use full-function 5250 emulation, you must not use the console attachment; you must use Twinaxial Data Link Control (APPC).

Restrictions:

- The **Setup API functions** of the **File** menu cannot be used.
- **Copy** is the only editing function available.
- The file transfer function cannot be used.
- The session type cannot be set to Printer. (AS/400)
- Multiple console sessions cannot be used.
- The Enhanced Non-programmable Terminal User Interface (ENPTUI) cannot be transferred from the host system.
- The PC Organizer cannot be used.
- The screen size is always 24 x 80, even if 27 x 132 is specified.
- The cursor position cannot be moved by the mouse.

Asynchronous Console

For the asynchronous console attachment, you must have a 2609 or 2612 adapter for the Multiple Function I/O Processor (MFIOP) on the AS/400 system. This connection also requires a special cable. The part numbers for the cables are 46G0450 (6m) and 46G0479 (2.5m).

Note: The AS/400 Advanced Portable Model P02 does not support the asynchronous console attachment.

An asynchronous console has the following restrictions:

- Multiple console sessions cannot be used.
- APIs are not supported
- The session type cannot be set to the **Printer**.
- The file transfer functions is not supported.
- The PC Organizer cannot be used.

Adapter Setup Hints and Tips

The following sections provide additional information about configuring adapters, including PCMCIA and PCI cards.

Using Coax (3270) Adapters

Personal Communications supports IBM AT-bus, Micro Channel (MCA), and Plug and Play coax adapters; the configuration of each is described in the following sections.

3278/79 Emulation Adapter (ISA-Bus)

This adapter has a fixed I/O-port address and interrupt level (IRQ), but you have to set the memory address, which you can do only through the Personal Communications configuration.

The buffer address must be set. The default is CE000. If you happen to know that this address is already being used by another device, you should change it, but, when you first try to connect, Personal Communications will check the registry to find an available address anyway.

Under Windows 2000, if Personal Communications cannot acquire a system resource (that is, an IRQ, a memory address, or an I/O address) needed by this adapter, Personal Communications displays an error panel identifying the unavailable resource. For an IRQ conflict (this adapter uses IRQ 9 only), Personal Communications automatically tries to activate the polling feature instead of using IRQ 9; if this succeeds then no error panel is displayed. For a memory address conflict, you should use the Personal Communications coax adapter configuration panel to select another memory address. For an I/O address conflict, you should reconfigure the device that is using the I/O address to use some other I/O address.

IBM 3270 Connection Adapter (Micro Channel)

Micro Channel adapters need the same types of resource as AT-bus but configuration is much easier because the resources are all set by the workstation's hardware configuration and Personal Communications is able to read them.

Configure Personal Communications in the normal way. The default buffer address will be the one set in the system configuration. You should not change it.

Plug-and-Play Adapters

Configure Personal Communications in the normal way. The **Plug-and-Play** radio button is active and you do not have to configure the buffer address.

The first time that you insert the 3270 Emulation Credit Card Adapter into a PCMCIA slot or start your PC with the PCI card installed, Windows 95 or Windows 98 or Windows 2000 will prompt you for the location of the .INF file for the card. The .INF file is located in the directory where Personal Communications is installed. Under Windows 2000, the file is named IBM3270X.INF. Under Windows 95 and Windows 98, the file is named IBM3270.INF.

Note: Removing the card while you have an active connection will have unpredictable results.

3270 ISA-Bus and MCA Adapters and ROM Shadowing

These adapters use 8KB of workstation memory; the default values for the memory addresses are as follows:

- Adapter #0 CE000h - CFFFFh
- Adapter #1 D0000h - D1FFFh
- Adapter #2 D2000h - D3FFFh
- Adapter #3 D4000h - D5FFFh

Some types of workstation may use these areas, by default, for ROM shadowing in BIOS (the IBM PC350 for example). You should check the ROM-shadowing settings before installing an adapter, and disable the range that will be used by the adapter that you are going to install.

OEM Adapters

Personal Communications has an open API that enables vendors and other equipment manufacturers (OEMs) to provide adapter cards that allow for additional connectivity options, for example, additional X.25, ISDN, SDLC. or twinax support. After installing the OEM adapter, you can begin to configure it in the usual manner described in *Quick Beginnings*. However, at some point in the configuration process you may need to provide information required by the manufacturer of the OEM adapter card.

Using Twinax (5250) Adapters

The configuration of each IBM adapter type is described in the following sections. All the IBM adapters are supported; OEM adapters are supported if their manufacturer has created a device driver that is compatible with the IBM driver. For a list of adapter types, see “Twinax Adapter Types” on page 80.

IBM 5250 Plug-and-Play Adapter

In Personal Communications, set the **Adapter Type** to IBM 5250 Plug-and-Play Adapter. You do not have to set the **Interrupt Level**, **I/O Address**, or **Memory Address** fields; these fields are grayed out. Personal Communications automatically reads the interrupt level, I/O address, and memory address from the adapter card.

The first time that you insert the 5250 PCMCIA or PC Card adapter into a PCMCIA slot, or start your PC with the 5250 PCI card or 5250 ISA Express card (with Plug-and-Play BIOS enabled) installed, Windows 95, or Windows 98 or Windows 2000 prompts you for the location of the .INF file for the card. The .INF file is located in the directory where Personal Communications is installed. Under Windows 2000, the file is named IBM5250X.INF. Under Windows 95 and Windows 98, the file is named IBM5250.INF.

If you experience problems getting a host connection with the 5250 Emulation PCI Adapter and you have an IBM personal computer, upgrading the BIOS might solve the problem. You can find the date of your system BIOS by using your system setup when you boot your personal computer. Then you can look on the Internet to see if there is a later version for your personal computer. The IBM File Library Web site that has the latest BIOS upgrade files is located at:
www.pc.ibm.com/listfiles.html

From there you can search for your specific IBM personal computer. If there is a flash BIOS upgrade date later than that on your personal computer, download the file to your personal computer and follow the instructions that come with the file. For non-IBM personal computers, contact the manufacturer of your personal computer for BIOS upgrade information.

IBM 5250 MicroChannel Adapter

In Personal Communications, set the adapter type to IBM 5250 MicroChannel Adapter. You do not have to set the **Interrupt Level**, **I/O Address**, or **Memory Address** fields; these fields are grayed out. Personal Communications automatically reads the interrupt level, I/O address, and memory address from the adapter card.

IBM 5250 ISA Adapter

In Personal Communications, set the adapter type to IBM 5250 ISA Adapter. You must then set the interrupt level, I/O address, and Memory address to match the values set on the adapter card. For a new configuration, Personal Communications shows the default settings.

To view or change the settings on the adapter card, use the adapter configuration utility provided with the adapter. For the IBM Enhanced 5250 Display Station Emulation Adapter only, change the I/O address using switches on the adapter itself.

Under Windows 2000, if Personal Communications cannot acquire a system resource (that is, an I/O address, a memory address, or an IRQ) needed by this adapter, Personal Communications displays an error panel identifying the unavailable resource. To resolve this resource conflict, use the Personal Communications configuration panel to select another I/O address, memory address, or IRQ. If a conflict still exists, reconfigure the device that is currently using the resource to use some other resource.

Note: Removing a 5250 PCMCIA card or 5250 PC Card, or stopping a PCMCIA adapter slot containing a 5250 PCMCIA card or 5250 PC Card, will have unpredictable results.

IBM 5250 ISA Adapter (Asia-Pacific)

In Personal Communications, set the adapter type to IBM 5250 ISA Adapter (Asia-Pacific). You must then set the interrupt level and memory address to match the values set on the adapter card. For a new configuration, Personal Communications shows the default settings. The **I/O Address** field is grayed out; you do not need to set this field. Personal Communications automatically reads the I/O address from the adapter card.

To change the I/O address on the adapter card, use the switches on the adapter itself. To view the I/O address, or to view or change the interrupt level or memory address on the adapter card, use the adapter configuration utility provided with the adapter.

Twinax Connections Through a 5494 Controller to an AS/400

To set up a twinaxial connection to an AS/400 through a 5494 controller:

1. Click **Programs** → **IBM Personal Communications** → **SNA Node Configuration** from the Windows **Start** menu.
2. Click **Configure Connections** from the list of **Configuration options** and then click **Twinaxial** from the list of DLCs.
3. Click an entry from the list of configured twinaxial connections and click **View** → **Change** → **Add**.
4. Check **Link to preferred NN server**.
5. Click the Security tab.
6. In the **Adjacent CP name** field, enter the network ID and CP name of the 5494 controller.
7. Click **OK** to save the connection information.
8. Click **Configure Partner LU 6.2** from the list of **Configuration options**.
9. Click an entry from the list of **Partner LU 6.2** definitions and click **View** → **Change** → **Add**.
10. In the **Partner LU name** field, enter the CP name of the AS/400 system. The CP name is also known as the system location name.
11. In the **Fully qualified CP name** field, enter the network ID and CP name of the 5494 controller.
12. Click **OK** to save the Partner LU 6.2 information.
13. Click **Save As...** from the **File** menu.

14. Enter a file name with an .ACG file extension, such as `CFG5494.ACG`. Click **Yes** to make this configuration the default.

Note: To enable this configuration, configure the 5494 controller as a network node (NN).

Installing Devices When Upgrading Personal Communications

If you have upgraded from Personal Communications Version 4.3 to Personal Communications Version 5.0 in Windows 2000, you may receive the following error message when trying to use some IBM Plug-and-Play adapters.

```
"PCSCOAX051 - The 3270 Plug and Play Adapter could not be found.
Please check that the adapter device drivers and the card are
correctly installed."
```

This message appears because Personal Communications 5.0 uses the Other devices category of device driver in Windows 2000, while Personal Communications 4.3 uses the Multifunction adapters category. Also, Windows 2000 does not provide a Have Disk option if it already has a .inf file that matches the adapter and the new .inf specifies an adapter of a different category. Certain IBM Plug-and-Play adapters that were used and devices that were supported by Personal Communications 4.3 in Windows 2000 will be affected if Personal Communications 5.0 is installed. The adapters are as follows:

- IBM 3270 Emulation PCI Adapter
- IBM 5250 Express PCI Adapter
- IBM 5250 PCI Adapter
- IBM 5250 Express ISA Adapter, when the adapter's Plug-and-Play BIOS is enabled
- IBM PCI Multiprotocol SDLC Adapter

The following procedure should be used when installing IBM Plug-and-Play adapters under Windows 2000 when upgrading from Personal Communications 4.3 to Personal Communications 5.0. The IBM 3270 Emulation PCI Adapter is used as an example in this procedure.

1. Add a new device (from Personal Communications 5.0) for the adapter.

   This step prompts Windows 2000 to make a private copy of the Personal Communications 5.0 .inf file for this adapter.

   a. Begin adding the new device, using the **Add/Remove Hardware** option in the Control Panel.

   b. Click **Add a new device** in the Choose a Hardware Device panel.

   c. Click **No, I want to select the hardware from a list** in the Find New Hardware panel.

   d. Scroll down the list in the Hardware Type panel and select **Other devices**.

   e. When selecting the device driver, do not use the manufacturers or models listed. Instead, click **Have Disk** and specify the directory in which Personal Communications 5.0 was installed. The default directory is C:\Program Files\Personal Communications.

   f. The Select a Device Driver panel lists the IBM Plug-and-Play adapters supported by Personal Communications 5.0. Select **IBM PCI 3270 Emulation Adapter** from the list and click **Next**.

   g. Click **Next** in the Start Hardware Installation panel.

   h. Click **Finish** in the Completing the Add/Remove Hardware wizard panel.

   i. Do not restart the computer when prompted. If you accidentally restart the computer, continue with step 2 after rebooting.

2. Delete both the old device (from Personal Communications 4.3) and the new device (from Personal Communications 5.0) for this adapter. This step ensures that the new device can be installed properly.
   a. Click the **System** icon in the Control Panel.
   b. Select the Hardware tab in the System Properties panel.
   c. Click **Device Manager**.
   d. Delete the old Personal Communications 4.3 device for this adapter, using the following steps.
      1) Expand the **Multifunction adapters** entry in the list of devices in the Device Manager.
      2) Select **IBM PCI 3270 Emulation Adapter** in the list and then press mouse button 2.
      3) Select **Uninstall** from the list of options.
      4) Complete the removal. The list of devices in the Device Manager will be updated.
   e. Delete the new Personal Communications 5.0 device for this adapter, using the following steps.
      1) Expand the **Other devices** entry in the list of devices in the Device Manager.
      2) Select **IBM PCI 3270 Emulation Adapter** in the list and then press mouse button 2.
      3) Select **Uninstall** from the list of options.
      4) Complete the removal. The list of devices in the Device Manager will be updated.
   f. Close the Device Manager and exit the System Properties panel.
3. Reinstall a new device (from Personal Communications 5.0) for this adapter.
   a. Begin adding the new device, using the **Add/Remove Hardware** option in the Control Panel.
   b. The Add/Remove Hardware wizard will begin the installation process. Click **Next** in the Welcome to the Found New Hardware panel.
   c. Click **Display a list of known drivers for this device so that I can choose a specific driver** in the Install Hardware Device Drivers panel.
   d. The Select a Device Driver panel displays a Models listbox. Select **IBM PCI 3270 Emulation Adapter** and click **Next**.
   e. The Start Device Driver Installation panel will be displayed.

      Note: The name of the adapter should be displayed with a big yellow question mark icon, indicating that this device belongs to the class called Other devices. If this is case, click **Next**. However, if the big yellow question mark icon does not appear, you have selected the wrong device driver. You should then click **Back** and go to the Select a Device Driver panel. You should then choose another device driver from the Models listbox.
   f. Click **Finish** in the Completing the Found New Hardware wizard panel.
   g. Reboot the system when prompted to do so.
4. You now should be able to use the adapter under Personal Communications 5.0.

Appendix B. SNA Client/Server Concepts

Terminology

Advanced Program-to-Program Communication (APPC)
An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

Advanced Peer-to-Peer Networking (APPN)
An enhancement for Systems Network Architecture (SNA) networks featuring:

- Dynamic exchange of network topology information that simplifies connections, route selection, network definition, and reconfiguration
- Automated resource registration and directory lookup
- Greater distributed network control that helps to isolate the effects of single points of failure

Common Programming Interface for Communications (CPI-C)
Personal Communications provides support for the Common Programming Interface for Communications (CPI-C) 2.0 industry standard interface from X/Open. The CPI-C interface enables greater application portability across different platforms. By using CPI-C 2.0, APPC programming is simplified, resulting in reduced cycle time, and enhanced client/server computing capability. This support provides the capability for distributed parts of an application to converse with one another. The implementation is consistent with the Conversational function described in the IBM Open Blueprint®.

Logical Unit Address (LUA)
System software and interfaces that supply input/output (I/O) service routines to support communications that use LU types 0, 1, 2, and 3 SNA protocols. These protocols support user defined data streams, SNA character streams, and SNA 3270 data streams. LUA services include only those services that support data communications. LUA does not supply any device emulation facilities.

Node An endpoint of a link, or a junction, common to two or more links in a network. Nodes can be linked to host processors, communication controllers, cluster controllers, terminals, or workstations.

End Node
Provides directory and routing services for a workstation on an APPN network.

If the workstation will not be connecting from an end node to a network node server, you need to define an SNA connection.

APPC Concepts

Personal Communications provides Advanced Peer-to-Peer Networking (APPN) end node support for workstations, allowing them to communicate more flexibly with other systems in the network.

Personal Communications provides advanced program-to-program communications (APPC) to support communications between distributed processing programs, called *transaction programs* (TPs). APPN extends this capability to a networking environment. The TPs can be located at any node in the network that provides APPC.

Introducing APPC and CPI-C

Advanced Program-to-Program Communication (APPC), also known as LU 6.2, is software that enables high-speed communications between programs on different computers, from portables and workstations to midrange and host computers. APPC software is available for many different IBM and non-IBM operating systems, either as part of the operating system or as a separate software package.

APPC serves as an interface between application programs and the network. When the communications application on your workstation passes information to the APPC software, APPC takes the information and sends it on to a network interface, such as a token ring adapter card. The information travels across the network to another computer, where the APPC software receives the information from the network interface. APPC puts the information back into its original format and passes it to the corresponding communications application.

APPC provides a consistent set of functions for program-to-program communications across different platforms. But, the architecture did not specify a common application programming interface (API) for implementing these functions. As a result, each operating system that supports APPC developed its own API, a set of verbs that closely resemble the operating system itself. These differences do not pose a problem if you are writing programs for two computers that use the same operating system. Most client/server applications run on different types of computers, however, to take advantage of the strengths of each computer. So, if you are designing programs for different operating systems, you must learn how to use two or more different sets of verbs.

The Common Programming Interface for Communications (CPI-C) eliminates this problem. CPI-C provides one standard set of verbs, known as CPI-C calls, for all systems that support CPI-C. As a result, you learn only one set of calls to write client/server applications for different systems.

What Is a Transaction Program?

The part of the communications application that initiates or responds to APPC communications is called a transaction program. A transaction program is not an entire, stand-alone program. Instead, it is the part of the program that handles transactions (exchanges of data) with another program.

When people talk with each other, we say that they are having a conversation. Likewise, the communication between two transaction programs is called a conversation.

A conversation between two programs is similar to a conversation between two people. When you have a conversation with another person, you follow unwritten rules that govern how you begin and end the conversation, take turns speaking, and exchange information. Similarly, APPC is called a protocol because it provides the rules that govern how conversations between transaction programs start and stop, which program “speaks” first, and how data is exchanged. Computers need complete and rigid rules for conversations between programs. For that reason, APPC consists of a set of well-defined and thorough rules to cover all possible communications situations.

An APPC program may have several conversations active at one time, with the same transaction program or with different transaction programs.

Every transaction program needs a partner to communicate with. Thus, transaction programs are developed in pairs called partner transaction programs.

People use different parts of speech to communicate with each other. Transaction programs are more limited in their communications; they use only verbs to communicate with each other. The verbs are the programming language you use to start, stop, and control conversations.

A transaction program consists of APPC and CPI-C verbs such as:

ALLOCATE (CMALLC in CPI-C)
Starts a conversation with another transaction program

SEND_DATA (CMSEND in CPI-C)
Sends data to the partner transaction program

RECEIVE (CMRCV in CPI-C)
Receives data from the partner transaction program

DEALLOCATE (CMDEAL in CPI-C)
Ends a conversation with another transaction program.

The APPC verbs make up the application programming interface (API) for APPC and CPI-C. In other words, these verbs represent the interface between the transaction program and the APPC software.

What Is the Difference between APPC and APPN?

APPC is a communications protocol that enables programs on different computers to “talk to” each other. APPC provides the interface between the programs and the networking hardware and software and defines the rules that programs use to exchange information.

Advanced Peer-to-Peer Networking (APPN) is the underlying networking protocol that routes APPC traffic through intermediate nodes in the network. For instance, when Program A uses APPC to talk to Program B, APPN finds the node where Program B is located and directs the APPC traffic through the network.

APPN includes several features that help reduce the amount of configuration required to set up and maintain a network. These features automate many tasks that are time-consuming, complicated, and error-prone. For example, if you’re installing a new workstation that uses APPN, you don’t have to set up configuration information for every workstation you want to communicate with. You simply provide the name of the computer and the address of the intermediate node that handles your traffic. APPN takes care of the rest of the information needed to route APPC traffic to and from your workstation.

If you connect to an APPN network, you simplify your own configuration and make it easier for other computers in the network to find you.

Side Information Definitions

Before starting a conversation with a partner program, a CPI-C program requires the following information:

- The name of the partner program
- The name of the LU on the remote computer

- The type of session used by the program
- Security information

If the CPI-C partner program uses a blank symbolic destination name, a side information definition is not necessary.

Improving Productivity Using APPC

The advanced features of APPC help speed the development of robust client/server applications and keep development costs low.

Client/server applications often prove to be especially challenging to the programmer. It’s not enough to understand the details about the computer and operating system that your application uses. If you’re designing client/server applications, you have to deal with computers used by both sides of the application, as well as the intervening network. For instance, implementing effective security measures is more important and more complicated, since you must ensure security throughout the network. In addition, synchronization and error reporting are often problematic in a distributed environment, because both sides of the application must coordinate their work.

One reason that APPC has become so widely used in client/server applications is that it furnishes a complete set of useful functions like security, synchronization, and error reporting. If you use other protocols, you must build these functions in every application you write. For example, if you use NetBIOS, you must design and implement a strategy for security for each application. Not only does this approach require additional work, it may result in a number of incompatible security systems in your network. By contrast, APPC includes a common set of security services that are consistent across all APPC platforms.

Similarly, most protocols do not include synchronization functions. Synchronization is required by any program that cannot continue processing data until the data sent to the partner program has been received and processed. Rather than writing your own synchronization routine, APPC provides a Confirm call that you can use to handle synchronization between two programs.

Improving Productivity Using CPI-C

Because many client/server applications are distributed between mainframe systems and workstations, host programmers and workstation programmers must work together to develop partner applications. CPI-C bridges the gap between these programmers by providing a common language for designing the communications part of the applications. CPI-C also enables you to write the communications portion of an application without knowing the details of the operating system. After you write a CPI-C application, you can easily move the programs from one operating system to another with few changes. So, by using the CPI-C interface, you can port both your applications and your programming skills from one system to another, quickly and cost-effectively.

What Is a Logical Unit?

Every TP gains access to an SNA network through a *logical unit* (LU). An LU is SNA software that accepts verbs from your programs and acts on those verbs. A TP issues APPC verbs to its LU. These verbs cause commands and data to flow across the network to a partner LU. An LU also acts as an intermediary between the TPs and the network to manage the exchange of data between TPs. A single LU can provide services for multiple TPs. Multiple LUs can be active in the node simultaneously.

LU Types

Personal Communications supports LU types 0, 1, 2, 3, and 6.2. LU types 0, 1, 2, and 3 support communication between host application programs and different kinds of devices, such as terminals and printers.

LU 6.2 supports communications between two programs located at type 5 subarea nodes, type 2.1 peripheral nodes, or both, and between programs and devices. APPC is an implementation of the LU 6.2 architecture.

Communication occurs only between LUs of the same LU type. For example, an LU 2 communicates with another LU 2; it does not communicate with an LU 3.

When Personal Communications is configured, your local and partner LUs are defined once for each machine. When you design programs, you must understand the capabilities supported by the LU in the particular machines you plan to use.

Dependent and Independent LUs

A *dependent LU* depends on a system services control point (SSCP) to activate a session. A dependent LU needs an active SSCP-LU session, which the dependent LU uses to start an LU-LU session with an LU in a subarea node. A dependent LU can have only one session at a time with the subarea LU. For communications with a TP at a subarea node, each dependent LU can have only one conversation at a time, and each dependent LU can support communications for only one TP at a time.

An *independent LU* does not depend on an SSCP to activate a session. An independent LU supports multiple concurrent sessions with other LUs in a subarea node, so you can have multiple conversations and support multiple TPs for communications with subarea TPs. LUs between peripheral nodes also use this support.

The distinction between a dependent LU and an independent LU is meaningful only when discussing a session between an LU in a peripheral node and an LU in a subarea node. Otherwise, dependent and independent LUs both support multiple concurrent sessions and conversations when communicating between type 2.1 peripheral nodes, for example, between two Windows NT workstations. A Personal Communications LU can support a single session with a dependent LU or multiple sessions with an independent LU.

What Is a Session?

Before TPs can communicate with each other their LUs must be connected in a mutual relationship called a *session*. A session connects two LUs, so it is called an *LU-LU* session. Figure 1 on page 96 illustrates this communication relationship. Multiple, concurrent sessions between the same two LUs are called *parallel* LU-LU sessions.

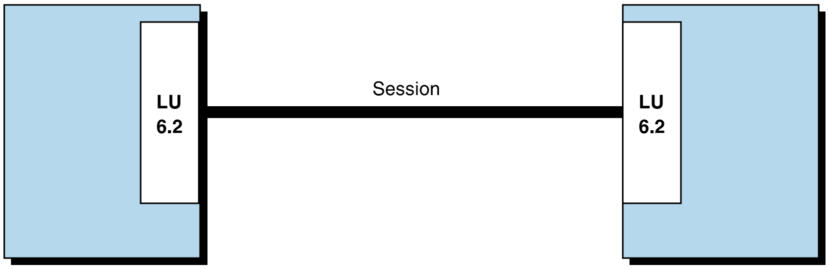

Figure 1. A Session between Two LUs

Sessions act as conduits that manage the movement of data between a pair of LUs in an SNA network. Specifically, sessions deal with things such as the quantity of data transmitted, data security, network routing, and traffic congestion.

Sessions are maintained by their LUs. Normally, your TPs do not deal with session characteristics. You define session characteristics when you:

- Configure your system
- Use the Session Services function in the Subsystem Management windows
- Use the management verbs

What Is a Conversation?

The communication between TPs is called a *conversation*. Conversations occur across LU-LU sessions. A conversation starts when a TP issues an APPC verb or CPI-C call that allocates a conversation. The conversation style associated with the conversation indicates the style of data transfer to be used, two-way alternate or two-way simultaneous. A conversation that specifies a two-way alternate style of data transfer is also known as a *half-duplex* conversation. A conversation that specifies a two-way simultaneous style of data transfer is referred to as a *full-duplex* conversation.

When a half-duplex conversation is allocated to a session, a send-receive relationship is established between the TPs connected to the conversation, and a two-way alternate data transfer occurs where information is transferred in both directions, one direction at a time. Like a telephone conversation, one TP calls the other, and they “converse”, one TP talking at a time, until a TP ends the conversation. One TP issues verbs to send data, and the other TP issues verbs to receive data. When it finishes sending data, the sending TP can transfer send control of the conversation to the receiving TP. One TP decides when to end the conversation and informs the other when it has ended.

When a full-duplex conversation is allocated to a session, both TPs connected to the conversation are started in send-and-receive state, and a two-way simultaneous data transfer occurs where information is transferred in both directions at the same time. Both TPs may issue verbs to send and receive data simultaneously with no transfer of send control required. The conversation ends when both TPs indicate they are ready to stop sending data, and each TP has received the data sent by the partner. If an error condition occurs, one TP may decide to end both sides of the conversation abruptly.

Conversations can exchange control information and data. The TP should select the conversation style best suited for its application.

A Conversation between Two TPs

Figure 2 shows a conversation between two TPs as it occurs over a session.

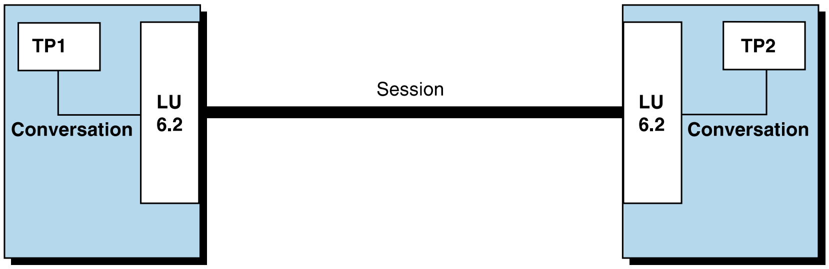

Figure 2. A Conversation between Two TPs

A session can support only one conversation at a time, but one session can support many conversations in sequence. Because multiple conversations can reuse sessions, a session is a long-lived connection compared to a conversation. When a program allocates a conversation and all applicable sessions are in use, the LU puts the incoming Attach (allocation request) on a queue. It completes the allocation when a session becomes available.

Two LUs can also establish parallel sessions with each other to support multiple concurrent conversations. A parallel session occurs when either TP allocates a conversation, and a session exists but is being used by a conversation. The LU can request a new session to satisfy the allocation.

Parallel Sessions between LUs

Figure 3 shows three parallel sessions between two LUs; each session carries a conversation.

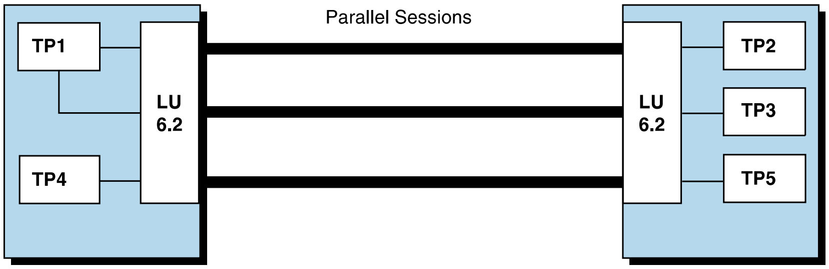

Figure 3. Parallel Sessions between LUs

SNA Communications

Personal Communications supports Systems Network Architecture (SNA) type 2.1 nodes (including SNA type 2.0 and SNA type 2.1 support for LUs other than SNA LU 6.2). This support lets you write programs to communicate with many other IBM SNA products.

You can write programs without knowing the details of the underlying network. All you need to know is the name of the partner LU; you do not need to know its location. SNA determines the partner LU location and the best path for routing data. A change to the underlying network, such as a physical address change, the addition of a new adapter, or the relocation of a machine, does not affect APPC programs. A program might, however, need to establish link connections over switched SDLC connections.

When Personal Communications starts, it establishes local LU and logical link definitions, which are stored in a configuration file. The system management application programming interface (API) provides functions that control configuration definition and adapter and link activation.

SNA Node Operations

With SNA Node Operations, either a user or system administrator can display information or take action on node resources that are known to the active node.

The following tasks are supported:

- Starting and stopping resources
- Deleting resources
- Displaying resource information
- Changing session limits
- Initiating path switches

Refer to the information about SNA node operations in the *3270 Emulator User's Reference*, *5250 Emulator User's Reference*, or the online help for information on using SNA node operations.

Appendix C. AnyNet SNA over TCP/IP

This chapter describes the AnyNet SNA over TCP/IP function of Personal Communications.

What Does AnyNet SNA over TCP/IP Do?

SNA over TCP/IP is one of the IBM AnyNet software offerings. AnyNet software enables application programs to communicate over different transport networks and across interconnected networks. Using AnyNet, you can reduce the number of transport networks and therefore reduce operational complexity. These benefits are gained without modification to your existing application programs or hardware.

The AnyNet function in Personal Communications enables SNA applications to communicate over an IP network. This includes APPC and CPI-C applications.

The following network configurations illustrate how SNA over TCP/IP access nodes and gateways can be used.

Running APPC or CPI-C Applications over a TCP/IP Network

Figure 4 illustrates how you can use the AnyNet SNA over TCP/IP function of Personal Communications to enable communication between SNA applications over an IP network. Configuration information for a similar configuration is provided in *Quick Beginnings*.

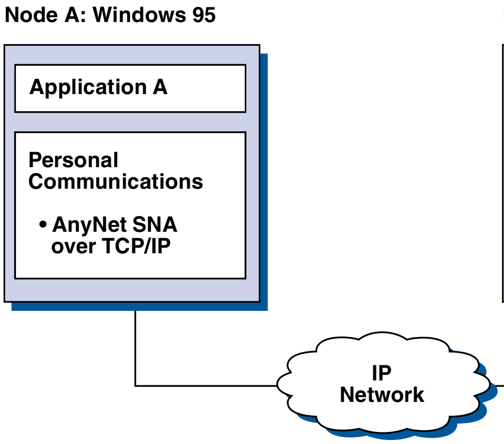

Figure 4. Running APPC or CPI-C Applications over a TCP/IP Network

Using AnyNet to Connect SNA Applications on Different Platforms

Figure 5 on page 100 illustrates some of the many products with AnyNet SNA over TCP/IP function. AnyNet gateways (Node F) allow SNA applications to communicate across a combination of TCP/IP and SNA networks.

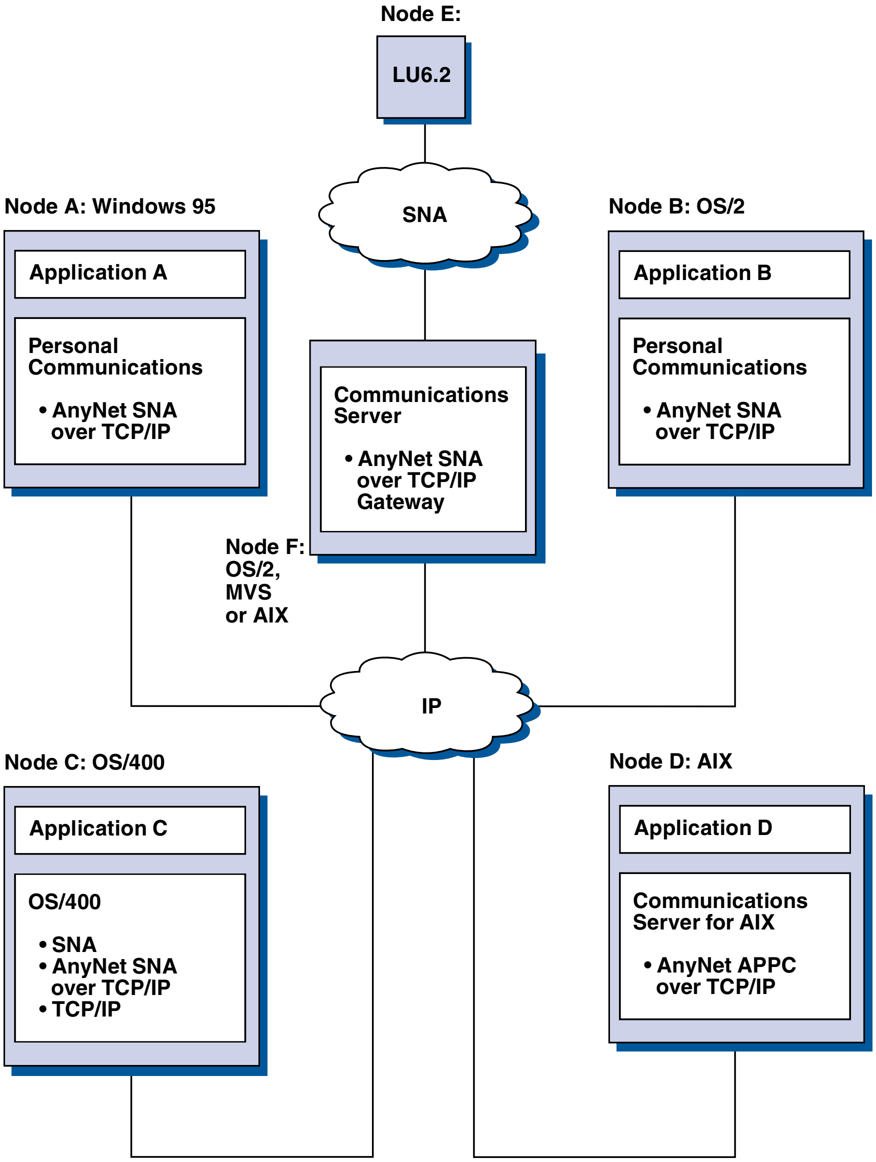

Figure 5. Using AnyNet to Connect SNA Applications on Different Platforms

Chaining Gateways to Connect Multiple SNA and IP Networks

Chained gateways enable the SNA network to connect multiple IP networks.

Note: While Figure 6 on page 101 shows three networks connected, the number of networks that can be concatenated is unlimited.

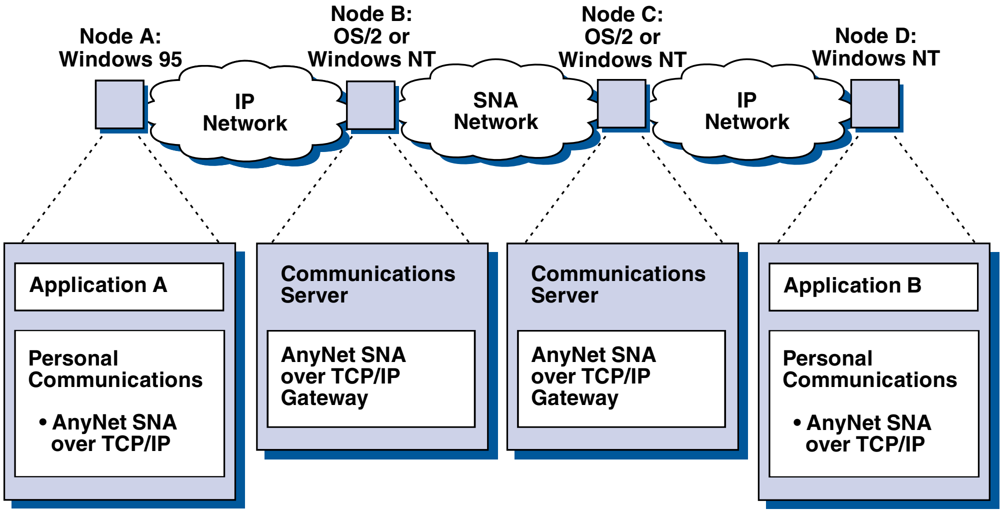

Figure 6. Chaining Multiple Gateways to Connect Multiple IP Networks

How Does SNA over TCP/IP Work?

SNA over TCP/IP uses protocols that bypass the lower transport layers of the SNA architecture. This process is transparent to the SNA application program. Using a supported API, an application program passes data to the presentation services of Personal Communications. This data, in turn, is passed through the SNA architectural layers and presented to SNA over TCP/IP at the data link control level. When Personal Communications initiates a session for an application program, SNA over TCP/IP translates the SNA routing information (network-qualified name) into IP routing information (IP address) and uses the IP address to create a TCP connection to the appropriate system.

Figure 7 on page 102 illustrates how an SNA over TCP/IP access node enables SNA application programs to communicate over IP networks.

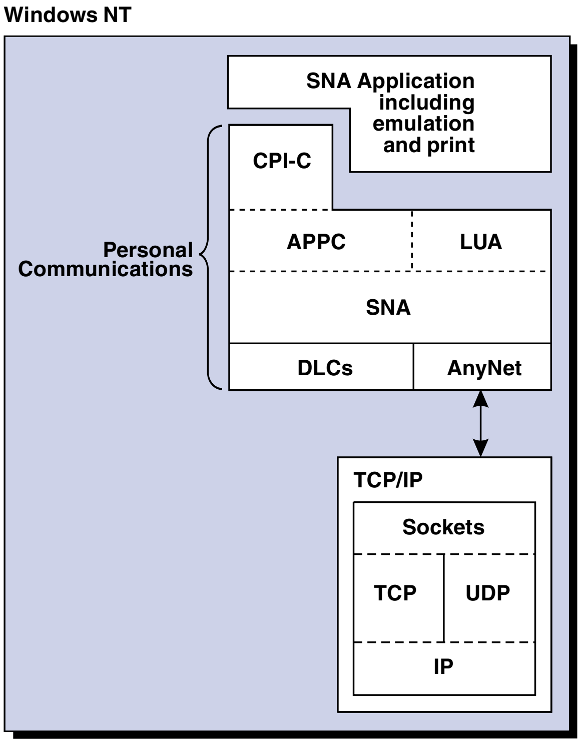

Figure 7. Structure of SNA over TCP/IP for Personal Communications

The configuration information you define enables SNA over TCP/IP to determine:

- Whether to route the data using SNA or to route the data using IP
- The IP address associated with the network-qualified LU name

SNA over TCP/IP uses both stream (TCP) and datagram (UDP) sockets that are bound to the well-known port (397). Any information received over this port is routed to AnyNet.

Mapping SNA Resources to IP Addresses

SNA over TCP/IP access nodes must determine the IP address of the partner before an SNA session can be established. The SNA identifier of the partner is mapped to an IP address using the following steps:

1. SNA over TCP/IP receives the SNA identifier from Personal Communications in one of the following formats:
   - For LU names, `netid.luname`
   - For CP names, `netid.cpname`
2. SNA over TCP/IP takes the identifier and generates a domain name:
   - For LU names, `luname.netid.snasuffix`
   - For CP names, `cpname.netid.snasuffix`

   Note: The default value for `snasuffix` is **SNA.IBM.COM**. For additional information on the SNA domain name suffix, refer to the online help.

   Figure 8 on page 103 shows examples of domain names generated by SNA over TCP/IP.

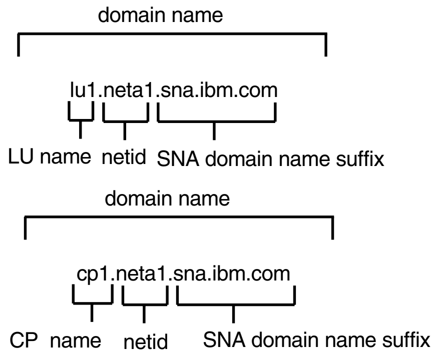

Figure 8. Formats of the Domain Names That SNA over TCP/IP Builds

3. SNA over TCP/IP requests that the domain name be translated into an IP address.
4. TCP/IP uses the HOSTS file or domain name server to translate the domain name into an IP address (for example, `9.67.192.28`).

When the IP network includes SNA over TCP/IP gateways, consider the following additional address mapping issue:

> If the partner LU can be reached through a gateway, the domain name of the partner must be mapped to the IP address of the gateway. If there are parallel gateways, the domain name should be mapped to each gateway IP address.

Defining Domain Names and IP Addresses

This section describes the TCP/IP name resolution function, used by AnyNet to map SNA resources to IP addresses. This function queries both the local HOSTS file and any domain name servers to convert a domain name (for example, `lu1.neta1.sna.ibm.com`) into an IP address (for example, 10.1.1.1).

HOSTS File

You can use TCP/IP HOSTS files to define domain names and IP addresses for your network. However, as your network becomes larger and maintaining the HOSTS file on each user workstation becomes too time-consuming, it is recommended that you use a domain name server.

The HOSTS file lists:

- IP address
- Domain name
- Other aliases for the domain name

Note: For Windows/NT this resides in the drivers\etc subdirectory of your NT system. For Windows 95 and Windows 98, this is in your Windows system directory.

For example, if your IP address is 10.1.1.1, network ID is NETA1, SNA resource name is LUA1, and SNA domain name suffix is the default (`sna.ibm.com`), enter the following in your HOSTS file:

```
10.1.1.1     lua1.neta1.sna.ibm.com
```

Domain Name Server

Domain names and IP addresses can also be defined in the domain name server database.

Each SNA identifier is mapped to a corresponding IP address by a domain name server. The location of these servers is configured in the Network section of the Control Panel.

For more information on HOSTS files and domain name servers, refer to your TCP/IP documentation. If your workstation is using the TCP/IP support in Windows 95, Windows 98, Windows NT, Windows Me, or Windows 2000, refer to the online TCP/IP documentation that is included with the Windows 95, Windows 98, Windows NT, Windows Me, or Windows 2000 product.

Defining Unique CP Names and Connection Network Names

For configurations that have two or more SNA over TCP/IP gateways connecting an SNA network with two or more IP networks, you must define a unique SNA control point (CP) name and a unique SNA connection network name for each IP network.

All LUs that reside on access nodes in the IP network appear to reside on a node with this CP name.

Use the reverse data file of the domain name server or the HOSTS file to define the CP name and the connection network name for a given IP network. Map the IP address 127.0.0.3 to the CP name and map the IP address 127.0.0.4 to the connection network name.

The following example shows entries in the reverse data file. For an IP network with SNA network ID NETA, CP name MYCPNAME, and connection network name MYCNET, you would define the following entries:

```
127.0.0.3       NETA.MYCPNAME.
127.0.0.4       NETA.MYCNET.
```

Notes:

1. A period is required at the end of the name only if the definition is in the DNS reverse data file. No period is used in HOSTS file definitions.
2. Do not include the SNA domain name suffix.

The AnyNet SNA over TCP/IP function of Personal Communications provides a default CP name ($ANYNET.$GWCP) and a default connection network name ($ANYNET.$GWCNET). In configurations with one IP network, you can use the default by not defining a CP name or a connection network name. In configurations with multiple gateways connecting multiple IP networks, one IP network can use the default. You must, however, define a unique CP name and connection network name for all other IP networks.

Figure 9 on page 105 shows how to define the CP name and the connection network name for a configuration with two IP networks. An example is provided in *Quick Beginnings*.

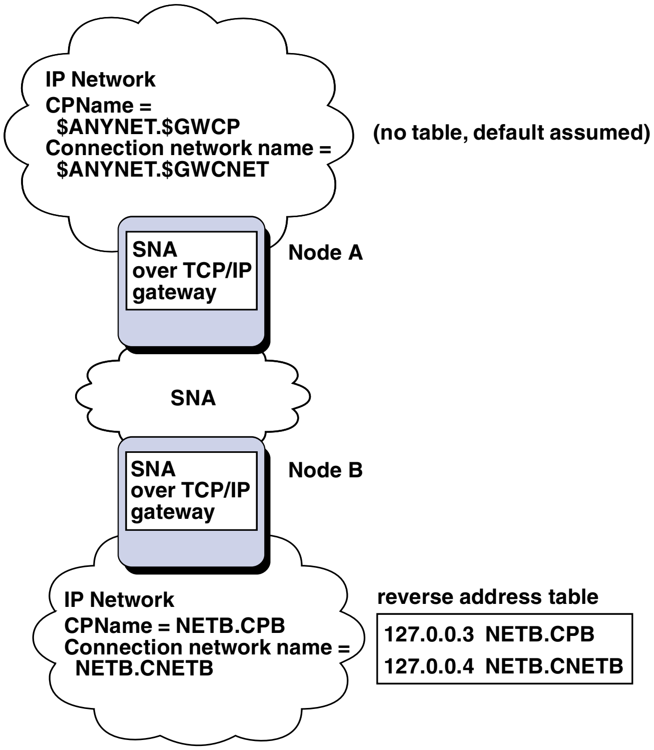

Figure 9. Defining a CP Name and a Connection Network Name

Setting and Modifying the Routing Preference Protocol

When an SNA application initiates a session, Personal Communications must first determine which transport to use, either SNA, IP, or a combination of the two.

Personal Communications uses the default routing preference for the session unless there is a specific routing preference set for the partner LU. Personal Communications then sets up a session for the partner LU using the preferred transport.

If the partner is not available through the preferred transport, Personal Communications can reroute the session request over the other available transport, depending on the setting in the routing preference table. For example, if the setting in the routing preference table for the destination LU is nonnative first, Personal Communications will attempt to set up the session over TCP/IP. If the partner is not available through TCP/IP, Personal Communications will route the session over SNA. However, if the setting in the routing preference table for the destination LU is nonnative only, Personal Communications will attempt to set up the session over TCP/IP. If TCP/IP is not available, Personal Communications will not route the session over SNA, because the setting allows only Personal Communications to use nonnative transport.

The routing preference table is used only for new sessions. Previously existing sessions use the same transport; they are not brought down and rerouted if the routing preference table is changed.

You can set or modify the default routing preference to one of the following:

Native first
Requests are routed over SNA. If no SNA route is available, requests are routed over TCP/IP.

Nonnative first
Requests are routed over TCP/IP. If no TCP/IP route is available, requests are routed over SNA.

Native only
Requests are routed only over SNA. If no SNA route is available, the connection will fail.

Nonnative only
Requests are routed only over TCP/IP. If no TCP/IP route is available, the connection will fail.

Helpful Hints

This section contains helpful hints on tuning, TCP/IP connectivity via SLIP or PPP, and dynamic IP addresses.

Tuning

If you can access an LU through multiple SNA over TCP/IP gateways, and you have mapped that LU name to multiple IP addresses, increase the Connection retry duration and Connection wait time limit when configuring the AnyNet base parameters. This ensures that TCP attempts to connect to all possible adapters and gateways. It can take as long as 90 seconds for a TCP connection to fail to an inactive IP address.

Connecting to AS/400

If you are unable to connect to AS/400 using SNA over TCP/IP, use the following procedure:

1. Make sure that the ANYNET support on the AS/400 is activated. Issue the command **DSPNETA** on the AS/400 and make sure the ANYNET status is yes.
2. Edit the HOSTS file on the PC, mapping the IP address to the CP name of the AS/400.
3. Reboot the PC; the SNA over TCP/IP connection is then activated.

Dynamic IP Addresses

Generally, AnyNet SNA over TCP/IP depends on SNA resources (for example, LU names, CP names, or idblk/num) being statically mapped to IP addresses. However, depending on your configuration and how your connections are initiated, you might be able to use AnyNet SNA over TCP/IP in environments where IP addresses are dynamically assigned (for example, DHCP).

APPC or CPI-C Applications

An SNA over TCP/IP access node with a dynamically assigned IP address may always initiate sessions to another SNA over TCP/IP access node or gateway with a static IP address.

The only way an SNA over TCP/IP access node or gateway with a static IP address (node A) can initiate a session to a partner with a dynamic IP address (node B) is:

- Node B initiated a session to or through node A first.
- The session initiated in Step 1 is still active.

Dependent LU Applications

Note: The information in this section applies to LU 0, 1, 2, 3, or dependent 6.2 applications.

SNA over TCP/IP access nodes with dynamically assigned IP addresses can support dependent LU communications if the following criteria are met.

- Dependent LU communication is occurring through an SNA gateway either through:
  - Communications Manager/2 V5 or later
  - Communications Server for Windows NT 5.0 or later
- The SNA over TCP/IP access node with a dynamically assigned IP address initiates connections to an SNA gateway with a static IP address.

Dependent LU communication through DLUS/DLUR over AnyNet SNA over TCP/IP is not supported if the DLUR node has a dynamically assigned IP address.

AnyNet Configuration Examples

This section includes examples of AnyNet running SNA over IP connections.The following configuration instructions are complete only for the Windows NT and Windows 95 operating systems. In all examples, the SNA domain name suffix is SNA.IBM.COM.

Notes:

1. In the following examples, Windows 95 is shown; Windows 98 can be treated the same.
2. Windows NT is shown; Windows 2000 can be treated the same.

Example 2. Running APPC or CPI-C Applications over a TCP/IP Network

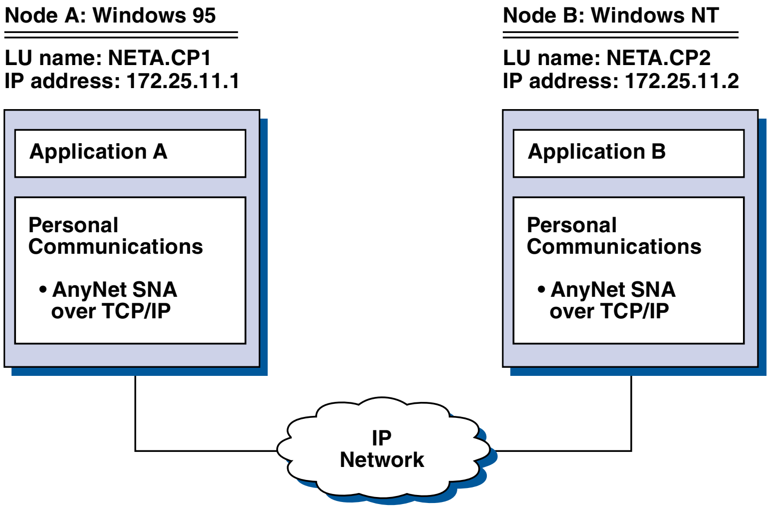

Figure 10. Running APPC or CPI-C Applications over a TCP/IP Network

Follow these steps to establish communication between a Windows NT node and a Windows 95 node. Note that in this example, the CP names are used as LU names.

For Windows 95 Node A, do as follows:

1. Add the following entry to the local HOSTS file:

   ```
   172.25.11.2  CP2.NETA.SNA.IBM.COM
   ```

2. Create a configuration using the Personal Communications configuration tool:
   a. Click the **SNA Node Configuration** icon; or click **Actions** → **Launch** → **SNA Node Configuration**. The Personal Communications SNA Node Configuration window is displayed.
   b. In the Configuration Options list, choose **Configure Node** and click **New**.
   c. On the Define the Node window on the Basic tab, enter:

      Fully qualified CP name: `NETA.CP1`

      Click **OK** to complete node configuration.
   d. Choose **Configure Devices**. In the **DLCs** list, choose **AnyNet SNA/IP** and click **New**.
   e. On the Define an AnyNet SNA over TCP/IP Device window on the Basic tab, enter:

      SNA domain name suffix: `SNA.IBM.COM`
   f. Click the **Routing Preferences** tab:

      Default Routing Preference: Nonnative only

      Click **OK** to complete configuration of the AnyNet device.
   g. From the Personal Communications SNA Node Configuration window, click **File**. Click **Save as...** and enter the desired file name to save.

For Windows NT Node B, do as follows:

1. Add the following entry to the local HOSTS file:

   ```
   172.25.11.1  CP1.NETA.SNA.IBM.COM
   ```

2. Create a configuration using the Personal Communications configuration tool:
   a. Click the **SNA Node Configuration** icon; or click **Actions** → **Launch** → **SNA Node Configuration**. The Personal Communications SNA Node Configuration window is displayed.
   b. In the Configuration Options list, choose **Configure Node** and click **New**.
   c. On the Define the Node window on the Basic tab, enter:

      Fully qualified CP name: `NETA.CP2`

      Click **OK** to complete node configuration.
   d. Choose **Configure Devices**. In the DLCs list, choose **AnyNet SNA/IP** and click **New**.
   e. On the Define an AnyNet SNA over TCP/IP Device window on the Basic tab, enter:

      SNA domain name suffix: `SNA.IBM.COM`
   f. Click the **Routing Preferences** tab:

      Default Routing Preference: Nonnative only

      Click **OK** to complete configuration of the AnyNet device.
   g. From the Personal Communications SNA Node Configuration window, click **File**. Click **Save as...** and enter the desired file name to save.
3. Start Personal Communications on each machine.
4. Start your applications (for example APING).

Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters

InstallShield Professional uses setup.exe as the bootstrap loader to call the Microsoft Windows Installer service. Setup.exe can accept command-line parameters that allow you to perform administrative installations, run silent installations, and complete other administrative tasks. Using the /v parameter, other parameters can also be passed through setup.exe to the Windows Installer database (MSI package). For information on using the /v parameter to perform initialization file processing see "Initialization File Processing Using Windows Installer" on page 35.

Setup.exe accepts the command-line parameters listed in Table 5. Descriptions of each parameter are listed in "Parameter Descriptions".

Table 5. InstallShield Command-Line Parameters

Parameter	Description
/v	Passes parameters to MSI package.
/s	Performs silent installation.
/l	Specifies the setup language.
/a	Performs administrative installation.
/j	Installs in advertise mode.
/x	Performs setup uninstall.
/f	Launches setup in repair mode.

Parameter Descriptions

Passing parameters to the MSI package

/v

The /v command-line parameter enables you to pass parameters supported by Windows Installer through setup.exe to the MSI package. For example, you can create and save a verbose log file to a location of your choice by passing the /L parameter through setup.exe to the MSI package. To create the log file, type:

```
E:\install\pcomm\setup.exe /v"/L*v C:\temp\setuplog.log"
```

where E: is your CD-ROM drive. For more information on supported command-line parameters and specific usage examples refer to the Web site http://www.msdn.microsoft.com.

Note: The /v argument must be the last InstallShield parameter on the command line. Though supported Windows Installer parameters may be passed through to the MSI package, no InstallShield command-line parameters can follow the /v argument.

Running setup.exe silently

/s

To prevent setup.exe from displaying a progress bar, use the /s command-line parameter. To have setup run silently with no dialogs, pass the Windows Installer /qn command-line parameter through setup.exe using the /v parameter. To run a silent installation, type:

```
E:\install\pcomm\setup.exe /s /v"/qn"
```

where E: is your CD-ROM drive. This example performs a typical installation of Personal Communications to your local hard drive without showing a progress bar or input dialogs. For information on property values and features included in a typical installation, see "Typical Installation" on page 21 and "Feature Selection" on page 24.

Note: You can pass an initialization file to the MSI package and run the installation silently using the /s /v /qn parameters in the following command:

```
E:\install\pcomm\setup.exe /s /v"USEINI=\"C:\Personal Communications\pcomm.ini" /qn"
```

For more information on initialization file processing see "Initialization File Processing Using Windows Installer" on page 35.

To install silently from source, where source medium is a network server, use the /s /v /qn parameters after pointing to the installation point in the command line. See "Chapter 5. Administrative Installation" on page 31 for more information on performing administrative installations and installing from a network server.

To uninstall Personal Communications silently, use the /s parameter in conjunction with the /x parameter as shown in the following example:

```
X:\install\pcomm\setup.exe /s /x
```

where X: is the location of the Personal Communications installation directory.

Specifying the setup language

/l

The /l command-line parameter enables you to specify what language to use during setup by using the appropriate decimal language identifier. For a list of language identifiers, see "Appendix E. National Language Support (NLS) Abbreviations and Language Codes" on page 113. For example, to change the setup language to Czech, type:

```
E:\install\pcomm\setup.exe /l"1029"
```

Administrative installation

/a

Administrative installation installs a source image to the network server. This enables users with access to the network to install Personal Communications directly from the network server.

Advertise mode

/j

Advertisement enables users to install features of Personal Communications when they need them rather than during setup. Features that are available for installation are advertised with shortcuts on the user's system for later installation.

Uninstall mode

/x

Uninstall mode removes Personal Communications from your system.

Repair mode

/f

Launching setup.exe in the repair mode checks the key file of every installed feature and reinstalls any feature that is determined to be missing or corrupt.

Appendix E. National Language Support (NLS) Abbreviations and Language Codes

Table 6 lists the abbreviations and language codes that are shipped with Personal Communications Version 5.5. These codes are used in conjunction with the /l command-line parameter and in language string tables and dialogs. For more information on the /l command-line parameter see "Appendix D. InstallShield Professional for Windows Installer (IPWI) Command-Line Parameters" on page 109.

Table 6. National Language Support Abbreviations and Language Codes

Language	**Abbreviations (CD-ROM)**	**Language Codes (shipped as *.mst transform files)**
Czech (Czech Republic)	cs_CZ	1029
Danish (Denmark)	da_DK	1030
Dutch (Netherlands)	nl_NL	1043
English (United States)	en_US	1033
Finnish (Finland)	fi_FI	1035
French (France)	fr_FR	1036
German (Germany)	de_DE	1031
Hungarian (Hungary)	hu_HU	1038
Italian (Italy)	it_IT	1040
Japanese (Japan)	ja_JP	1041
Norwegian (Bokmål) Norway)	no_NO	1044
Polish (Poland)	pl_PL	1045
Portuguese (Brazil)	pt_BR	1046
Portuguese (Portugal)	pt_PT	2070
Russian (Russia)	ru_RU	1049
Slovenian (Slovenia)	sl_SL	1060
Spanish (Traditional-Spain)	es_ES	1034
Swedish (Sweden)	sv_SE	1053
Turkish (Turkey)	tr_TR	1055
The following languages are provided in separate, single-language, packages:		
Korean (Korea)	ko_KR	1042
Simplified Chinese (People's Republic of China)	zh_CN	2052
Traditional Chinese (Taiwan)	zh_TW	1042

For more information on using transform files, refer to http://www.msdn.microsoft.com.

Appendix F. Notices

This information was developed for products and services offered in the United States. IBM may not offer the products, services, or features discussed in this information in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this information. The furnishing of this information does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS INFORMATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this information at any time without notice.

Any references in this information to non-IBM documentation or non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those documents or Web sites. The materials for those documents or Web sites are not part of the materials for this IBM product and use of those documents or Web sites is at your own risk.

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
Department T01
Building 062
P.O. Box 12195
Research Triangle Park, NC 27709-2195

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Programming License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries, or both:

400
ACF/VTAM
AFP
AIX
AIXwindows
AnyNet
APL2
APPN
AS/400
AT
Advanced Peer-to-Peer Networking
Application System/400
BookManager
CICS
CICS/MVS
CICS/VSE
COBOL/2
CUA
Common User Access
Client Access
Client Access/400
Current
DB2
DB2/400
DRDA
DisplayWrite
Distributed Relational Database Architecture
ExecJet
GDDM
Global Network
IBM
IBMLink
IIN
IMS
InfoWindow
MVS/ESA
MVS/XA

Microsoft, Windows, Windows NT©, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

PC Direct is a registered trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

C-bus is a trademark of Corollary, Inc.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

Readers' Comments — We'd Like to Hear from You

Personal Communications for Windows, Version 5.5
Access Feature

Publication No. SC31-8684-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

SC31-8684-02

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

IBM®

Program Number:

♻ Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC31-8684-02