APPENDIX 1

Getting Started with Remote Access Service

This chapter helps users install and get started with Remote Access Service. For details, see online help.

Overview and Planning

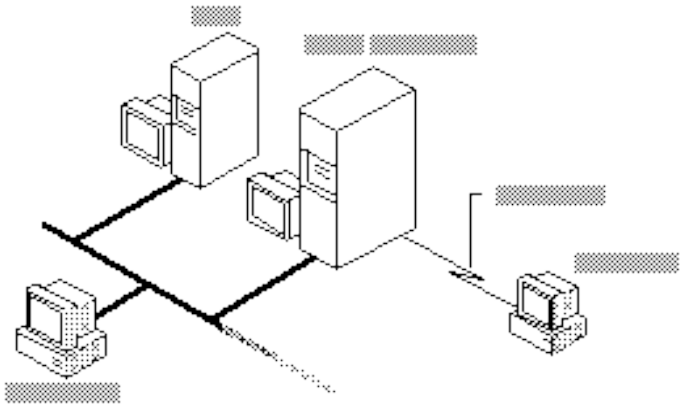
Windows NT Remote Access Service contains two main components:

Remote Access Components

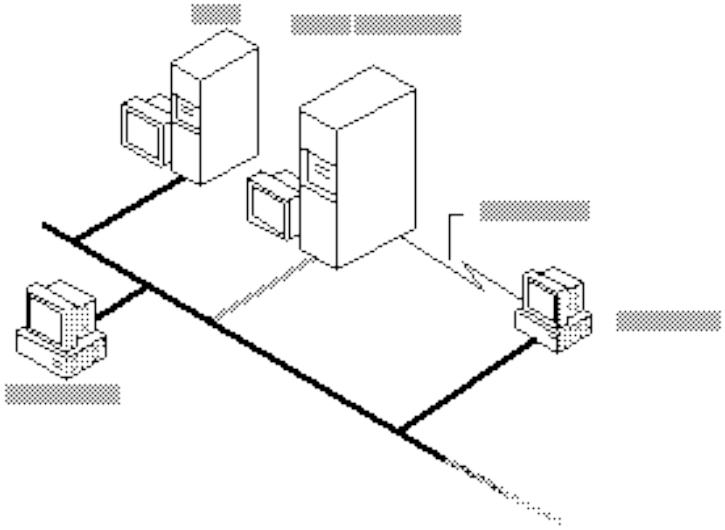
Component	Description
Remote Access Server	A Windows NT workstation configured to accept incoming calls.
Remote Access Client	A Windows NT, MS-DOS, or Microsoft Windows computer that dials in to a server.

Windows NT can act as both a server and a client.

A *remote client* is a computer (or workstation) that is not directly connected to a network. The user calls a server and connects to the network through a telephone line, as shown in the following illustration.



Once connected, the telephone link is transparent. From the remote client, users can see and gain access to network resources on the LAN just as they do in the office from a computer physically connected to the LAN. In this way, Remote Access Service acts as a *gateway* between the remote client and the network, as shown in the following illustration.

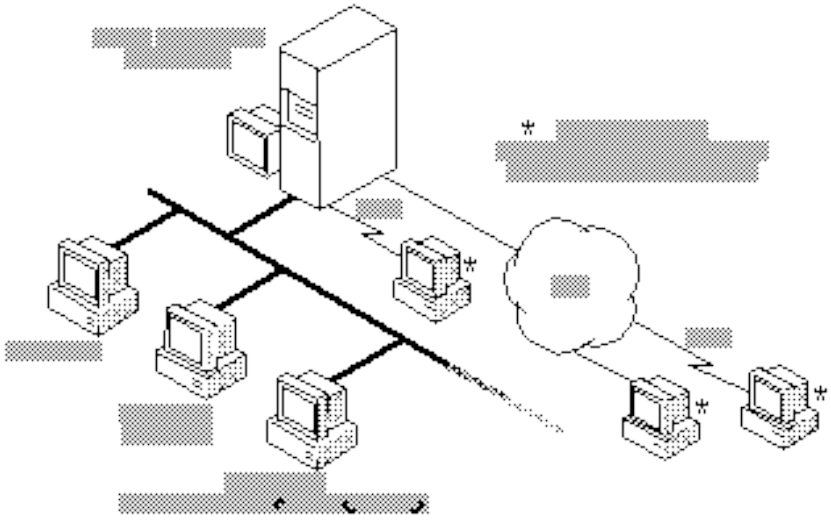


Remote Access Service features the Remote Access Phone Book program (RASPHONE.EXE) for entering and maintaining the names and telephone numbers of remote networks. Clients can connect to and disconnect from these networks through the Phone Book. (For information about using the Remote Access Phone Book, see the online help.)

Remote Access Service also has an Administrator's utility, which is a graphical user interface for system administrators. Through the Administrator's utility, you can do the following:

- Start, stop, pause, or continue the Remote Access server.
- Grant Remote Access permission to or revoke it from individual users.
- Monitor Remote Access traffic and user accounts.

The Administrator's utility also runs on Windows NT workstations, allowing you to monitor Remote Access servers and users from any computer on the network, including a remote one. The Windows NT Event Viewer, located in the Administrative Tools group, lets you see events and errors audited by Remote Access Service. For details about the Event Viewer, see the *Microsoft Windows NT System Guide.*



Overview of Windows NT Remote Access Service

Features

Windows NT Remote Access Service offers the following features:

- Compatibility with workstations and servers running Remote Access Service versions 1.0 and 1.1.
- Support for X.25 wide-area networks.
- Support for modem data compression.
- Transparent access to any network running Windows NT, LAN Manager for UNIX, LAN Manager version 2.x, and LAN Server.

- Security:
  - Integration with Windows NT user accounts.
  - Explicit Remote Access permissions.
  - Encrypted authentication.
  - Support for third-party security hosts that authenticate users.
- Callback for either added security or user convenience.
- Central administration of servers and users.
- Support for all the modems listed in the Remote Access online help.
- Support for NetBIOS, named pipes, RPC, and the LAN Manager application programming interface (API).

Setting Up Remote Access Service

1. In the Windows NT Control Panel, double-click the Network icon.
2. Click Add Software.
3. From the drop-down list, click Remote Access.
4. Click Continue.
5. From the Installation Options dialog box, choose the software you want to add to your Windows NT setup: Remote Access Server, Remote Access Client, and/or Remote Access Admin Program.
6. Click OK.
7. Follow the instructions on the screen.

   If you need help, click the Help button on any of the Remote Access Setup screens.
8. When the software is installed, reboot the machine.

When you return to Windows NT, you will see the Remote Access Service group, which contains the Remote Access icon(s).

Allowing Others to Connect to Your Workstation

Without permission, users cannot dial in to your workstation, even if the Remote Access client software has been installed on their computers.

To grant Remote Access permission to users

1. Start the Administrator's utility by double-clicking the RAS Admin icon in the Remote Access Service group.
2. From the Users menu, choose Permissions.

   The Remote Access Permissions dialog box appears.

You can grant or revoke Remote Access permissions to either one user at a time or to all users at once. For more information on granting Remote Access permissions, click Help.

X.25 Support

The Remote Access Service lets you access an X.25 network in two general ways:

Method of access	Server/Client
Asynchronous PADs	Client (for the Windows or Windows NT system)
Direct connections	Server and client (for the Windows NT system only)

X.25 Configurations

Remote Access Service for X.25 networks offers three configurations for the client and two for the server:

Client/ Server	Configuration
Client	Dial-up PAD
Client	Direct connection through X.25 smart card
Client	External PAD
Server	Direct connection through X.25 smart card
Server	External PAD

Accessing X.25 Through Dial-Up PADs

Operating between the client and the Remote Access server, an asynchronous PAD converts serially transmitted data into X.25 packets. When the PAD receives a packet from an X.25 network, it puts the packet out on a serial line, making communication possible between the client and the X.25 network.

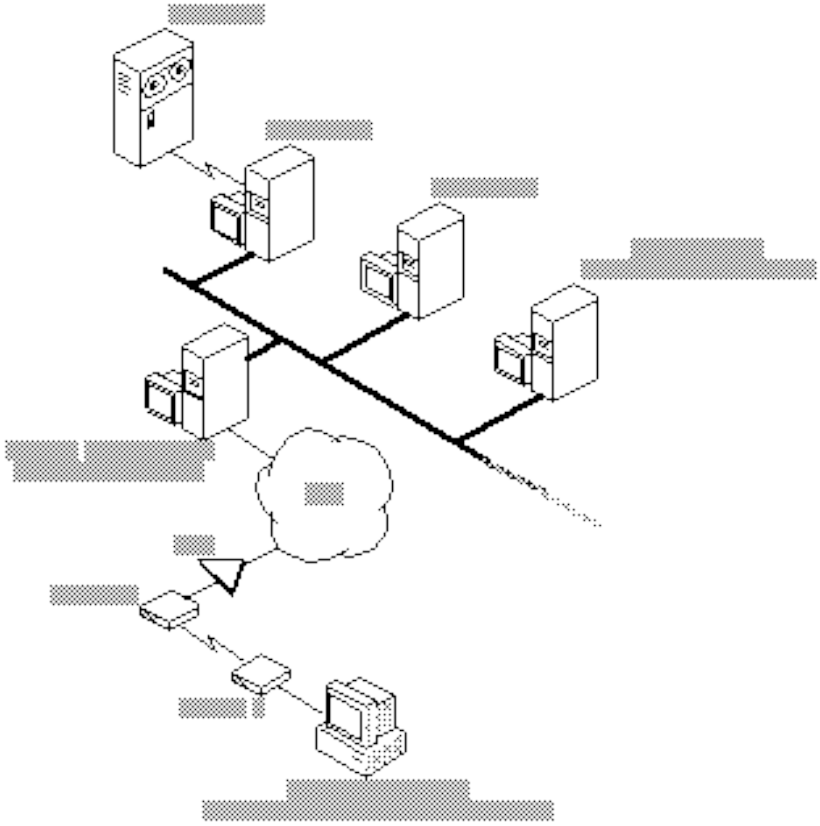
Remote Access clients can connect with Remote Access servers through dial-up PAD services supplied by X.25 carriers, such as Sprintnet and Datapac. Once the client's modem (modem A in the following illustration) connects to the PAD's modem (modem B), the client software must converse with the dial-up PAD. When their conversation is successfully completed, a connection is established between client and server.

Note

To avoid problems, make sure the client modem is compatible with the PAD carrier's modem. For further information, contact the PAD carrier and ask what type of modem makes the best connection.

The conversation (command/response scripts) for the PADs supported by an X.25 carrier is stored in the PAD.INF file. Remote Access software supplies one example. To customize for your PAD, see “PAD.INF Format” later in this chapter, and use the editing program you’re familiar with.

The following illustration shows how a client connects to the Remote Access server through a dial-up PAD and the X.25 network.



How Remote Access Connects to the Server Through a Dial-Up PAD

Dial-up asynchronous PADs constitute a practical choice for Remote Access clients because they don’t require an X.25 line plugged into the back of the workstation. Their only requirement is the telephone number of the PAD service for the carrier.

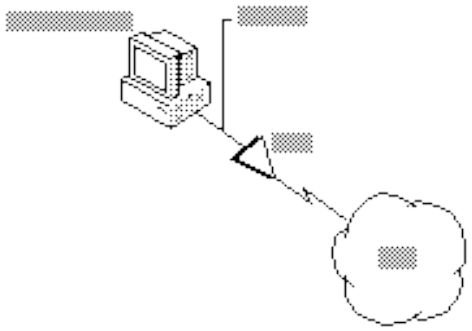
The following table compares connecting through dial-up PADs and connecting directly:

Comparison of Dial-Up PADs to Connecting Directly

Dial-Up PAD	Direct connection
Saves the expense of a dedicated leased line (direct connection).	Requires expensive leased line.
Allows connections from hotels, airports, homes—anywhere a phone line is available.	Requires users to dial in from a fixed location.
Requires two steps to connect.	Connects conveniently in one step.
Limits maximum communication speed to 9600 bits per second (bps).	Lets communication take place up to the speed of a leased line, 56 kilobytes (K).
Allows less control in configuring PADs.	Offers greater reliability.

Client External PAD

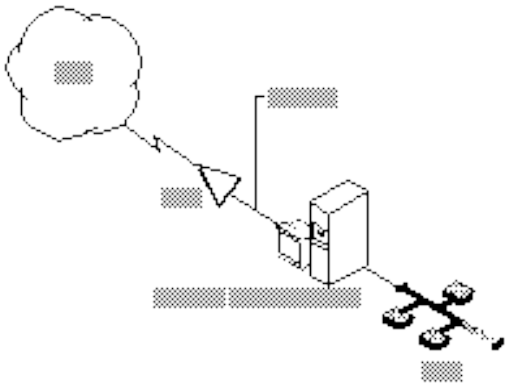
In this configuration, the PAD is connected to the client workstation by an RS-232 cable attached to a serial port. In the PAD.INF file, create a section that contains a dialog script for connecting to a server. For examples, see the MODEM.INF file.



Client Connecting to the X.25 Network Through an External PAD

Server External PAD

Servers with external PADs must be configured to receive incoming calls. As with the client, in the PAD.INF file create a section that contains a dialog script for connecting to clients. For examples, see the PAD.INF file.



Server Connecting to the X.25 Network Through an External PAD

PAD and Serial Configuration

To configure your PAD correctly, set the X.3 parameters as shown in the following table.

X.25 Configuration Values

Parameter number	X.3 parameter	Value
1	PAD Recall	0
2	Echo	0
3	Data Fwd. Char	0
4	Idle Timer	1
5	Device Ctrl	0
6	PAD Service Signals	1
7	Break Signal	0
8	Discard Output	0
9	Padding after CR	0
10	Line Folding	0
11	*Not Set*	
12	Flow Control	0
13	Linefeed Insertion	0
14	Padding after LF	0
15	Editing	0
16	Character Delete	0

X.25 Configuration Values (*continued*)

Parameter number	X.3 parameter	Value
17	Line Delete	0
18	Line Display	0
19	Editing PAD Srv Signals	0
20	Echo Mask	0
21	Parity Treatment	0
22	Page Wait	0

Caution

Failure to set these values as shown prevents the Remote Access Service from functioning properly. For information on setting these values, see the instructions with your X.25 smart card.

Also, configure external and dial-up PADs to the following serial communication settings:

- 8 databits
- 1 stopbit
- No parity serial communication

For dial-up PADs, make sure your vendor supports this configuration. The PADs are often already set to the correct configuration for connecting directly through an internal X.25 smart card. Do not change it.

Connecting to the X.25 Network Directly

The Remote Access Service also supports connecting directly from the remote workstation to the X.25 network through a smart card. An *X.25 smart card* is a hardware card with a PAD embedded in it. To the personal computer, the X.25 virtual circuit looks like a communication port with an advanced modem connected to it.

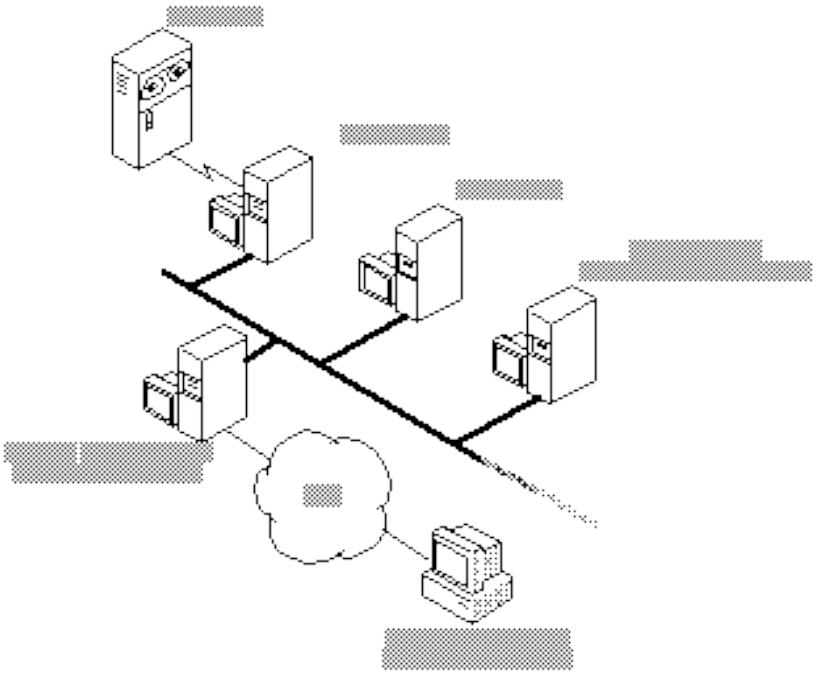
To access the X.25 network through a direct connection, you need:

- A direct line connection to an X.25 network (clients only).
- A smart card.

Note

The server side always requires an X.25 smart card, but the client side requires one only when connecting to the X.25 network directly.

The following illustration shows how the server and a Windows NT – based client (both equipped with smart cards) connect to the X.25 network directly.



Connecting to an X.25 Network Directly

Callback

The Remote Access server does not support callback on X.25 networks.

Setting Up the Remote Access Server for an X.25 Network

To set up the server to connect through an X.25 network

1. Install the X.25 smart card (according to the manufacturer's instructions).

A communications driver for the X.25 smart card supplied by the hardware manufacturer or a third party then emulates communication ports.

2. Make sure your X.25 smart card is configured with the X.3-parameter values shown in the X.25 Configuration Values table earlier in this chapter.
3. Install Remote Access Service through the Windows NT Control Panel.
4. From the list of devices on the Remote Access Setup screen, select an entry corresponding to the X.25 smart card.
5. In setting up the Remote Access server, make sure that the ports selected are configured for dial in.

Note

Make sure that the speed of the leased line can support all the serial communication (COM) ports at all speeds at which clients will dial in. For example, 4 clients connecting at 9600 bps (through dial-up PADs) will require a 38,400-bps (4 times 9600) leased line on the server end. If the leased line does not have adequate bandwidth, it can cause timeouts and can cause the performance for connected clients to degrade.

Setting Up a Remote Access Client

This section tells you how to set up a Windows NT Remote Access client so that it can do the following:

- Connect to the X.25 network through PAD services.
- Connect to the X.25 network directly.

Connecting Through Dial-Up PADs

In general, a client connects to an X.25 network in two steps:

1. Dial from the client's modem to a PAD (modem-to-modem).
2. Establish a connection over the X.25 network between the PAD and the server-side X.25 smart card.

Once you've established a connection, communicate as you would through any asynchronous connection. For a more complete description of connecting through dial-up PADs, see "Accessing X.25 Through Dial-Up PADs" earlier in this chapter.

Configuring Client PADs

The client PAD, through which a remote workstation connects to the X.25 network, may have previously been set to X.3-parameter values that are incompatible with the Remote Access Service. Therefore, it is very important to configure the X.25 smart

card on the Remote Access server so that it changes the client PAD's X.3 settings to the values in the X.25 Configuration Values table (earlier in this chapter) as soon as a connection is established through X.29 commands. To configure an X.25 smart card to make these changes, see the configuration manual for your specific card.

Note

If the X.25 smart card on the server end does not support commands for the X.29 language, the client PAD script must set the X.3 parameters locally. If you have problems, contact the support site for your X.25 smart card vendor.

Connecting Directly

To set up the client for connecting directly to the X.25 network, follow the same procedures as you did in setting up the Remote Access server. See "Setting Up the Remote Access Server for an X.25 Network" earlier in this chapter. Make sure the communication ports are selected as dial out.

Configuring Remote Access Software for X.25

Connecting to a server through an X.25 network is similar to connecting through a phone line. The only difference is that the phone book entry must specify an X.25 PAD type and an X.121 address. Follow these steps:

To add a phone book entry with X.25 or to add X.25 to an existing entry

- See Remote Access online help.

PAD.INF Format

Similar in format to MODEM.INF, PAD.INF contains the conversations between the client software and the PAD, whereas MODEM.INF contains script information used to talk to the modem. You can find PAD.INF in the \NT\SYSTEM32\RAS subdirectory.

The macros in the following list are *reserved words*, which you cannot use in PAD.INF to create a new entry. Reserved words are case insensitive.

- **x25address**
- **diagnostics**
- **userdata**
- **x25pad**
- **facilities**

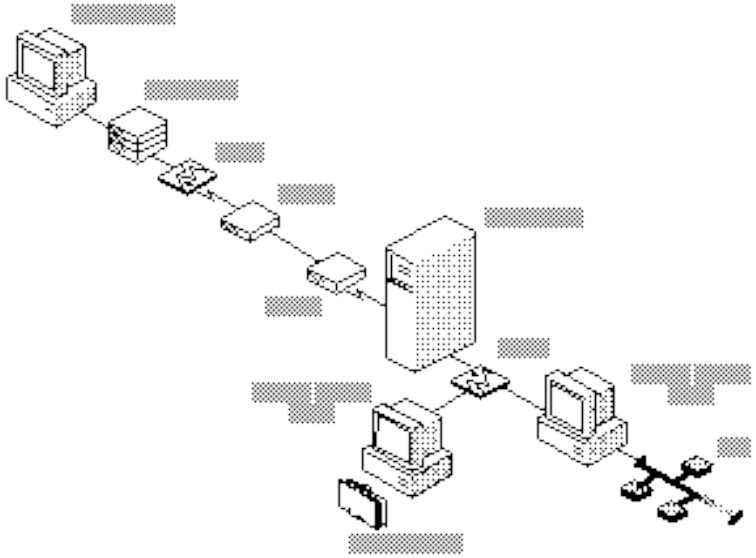
Caution

Using reserved words as macro names in PAD.INF could result in unpredictable behavior of the Remote Access software.

Support for Security Hosts and Switches

Remote Access Service for Windows NT supports various kinds of *intermediary devices* (switches and hosts) between the Remote Access client and the Remote Access server. These devices include:

- Modem-pool switch
- Security host
- X.25 network



Sample Configuration with Modem Pool and Security Host

Connecting Through Intermediary Devices

Before a client can connect to the Remote Access server through intermediary devices, it usually has one of two possible dialogs with each intermediary device:

Static
: A dialog that's always the same and requires no input from the user.

Interactive
: A dialog that always changes, requiring input from the user.

You must prepare the client to conduct the correct dialog with each intermediary.

With a configuration that requires both types of dialogs, preparation takes two general steps:

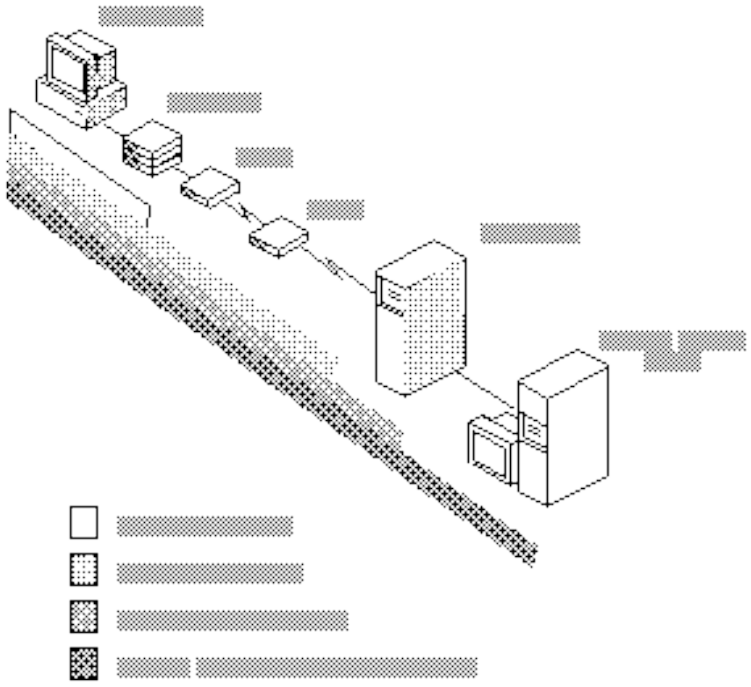
1. Write a script for the static dialog.
2. Activate terminal mode for the interactive dialogs.

If your configuration requires only one kind of dialog, take only one of these steps. For example:

- If your clients connect through only one intermediary with a static dialog, such as an X.25 network, take step 1 only.
- If your clients connect through a security host with an interactive dialog, take step 2 only.

Writing Scripts

To write a script for static dialogs, such as the one between the client, modem pool, and security host, as shown in the following illustration, add the modem pool and security host to the SWITCH.INF file.



Dialogs Between Client and Intermediary Devices

In this illustration, X.25 conducts a post-connect dialog. Since connecting through X.25 is a common occurrence, Remote Access simplifies it through special treatment:

- Users select X.25 scripts from the X.25 dialog box rather than from the Switch dialog box.
- Remote Access allows the user to have another post-connect dialog after the X.25 dialog, which happens in no other connection sequence.

To write a script

1. In the client's SWITCH.INF file, type the name of the device within brackets.
2. Add one or more commands followed by zero or more responses.

Note

As with PAD.INF, responses in SWITCH.INF immediately follow their commands.

Here is a sample entry from a SWITCH.INF file:

```
[AT&T&Teleswitch]
COMMAND=<cr><cr>
OK=Ready<cr>
Error=Failure<cr>
```

To add an entry to your SWITCH.INF file, create a sequence of commands and responses that follows the order in the sample SWITCH.INF file.

The Remote Access Terminal feature lets the user communicate with intermediary devices that require an interactive dialog. For instructions about activating Terminal, see Remote Access online help.

BLANK PAGE

IMPORTANT: This text will appear on screen, but will not print.

Do not type any additional text on this page!