Network Manager's Guide

PassageWay™ Solution

Telephony Services

The shortest distance between your phone and your database

AT&T

disclaimer

Novell®, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability of fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its contents, at any time, without obligation to notify any person or entity of such changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software, at any time, without any obligation to notify any person or entity of such changes.

Novell Trademarks

Novell, NetWare, the N-Design, and the NetWare Logotype are registered trademarks of Novell, Inc. NetWare® Telephony Services™ is a trademark of Novell, Inc.

Third Party Trademarks

Microsoft, MS-DOS, and the Microsoft Logo are registered trademarks of Microsoft Corporation. The AT&T logo is a registered trademark of AT&T. All products and company names are trademarks or registered trademarks of their respective holders.

IMPORTANT!

Please read the file called README.TXT on the license disk.

You must use the installation instructions IN THIS FILE. The instructions in the manual are incomplete.

Security

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, AT&T can assume no responsibility for any errors. Changes and corrections to the information contained in this document maybe incorporated into future reissues.

Your Responsibility for Your System's Security

You are responsible for the security of your system. AT&T does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunications services or facilities accessed through or connected to it. AT&T will not be responsible for any charges that result from such unauthorized use. Product administration to prevent unauthorized use is your responsibility and your system administrator should read all documents provided with this product to fully understand the features available that may reduce your risk of incurring charges.

Table of Contents

List of Figures

List of Tables

Introducing NetWare® Telephony Services

chapter

1 Introducing NetWare Telephony Services®

The NetWare Telephony Services product integrates telephony monitoring and control with applications on enterprise-wide networks. One or more Telephony Servers (Tservers) integrates the existing telephones on users' desktops with telephony-enabled or telephony-based applications. These applications can reside either on the server where they are referred to as "server applications" or on the desktop PC where they are called "client applications."

Users' desktops do not require any special telephones, connectors, PC circuit packs, or new wiring. Hardware at the Tserver provides the physical control link between the Tserver and the PBXs to which the users' telephones connect.

The NetWare Telephony Services product consists of software that runs on a NetWare server and software that supports an Application Programming Interface (API) on a windows client. A PC application, acting on behalf of a user, can use the API to monitor and control calls at a device associated with the user.

This book is organized as follows:

- Chapter 2 describes client and server applications, architecture, and software components.
- Chapter 3 discusses the requirements for the NetWare server and client workstations.
- Chapter 4 discusses how to install, load, and run the Tserver components.
- Chapter 5 describes the Tserver administration and maintenance components.
- Chapter 6 presents an overview of administering the Tserver.
- Chapter 7 presents step-by-step details on administering the Tserver.
- Chapter 8 presents troubleshooting information, including all error codes.

System Use and Components

chapter 2

System Use and Components

This chapter describes client and server applications, the client and server architecture, and the software in the NetWare® Telephony Server (Tserver). The Tserver is the foundation for Computer Telephony Integration (CTI) applications in Novell® LAN environments. CTI applications can provide workstations with a variety of telephony monitoring and control features such as:

- Call Center
- Multimedia Desktop
- Call Logging
- Call Management
- Call Screening
- Conference Management
- Incoming Call Routing
- Custom Call Distribution
- Telemarketing Agent Reporting
- Review or Predictive Outbound Calling
- Voice Response Front End to Agent Pool
- Boss/Secretary
- Call Tracking, Reporting, and Billing
- Dialing Integration with Non-CTI Applications
- Directory Dialing from User and Corporate Directories

- Integration of the Message Waiting Indicator with Emil or Other LAN-based Messaging Applications

Especially important are applications in a customer service environment where integration of telephony information (such as calling number) and LAN access to customer databases can provide automated "screen pop," voice/screen consultation with a supervisor, and/or voice/screen transfer. The application might also incorporate an easy-to-use Graphical User Interface (GUI). In addition, a CTI application might access caller database records on a local network file server or on a remote minicomputer or mainframe (through a gateway). A client or server application thereby integrates access to all the information needed to support an efficient, automated inbound customer service center.

While many applications may be implemented as either client or server applications, certain factors may result in one approach being more satisfactory, economical, or manageable than the other. Consider the following:

- **Round-the-clock application availability:** Implementing an application on the server could eliminate the problem of a key application being down when a client PC is powered off.

- **Backup:** System administrators (or some automatic procedure) typically back up servers on a regular basis, while users determine when to backup client PCs.

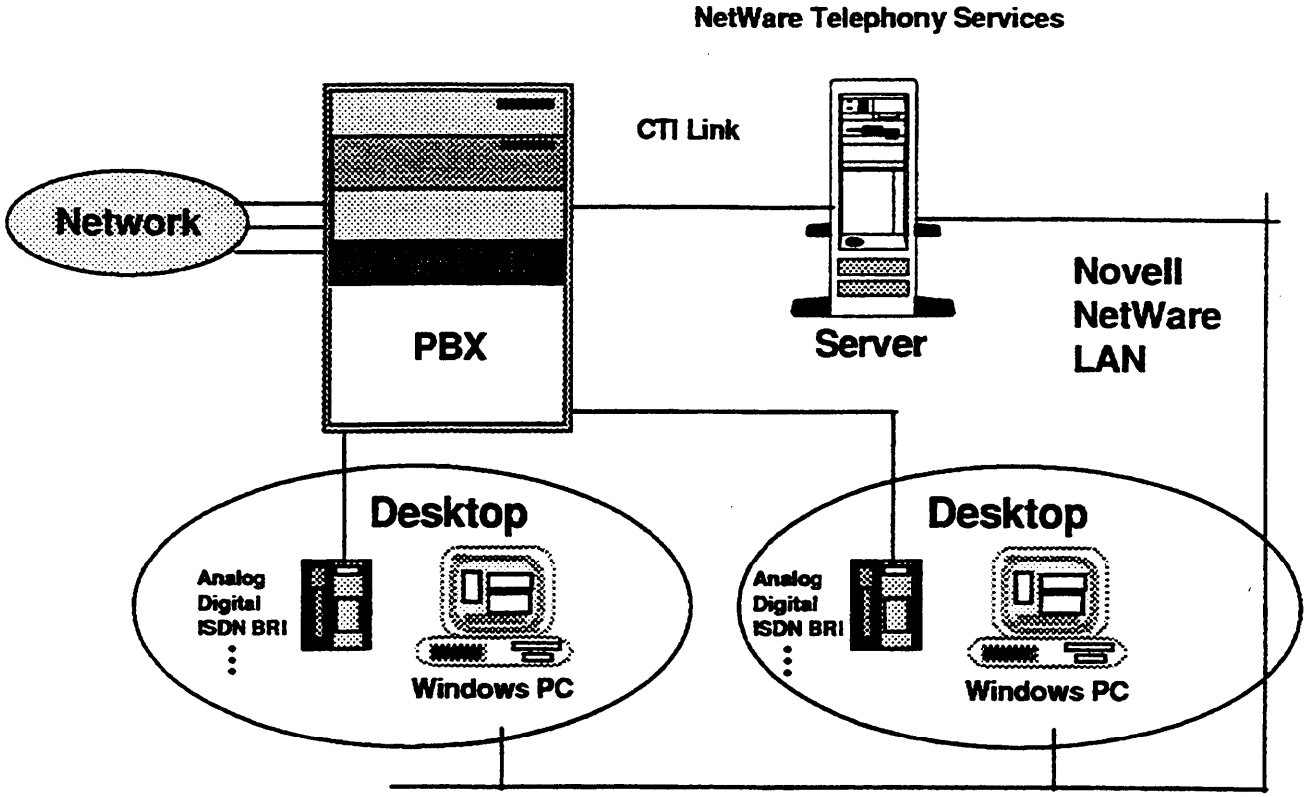
- **Scarce or expensive resources:** Such resources can be centralized, especially when light usage makes their inclusion in the client PC impractical.

- **Single instance running on behalf of multiple users:** Certain applications (such as tracking and billing) can run on behalf of a number of users. A single application instance is often more manageable than many copies of a distributed application.

- **Centralized, shared data:** Data files on a server are more available and more manageable than synchronizing shared data files across client PCs.

The Telephony Services configuration is illustrated in Figure 2-1.

Figure 2-1
Telephony Services Configuration



The NetWare Telephony Services product is a distributed client/server application environment that logically integrates the telephone on a user's desktop with an application running on his/her personal computer. The system accomplishes this logical integration without the need for special telephones or hardware devices at users' worktops.

Typically, the hardware on the user's desktop remains unchanged when the NetWare Telephony Services product is installed. The user's telephone is connected to the telephone system - most often a Private Branch Exchange (PBX) -in their building in the usual fashion.

Similarly, the user's PC -if already connected to a LAN using Novell NetWare - will not require any new hardware to use Telephony Services. Note that the telephone and the PC do not physically connect to each other. Instead, the Tserver logically integrates the telephone and the PC.

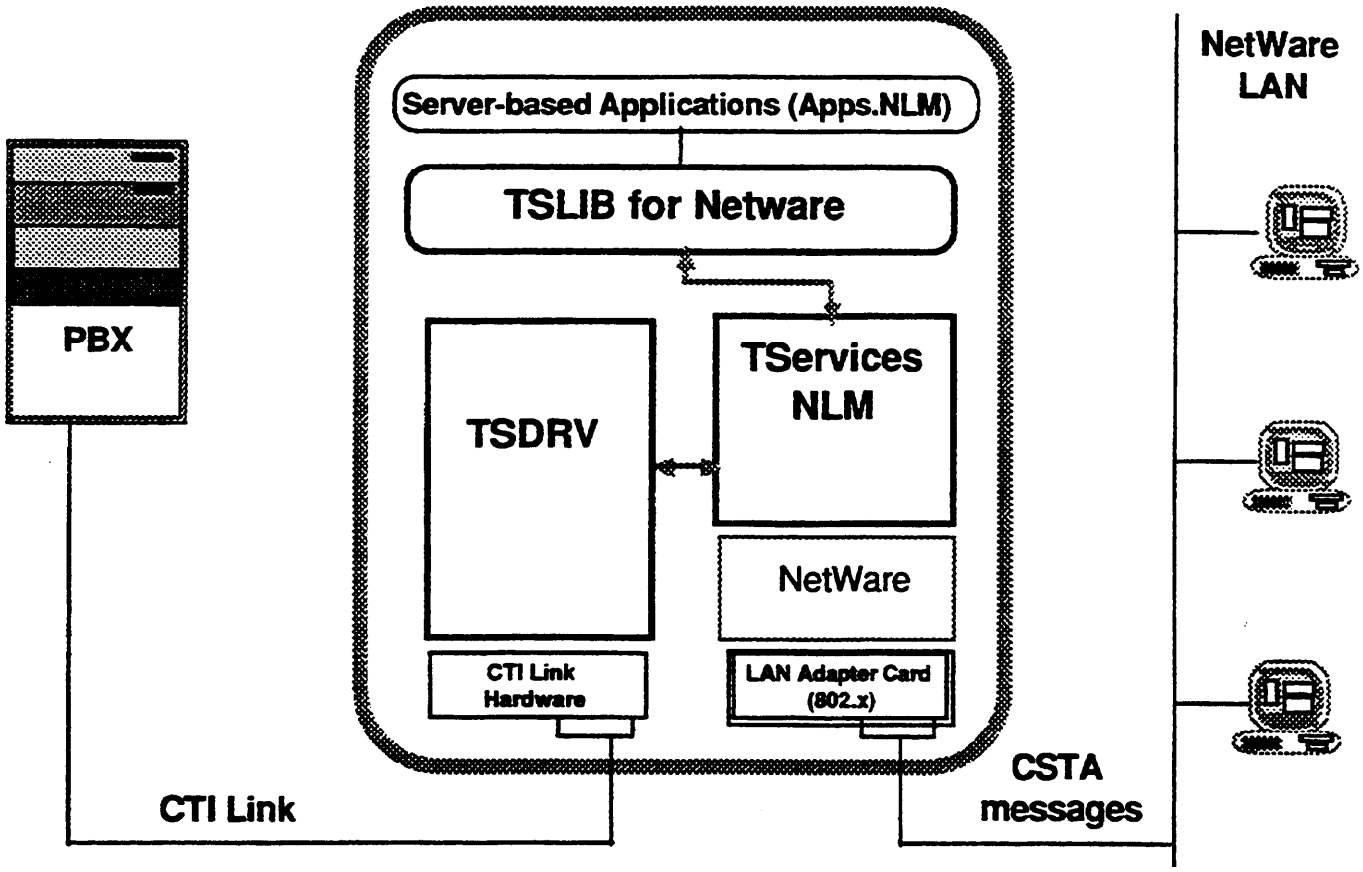
The PBX provides a CTI link. Major PBX manufacturers have products that provide this type of link for their switches. CTI links allow the integration of telephony and computer resources at the application level. For example, an application in the computing environment can use a CTI Link to request that a telephone call be placed by the PBX between one endpoint and another, or that call activity be monitored at a telephone. PBX vendors differ in the range of capabilities that they support over their CTI links, but most vendors support a basic set of capabilities that include making, monitoring, and controlling calls (e.g., transfer, conference, hold, reconnect).

The telephony and computing environments come together on the server running NetWare Telephony Services. Given that the user's desktop already has a telephone and a PC connected to a Novell LAN and that the PBX has been properly equipped and administered with a CTI Link, the server hardware and software are the only incremented expenses required to provide an environment for integrated applications.

Server Architecture

Figure 2-2 illustrates the major architectural components of the server portion of NetWare Telephony Services.

Figure 2-2
Server Architecture



The server running NetWare Telephony Services is a standard NetWare server running NetWare 3.11 or 3.12. There are additional hardware requirements for the specific CTI link to the PBX, and for the adapter card connecting the server to the LAN.

The server software consists of two major modules. The Tserver NetWare Loadable Module (Tserver NLM) is a PBX-independent module that manages communication between a client workstation application and the second major module, the Telephony Services Drivers (TSDRVs). A TSDRV is a PBX-specific NLM that provides vendor-specific telephony services to the client applications.

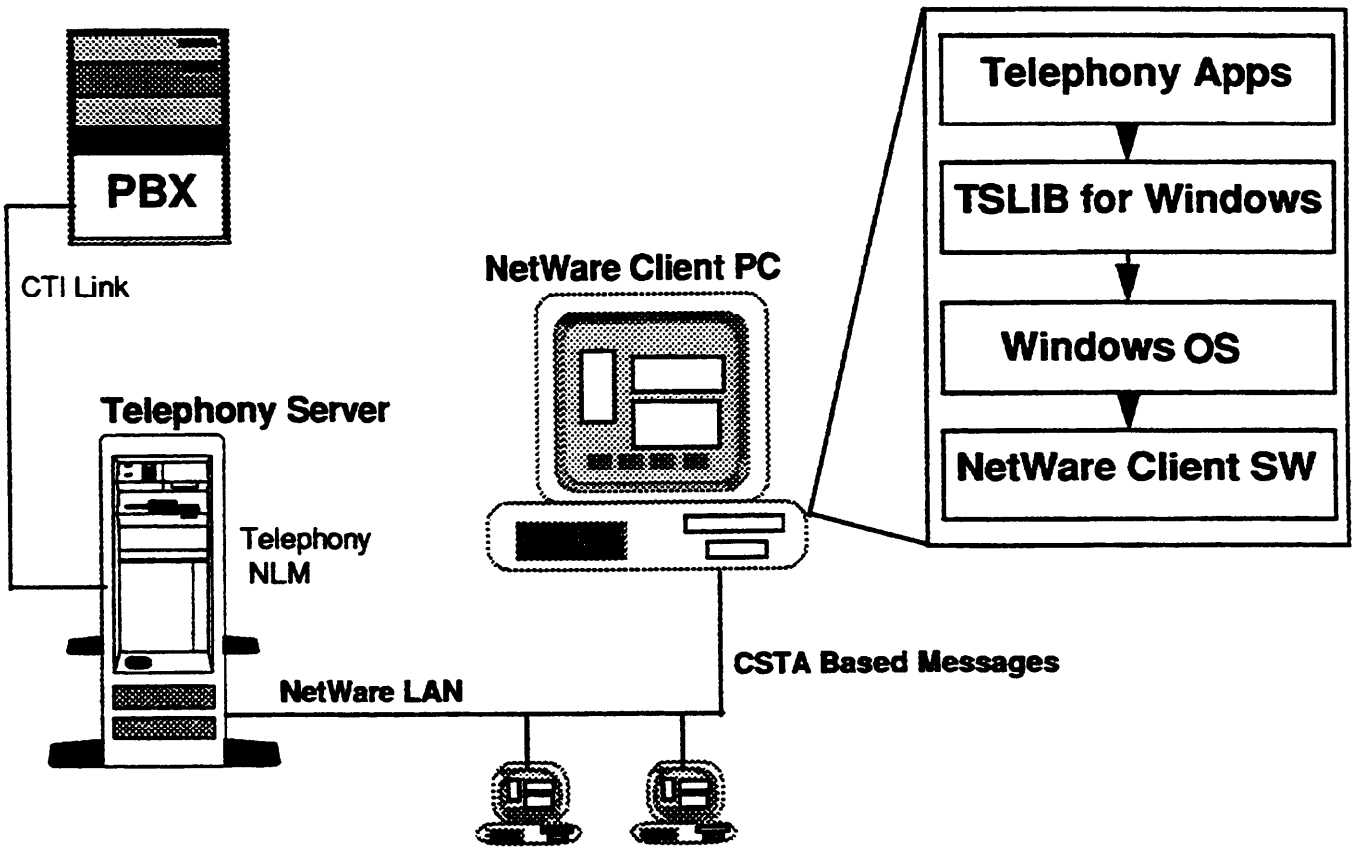
The server architecture also supports the development of server-based applications through the Telephony Services Application Programming Interface (TSAPI). TSAPI is based on the European Computer Manufacturing Association (ECMA) standard for Computer-Supported

Telecommunications Applications (CSTA). A developer can use TSAPI to develop applications that integrate Telephony Services with other types of applications. For example, a server application could use Telephony Services to obtain call event information such as the telephone number of the person making the call, or the dialed number of the call. The application could use Btrieve or other NetWare-supported database services to retrieve this information and then use the information to instruct Telephony Services on how to best route the call. A library known as TSLIB for NetWare provides TSAPI in the server environment.

Client Architecture

Figure 2-3 shows the major architectural components of the client portion of NetWare Telephony Services.

Figure 2-3
Client Architecture



The Telephony Services Library for Windows (TSLIB for Windows) is the primary software module allowing the development of client applications. This library supports the Telephony Services API (TSAPI) in the client.

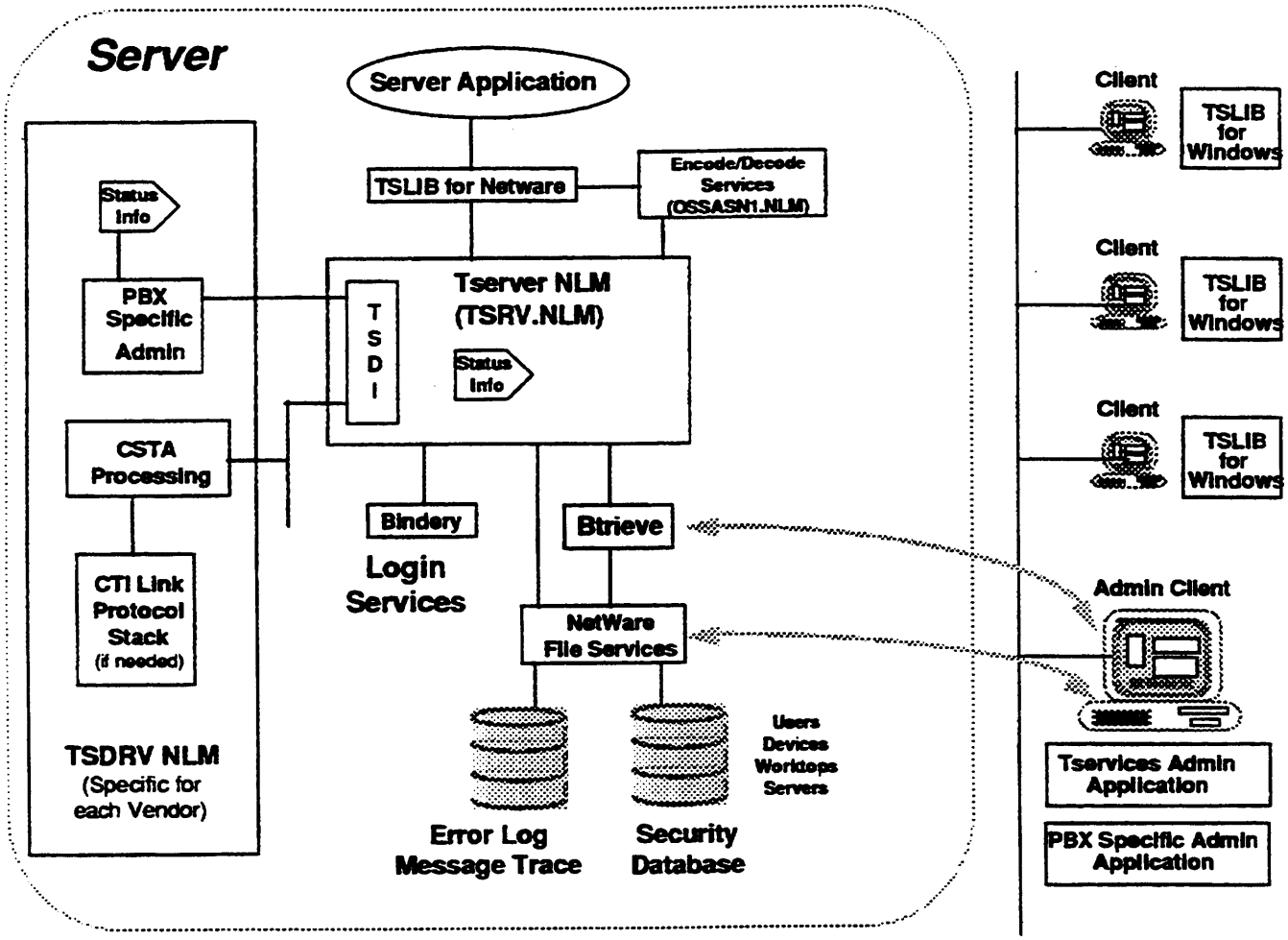
The API is a set of C language routines that support telephony control capabilities for a generic PBX environment.

When a client application issues a TSAPI request, the library formats the request into a machine-independent byte stream (a CSTA message) and sends the request to the server through the network using the standard Novell communications protocols IPX/SPX.

Software Architecture

Figure 2-4 illustrates the major software modules used by NetWare Telephony Services. There are three basic types of software modules server, client, and administration.

Figure 2-4
Major Software Modules



Server Software

The major server software modules are:

- Tserver NLM (TSRV.NLM) provides the communications functions required between the networked clients and the server.

  Tserver's primary function is routing messages from TSDRVs to the client workstation applications. In addition, Tserver manages a security database using NetWare Btrieve and File Services. When client applications issue telephony smites requests, Tserver determines whether to grant the request based on information in this database. If the client's request is permissible, Tserver forwards the request to the appropriate driver for processing. Tserver uses NetWare Bindery services to authenticate users via their NetWare file services passwords. When configured to do so, Tserver creates and maintains error logs and message traces. Tsever informs prospective clients of all TSDRV and administration services it hosts by using the NetWare Service Advertising Protocol. Tserver records service traffic patterns, accessible through Telephony Services Administator (TSRVOAM.EXE).

- TSDRV NLM is the generic name for any software drivers that handle the specific CTI Link messages for a particular PBX. There is a different TSDRV module for each vendor's PBX. Part of the installation process is to install the drivers corresponding to the PBX(s) in the system. Each TSDRV module performs the following functions:

  - Provides a low-level interface to the hardware driver for the CTI Link supported by the specific PBX (if required)
  - Maintains any necessary CTI Link protocol stack
  - Maps PBX-specific CTI Link messages to CSTA messages
  - Supports PBX-specific administration functions and maintains status information relating to the performance of the TSDRV.

- Telephony Server Driver Interface (TSDI) exchanges messages between Tserver NLM and all TSDRV NLMs in the system. Tserver

NLM provides the set of function calls that comprise this interface. The TSDI allows a TSDRV module to "register" with the Tserver NLM. After a connection has been registered, the Tserver NLM and the TSDRV NLM can exchange messages using a send and receive programming model.

- TSLIB for NetWare provides the TSAPI to NLMs. This allows server-based applications to access Telephony Services. Multiple client applications can share TSLIB simultaneously, allowing them to communicate with any Telephony Server on the network.

- Encode/Decode Services (OSSASN1.NLM) allows machine-independent encoding and decoding of CSTA messages. in particular, OSSASN1.NLM provides its encoding engine to server-based modules - TSLIB and Tserver.

Client Software

The primary software module in the windows client device is the Telephony Services Library for Windows (CSTA.DLL). TSLIB for Windows is a Dynamic Link Library (DLL) that provides the TSAPI to windows applications.

Telephony Services Administration Software

The Telephony Services administration functions are provided by windows-based client application - Telephony Services Administrator (TSRVOAM.EXE). Authorized administrators may use this application to administer the Telephony Services security database and monitor Tserver status and traffic. The Telephony Services Administrator also configures Tserver message tracing and error logging.

PBX vendors provide PBX-specific administration applications. The capabilities of such programs may vary among vendors. PBX-specific administration packages need not be windows applications.

The following types of capabilities can be found in some TSDRV adminstration packages:

- CTI Link hardware administration

- Tests/Diagnostics of the CTI Link and its associated hardware
- Administration of CTI Link alarms
- Message tracing
- CTI Link restart
- CTI Link traffic analysis

Contact individual vendors for PBX-specific administration information.

Server and Client Requirements

chapter

3 Server and Client Requirements

This chapter discusses the requirements for the NetWare server and the client workstation.

NetWare® Server Requirements

The server that runs NetWare Telephony Services should be a 386 class machine with at least 8 megabytes of RAM when using NetWare 3 or at least 10 megabytes of RAM when using NetWare 4. NetWare Telephony Services does not support NetWare versions earlier than 3.11.

Client Workstation

Windows Version

TSLIB for Windows requires an 80386-class PC running Windows 3.1 in enhanced mode. TSLIB for Windows is not compatible with standard mode or Windows 3.0.

Network Software Versions

Some older versions of DOS and Windows NetWare client software are incompatible with NetWare Telephony Services. Novell recommends that you update client workstations with the latest versions of the ODI protocol stack components - LSL.COM and IPXODI.COM. This software can be obtained from Novell's forum on CompuServe.

The following is a table of components that you should compare with the versions on your workstations. If you are using the same or later version, you need not change client protocol stack configuration. If you have earlier versions of these components, you need to update your client workstations.

This table contains versions for ODI software only. If you are using an NDIS stack, you need to check the version of your IPX; it should be at least 3.10.

You can check the IPX version that you are using by typing the name of the IPX executable (either *IPX, IPXODI,* or *MSIPX)* followed by a forward slash *(/)* and *I* (for example, *IPX /I).* Other NetWare DOS client components support this method as well.

Table 3-1
Required Client Networking Components

Component	Required Version
LSL.COM	2.05
IPXODI.COM	2.12
NETX.EXE, EMSNETX.EXE, XMSNETX.EXE	3.32
VLM.EXE (and all VLMs)	1.10
VIPX.386	1.17
VNETWARE.386	2.03
NWIPXSPX.DLL	**4.05 (This version is provided on Disk Two and is part of the windows workstation setup)**
NWCALLS.DLL	**4.04 (This version is provided on Disk Two and is part of the windows workstation setup)**
NETWARE.DRV	**2.02 (for NETX clients), 3.02 (for VLM clients)**

All of these files with the exception of NWIPXSPX.DLL 4.05 can be found in DOSUP9.EXE and WINUP9.EXE, two packages of updates available through Novell.

User Licensing

The Tserver holds and enforces a specific number of concurrent connections. These connections are designed to allow user login ID/user workstation combinations to use the CTI links. Such a connection is called a license.

Each Tserver is purchased for a specific number of licenses. Accordingly, if there are three Tservers on the Local Area Network (LAN), for example, each Tserver may hold a different number of licenses.

Specifically, a license is defined as a connection that

- Is associated with and goes out from one user login ID/user workstation combination
- Passes through just one Tserver, and
- Goes out over one unique CTI link (CTI links connect the PBX driver to one or more PBXs).

In other words, a single license is a connection over a single combination of the following: one user (login ID), one user workstation, one Tserver, one CTI link.

A new license is used whenever a user starts an application unless the path of that application is the same as that for an application that was previously started and is still active. In such a case, the new application is associated with the license for the application previously started.

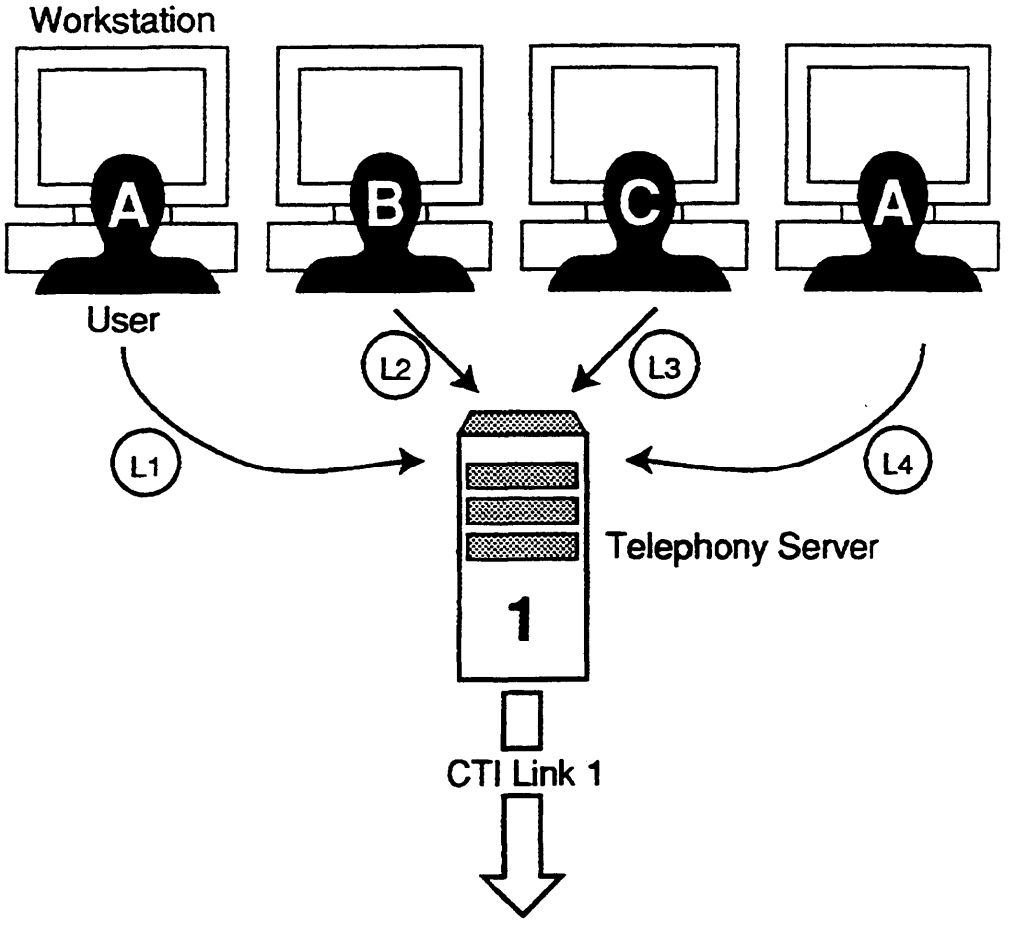
One or more streams maybe associated with each license (a stream is opened whenever you start an application). A maximum of 1800 streams (SPX connections) at a time may be opened on a NetWare file server.

If all the streams associated with a license become closed, the license is "freed up" for new applications that may or may not follow the same path as the applications previously associated with the license.

Licensing Examples

The following figure illustrates licensing that involves three user login IDs, four user workstations, one Tserver, and one CTI link:

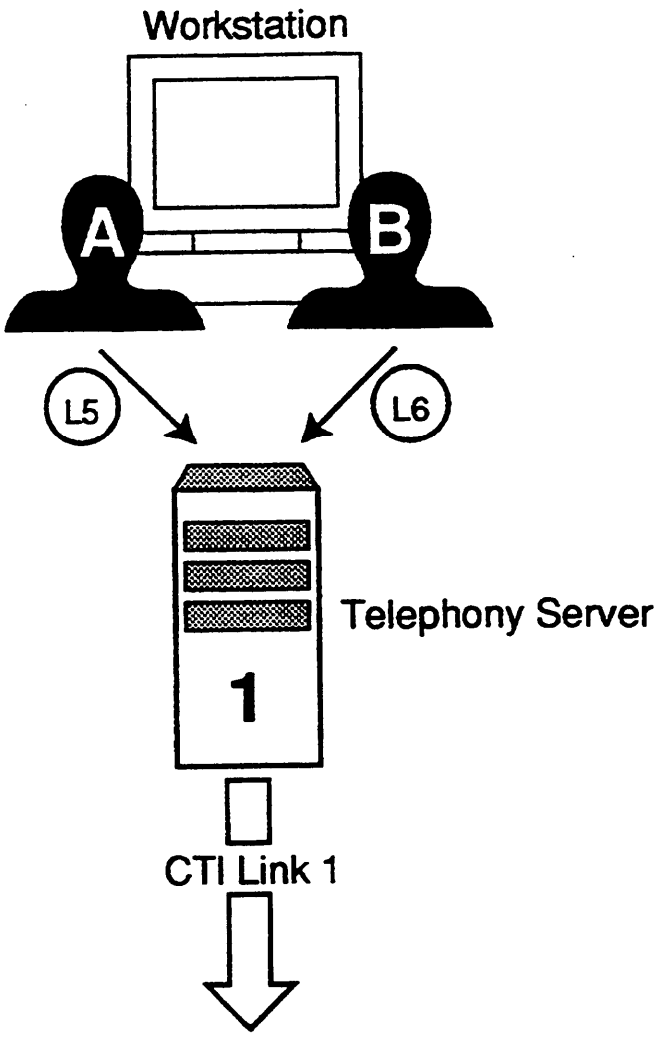
Figure 3-1
User License Scenario One



Here, four licenses (L1 through L4) from Tserver 1 are used because there are *four user login ID/user workstation combinations.* All the streams go out to the same Tserver and out over the same CTI link. Note that User A requires two licenses since this user is accessing CTI Link 1 from two different workstations. Note also that each license has multiple streams associated with it.

The following figure illustrates licensing that involves two user login IDs, one user workstation, one Tserver, and one CTI link:

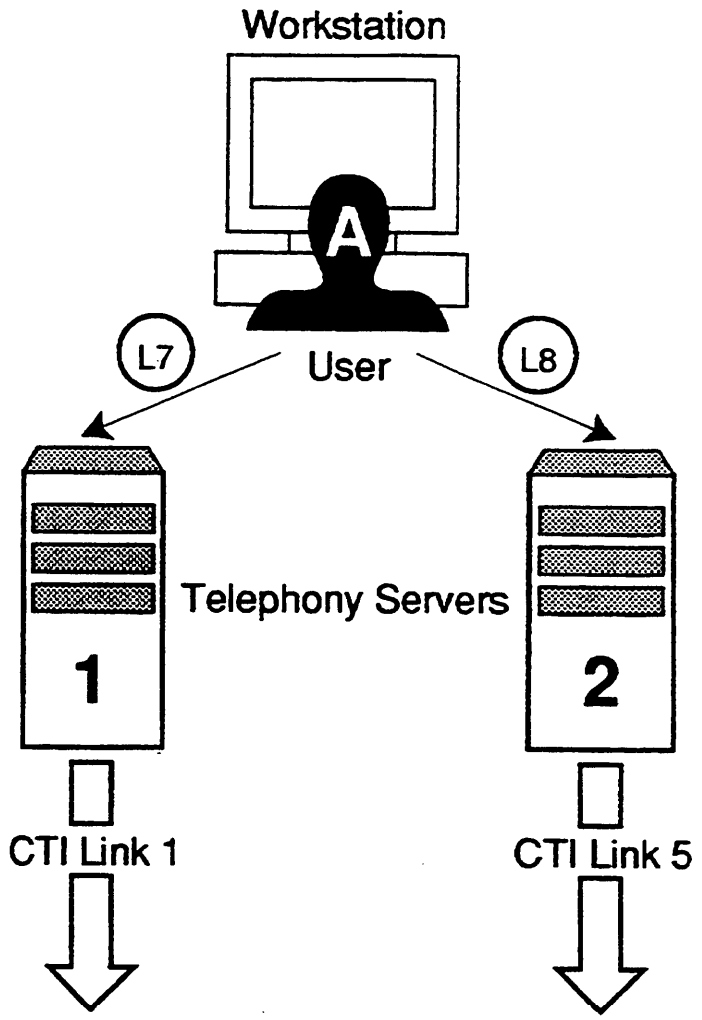
Figure 3-2
User License Scenario Two



Here, two licenses (L5 and L6) from Tserver 1 are used because there are *two user login ID/user workstation combinations* (from just one user workstation). Once again, the streams for each combination go out to the same Tserver and out over the same CTI link. A practical application for this scenario could involve a supervisor who has both a Supervisor login and User login on the system.

The next figure illustrates licensing that involves one user login ID, one user workstation, two Tservers, and two CTI links:

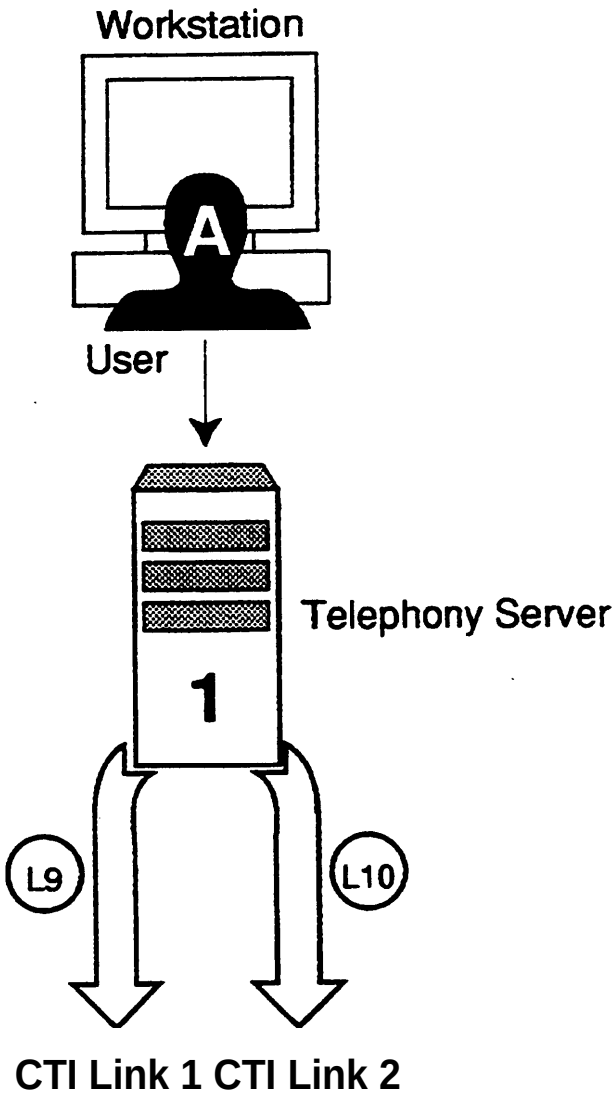
Figure 3-3
User License Scenario Three



Here, two licenses (one from each Tserver) are used because the streams for User A are opened from one user workstation, go to Tserver 1 and out over CTI Link 1 in one case (L7), and go to Tserver 2 and out over CTI Link 5 in another case (L8).

The final figure illustrates license support for a scenario involving one user login ID, one Tserver, and two CTI links:

Figure 3-4
User License Scenario Four



Here, two licenses (L9 and L10) from Tserver 1 are used because the streams for User A are opened from one user workstation, go to Tserver 1, and then go to two different CTI links (accounting for L9 and L10).

Summary

To summarize, you are using one license whenever any one of the following is true:

- You start an application from a PC by using a login ID, and the resulting stream(s) go out to a Tserver and over a CTI link.

- You start two or more applications from one PC by using the same ID login in each case, and all the resulting stream(s) go out to the same Tserver and over the same CTI link.

On the other hand, you are using two (or more) licenses whenever any one of the following is true:

- You start two (or more) applications from one client workstation by using at least two different login IDs (the Tservers and CTI links eventually reached are irrelevant).

- You start one (or more) applications from one client workstation by using the same login ID in each case, and the resulting streams for each application go out to at least two different CTI links.

- You use the same login ID to run one or more applications from two (or more) workstations (the Tserver(s) and CTI link(s) eventually reached are irrelevant).

Keep in mind that you are not necessarily using a new license whenever start an application requests service from a Tserver. If the stream path for an application you start now is the same as for one you started previously, and if the application you started previously is still active, you are using the license for the application you started previously.

Licensing Availability and Recommendations

Licenses are available in the following increments: 25, 50, 100, 250 and 250+ (plus).

When deciding which license to purchase, you should consider the:

- Potential growth rate of Telephony Services vis-à-vis the number of users

- Number of PCs available to each user

- Number of Tservers in the system
- Number of CTI links in the system
- Required applications (contact your applications publisher(s) for input on the number of required licenses)

Installation

chapter

4 *Installation*

This chapter discusses how to install, load, and run the Telephony Services components.

Installing NetWare Telephony Services consists of three steps:

- ♦ Installing the Telephony Services software on a NetWare file server.
- ♦ Configuring a file server for Telephony Services requirements.
- ♦ Installing client workstation software.

For the latest information concerning installation, see the README.TXT file in the root directory of the License Disk (TSRVDSK1).

Installing Telephony Services Software

This section describes how to install Telephony Server and Client software on a NetWare File Server. If you are not installing a Telephony Server and wish to install only windows workstation software, go to "Installing Client Workstation Software."

Server Software Requirements

- ❑ NetWare 3.11, 3.12 or 4 is required. The Telephony Server is incompatible with all other versions of NetWare.
- ❑ The SYS volume must be mounted. Telephony Services components must be installed on the SYS volume.
- ❑ The modules shown in Table 4-1 must be installed on the server. When you install NetWare, these modules are automatically installed.

Table 4-1
Required Server Modules

Module	Description
STREAMS.NLM	The STREAMS module is used by the Telephony Services installer and subsequently by other Telephony Services components. The STREAMS module resides in SYS:SYSTEM.
CLIB.NLM	The CLIB module is used by the Telephony Services installer and subsequently by other Telephony Services components. The CLIB module resides in SYS:SYSTEM.
BTRIEVE.NLM	The BTRIEVE module is used by the Telephony Server to maintain the Telephony Services security database. The BTRIEVE module resides in SYS:SYSTEM.

Using the NetWare Installer

The Telephony Services installer examines your file server for components that are missing or that need to be updated and installs the Telephony Server and client software.

If you are installing on a server that has no telephony security database files on it, the installer will install new copies. The installer will never replace existing copies of the security database.

The Telephony Services Installer may update modules on your file server such as STREAMS.NLM, CLIB.NLM, MATHLIB.NLM and NetWare patches such as SPXDDFIX.NLM. Such updates fix known problems with some versions of NetWare and may potentially affect the behavior of other modules on your NetWare server.

When performing a complete installation, the Telephony Services installer places windows workstation software on the file server.

If you do not wish to install one or any of these modules, do not select the default installation options as outlined immediately below. Refer instead to “Customizing PINSTALL Behavior.”

1. Load the NetWare install module.

At the console promp, type

```
LOAD INSTALL <Enter>
```

2. Add a product in the Product Options screen by pressing the "Insert" (<Ins>) key. When prompted for an installation disk, designate the NetWare Telephony Services user license disk.

Under NetWare 3, the Product Options screen can be found directly under INSTALL.NLM's main menu. Under NetWare 4, you must select "Maintenance Options" and then "Product Options."

3. Configure installation options.

You will be asked to select several parameters that affect how the Telephony Services installer operates. Follow the instructions below for each prompt:

```
Make backups of install files that may be
overwritten?  (yes/no/quit)
```

Type "yes" and press <Enter>.

```
Prompt for Warnings or file overwrites?
 (yes/no/quit)
```

Type "no" and press <Enter>.

```
Please enter drive to Install from: [default =
a:]
```

Type your floppy drive letter and press <Enter>.

```
Please enter the full path name of the directory
where you wish to copy windows client files that
will be installed.

Enter  path  [default=sys:\csta]
```

Press <Enter>.

4. Initiate a complete installation.

You will be presented with a menu listing every module that can be installed. Choose the “Complete Installation” option:

```
Enter Number:
```

Type 1 and press <Enter>.

5. Follow instructions presented by the installer.

In order to copy files, the installer asks for each of the Telephony Services disks. When the installer requests a disk, place the disk in the floppy drive and press <Enter>.

6. Verify that no problems occurred during installation.

When the installer has finished copying files, it displays a list of results. You can find out if any files could not be copied by reading this list.

When you are finished, press <Enter> to return to the NetWare install module.

The Telephony Services Installer does not update the list of installed products displayed by the NetWare installer. Even when an installation completes successfully, you will not see the Telephony Server in the list of installed products.

You may now skip to “Configuring the File Server Environment.”

Customizing Installation

The Telephony Services installer offers several options when installing, including the following:

- **Backups** — the installer can automatically save copies of software that it replaces while installing Telephony Services.
- **Interactive Warnings** — Before installing older software over newer versions, deleting write-protected files or taking other unusual actions, the installer can prompt for permission to take such actions.

- **Windows Component Destination** — You may choose the directory in which the installer places windows components.

- **Selective Installation** — You may specify one or many files from the complete list to install rather than a full installation.

Requesting Backups

As the installer copies files onto your file server, it may need to replace files that already exist with copies bundled with Telephony Services. The installer prompts you with the following question to determine whether any software it replaces should be backed up first:

```
Make backups of install files that may be
overwritten? (yes/no/quit)
```

If you answer "yes," the installer copies any files that it needs to replace to your file server's SYS:SYSTEM\TSRV.BAK directory.

The installer makes only one backup copy of files that it needs to replace. If a file already exists in the backup directory, the installer will replace it with the new backup.

Interactive Warnings

If the installer discovers that a file it is installing already exists on the server, it usually examines the version of each file to determine which one to leave on the server. The installer automatically replaces older versions and skips installation over newer versions of any file.

If you wish to override this default behavior, answer yes to the following question the installer poses when loaded:

```
Prompt for Warnings or file overwrites?
(yes/no/quit)
```

When you request this option, the installer asks whether or not to copy over any file that it finds on the server. When it finds such duplicate files, the installer also displays the relative file versions (for example, the source file

is older than the destination file), and it offers the option of quitting installation.

Do not rely on the installer's assessment of whether any windows components are newer or older than copies that may exist on your file server.

As the installer copies a file, it changes its date to the current date. i.e. if you are installing files on June 1, 1994, all copied files will be given the date June 1,1994.

Before the installer replaces windows components that it finds on your server, it compares the source file's date (to be installed) with the destination file's date (to be replaced). This is how the installer determines whether windows components need to be replaced or not. Unless you have reason to believe that windows software on your server is newer than that provided with Telephony Services, you should always elect to replace existing windows software.

When copying NLMs, the installer uses a NLM-specific method for determining version information; it never warns you that a file is newer on your server unless it really is.

When you install a single version of Telephony Services on the same file server twice, the installer warns that all windows components it tries to install the second time are older. You should ignore these warnings.

Refer to "Advanced Topics" for more information on determining the exact versions of software on your system.

Windows Component Destination

By default, the installer places windows workstation components — TSLIB for Windows, Telephony Services Administrator and windows workstation setup — in the SYS:\CSTA directory on your file server.

If you do not wish to install windows components, refer to "Selective Installation."

You may change this destination by entering a full path name in response to the following prompt the installer issues when loaded:

```
Please enter the full path name of the directory
where you wish to copy windows client files that
will be installed.

Enter path [default=sys:\csta]
```

Selective Installation

You need not install all components when using the installer. Instead, you may select individual components for installation by requesting Option 2, "Custom Installation," at the Component Installation Menu.

If you select the Custom Installation option, the installer presents the name and brief description of each component and asks whether to install it. When you have answered this question for each component, the installer displays the list of files you selected for installation. After examining the list, you must enter a confirmation before the installer proceeds with installation.

One reason for using a custom installation is to prevent the installer from placing windows components on your file server. You may wish to install windows components on a different file server — or none at all.

Every major component on the list — TSRV.NLM, TSLIB.NLM, CSTA.DLL, and TSRVOAM.EXE — has an associated list of support files. The installer will warn you if you try to install a major component without all of the support files for that component.

Configuring the File Server Environment

This section describes how to adjust file server parameters needed by the NetWare Telephony Services product.

Before making changes to your server's environment, pick a time when it will be safe to bring the system down and up.

Allocating Short-Term Memory

The Tserver NLM consumes a NetWare resource called "Short Term Alloc Memory." This resource is limited by a user-configurable threshold. Other NetWare modules use this resource and may fail if the threshold is set too low.

1. Compute Telephony Server alloc memory requirements.

```
Short Term Memory Requirement = Number of users
on the system X 3000
```

2. Determine the current maximum short term alloc memory setting.

Type **`set maximum alloc short term memory`** at the console and record the current setting.

3. Add Telephony Server requirements to current setting and record the new setting in the AUTOEXEC.NCF file.

Add the following command to your server's AUTOEXEC.NCF file

```
set maximum alloc short term memory = X
```

where **`X`** is the new setting.

File Commit

Telephony Service Administrator performance may be very slow when administering files that reside on servers with the ncp file commit option

turned on. You must turn this setting off on servers running NetWare 3.12 or 4.

When NCP file commitment is turned on, all files being written to are immediately updated as they change. With NCP file commitment off, NetWare delays flushing changed files from its write cache to disk.

1. Add the following statement to the server's AUTOEXEC.NCF file:

```
set ncp file commit=off
```

Btrieve Settings

1. Load the BSETUP module.

At the file server console, type

LOAD BSETUP <Enter>

If BSETUP.NLM, a module included with all versions of NetWare, is not present on your file server, the LOAD BSETUP command will fail. If you encounter this problem, refer to your NetWare installation manuals for instructions on installing BSETUP, a component of Btrieve.

2. Verify the following Btrieve settings

When you load BSETUP, your Btrieve version is displayed at the top of the console. Verify the requirements on the list below that matches your version of Btrieve.

Btrieve 5:

- ❑ **Number of open files** greater than or equal to 20
- ❑ **Number of handles** greater than or equal to 20
- ❑ **Number of transactions** greater than or equal to 1

- ❑ **Number of files per transaction** greater than or equal to 12
- ❑ **Largest Record Size** greater than or equal to 8192
- ❑ **Largest Page Size** greater than or equal to 4096

Btrieve 6:

- ❑ **Number of open files** greater than or equal to 1
- ❑ **Number of handles** greater than or equal to 20
- ❑ **Number of transactions** greater than or equal to 1
- ❑ **Largest Record Size** greater than or equal to 8192
- ❑ **Largest Page Size** greater than or equal to 4096

Completing Environment Changes

To finish changing the NetWare environment bring the server down and restart.

Installing Client Workstation Software

This section describes how to configure windows workstations for Telephony Services and install the Telephony Server Administrator Client Application.

Workstation Software Requirements

- ❑ Windows 3.1 or newer (Windows for Pen, Windows for Workgroups) must be installed.
- ❑ NetWare shell 3.26+ or VLM software must be loaded *(necessary for setup over network only).*
- ❑ Under Windows 3.1, NetWare shell 3.26+ or VLM software must be designated as an active "Network" *(necessary in all cases).*

Refer to Chapter 3 for client network software requirements

Windows Setup

The NetWare Telephony Services client disk contains a program called SETUP.EXE that automatically installs all workstation software onto a PC running windows.

The windows workstation setup program installs DLLs into a user's windows system directory. When using the installer to configure a sharable network copy of windows for Telephony Services, you must log in as a user that has create and write rights in the windows system location on your file server. in this case, you only need run the installer once for all users to be able to use Telephony Services.

1. Run SETUP.EXE from a windows workstation.

If you installed Telephony Services on a file server:

Log into the file server on which you installed Telephony Services. Switch to the windows installation directory, by default SYS:\CSTA\TSNWSETP. Type the following to launch windows automatically and run setup

SETUP <Enter>

Or if you wish to install from the installation diskette:

Insert Telephony Services Disk Two into your windows workstation's floppy drive. Type the following to launch windows automatically and run setup:

DRIVE LETTER: **\WINDOWS\TSNWSETUP\SETUP.EXE** <Enter>

2. Follow the instructions that appear after the "Welcome" dialog box.

SETUP contains two dialog boxes that appear after the 'Welcome" splash screen.

The first set of instructions offers to install Telephony Services workstation software.

The second set of instructions asks whether you want to install the Telephony Services Administrator. If TSRVOAM.EXE is missing from the setup directory or you do not have rights to copy it, you will not see this dialog box. You need only install Telephony Services Administrator on network managers' machines; regular telephony services need only the first half of the windows workstation setup.

If you just want to ready a windows workstation for Telephony Services and do not wish to install the Telephony Services Administrator, select the default button in each dialog box by pressing <Enter> within each dialog box. (The default button is always the lower-leftmost button.) This will configure the workstation automatically.

You may now skip to "Invoking the Telephony Server."

Advanced Topics

This section describes advanced installation topics, including determining versions of Telephony Services software, manually installing the software, and preventing users form installing the Telephony Services Administrator.

Determining Versions

To determine a Telephony Services NLM version, go to the console of the server that NLM is running on.

Type “DISPLAY MODULES” and press <Enter>.

A list of every module running on your server will appear, containing a description of each and its version.

You can use the VERSION.EXE utility to determine the version of any Telephony Services windows components. VERSION.EXE comes with NetWare 3 and is usually found in the SYS:\PUBLIC directory of any file server. Syntax is as follows:

VERSION *[module name]*

Creating a New Security Database

The Telephony Services installer never replaces any security database it finds on a server. If you wish to replace an existing security database with a new, empty copy, follow the procedure below:

1. **Unload the Telephony Server from server memory.**

2. **Delete all files in the security database directory: SYS:\SYSTEM\TSRV\SDB**

3. **Use the Telephony Services installer to do a custom installation, and only install**

File Destinations

When the Telephony Services installers run, they install files to several locations.

These Telephony Services files are meant to be installed as a complete set.

Table 4-2
Server Component Destination (NetWare 3.11)

User License Disk Location	Server Destination	Installation Conditions
\NETWARE\TSRV.NLM	SYS:\SYSTEM\TSRV.NLM	
\NETWARE\OSSASN1.NLM	SYS:\SYSTEM\OSSASN1.NLM	
\NETWARE\TSLIB.NLM	SYS:\SYSTEM\TSLIB.NLM	
\NETWARE\SUPP\STREAMS.NLM	SYS:SYSTEM\STREAMS.NLM	only if newer than original
\NETWARE\SUPP\CLIB.NLM	SYS:\SYSTEM\CLIB.NLM	only if newer than original
\NETWARE\SUPP\MATHLIB.NLM	SYS:\SYSTEM\MATHLIB.NLM	only if newer than original
\NETWARE\311\SPXDDFIX.NLM	SYS:\SYSTEM\SPXDDFIX.NLM	only if newer than original
\NETWARE\311\SPXFIX2.NLM	SYS:SYSTEM\SPXFIX2.NLM	only if newer than original, replaces SPXFIX1.NLM
\NETWARE\311\SPXFSFIX.NLM	SYS:\SYSTEM\SPXFSFIX.NLM	only if newer than original
\NETWARE\311\SPXLISFX.NLM	SYS:\SYSTEM\SPXLISFX.NLM	only if newer than original
\NETWARE\311\XMDFIX.NLM	SYS:SYSTEM\XMDFIX.NLM	only if newer than original
\NETWARE\311\PATCHMAN.NLM	SYS:SYSTEM\PATCHMAN.NLM	only if newer than original

Table 4-3
Server Component Destinations (NetWare 3.12)

User License Disk Location	Server Destination	Installation Conditions
\NETWARE\TSRV.NLM	SYS:\SYSTEM\TSRV.NLM	
\NETWARE\OSSASN1.NLM	SYS:\SYSTEM\OSSASN1.NLM	
\NETWARE\TSLIB.NLM	SYS:\SYSTEM\TSLIB.NLM	
\NETWARE\SUPP\STREAMS.NLM	SYS:\SYSTEM\STREAMS.NLM	*only if newer than original*
\NETWARE\SUPP\CLIB.NLM	SYS:\SYSTEM\CLIB.NLM	*only if newer than original*
\NETWARE\SUPP\MATHLIB.NLM	SYS:\SYSTEM\MATHLIB.NLM	*only if newer than original*
\NETWARE\312\SPXDDFIX.NLM	SYS:\SYSTEM\SPXDDFIX.NLM	*only if newer than original*
\NETWARE\312\PM312.NLM	SYS:\SYSTEM\PM312.NLM	*only if newer than original*

Table 4-4
Server Component Destinations (NetWare 4)

User License Disk Location	Server Destination	Installation Conditions
\NETWARE\TSRV.NLM	SYS:\SYSTEM\TSRV.NLM	
\NETWARE\OSSASN1.NLM	SYS:\SYSTEM\OSSASN1.NLM	
\NETWARE\TSLIB.NLM	SYS:\SYSTEM\TSLIB.NLM	
\NETWARE\SUPP\STREAMS.NLM	SYS:\SYSTEM\STREAMS.NLM	*only if newer than original*
\NETWARE\401\SPXDDFIX.NLM	SYS:\SYSTEM\SPXDDFIX.NLM	*only if newer than original*
\NETWARE\401\PM401.NLM	SYS:\SYSTEM\PM401.NLM	*only if newer than original*

Table 4-5
Windows Workstation Component Destination

User License Disk Location	Workstation Destination	Installation Conditions
\WINDOWS\CSTA.DLL	\WINDOWS\SYSTEM	
\WINDOWS\NWIPXSPX.DLL	\WINDOWS\SYSTEM	
\WINDOWS\NWCALLS.DLL	\WINDOWS\SYSTEM	*only if newer than original, and only if installing Telephony Services Administrator or on a workstation with NEXT or VLMs*
\WINDOWS\TSRVOAM.EXE	your choice	
\WINDOWS\TSRVOAM.HLP	same as for TSRVOAM.EXE	
\WINDOWS\WBTRCALL.DLL	\WINDOWS\SYSTEM	
\WINDOWS\THREED.VBX	\WINDOWS\SYSTEM	

Restricting Installation

Only administrators need to install Telephony Services Administrator. You may wish to prevent users from installing this application.

To control installation, remove TSRVOAM.EXE from the windows component directory on your server. Alternatively, you may revoke the scan trustee rights on TSRVOAM.EXE of any users or groups to whom you do not wish to grant Administrator access.

Do not remove any other files from the windows component directory; SETUP.EXE will not function if any other components are missing.

Invoking the Telephony Server

Loading Automatically

1. Edit your file server's AUTOEXEC.NCF file

Place the following commands into your server's AUTOEXEC.NCF file. After doing so, type them at the console to load the Telephony Server without restarting. You need never type these commands again; they will be executed automatically every time your server starts up.

1a. For all versions of NetWare:

Place the BSTART command immediately after the FILE SERVER NAME and IPX INTERNAL NET directives. This should make BSTART the third command in the AUTOEXE.NCF file.

1b. For NetWare 3.11:

```
LOAD  SPXDDFIX
LOAD  SPXFIX2
LOAD  SPXFSFIX
LOAD  SPXLISFX
LOAD  XMDFIX
LOAD  TSRV
```

1c. For NetWare 3.12 and 4.01:

```
LOAD  SPXDDFIX
LOAD  TSRV
```

1d. (optional) Load TSLIB for NetWare.

If you have applications that use TSLIB for NetWare, you must also add the following line to your AUTOEXEC.NCF file and subsequently type it at the console:

```
LOAD TSLIB
```

Example AUTOEXEC.NCF File

Before installing Telephony Services, a 3.11 server with an NE2000 LAN card might have an AUTOEXEC.NCF file such as this:

```
FILE SERVER NAME TSRV
IPX INTERNAL NETWORK A386
LOAD NE2000 PORT=360 IRQ=5 FRAME=ETHERNET_802.3
BIND IPX TO NE2000 NET=10
LOAD MONITOR
LOAD INSTALL
```

After installing Telephony Services, this same file server might have the following AUTOEXEC.NCF.

```
FILE SERVER NAME TSRV
IPX INTERNAL NETWORK A386
# ADD THE BSTART DIRECTIVE
BSTART

# SET MAXIMUM ALLOC SHORT TERM MEMORY & FILE COMMIT
SET MAXIMUM ALLOC SHORT TERM MEMORY=3500000
SET NCP FILE COMMIT=OFF

LOAD NE2000 PORT=360 IRQ=5 FRAME=ETHERNET_802.3
BIND IPX TO NE2000 NET=10
LOAD MONITOR
LOAD INSTALL

# LOAD SUPPLEMENTAL PATCHES
LOAD SPXDDFIX
LOAD SPXFIX2
LOAD SPXFSFIX
LOAD SPXLISFIX
LOAD XMDFIX

# LOAD TELEPHONY SERVER
LOAD TSRV
```

Loading from the Console

1. Load supplemental modules by typing

1a. For NetWare 3.11

```
LOAD  SPXDDFIX
LOAD  SPXLISFIX
LOAD SPXFIX2
LOAD  SPXFSFIX
LOAD  XMDFIX
```

1b. For NetWare 3.12 and 4.01

```
LOAD  SPXDDFIX
```

2 Load Btrieve by typing "BSTART" and pressing <Enter>.

If you see "This module is ALREADY loaded and cannot be loaded more than once" appear, you must unload any NLMs using Btrieve already, type "BSTOP" and press <Enter>. Then, load Btrieve by typing "BSTART" and pressing <Enter>.

3. Load the Telephony Server by typing

```
LOAD TSRV <Enter>
```

4. Load any Telephony Services Drivers.

Refer to your Telephony Service Drivers manuals for instructions on how to load TSDRV modules into memory.

5. (optional) Load TSLIB for NetWare.

If you have applications that use the NetWare version of TSLIB, you must load it into memory as well by typing

```
LOAD TSLIB <Enter>
```

Verifying Tserver Status

To determine whether the Telephony Server is loaded into your file server's memory, type the following to view a list of loaded modules:

```
DISPLAY MODULES <Enter>
```

You should see Telephony Server (TSRV.NLM) on the list of loaded modules.

Tserver Administration and Maintenance Components

chapter

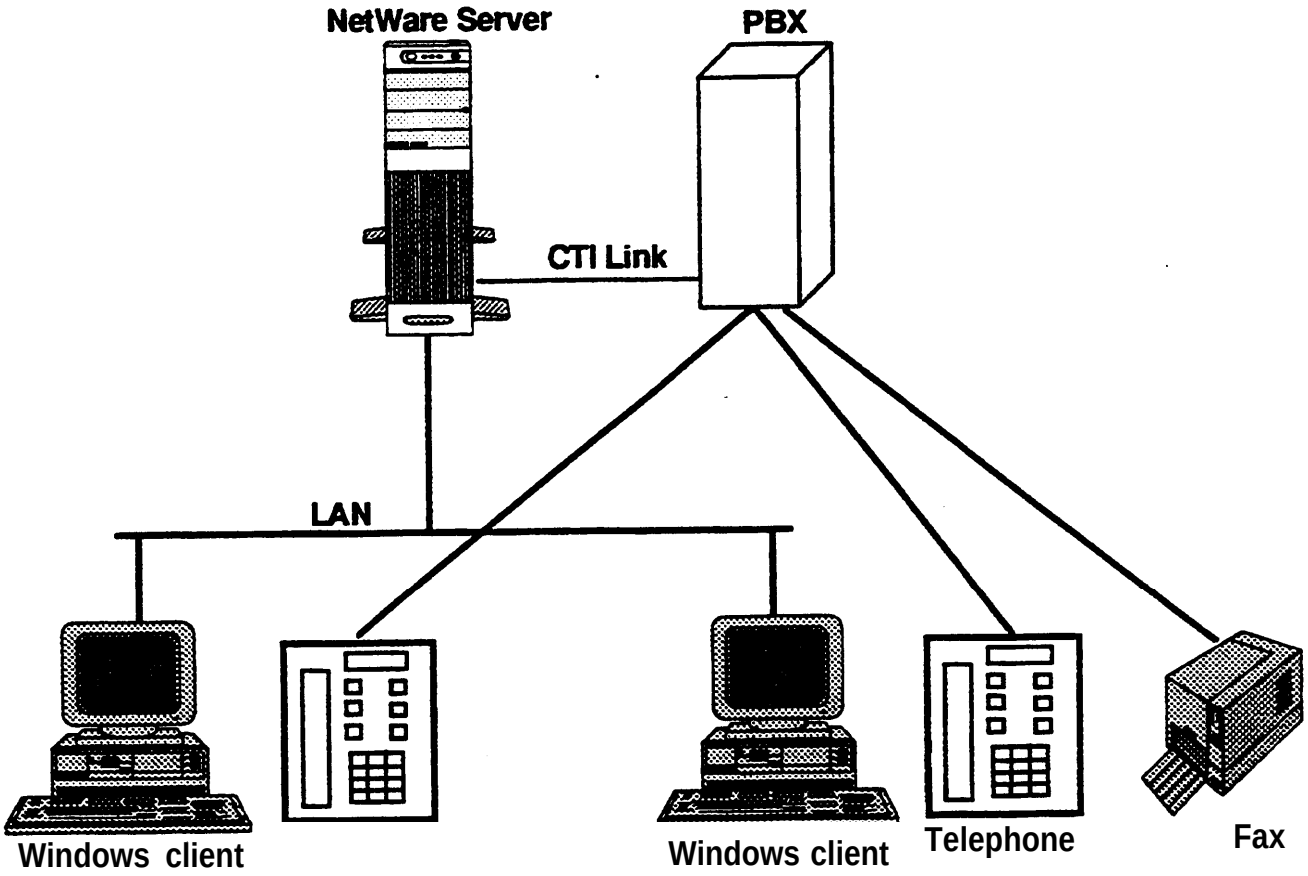
5 Tserver Administration and Maintenance Components

The Tserver Administrator application allows an administrator to administer, maintain, and obtain status information about the NetWare® Telephony Services functional components. The Administrator application is a windows client and uses a screen-based graphical user interface. Administration capabilities allow the user to create, edit, view, and delete each fictional component. Maintenance options include error logging and message tracing. Status information can be obtained for specific Telephony Services drivers and for client devices.

Introduction

Figure 5-1 illustrates a typical system configuration. Key elements of the system are: a PBX; devices which include telephones, modems, and fax machines attached to the PBX; a NetWare Server running NetWare Telephony Services; a CTI link linking the PBX to the Server; Windows PCs attached to the same LAN as the server; applications that run on the PCs; and users who might have a telephone and windows PC at their desktop.

Figure 5-1
Typical System Configuration



A typical flow of events in this system maybe: a user takes some action at the PC application like steps to launch a call; the Telephony Services client and server software checks the message for errors, runs a security check to determine that the telephone to be used for launching the call is assigned to the user, then sends the request over the CTI link to the PBX; the PBX causes the telephone to go off-hook and start dialing and also returns a confirmation over the CTI link to the application.

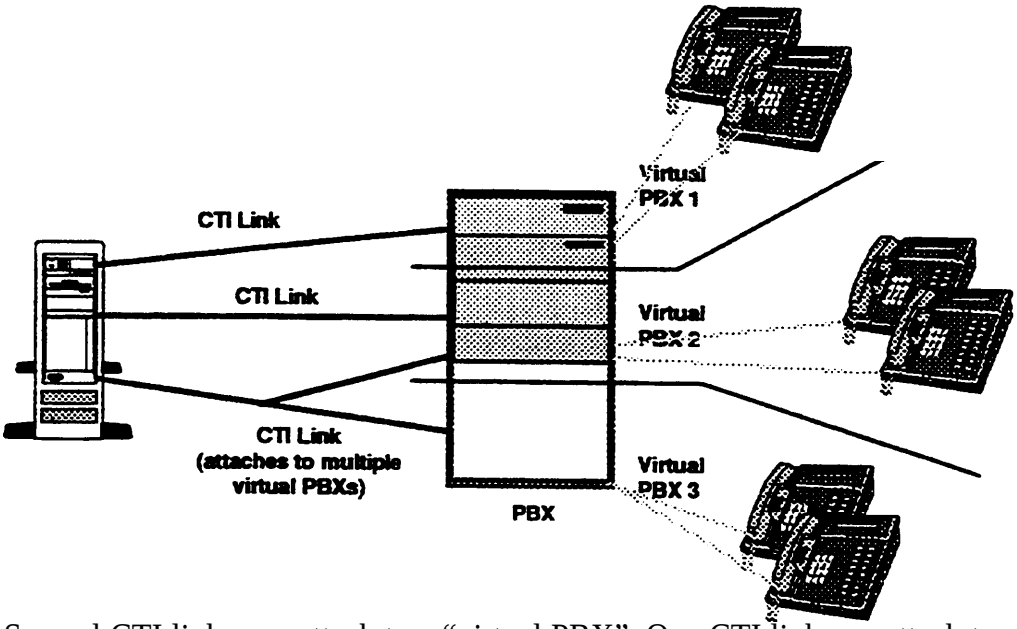
Administration is required to establish CTI links and associations between users and devices and is detailed later in this Chapter and in Chapter 6 through 7.

A CTI link connects the Tserver to a PBX; as mentioned before, the Tserver sends requests received from an application to the PBX over this CTI link. To handle application requests efficiently, the Telephony Services product supports multiple CTI links.

Your PBX can be divided into “virtual PBXs.” A virtual PBX is a set of devices (stations, phone numbers, ACD splits, and so forth). A virtual PBX can have one or more of its own CTI links, and consequently can function as a separate resource from the applications viewpoint. With a virtual PBX, you can allow separate organizations to have customized applications separate from one another. This means that heavy traffic in your billing organization, for example, will not degrade service elsewhere in the organization.

Virtual PBXs will also allow you to balance traffic over multiple links where you know there will be heavy link traffic. You create virtual PBXs yourself based on your requirements; see Chapter 7 for more details.

Figure 5-2
CTI Links and Virtual PBXs



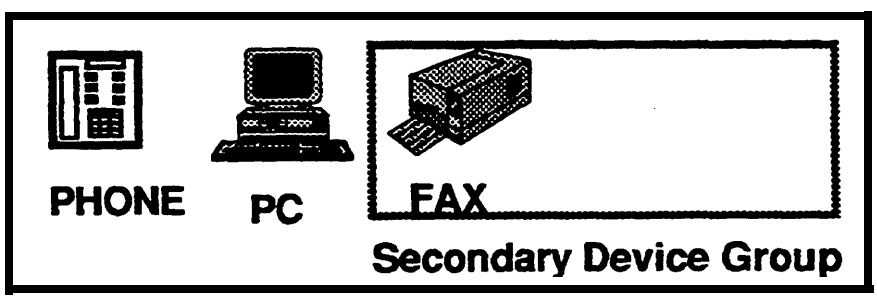
Several CTI links can attach to a “virtual PBX”. One CTI link can attach to multiple “virtual PBXs”. CTI link administration includes specifying which "virtual PBXs" are supported over that link. The Tserver enforces this when an application makes a request over the link.

An application residing on a client or server PC may act on behalf of a user, using the user's Tserver login/password to start a session with the Tserver. The session is started with the application connecting to the PBX via a CTI link (this is called “opening a stream”). The application can then issue requests on a device associated with the user. The Tserver will reject requests to devices that the user is not permitted to use.

The basic purpose of the Telephony Services product is to allow an application on a PC to control a set of PBX-connected devices. In order to manage which devices an application can control, devices are grouped together and associated with users. This is for security purposes, and also to associate devices with the individuals who need to use them.

The groups are: Worktop Groups, Secondary Device Groups, Call Control Groups, Monitor Groups, and Routing Groups.

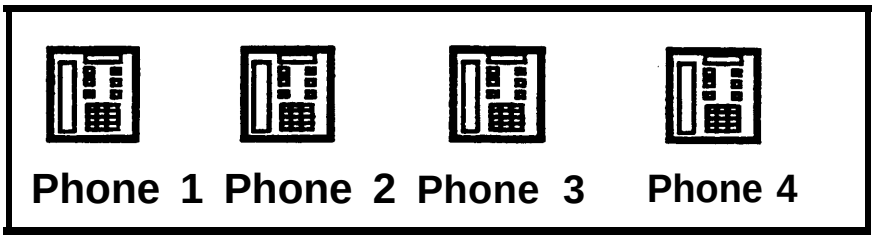
A Worktop group associates a user’s phone with the user’s PC. A worktop group contains a “primary device” which is intended to be the users primary phone on their desk a “PC” which is intended to be the Client PC that will control the phone on the desk and a “secondary device group” which contains all the other devices the user may want to control from their desktop PC. A secondary device group might contain for example a fax machine, a modem, or even the phones that a secretary has responsibility for covering. When a worktop group is assigned to a user, the user has privileges to control all the phones on that worktop.



Worktop Group

A Call Control Group is a group of phones. When the group is assigned to a user, an application acting for the user can control the group of phones. This is typically not used for desktop applications but for boss/secretary applications and call center applications. An example from outbound calling is a group of phones used by ACD agents, an application acting for a user

assigned the group may make outbound calls and transfer calls to the free agents.



Call Control Group or Monitor Group

A Monitor Group is a group of phones. When the group is assigned to a user, an application acting for the user can monitor the group of phones. This is typically not used for desktop applications but for billing applications and call center applications. In general, devices in a Call Control Group should also be in a Monitor Group because the information learnt from monitoring is required to request control of the devices. Although, devices in a Monitor Group may not be required in a Call Control Group, as in a billing application where calls are timed. Users have the permission to control and monitor all the devices in their worktop.

A Routing Group is a group of devices. When the group is assigned to a user, an application acting for the user can request CSTA routing on the devices in the group.

For the typical system described in Figure 5-1, Tserver administration needs to be done to administer the CTI link, the two Telephones, two worktop groups each containing the LAN address for a Windows client and a telephone and two users where each is assigned a worktop group. Details about each administration is described later in this guide.

Administration Components and Relationships

The administrator application operates on the following functional components:

- Servers and Drivers
- PBXs

- Admin Access Groups
- Devices
- Device Groups
- Worktops
- Users
- Security Database

Servers and Drivers

Various software modules register with the Tserver on installation:

- Tserver Administrator
- PBX-specific Drivers (TSDRV NLMs)
- PBX Driver Admin
- PBX Simulators

As the administrator, you use the Administrator application to administer identifiers for these four types of software modules. The information that you administer has already been or will be provided by the PBX Driver when it registers with the Tserver. The administration of these identifiers does not in anyway affect the identifiers used by the PBX Driver or Tserver. Therefore, you must know beforehand what identifiers the PBX Driver and the Tserver are using or will be using when they advertise on the NetWare network On the application screens, these identifiers are known as Admin links if they refer to the Tserver Administrator or CTI links if they refer to TSDRV NLMs or PBX simulators. When you create an identifier for one of these modules, you must specify the appropriate type of module. You associate the CTl links (corresponding to PBX Drivers) with various Devices (such as telephone extensions), thereby telling a Tserver which CTI links can monitor or control a Device.

Note When an application opens a stream to control a device, it gives the PBX Driver name. The association described allows the Tserver to determine if a request to control the Device on that link is valid; however, the Tserver does not 'choose" the CTI link. To make this association, you should first associate the CTI link with the PBX via the Tserver Administrator and then associate specific Devices with those PBXs.

The other types of software modules are all administration entities. Each Tserver uses NetWare Service Advertising to make these administration modules available to client applications. As the administrator, you must give a user permission to access these modules or the user cannot do so. To give these permissions, the administrator creates Admin Access Groups for a set of administration modules (see Admin Access Groups) and then associates these groups with users.

PBXs

As already described, you associate Devices and CTI links via PBX administration. Each PBX you create is given a name. You may then associate a device with this "virtual" PBX. Thus, the Tserver can determine that a request to control a particular device on a particular link is valid.

You must always administer "virtual" PBXs so that a Device is associated with CTI links to the "physical" PBX where the Device is wired. You may define PBXs and their respective Device associations such that all CTI links to a specific "physical" PBX are in one "virtual" PBX. You may also administer your system such that the Tserver only permits a specific CTI link to be used to control specific sets of devices, thus creating multiple "virtual" PBXs out of one "physical" PBX. This partitioning is useful for load balancing CTI links.

Note Note the following important administration rules:

- Only one Tserver maybe installed on any single server PC.
- One or more CTI links maybe installed on a single server PC.

- A CTI link may be associated with one or more “virtual” PBXs.
- A Device may only be associated with one “virtual” PBX.
- The CTI links contained in a “virtual” PBX may be on different servers.

Admin Access Groups

Another administrative responsibility is to associate Tserver/PBX Driver pairs for administration software modules (that is, Tserver Administrator, PBX Driver Admin, and PBX Simulators) into Admin Access Groups. The “Servers and Drivers” section described these administration software modules. As with PBXs, you must also name your Admin Access Groups as you create them.

While a PBX is associated with a Device, an Admin Access Group is associated with one or more specified users. A user may only access the administration modules in an Admin Access Group if you confer the appropriate access permissions.

Note the following important administration rules for Admin Access Groups:

- An administration module may appear in more than one Admin Access Group.
- A user may have only one associated Admin Access Group.
- Administration modules in an Admin Access Group may be located on different servers.
- Administration modules in an Admin Access Group may be provided by different vendors.

Devices

Devices are the communications objects that an application can monitor and control. These objects can be physical devices such as telephones or logical devices such as pilot numbers associated with Automatic Call Distribution (ACD) groups. Typically, a device is identified by its extension number on the PBX. Attributes of devices include:

- **Device ID** (mandatory): The exact dial string that the PBX requires. Refer to your PBX vendor's administration or implementation documentation for detailed information on the required string.

- **Device Type** (optional): The Administrator application provides the following device types: "phone," "fax," "modem," and "ACD." This attribute is provided solely for your convenience in record keeping. The Tserver does not use it when processing application requests.

- **Location** (optional): This field is provided solely for your convenience in record keeping. The Tserver does not use it when processing application requests.

A Device must be associated with a "virtual" PBX before an application can monitor or control it. The CTI links associated with the "virtual" PBX should all connect to the same "physical" PBX to which that Device is wired.

Note the following important administration rules for Devices:

- A device has only one PBX associated with it.

- A device maybe a member of one or more Device Groups.

- A device maybe the primary device of (at most) one Worktop.

Device Groups

You can associate Devices together into Device Groups, and assign a name to each such group. A device maybe included in one or more Device Groups. If desired, you may define a Device Group as an "Exception Group." An Exception Group is a time-saving feature that enables you to define groups equivalent to "all Devices except ...". For example, in an ACD Call Center environment if all agents can access all devices except the supervisor's extension and fax machine, then the Device IDs for the supervisor's telephone and fax machine would comprise an Exception Group. That Exception Group would then be specified as the Device Group for each ACD agent. In other words, the agents would be able to use every device except those listed in the Exception Group.

Note that a maximum of one Device Group may provide:

- A list of "secondary Devices" at a Worktop.
- An explicit list of Devices on which a user has permission to request CSTA Device/Device control.
- An explicit list of Devices on which a user has permission to request CSTA Call/Device control.
- An explicit list of Devices on which a user has permission to request CSTA Call control.
- An explicit list of Devices on which a user has permission to request CSTA Routing control.

Worktops

A Worktop is defined as the resources available to a user in his or her work environment. Typically, these resources include computing resources and communications resources. In most cases involving NetWare Telephony

Services, the computing resource is a PC connected to a Novell LAN which therefore has a LAN address. The communications resources typically include a primary Device (the voice telephone) and a number of secondary Devices (faxes, modems, etc.)

Worktop attributes include:

- **LAN Address** (mandatory). In certain configurations, the Tserver will not use the LAN address entry in the Security Database. However, you must still provide a unique identifier for this attribute. You must provide the *actual* LAN address if, and only if
  - You did *not* select the "Restrict user to Home Worktop" option, and
  - You want a user to be able to control the primary and secondary Devices at any Worktop at which he or she logs in.
- **Primary Device** (optional). This is typically the extension of the voice telephone at that Worktop.
- **Device Group** (optional). This is typically a Device Group containing other Devices that are present in that Worktop environment (additional telephones, faxes, etc.)

Note that a Worktop may be the Home Worktop for many users.

Users

Users are the individuals who use the NetWare Telephony Services product. A user can be an actual person or an application. User attributes are:

- **Login** (mandatory). An attribute that must contain the NetWare login identifier for the user on the server.
- **Name** (optional). A text attribute provided solely for the administrator's convenience.
- **Home Worktop Device ID** (optional). An attribute that may contain a Device ID for a primary Device at a Worktop. A Worktop may be a

Home Worktop for many users. Thus, the Security Database can accommodate a shared office, for example.

- **Classes of Service** (optional). Attributes that contain:
  - Optional Device groups specifying Devices for which the user may issue CSTA Monitoring-Only Services (Device/Device, Call/Device, and Call/Call) requests
  - CSTA Call/Device monitoring requests
  - CSTA Call Control Services
  - CSTA Routing Services
- **Admin Authorization,** an optional attribute containing a designated Admin Access Group. Users may access the administration software modules in the Admin Access Group.

Note that a user may:

- Have at most one Home Worktop.
- Have at most one Device Group for CSTA Device/Device monitoring.
- Have at most one Device Group for CSTA Call/Device monitoring
- Have at most one Device Group for CSTA Call Control.
- Be a member of at most one Admin Access Group.

Classes of Service

Many of the user attributes just described define the user's Classes of Service. Classes of Service define which CSTA services a user may request, and on which Devices he or she may request them. Class of Service attributes include:

Call Control Services

- **Call Control Access Group:** A user has permission to originate calls from the Devices in this Device Group. Note that the Monitoring attributes of Classes of Service must be set. A user may request CSTA Call Control on the Devices in this Device Group. Note that user also has Call Control monitoring at his/her Home Worktop via the Primary Device and the Secondary Device Group associated with it.

Monitoring-Only Services

- **Device/Device Monitoring:** CSTA Device monitoring provides an application with notification when a call arrives at a device, but stops providing information if the call is diverted to another endpoint (for example, transfer or coverage). A user may request CSTA device monitoring on the Devices in this Device Group. Note that user also has Device/Device monitoring at his/her Home Worktop via the Primary Device and the Secondary Device Group associated with it.

- **Call/Device Monitoring:** CSTA Call Monitoring provides an application with notification when a call arrives at a particular device and continues to provide information about the call as long as the call is being handled by the switch, even if it leaves the device on which the application had requested monitoring. A user may request CSTA Call Monitoring on the Devices in this Device Group. Note that user also has Call/Device monitoring at his/her Home Worktop via the Primary Device and the Secondary Device Group associated with it

- **Call/Call Monitoring:** CSTA Call/Call Monitoring provides an application with information about a call regardless of how many devices the call may be associated with during the life of the call. Call/Call Monitoring differs from Call/Device Monitoring in how the

monitor is started. In Call/Device Monitoring, the application monitors a particular Device and event notification begins when a call arrives at that Device. In Call/Call Monitoring, the application knows the identifier of a particular call and requests to monitor the call. Unlike Call/Device Monitoring where the monitoring of the call is device-dependent, Call/Call Monitoring is call-dependent and device-independent. A user may request CSTA Call/Call Monitoring when this attribute is set (it is a "yes/no" attribute indicated by a checkbox).

Routing Services

- **Routing.** A user may request CSTA Routing on the Devices in this Device Group.

User Authorization and Permissions

User authorization can involve multiple authorization mechanisms. To run an application that uses the Tserver, a user must have a valid Login and Password in the NetWare Bindery. When an application asks to open a stream, the Tserver NLM uses NetWare Bindery services to validate the user's login/password pair. Once validated, the user's application has an open ACS stream to a specific CTI link. The application can then request various CSTA telephony services.

Regardless of where they log in, the Tserver will always permit users to make CSTA

- Requests for the primary Device at the user's Home Worktop.
- Requests for the Devices in the secondary Device Group at the user's Home Worktop.
- Device/Device requests for Devices specified in the user's Class of Service for Device/Device access.
- Call/Device requests for Devices specified in the user's Class of Service for Call/Device access.
- Call Control requests for Devices specified in the user's Class of Service for Call Control across.

- Routing requests for Devices specified in the user's Class of Service for Routing access.

- Call/Call monitoring requests on all Devices only if the user's Class of Service for Call/Call Monitoring is set to "yes" via the checkbox.

You can also administer the system in such a way that, in general, a user will be able to control the primary and secondary Devices at any Worktop where he or she logs in. To enable this feature, you must:

- Disable the "Restrict User Access to Home Worktop" option.

- Administer the LAN address for all Worktops (where login should grant control permissions) to be the actual LAN address.

Security Database

The Security Database consists of a set of Btrieve files that are automatically created when the Tserver is installed. These files list all the users, devices, worktops, and so forth, associated with that Tserver, and the permissions associated with each of these components. The files are updated automatically as the administrator performs administrative functions.

Each Tserver has its own Security Database; however, these databases are not linked together. Hence, changing one does not automatically change the others. Consequently, it is recommended that you choose one Tserver Security Database to act as your "master" database, and use that database to overwrite any other.

Maintenance Components

The Administrator application provides three maintenance function components: an error log, a tracing utility, and status information for various system components.

Error Log

The Tserver always logs the following events in its error log:

- **Fatal Errors:** These are fatal error conditions in the Tserver or a registered PBX Driver.

- **Errors.** These are service-affecting, but not fatal conditions.

Along with the conditions that the Tserver always logs, you may also direct a Tserver to log:

- **Warnings.** These are not service-affecting, but may become so over time.

- **Audit Trail Events.** These are events that track system operations such as PBX drivers being loaded, a CTI link being reset, etc.

- **Cautions.** These are unexpected software conditions that are not fatal. The software is expected to recover gracefully.

- **Debugs.** These are trace messages for system and application debugging purposes.

Tracing Utility

As the administrator, you may direct a Tserver to trace messages flowing between the Tserver and the following:

- Selected connected client applications

- Selected registered PBX Drivers

- All Clients for selected PBX Drivers (including those that connect after tracing is started)

- All current and future registered PBX drivers

- All current and future connected client applications

The Tracing utility operates independently for each Tserver.

Status Information

A system administrator may request the following status information from a Tserver:

- **Tserver Status Information** provides:
  - The number of open streams
  - The number of clients with active streams
  - A list of the longest open streams
  - A list of the clients with the most open streams
  - A list of the clients with the most traffic
  - A list of the connected applications with the most instances
- **Client Detail Information** tells you, for each connected client, the:
  - Number of streams open.
  - User's NetWare login.
  - Number of streams closed.
  - Number of messages sent to the Tserver.
  - Number of messages the Tserver has sent to the Client.

  Selecting an item from this list will provide further detail information about the user or applications' interactions with the Tserver.
- **Registered TSDRV Information** tells you, for each PBX Driver:
  - PBX Driver name
  - Security information
  - TDI buffer space
  - Number of open connections

Selecting a PBX Driver from this list will provide further PBX Driver details.

Overview of Tserver Administration

chapter

6 Overview of Tserver Administration

This chapter presents an overview of administering a Tserver using the Administrator application.

Administrators

After installation, the Tserver allows the Supervisor login to access and administer the Tserver. The Supervisor login may make entries in the Security Database to grant other users permission to administer and maintain Tserver(s) Once a user has permission, then that user may, in turn, give other users administration and maintenance permissions. Users may be given permissions to administer or maintain only selectd Tservers.

As the administrator, you should:

- Place the administration software modules into Admin Access Groups.
- Name the Admin Access Groups you create. You may then associate a user with an Admin Access Group. Thus, the user has access permissions for the administration modules in the designated Admin Access Group.

Note the following important administration rules for Admin Access Groups:

- An administration module may appear in multiple Admin Access Groups
- A user maybe associated with only one Admin Access Group
- The administration modules in an Admin Access Group may be located on different servers.

- The administration modules in an Admin group may be administration modules from different vendors.

- Once a user has been given administration permissions for a Tserver, that user must also be given NetWare Read/Write permissions on that server's directory (SYS:\SYSTEM\TSRV\SDB). This directory contains Btrieve files that are part of the Security Database.

- Once administrators are defined (and they have the necessary NetWare permissions for the Security Database files), the Supervisor or any of these administrators can administer any aspect of the system.

- Only one administrator at a time may access the Security Database on a server. Thus, only one administrator may run the Tserver Administrator client application at any time.

Tserver Options

The Tserver Administrator application provides three options that you may administer on a Tserver-wide basis. These are:

- **Pop-up Alarms:** instructs the system to display a dialog box while the Administration and Maintenance application is running whenever an alarm occurs on the attached Tserver. When this option is enabled, the system will display the dialog box even if you have minimized the Tserver Admin client application on your screen. This dialog box must be dismissed before you can resume normal administration and maintenance tasks. If you do not check this box, the system will log any alarms, but will not display such a dialog box.

- **Restrict User to Home Worktop:** prevents users from controlling the Primary and Secondary Devices at any Worktop where they might log in. Enabling this option does not restrict users from opening streams at worktops other than their Home Worktops. However, it does prevent

users from controlling the Devices associated with worktops (other than their Home Worktops) at which they may log in.

- **Message Rate HWM:** instructs the system to write an error log entry if, in a 10-second interval, more than the specified number of messages passes across any of the following four interfaces: Client applications to Tserver, Tserver to Client applications, Tserver to PBX Drivers, PBX Drivers to Tserver.

PBXs

System administration requires that a Device be associated with a CTI Link. Tservers use a CTI Link to the PBX where the Device is wired.

Remember the following administration rules regarding Tservers, PBX Drivers, and PBXs:

- CTI Links can be grouped into “virtual” PBXs.
- Devices are associated with “virtual” PBXs.
- A Device is associated with only one “virtual” PBX.
- Only one Tserver maybe installed on any single server PC.
- Many CTI Links maybe installed on a sewer PC.
- A CTI Link maybe in many “virtual” PBXs.
- All CTI Links associated with a “virtual” PBX should correspond to CTI Links that terminate on the same “physical” PBX.

- Devices associated with a PBX should be wired to that PBX.

- A server that has multiple CTI Links to a single "physical" PBX requires only one "virtual" PBX unless there is some administrative reason to apportion Devices among the CTI Links.

- A server that has CTI Links to multiple PBXs will require, at a minimum, the same number of "virtual" PBXs as there are PBXs that connect to it.

In a configuration with multiple servers having multiple links to multiple PBXs, these rules apply. Note that in the special case of multiple servers with multiple links to the same PBX, all the CTI Links could be associated with the same "virtual" PBX. Thus, if an application sends a Tserver a request to control a Device, the Tserver need only find one active CTI Link in the "virtual" PBX with which the Device is associated. Doing so would be advantageous because a PBX Driver registers itself with the Tserver when it begins service.

Note PBX vendors may issue additional instructions about PBX administration for multiple server, multiple PBX configurations. Familiarize yourself with the installation procedures for your PBX drivers before administering PBXs.

Figure 6-1 illustrates a server with multiple CTI Links to two "physical" PBXs. The accounting, sales, and purchasing departments have phones wired to PBX1. The customer service department has phones wired to PBX2. The administrator created "virtual" PBXs: pbx1, accounting, sales, and pbx2. Note that the Tserver does not select the CTI Link. The Client application must specify to which CTI Link the stream should be opened. The Devices in the scenario depicted in Figure 6-1 are associated with the CTI Links such that applications must use:

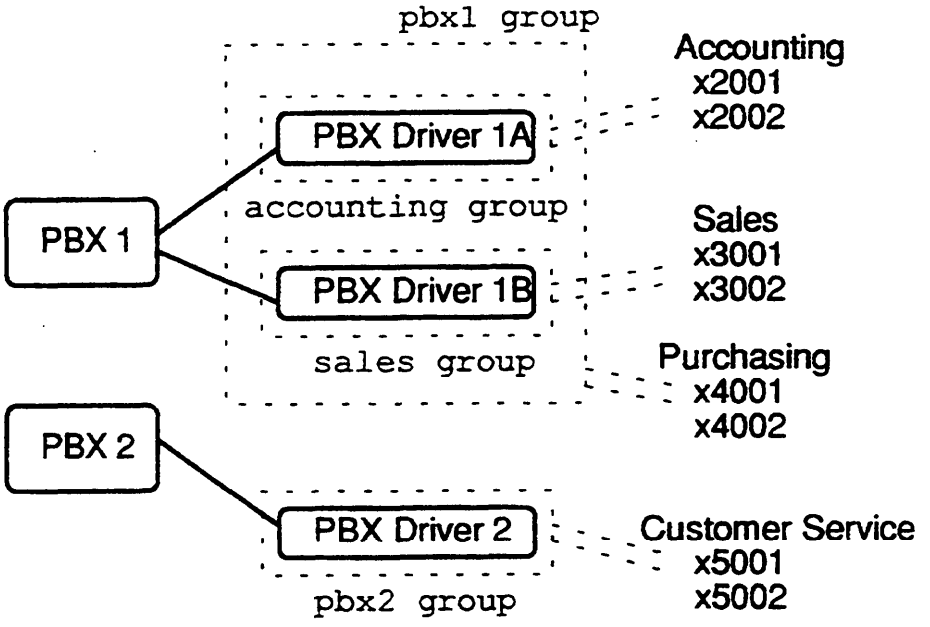
- PBX Driver 1A for telephones in the accounting department.

- PBX Driver 1B for telephones in the sales department

- Any PBX Driver for a CTI Link to PBX1 for telephones in the purchasing department.

- The PBX Driver for the CTI Link to PBX2 for telephones in the customer service department.

Figure 6-1
PBX Driver Scenario



Administering Multiple Tservers from a Single Security Database

In a configuration that contains multiple Tservers, it is possible to administer one copy of the Security Database for all Tservers and then copy it to the various servers. First, decide which Tserver will contain the "master copy" of the database. Define the Admin Link for the Administrator Application for this Tserver. Place this link into Admin Access Group(s) as needed to provide access to this application to any user who will administer the "master copy." Then, associate the Admin Access Group with these users.

To administer the "master copy" Security Database, the user must log in or attach to the server where the "master copy" resides. All Devices, Worktops, and users should be administered in the "master copy,"

regardless of the PBX to which the Device is connected. All administration for all Tservers goes in the master database.

When you add CTI Links, PBX Driver Admin modules, and PBX Simulators to the "master database," you specify the Tserver (where they reside) and their installed name when you create them. In this way, you add device information about CTI Links and administrative modules on other servers.

Each time an administrator updates the "master copy," you must update other copies of the Security Database residing on other servers. To do so, copy the files in Security Database directory SYS:\SYSTEM\TSRV\SDB to that same directory on other servers.

This is a manual process; the Admin application does not automatically copy the files.

Order for Administration

Generally, a Tserver should be administered in the following order:

1. **Global Options for the Tserver.**

   Administer the three global options described in the "Tserver Options" section of this chapter.

2. **CTI Links.**

   Administer the CTI Links and administration software module identifiers.

3. **PBXs.**

   Associate CTI Links that terminate on the same PBX with that PBX by creating one or more "virtual" PBXs.

4. **Admin Access Groups.**

   Give administration users permissions for sets of administration software modules.

5. Devices, Device Groups, Worktops, and Users.

Provide the Security Database for CTI applications.

The following section describes several approaches to administering these interrelated entities.

Device, Worktop, User Order

A Device must be administered to specify the primary Device for a Worktop. Similarly, a Worktop must be defined to specify the Home Worktop for a user. Thus, the order of administration for the components associated with any given user is: Device, Worktop, user. In addition, any Device Groups that are specified as the Secondary Worktop Devices or administered with user Classes of Service are prerequisite to complete user specification. However, you may opt to enter only the required user information and then later add these attributes. As the administrator, you could approach the data entry in two ways:

- Enter the Device, Device Groups, Worktop, and user data for each user sequentially.
- Enter all the Devices, then all the Device Groups, then all the Worktops, then all the user data.

Quick Administration via "Quick Add"

The "Quick Add" method is abbreviated because one Device Group must be used in all Classes of Service entries that use a Device Group. If you require more customization in your users' Classes of Service attribute administration, then you must administer Classes of Service via the user screen.

Common Configurations

You will encounter a number of common system applications, each with somewhat different permissions requirements. The following sections describe how to administer some common configurations.

Users Only Control Devices on their Home Worktops

The most efficient way of ensuring that users can only control Devices located on their Home Worktops is to enable the “Restrict User Access to Home Worktop” system option.

If specific users must control other devices, you can put those other Devices into Device Groups and specify those Device Groups as the Device Lists associated with the users’ Classes of Service attributes. Even with the “Restrict User Access to Home Worktop” system option enabled, those users will still be able to control the Devices specified in the Device Lists associated with their Classes of Service attributes.

If a subset of the user community needs permissions to control the Devices at a designated set of Worktops where they log in, then you can create a Device Group for each user containing the devices at the Worktops where they log in. Specify that Device Group in the Device Lists associated with the user’s Classes of Service attributes. Even with the “Restrict User Access to Home Worktop” system option enabled, those users will still be able to control the Devices specified in the Device Lists associated with their Classes of Service attributes regardless of the worktop at which they log in.

Similarly, creating a Device Group that you use as a Class of Service Device List will grant a variety of permissions that maybe exceptions to the more general need to restrict users to controlling only the Devices at their Home Worktops.

Use of this option can simplify your Worktop Administration. With this option, the Tserver does not use the LAN Address field from the Worktop screen. While the LAN address must be unique across all Worktop records, you may enter some unique string to avoid the tedious entry of LAN addresses. Using the Worktop’s primary telephone extension is one way to do this.

Users Control Devices at Worktop Where they Log In

The most efficient way of ensuring that users can control only the Devices associated with their Home Worktop and the Devices associated with any Worktop where they may log in is to:

- ♦ Disable the "Restrict User Access to Home Worktop" system option
- ♦ Administer an accurate LAN address

The exception cases described in the "Users Only Control Devices on their Home Worktops" can be handled in the same way here

Portion of User Community Shares Worktops

In a configuration where some users may log in at any of a number of Worktops (shift work, ACD agents, etc.) and where these users should not control other Devices (and vice versa), you should:

- ♦ Enable the "Restrict User Access to Home Worktop" system option
- ♦ Create a Device Group consisting of Devices from the shared Worktops
- ♦ Specify that Device List in the Classes of Service attributes for the users who share those Worktops

Boss/Secretary

You can enable a secretary to control a boss's telephone (or monitor several bosses' telephones) via the following method:

1. Set the "Restrict User Access to Home Worktop" system option as desired for other users.

2 Create a Device Group containing the boss's Devices.

3. Specify that Device List in the Classes of Service attributes for the Secretary.

However, in most cases, it may be simpler just to place the Devices that need to be controlled or monitored in the secretary's Secondary Device Group associated with his/her Home Worktop. If you choose to administer the Classes of Service attributes for the secretary, then you must be sure to administer the "Call/Device Access Group" option AND check the "Allow Call/Call Monitoring" option check box.

Call Monitoring Application for Phones

For applications such as billing, agent tracking/reporting, or virtual key telephone set:

- Enable the "Restrict User Access to Home Worktop" system option.
- Set the "Restrict User Access to Home Worktop" system option as desired for other users.
- Create a Device Group containing the monitored Devices.
- Check the "Allow Call/Call Monitoring" Class of Service check box.

How to Use the Tserver Administrator Client Application

chapter

7 How to Use the Tserver Administrator Client Application

The Telephony Server (Tserver) Administrator Client Application is an MS Windows interface to the Tservers comprising your system. Using the application's menus, you can perform operation, administration, and maintenance tasks, and get system status information and help. After installation, only the supervisor login can access and administer the Tserver.

Before You Begin . . . .

Before you can perform any administration or maintenance task, you must attach (log in) to a Tserver with a Security Database containing data for the Tserver that is to be administered or maintained. When there are multiple Tservers on a LAN, a convention may be established for administering all Tservers from one specific instance of the Security Database. A copy of this source must then be copied to the various Tservers. If you decide to administer your system in this way, then you must attach or log into the one Tserver that contains the official Security Database. If you do not do this, then any changes you make will be overwritten by a later copy of the official source when that source is copied to the Tservers on your system. The application does not automatically propagate changes made on the various Tservers on the LAN. If you want the same change to be made on each Tserver on the LAN, then you must make that change in the official instance of the Security Database and copy that source file to each Tserver comprising your system.

The actions described here assume the use of a mouse. However, the underlined character in menus and selections represents a keyboard equivalent that can be used instead.

Starting the Application

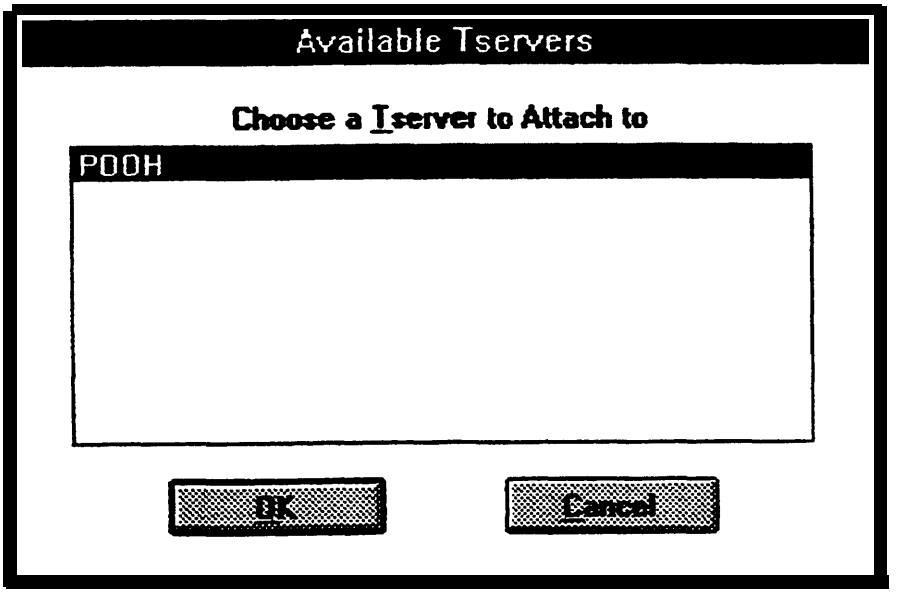
Procedure

1. **Log in or attach to a Tserver with a Security Database containing data for the Tserver that is to be administered or maintained.**

2. **Double click on the "Tservices Admin" icon to execute the Tserver Administrator application. The "Available Tservers**

   After installation, the Tserver allows the supervisor login to access and administer the Tserver.

Figure 7-1
Available Tservers Dialog Box



A dialog box will tell you if you do not have access permission for the Tserver you have chosen. After you dismiss this dialog box, the "Available Tserves" dialog box again becomes active.

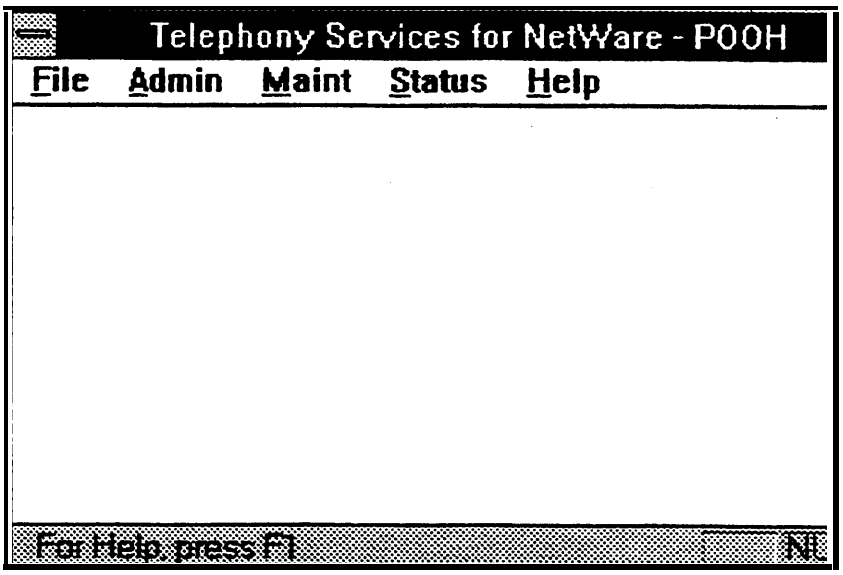
Note

Only one user may administer or maintain a Tserver at one time.

Performing Administrative Tasks

After you attach to a Tserver, the Administrator window is displayed. The title bar displays the name of the Tserver to which you have attached.

Figure 7-2
Administrator Window



Whenever a command completes, the dialog box associated with the command disappears, and the corresponding status bar displays "Command Successfully Completed." This message remains until you browse through the applications menu items.

Remember the following attributes of the Tserver Administrator application:

- You can adjust the size of the application window. Since the main window does not display significant information, it is recommended that you make the main window as small as possible, yet large enough so you can see the menu items and the status bar.

- Like any standard windows application, the Administrator application itself can be maximized or minimized.

Note

Pop-up alarm windows will appear on your screen even if you have minimized the application.

♦ Only one user may administer or maintain a Tserver at one time.

The Administrator window choices are:

♦ F ile

♦ A dmin(istration)

♦ M aint(enance)

♦ S tatus

♦ H elp

F ile Menu

The "F ile" submenu has two options:

♦ L ogout terminates your attachment to the Tserver that you are currently administering or maintaining. Once the attachment has been terminated the application again displays the "Available Telephony Servers" dialog box. You can then attach to another Tserver.

♦ E x it terminates the Tserver Administrator application.

Pop-up Alarm Notification occurs only for the Tserver to which you are attached. If you log out, you are no longer attached. Selection of Pop-up Alarm Notification does not carry forward to any other server to which you may attach. You must specifically set this Option (on the "A dmin" menu) each time you attach to a new Tserver.

A dmin Menu

The Admin menu offers the following choices:

♦ O ptions

♦ Advertised N ames

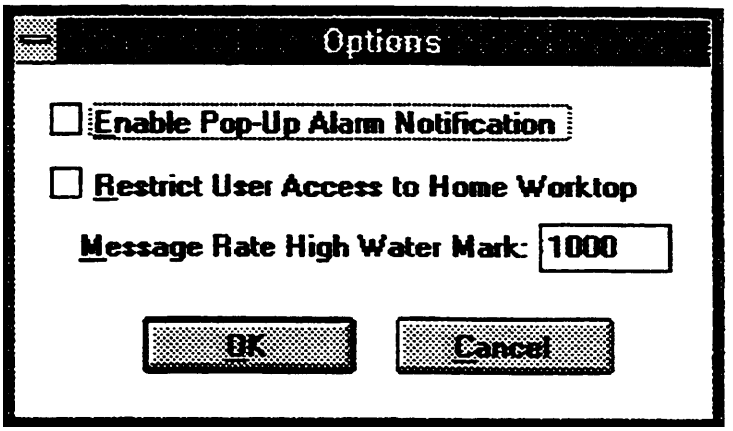
- P BXs
- D evices
- Device G roups
- W orktops
- U sers
- Ad m in Access Groups
- Q uick Add

Setting Options

Procedure 23

1. **At the "A dmin" menu, select "O ptions" to open the "Options" dialog box.**
2. **Specify one or more of the following options for the Tserver to which you are attached; that is, to which you have logged in.**

Figure 7-3
Options Dialog Box



The options are:

- **Enable Pop-up Alarm Notification** instructs the system to display a dialog box (of the type that you must dismiss before

continuing) when an alarm occurs on the Tserver while the Tserver Administrator application is running. If you do not check this box, the system will log alarms, but will not display a such a dialog box. It is recommended that you check this option if you are running critical applications so you can be notified of any problems as they occur.

- **Restrict User Access to Home Worktop** is a fast way to administer a Tserver for a configuration where all Tserver users may only monitor or control the telephone at their home worktop.

If a user needs to control a Device other than one associated with his or her Home Worktop, then do not check this box.

Using this option can simplify your Worktop administration. With this option, the Tserver does not use the required LAN Address field from the Worktop administration screen. While the LAN address must be unique across all Worktop records, you may enter any unique string to avoid the tedious entry of LAN addresses. Using the Worktop's primary telephone extension is an easy way to do this.

- **Message Rate High Water Mark** instructs the system to write an error log entry if, in a 10-second interval, more than the specified number of messages passes across any of the following four interfaces:
  - Client applications to Tserver
  - Tserver to Client Applications
  - Tserver to PBX Drivers
  - PBX Drivers to Tserver

The message counts are taken over a series of discrete 10-second time intervals; they are not a rolling average computation. The system counts messages for each of the four interfaces independently; it does not total the message counts across these interfaces.

Administering Advertised Names

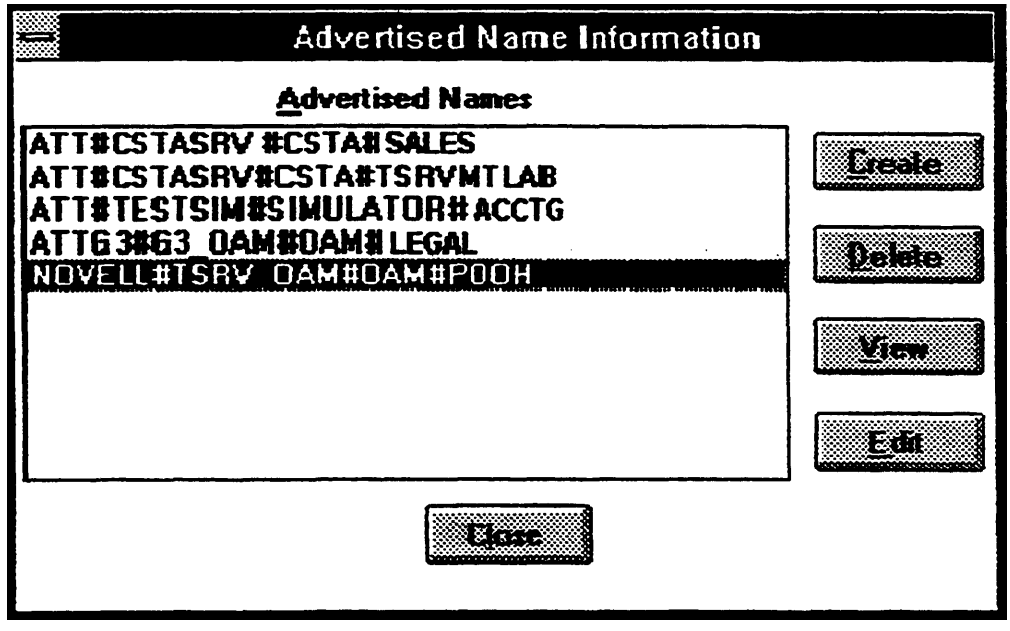
You must administer advertised names in order to later create:

- **Admin Access Groups** which maybe used to confer administration permissions on users for a specified set of Tservers or PBX Drivers. TSDRV Admin, Simulator, and Tserver Admin advertised names may be placed in Admin Access Groups.
- **PBXs** which associate CTI Links that connect to a particular "physical" PBX. An administered "virtual" PBX provides away to refer to a set of CTI Links to a given "physical" PBX. Later association of Devices (extensions) with a PBX tells the system which Tserver and PBX driver(s) may control or monitor the Devices. CTI link advertised names may be associated with PBXs.

Procedure 23

1. At the "A dmin" menu, select "Advertised N ames" to display the "Advertised Name Information" dialog box.

Figure 7-4
Advertised Names Dialog Box



This dialog box contains a list of previously administered Advertised Names. Each entry in the Advertised Names list is a NetWare®

advertising handle that contains four substrings separated by a pound sign.

The first substring is the vendor of the item; the second is the CTI Link or Administrator software module type; the third is the NetWare advertising type; the fourth is the name you give to the Tserver when you create or edit it.

2. Scroll or browse through the list of all administered Advertised Names.

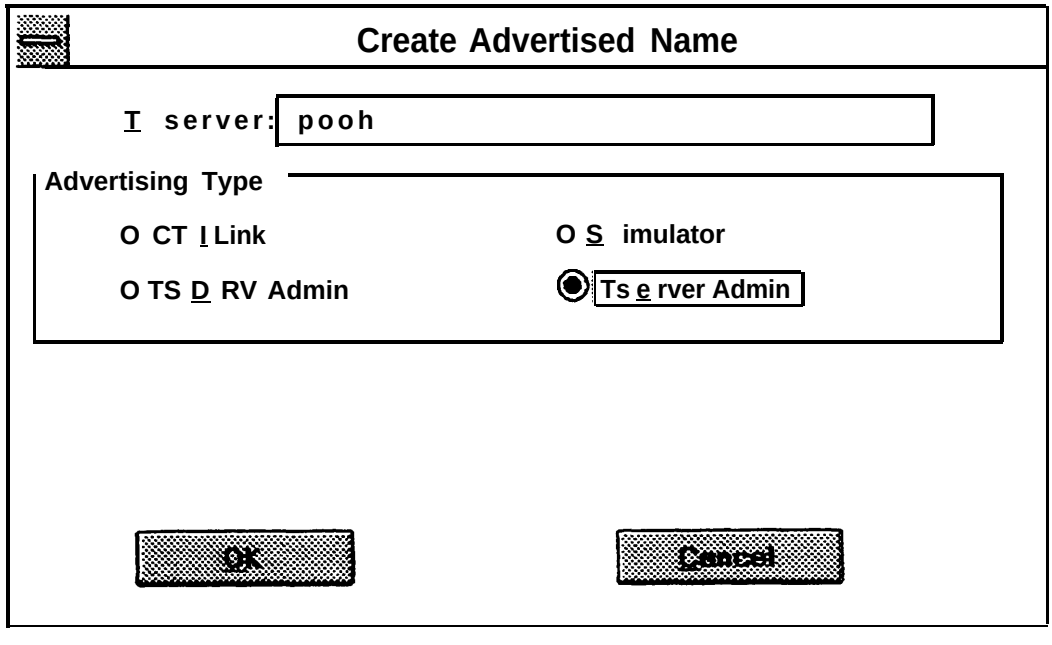
Then either select an existing Advertised Name or create a new one.

Creating an Advertised Name

Procedure 23

1. Select "C reate" on the "Advertised Name Information" dialog box.

Figure 7-5
Create Advertised Name Dialog Box



The fields are:

- **Tserver** is the NetWare name of the file server where the CTI Link, Tserver or PBX Driver administrative module, or PBX simulator is located. Since the application allows you to keep information about multiple Tservers in the Security Database, the name of the file server to which you attached does not have to be the same as the server named in the "Available Tservers" dialog box.

  The string you enter may not exceed 23 upper or lower case characters and may not contain the pound sign (#).

- **Advertising Type** refers to the kind of service provided by a PBX Driver, PBX Simulator, or a Tserver. Four kinds of service are currently advertised CTI Link, TSDRV Admin, PBX Simulator, and Tserver Admin:

  - **CTI Link** specifies the name of the logical link between a PBX and a driver. Some vendors' PBX Drivers may aggregate multiple physical links into a single logical link. You will use this information later to associate CTI Links with a PBX. The name of the PBX then gives you a single name by which to refer to all CTI Links to that PBX. Fill in the PBX Name field with the link name used to install the PBX driver, and fill in the Vendor field with name of the vendor that provided your PBX.

  - **TSDRV Admin** specifies that the advertised service type is the administration and maintenance of a PBX Driver. You can include this type of service in an Admin Access Group to give users administration permissions for that PBX Driver. Fill in the Driver Admin Name field with the physical name used to install the PBX driver, and fill in the Vendor field with the name of the vendor that provided your PBX Driver. Refer to the appropriate documentation for your PBX Driver for details on the administration and maintenance of the PBX Driver.

  - **Simulator** specifies that the advertised service type is for accessing a PBX Simulator. You can include this type of service in an Admin Access Group to give users permissions to access that PBX Simulator. (Client

applications may make requests of a PBX simulator just as they do of any Tserver.)

- **Tserver Admin** specifies that the advertised service type is the administration and maintenance of a Tserver. You can include this type of service in an Admin Access Group to give users administration on permissions for the Security Database located on that Tserver. The system does not require identifying vendor/name information for Tserver Admin.

2. Enter the name of the desired Tserver.

3. Select the desired Advertising Type.

If you select "CTI Link," "TSDRV Admin," or "Simulator" as the Advertising Type, the system will request that you fill in the identifying information for the vendor and either the Driver or simulator as appropriate.

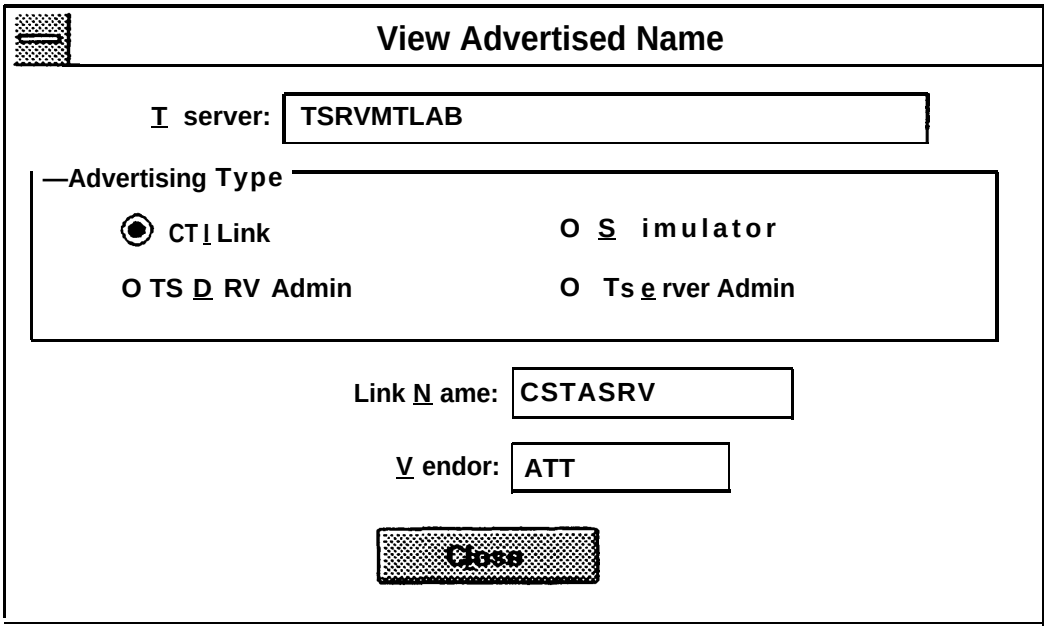
4. Choose "O K" to record the Advertised Name information in the Security Database, or "C ancel" if you do not wish to record the information.

Viewing Advertised Name Information

1. Select the Advertised Name that you want to view.

2 Choose "V iew" on the "Advertised Name Information" dialog box.

Figure 7-6
View Advertised Name Dialog Box



Note

You cannot make any administration changes to the field contents from this dialog box.

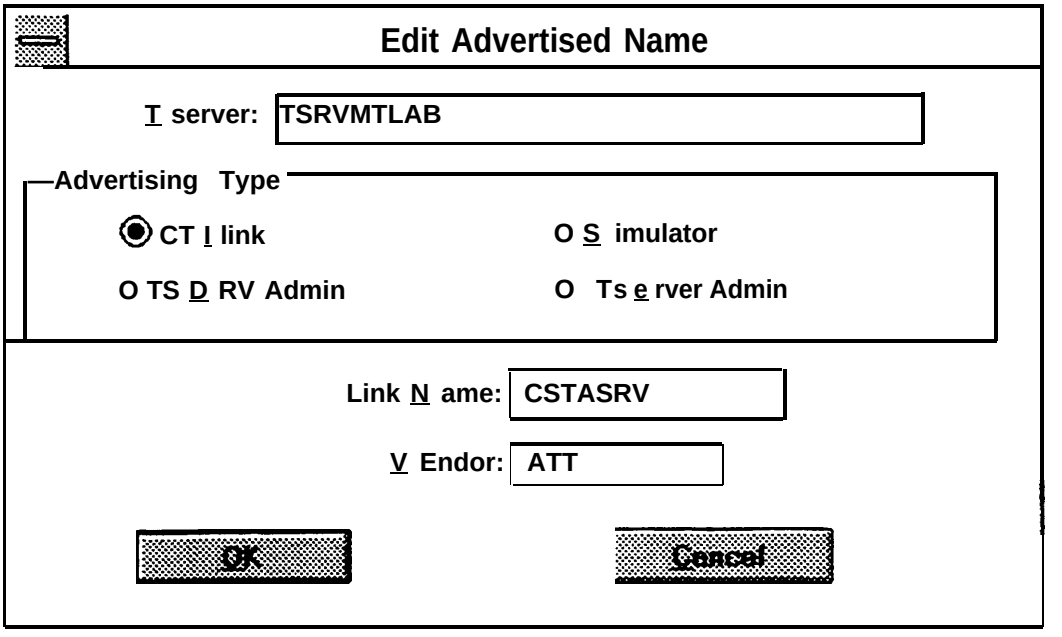
3. **Choose "Close" when you have finished viewing the information for the selected Advertised Name.**

Editing Advertised Name Information

Procedure

1. **Select the Advertised Name you want to modify.**
2. **Choose "Edit" on the "Advertised Name Information" dialog box.**

Figure 7-7
Edit Advertised Name Dialog Box



3. Make the desired modifications to the displayed Advertised Name information.

4. Choose "O K" to record the modified information for the selected Advertised Name in the Security Database, or chose "C ancel" if you do not wish to record the information.

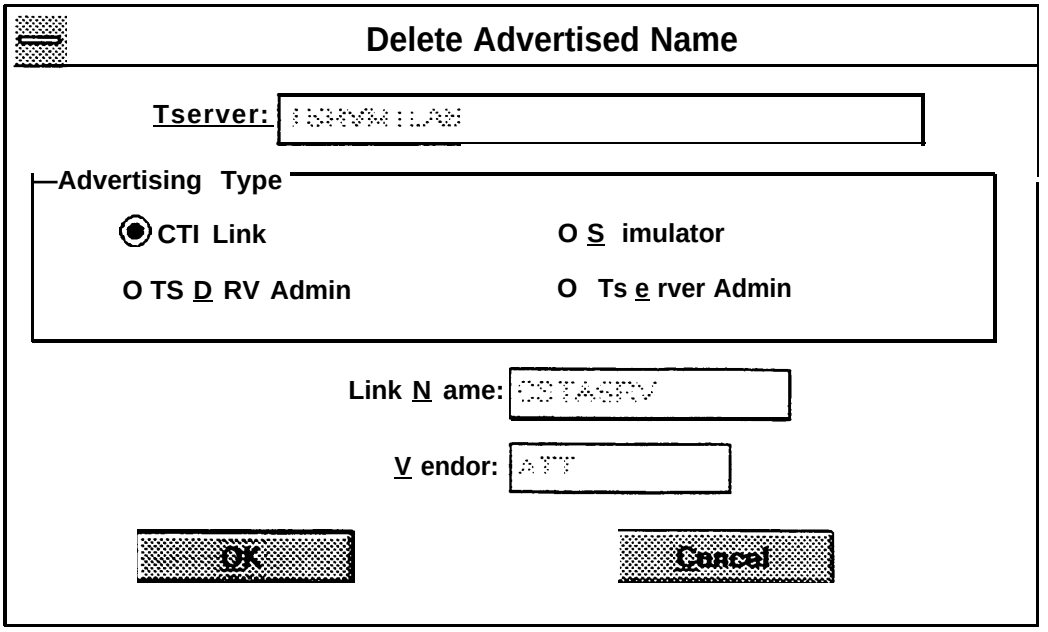
Deleting Advertised Name Information

Procedure 23

1. Select the Advertised Name that you want to delete.

2. Choose "D elete" on the "Advertised Name Information" dialog box.

Figure 7-8
Delete Advertised Name Dialog Box

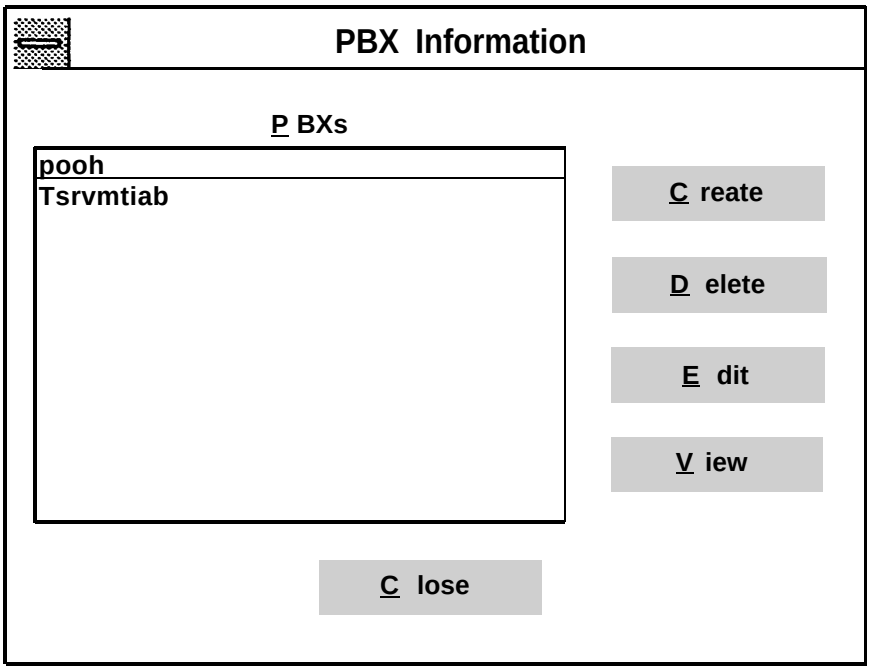


3. Choose "O K" to delete the selected Advertised Name from the Security Database, or "C ancel" if you decide not to delete it.

Administering PBXs

At the "A dmin" menu, select "PBX" to open the "PBX Information" dialog box.

Figure 7-9
PBX Information Dialog Box



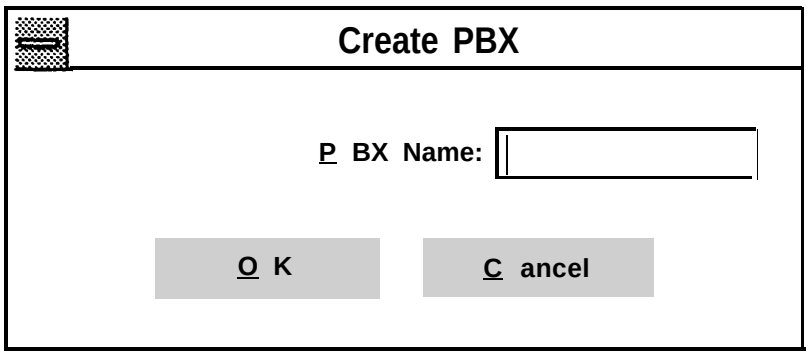
This dialog box displays all administered PBXs.

Creating a New PBX

Procedure 23

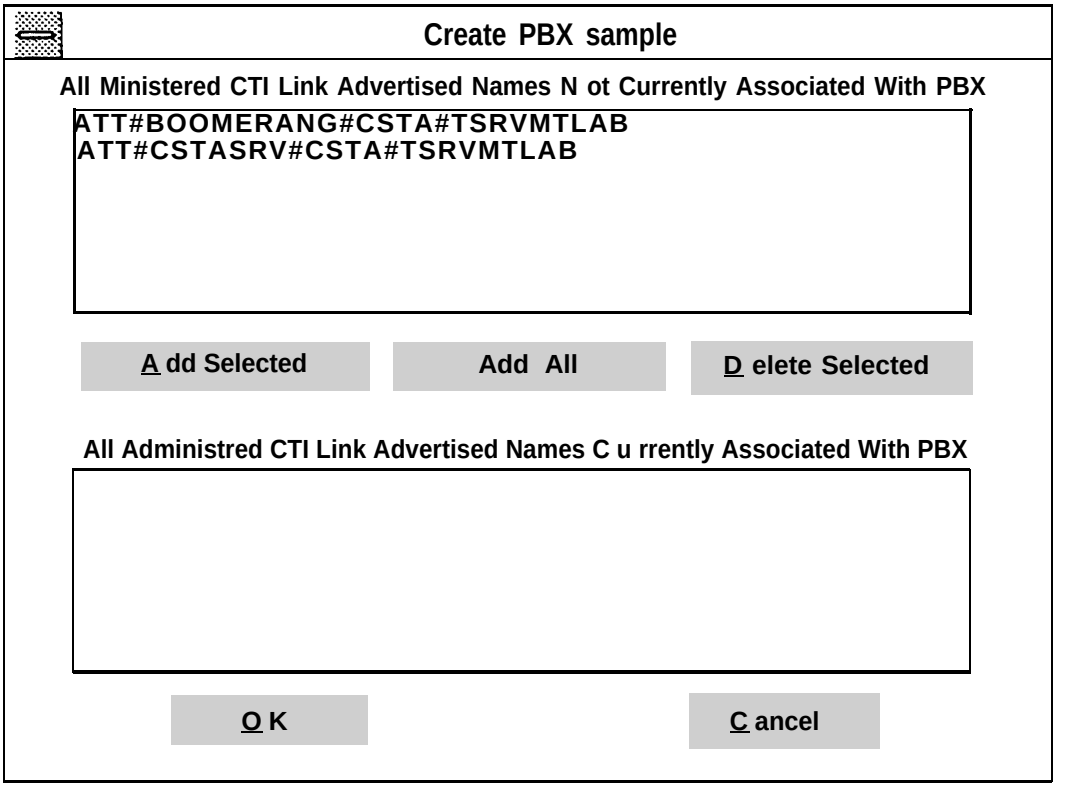
1. **Choose "Create" on the "PBX Information" dialog box.**

Figure 7-10
Create PBX Dialog Box



2. **Once you have created and named a PBX, the "Create PBX <NAME> dialog box is displayed.**

Figure 7-11
Create PBX <NAME>
Dialog Box



This dialog box contains two lists:

- **CTI Link Advertised Names N ot Currently Associated With PBX** lists all Advertised Names of type "CTI Link" that are not associated with the selected PBX.

- **CTI Link Advertised Names C u rrently Associated With PBX** lists all CTI Links that are currently associated with the selected PBX.

3. Select the desired PBX. From the available choices listed in the top list box, select one or more CTI Links that you want to add to the selected PBX.

Note

To select multiple entries within the list, hold down the "Control" key as you make your selections with the mouse. To select several contiguous

entries within the list, hold down the “Shift” key as you make your selections with the mouse.

4. **Choose the appropriate “Add” button to associate a CTI link with a PBX.**

   All CTI links associated with a PBX must terminate on that PBX. Therefore, if all the CTI Links listed meet this criterion and you want to associate all of them with the desired PBX, then choose the “Add All" button.

5. **Choose the “Delete Selected” button to remove a CTI link from a PBX.**

6. **Choose “O K to record the changes in the Security Database, or choose “C ancel” to return to the “PBX Information” dialog box without recording in the Security Database any of the changes you specified on the screen.**

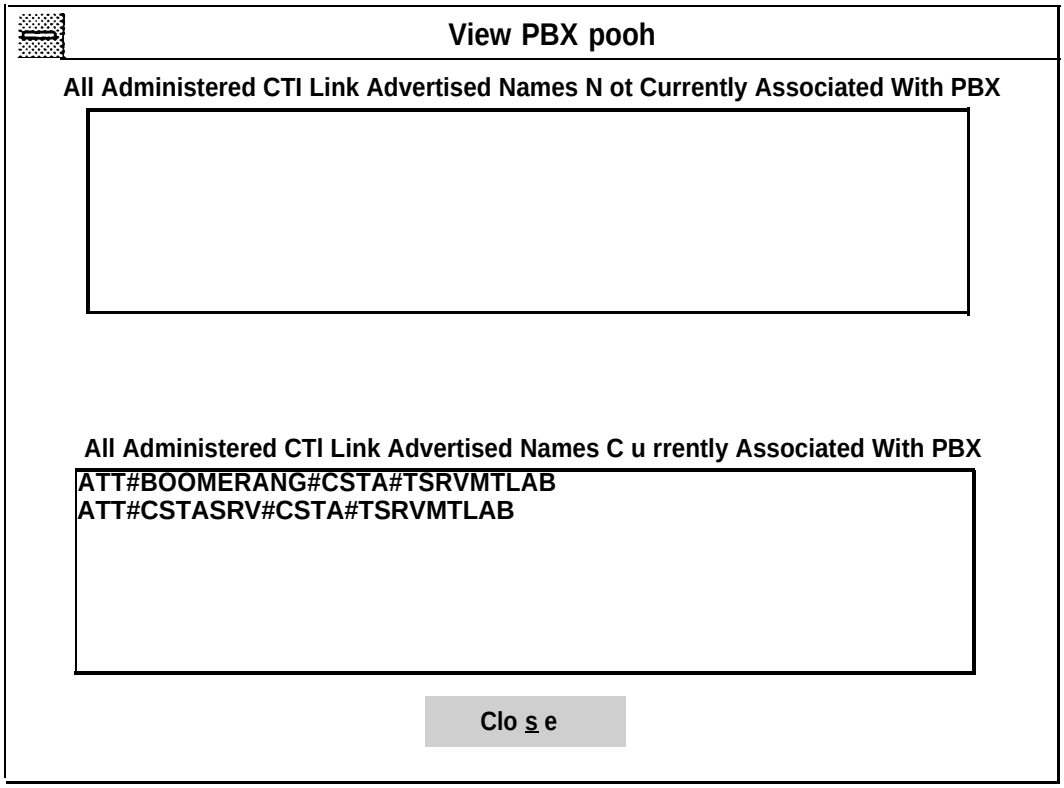
Viewing a PBX

You cannot make any administration changes to the field contents from this dialog box.

1. **Select the desired PBX.**

2. **Choose “V iew” on the “PBX Information” dialog box to enable you to view the selected PBX.**

Figure 7-12
View PBX Dialog Box



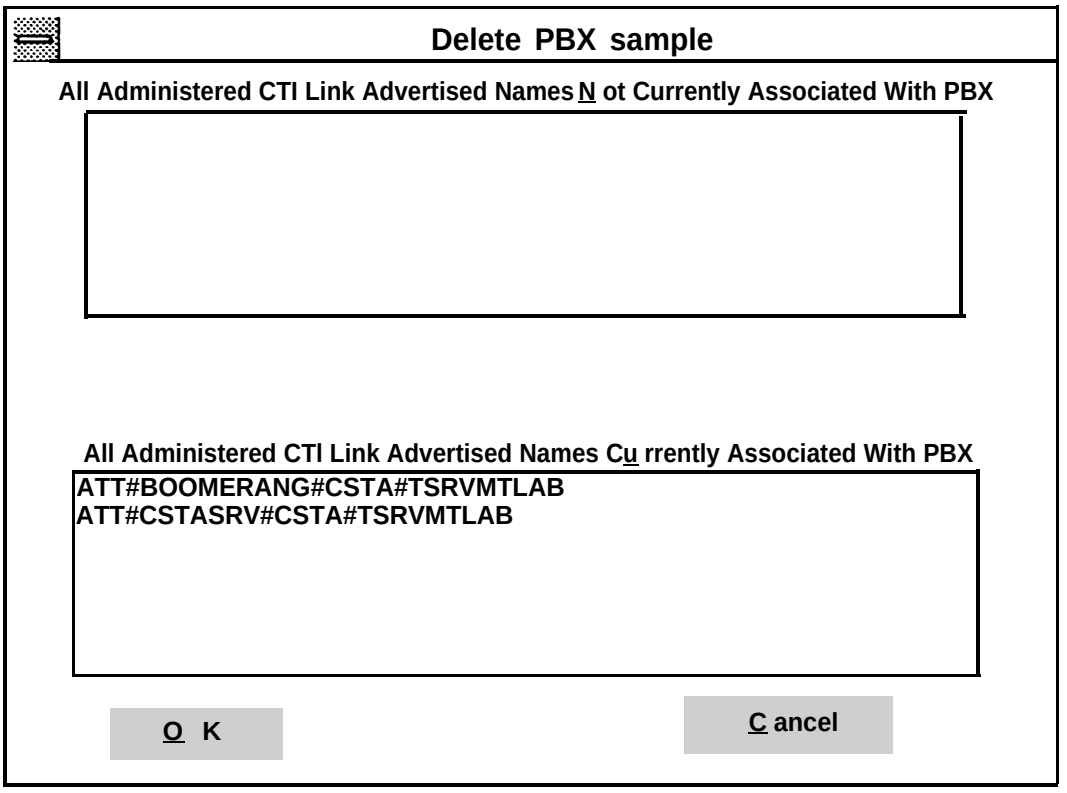
3. Choose "Clo s e" when you have finished viewing the selected PBX.

Deleting a PBX

Procedure

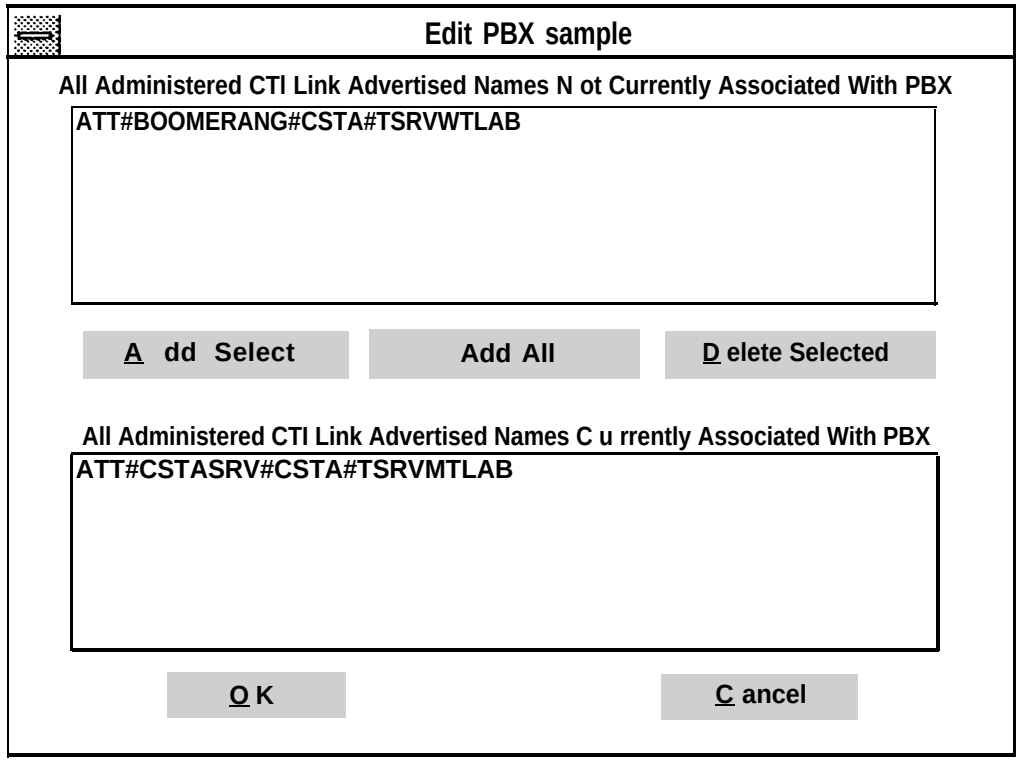
1. Select the desired PBX.
2. Choose "D elete" on the "PBX Information" dialog box to enable you to view the selected PBX.

Figure 7-13
Delete PBX Dialog Box



3. Choose "OK" to record the changes in the Security Database or choose "Cancel" to return to the "PBX Information" dialog box without recording deletion of the specified PBX in the Security Database

Figure 7-14
Edit PBX Dialog Box



This dialog box contains two lists:

- **CTI Link Advertised Names Not Currently Associated With PBX** lists all Advertised Names of type "CTI Link" that are not associated with the selected PBX.
- **CTI Link Advertised Names Currently Associated With PBX** lists all CTI Links that are currently associated with the selected PBX.

Procedure 23

1. Select the desired PBX. From the available choices listed in the top list box, select one or more CTI Links that you want to add to the selected PBX.

Note

To select multiple entries within the list, hold down the "Control" key as you make your selections with the mouse. To select several contiguous

entries within the list, hold down the "Shift" key as you make your selections with the mouse.

2. **Choose the appropriate "Add" button to associate a CTI link with a PBX.**

   All CTI links associated with a PBX must terminate on that PBX. Therefore, if all the CTI Links listed meet this criterion and you want to associate all of them with the desired PBX, then choose the "Add A l l" button.

3. **Choose the "Delete Selected" button to remove a CTI link from a PBX.**

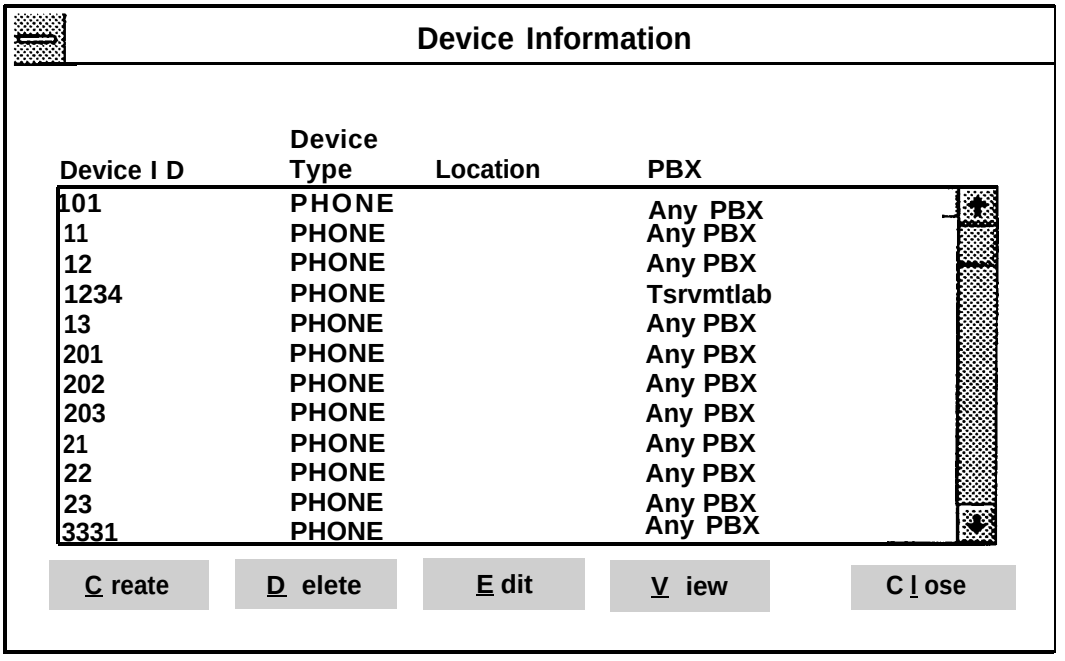
4. **Choose "O K" to record the changes in the Security Database, or choose "C ancel" to return to the "PBX Information" dialog box without recording in the Security Database any of the changes you specified on the screen.**

Administering Devices

The following steps are not required if you use Quick Add.

1. **At the "A dmin" menu, select "D evices" to open the "Device Information" dialog box.**

Figure 7-15
Device Information Dialog Box



The dialog box lists previously administered devices.

The fields are:

- Device ID is the exact string that the PBX demands to be dialed to access that particular device. Refer to your vendor's PBX documentation for detailed information on the required string. If a Device ID is too long for the display, the complete ID will not appear on the screen. If this is the case, choose "Edit" or "View" to see the complete Device ID.
- Device Type (telephone, fax, modem, ACD) is an optional entry that shows the administered type for the device.
- Location is an optional entry that typically contains the room number where the device is located.
- PBX is the switch to which the device is associated.

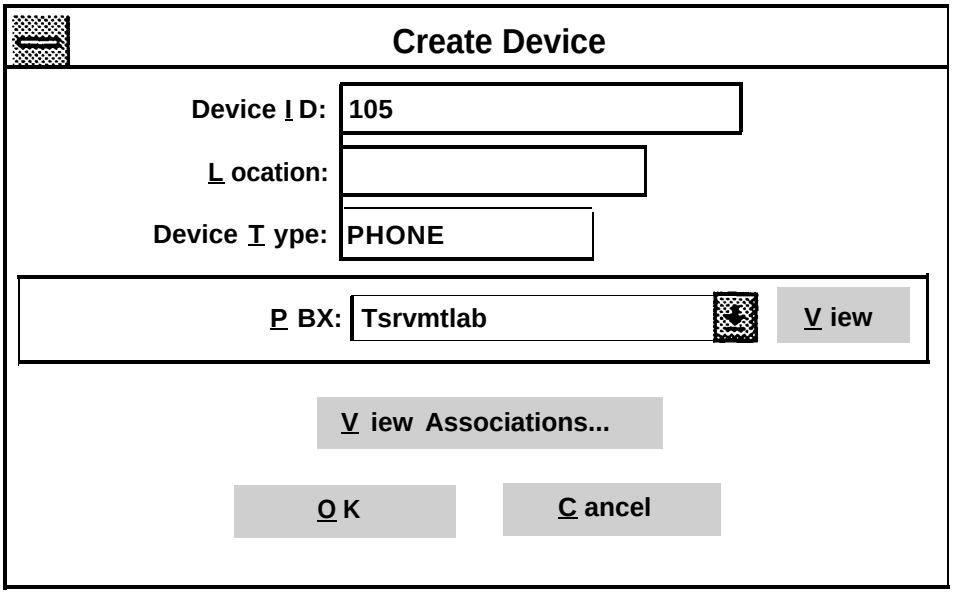
2. **Scroll or browse through the list of any administered Devices. Then either select an existing Device Name or create a new one.**

Creating a Device

Procedure 23

1. **Choose "C reate" on the "Device Information" dialog box if you wish to create a device.**

Figure 7-16
Create Device Dialog Box



The fields are:

- **Device I D** is a mandatory unique identifier for the device that is the exact string that the PBX demands to be dialed to access that particular Device. Refer to your vendor's PBX documentation for detailed information on the required string. The Device ID must be unique across all devices in the Security Database.
- **L ocation** is an optional entry that you may use to track room numbers, etc.
- **Device T ype** is an optional entry that you may select from a drop-down list of device types (telephone, fax, modem, ACD, etc.). Device types are provided solely for your convenience in

maintaining the Security Database. The Tserver does not use this information for type-checking CSTA requests. Thus, it is permissible to enter a device type of "phone" for the extension of an Automatic Call Distributor. The default value for device type is "phone."

- **P BX** is a drop-down list showing all administered PBXs. You associate the Device with the PBX that can monitor and control it. This is a single-selection list (that is, you select from one of the choices in the list).

2. Enter the required information into the mandatory fields ("Device ID" and "PBX").

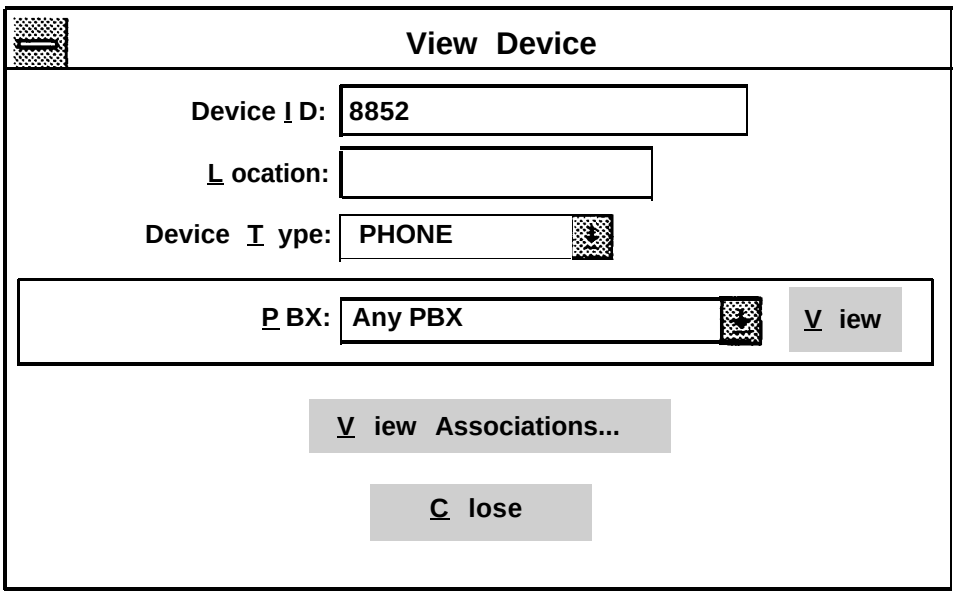
3. Choose "O K" to record the new device information in the Security Database, or choose "C ancel" if you do not want to record the new device information in the Security Database.

Viewing Device Information

1. Select the device that you want to view on the "Device Information" dialog box.

2. Choose "V iew" on the Device information dialog box to open the "View Device" dialog box.

Figure 7-17
View Device Dialog Box



Note

You cannot make any administration changes to the field contents from this dialog box.

3. (Optional) Select a PBX via the drop down list and choose "View" to see it.

4. (Optional) Choose "View Associations" to see any users and Worktops associated with this device.

5. Choose "Close" when you have finished viewing the information for the selected device.

The system redisplays the "Device Information" dialog box.

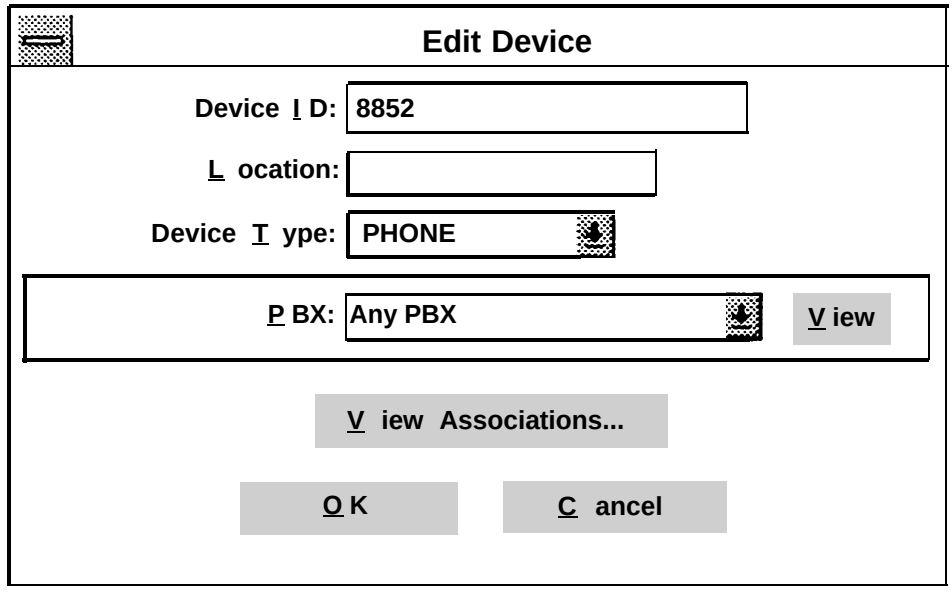
Editing a Device

Procedure

1. Select the device that you want to edit on the "Device Information" dialog box.

2. Choose "Edit" on the "Device Information" dialog box.

Figure 7-18
Edit Device Dialog Box



3. **Select the appropriate PBX using the drop-down list.**

4. **Choose "View" to view all administered CTI Link Advertised names currently associated with the selected PBX. Choose "View Associations" to view device groups to which the device belongs and worktops and users associated with this device.**

Note

You cannot make any administration changes to the field contents from this dialog box.

5. **Choose "Close" when you have finished viewing the PBX information in the dialog box.**

   The system redisplays the "Edit Device" dialog box.

6. **Make any other desired changes to the remaining fields (for example, to the Device Type field).**

7. **Choose "OK" to record the new device information in the Security Database, or choose "Cancel" if you do not want to record the new device information in the Security Database.**

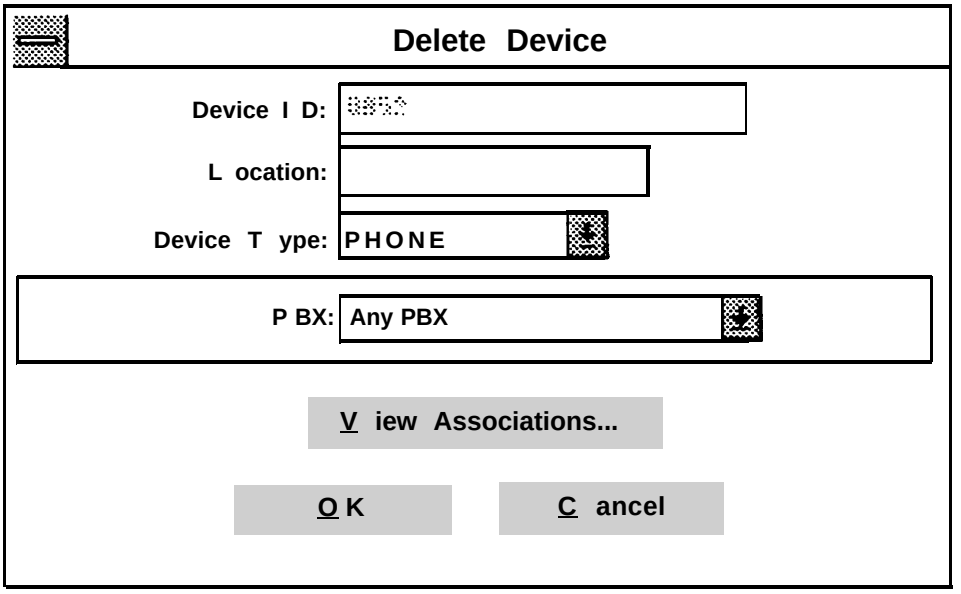
Deleting a Device

Procedure

1. **Select the device you want to delete from the scrollable list on the "Device Information" dialog box.**

2. **Choose "D elete" on the "Device information" dialog box. The device information for the previously selected device is displayed.**

Figure 7-19
Delete Device Dialog Box



3. **Choose "V iew Associations" to see which Device Groups, Worktops, and users are associated with this Device. "V iew Associations" is a useful way of determining if it is possible to delete a Device.**

Important

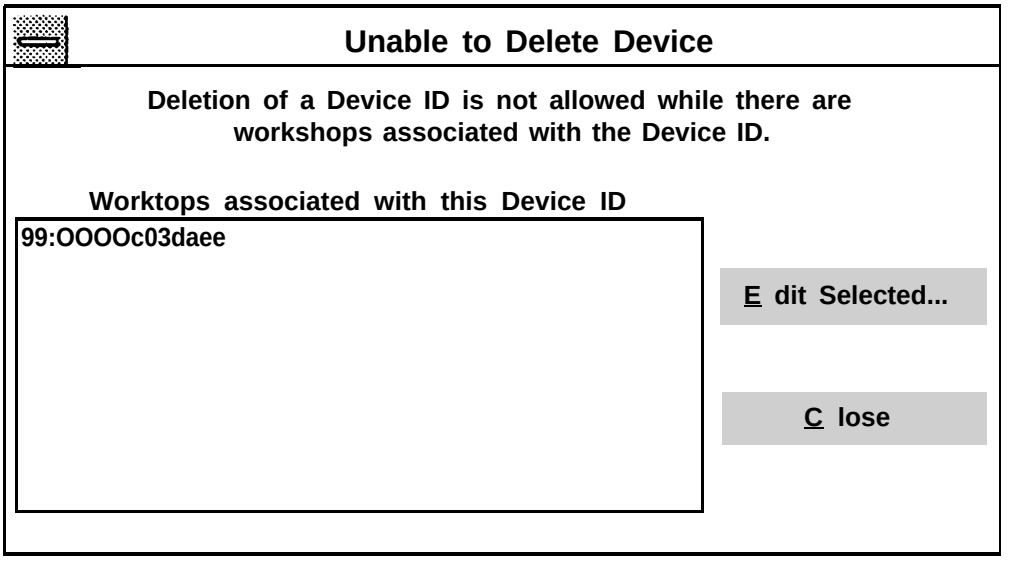
You cannot use the "View Associations" dialog box to modify any items. However, if the device you want to delete has worktops and users associated with it, you must readminister these components so that they will be associated with one or more devices (or deleted) instead. Failure to do so causes the system to display them and prevent your deleting the Device.

4. **Choose "O K" to record the deletion of the device in the Security Database, or choose "C ancel" to return to the**

"Device Information" dialog box without recording the deletion in the Security Database.

If either a user or a worktop is associated with this device, the system will not allow you to delete the device, but instead will respond by displaying an "Unable to Delete Device" dialog box, like the following:

Figure 7-20
Devices Linked to Worktop Warning



In this example, one Worktop is associated with this Device ID. From this dialog box, you can:

- Select the Worktop and choose "E dit Selected" in which case the appropriate "Edit Worktop" dialog box will be displayed. Use the drop-down list to select a different Primary Device ID for this device.

- Choose "C lose" and exit the "Unable to Delete Device" dialog box without making any changes to the Worktop associated with the Device ID.

5. Choose "O K" when you have made the necessary changes.

The system redisplays the "Device Information" dialog box with the device previously selected for deletion still highlighted.

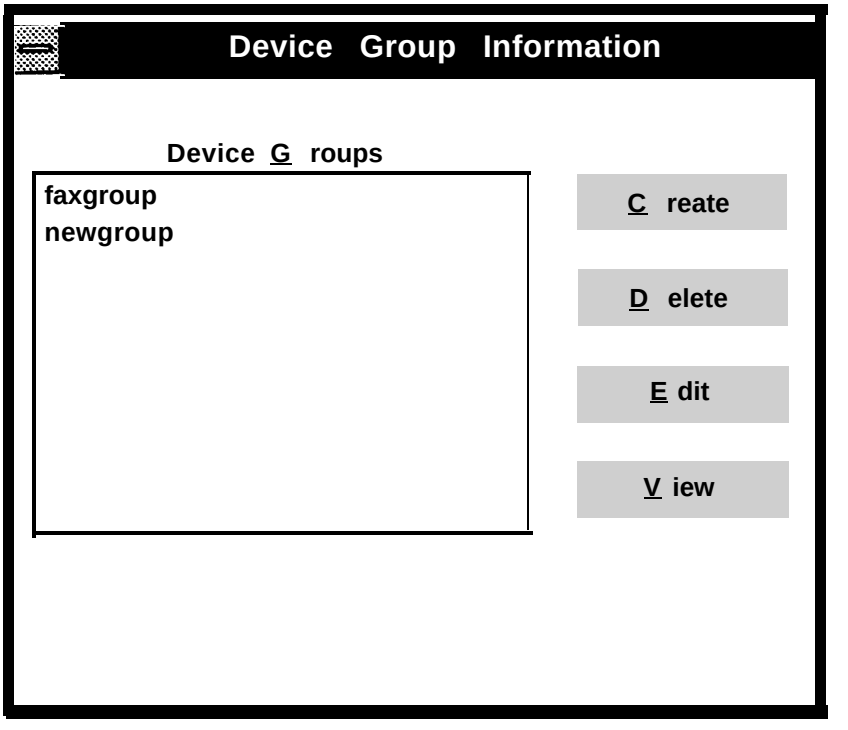
6. **Choose "D elete" to delete the selected device.**

Administering Device Groups

Procedure 23

1. **Select "Device G roups" on the "A dmin" menu to open the "Device Group Information" dialog box.**

Figure 7-21
Device Group Information Dialog Box



2. **Scroll or browse through the list of any administered Device Groups. Then either select an existing Device Group or create a new one.**

Note

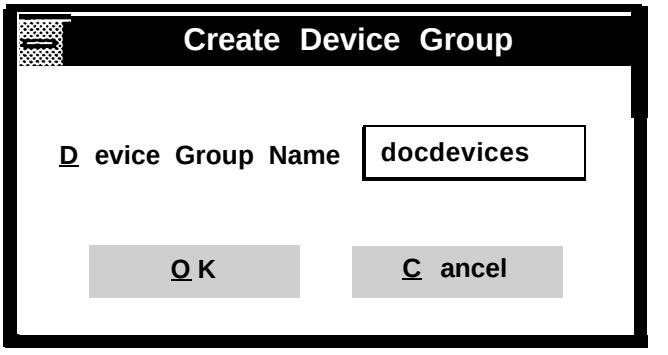
Device groups which users are not permitted to access are called "Exception Groups."

Creating a Device Group

Procedure

1. Choose "C reate" on the "Device Group Information" dialog box to open the "Create Device Group" dialog box.

Figure 7-22
Create Device Group Dialog Box



2. Enter the name for the new Device Group.

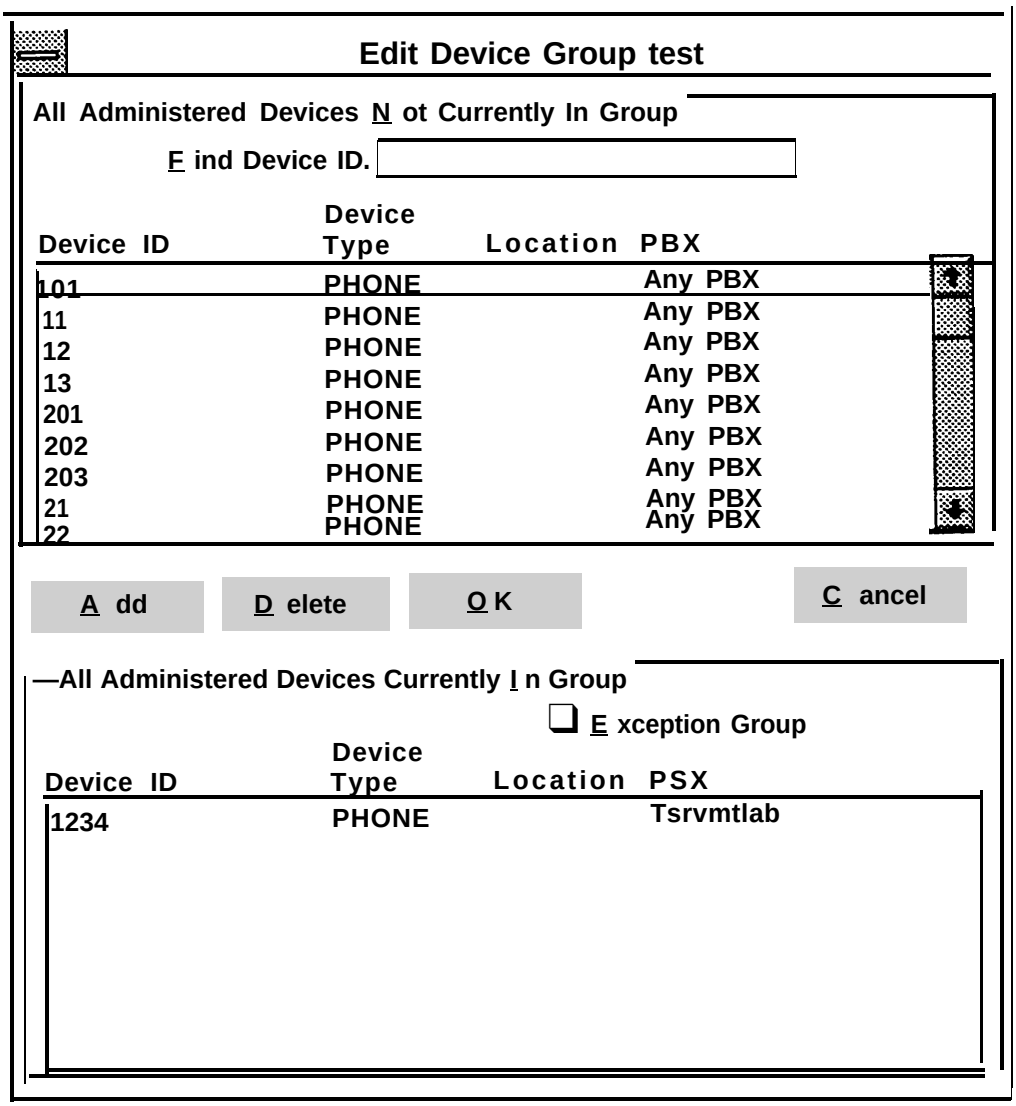
3. Choose "O K" to record the addition of the Device Group in the Security Database, or choose "C ancel" to return to the "Device Group Information" dialog box without recording the addition you specified on the screen in the Security Database.

Editing a Device Group

Procedure

1. Select a Device Group from the Device Groups listed on the "Device Group Information" dialog box.

Figure 7-23
Edit Device Group Dialog Box



As you enter digits into "Find Device ID", the top list box will scroll to display entries that correspond to the numbers you have entered.

The system displays a scroll box containing information about the devices in the Device Group, one per line. The field definitions are the same as those for the "Devices Not Currently In Group" box. Note also that the application enables the "Add" button when there is at least one device in the "Devices Not Currently In Group" list box.

2. **From the available choices list in the "Devices N ot Currently In Group" box, select one or more devices that you want to add to the previously selected Device group.**

To select multiple entries within the list, hold down the "Control" key as you make your selections with the mouse. To select several contiguous entries within the list, hold down the "Shift" key on your keyboard as you make your selections with the mouse.

3. **Choose "A dd" to move the selected device from "Devices N ot Currently In Group" to "Devices I n Group."**

4. **If you want you can make the "Devices I n Group" list an "Exception Group" list by checking the "Exception Group" box.**

   If you do this, you can prevent specific users from controlling the devices for the corresponding Device IDs in the specified "Devices Currently I n Group" list by properly administering the worktops and users in the system (see "Worktop Administration" and "User Administration" later in this chapter).

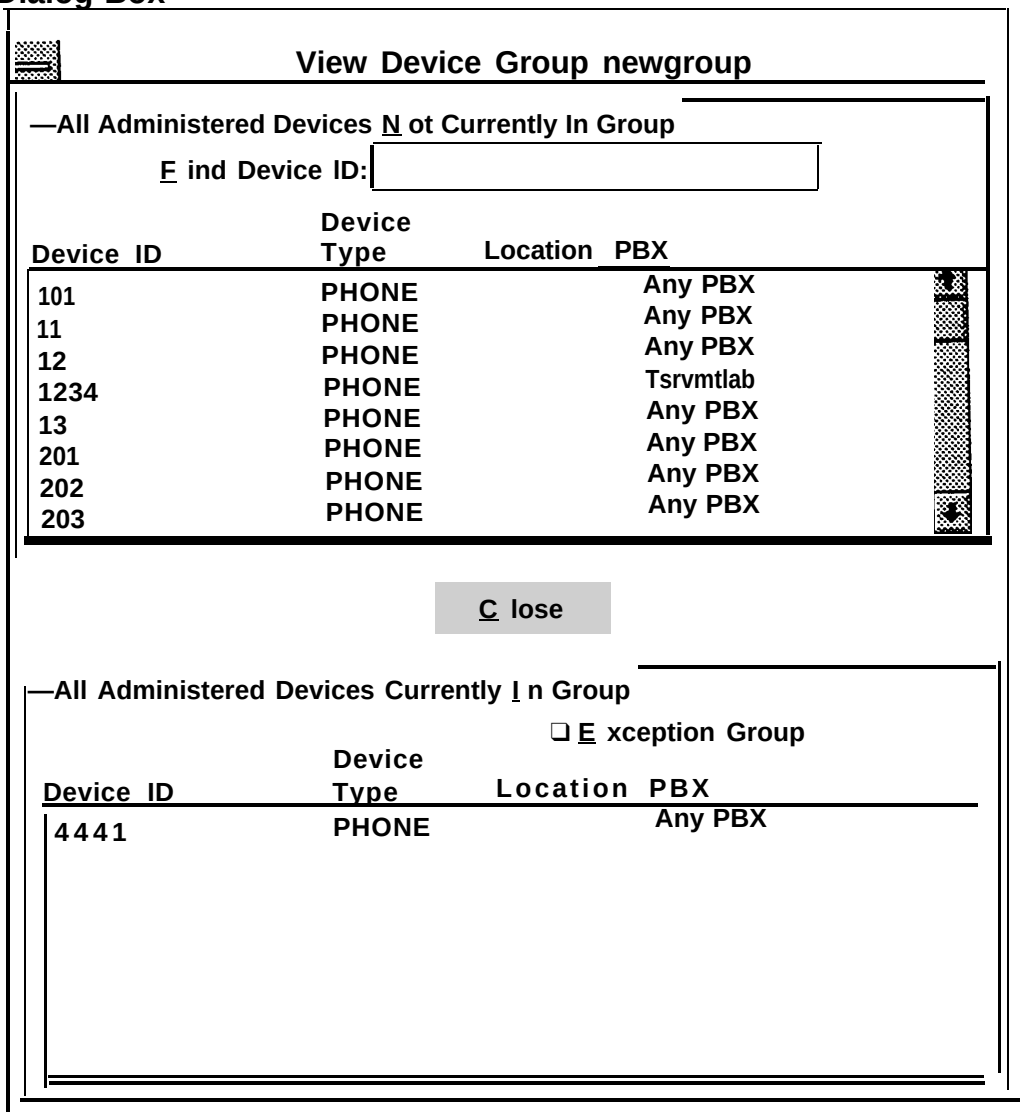
5. **Choose "O K" to record the changes in the Security Database or choose "C ancel" to return to the "Device Information Group" dialog box without recording any of the changes in the Security Database.**

Viewing a Device Group

1. **Select the desired Device Group on the "Device Group Information" dialog box.**

2. **Choose "V iew" to see more detailed information on the selected Device Group.**

Figure 7-24
View Device Group Dialog Box



Note

You cannot make any administration changes using this dialog box.

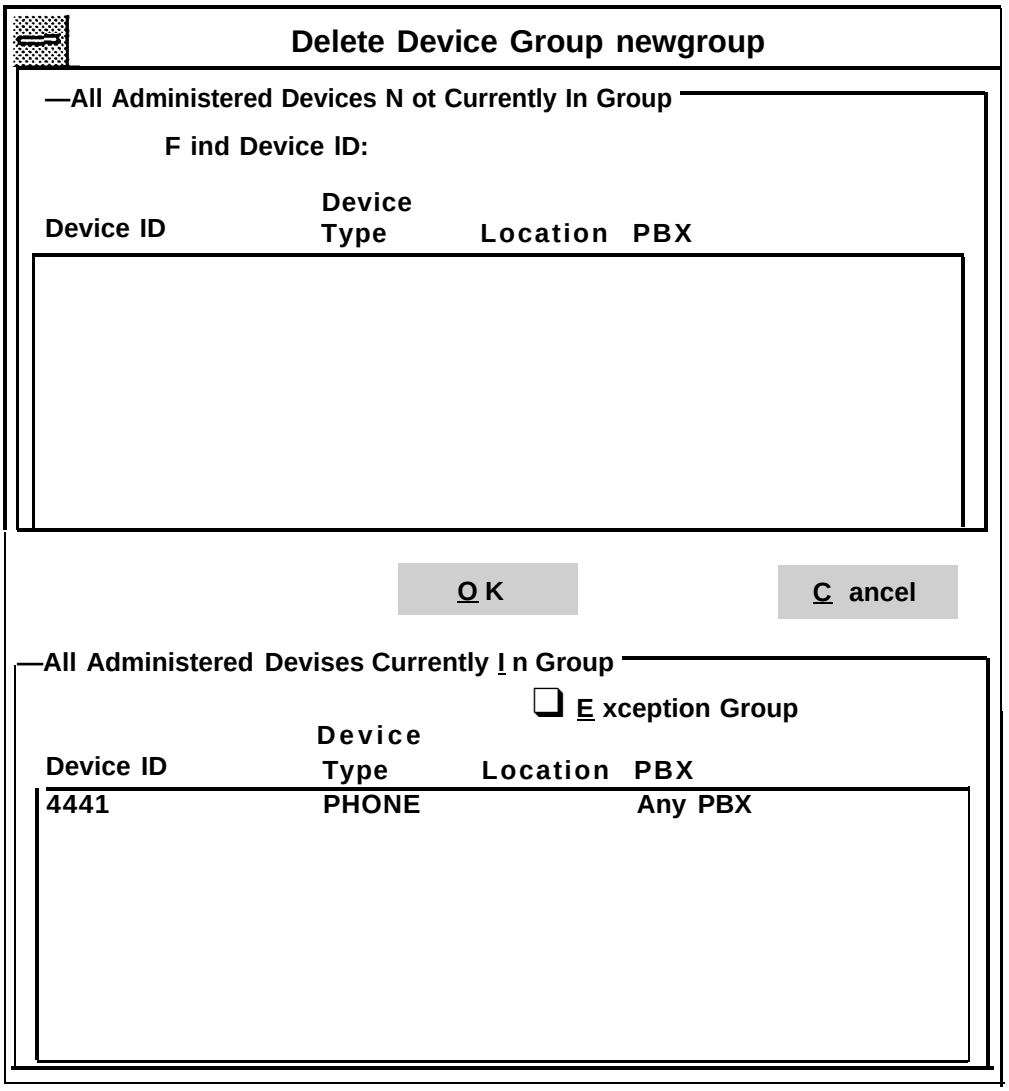
3. **Choose "Close" to return to the "Device Group Information" dialog box.**

Deleting a Device Group

Procedure

1. Select the desired Device Group on the "Device Group Information" dialog box.
2. Choose "D elete" to see more detailed information on the selected Device Group.

Figure 7-25
Delete Device Group Dialog Box



Note

The "Devices N ot Currently In Group" list is always empty on a delete.

3. **Choose "O K" to delete the Device Group definition in the Security Database.**

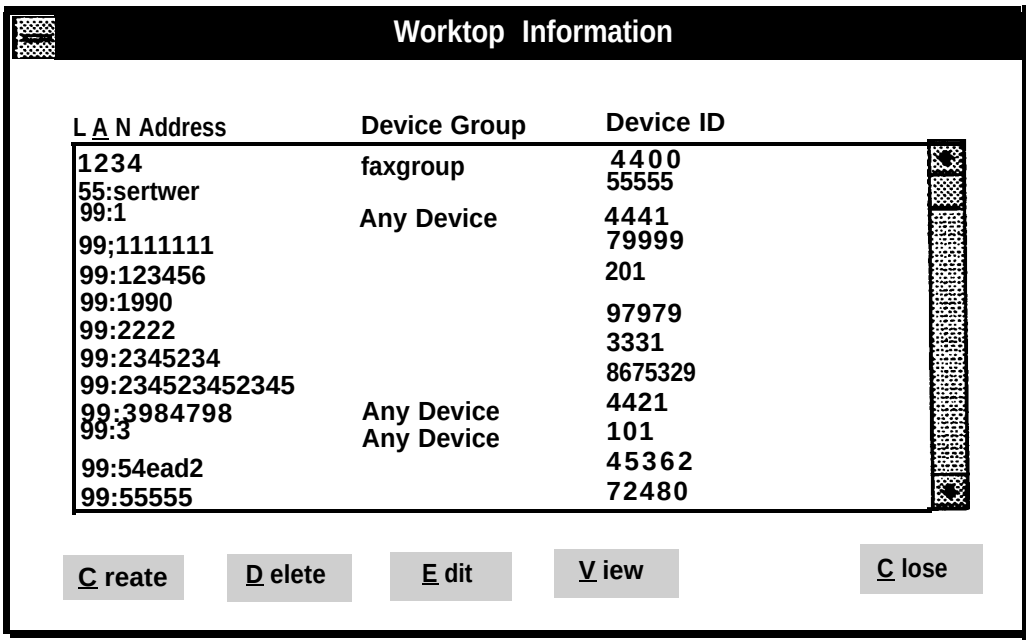
4. **Choose "C ancel" to return to the "Device Group Information" dialog box without deleting the Device Group from the Security Database.**

Administering Worktops

Procedure 23

1. **At the "A dmin" menu, select "Worktops" to open the "Worktop Information" dialog box.**

Figure 7-26
Worktop information Dialog Box



The fields are:

- **L A N Address.** The administered LAN address for the Worktop.
- **Device Group.** The group of secondary Devices for the Worktop.
- **Device ID.** The Primary Device at the Worktop; refers to the exact string that the PBX demands to be dialed to access that

Device. Refer to your vendor's PBX documentation for detailed information on the required string. If a Device ID is too long for the display, the complete ID will not appear on the screen. If this is the case, choose "E dit" or "V iew" to see the complete Device ID.

2. Scroll or browse through the list of any administered Worktops. Then either select an existing Worktop or create a new one.

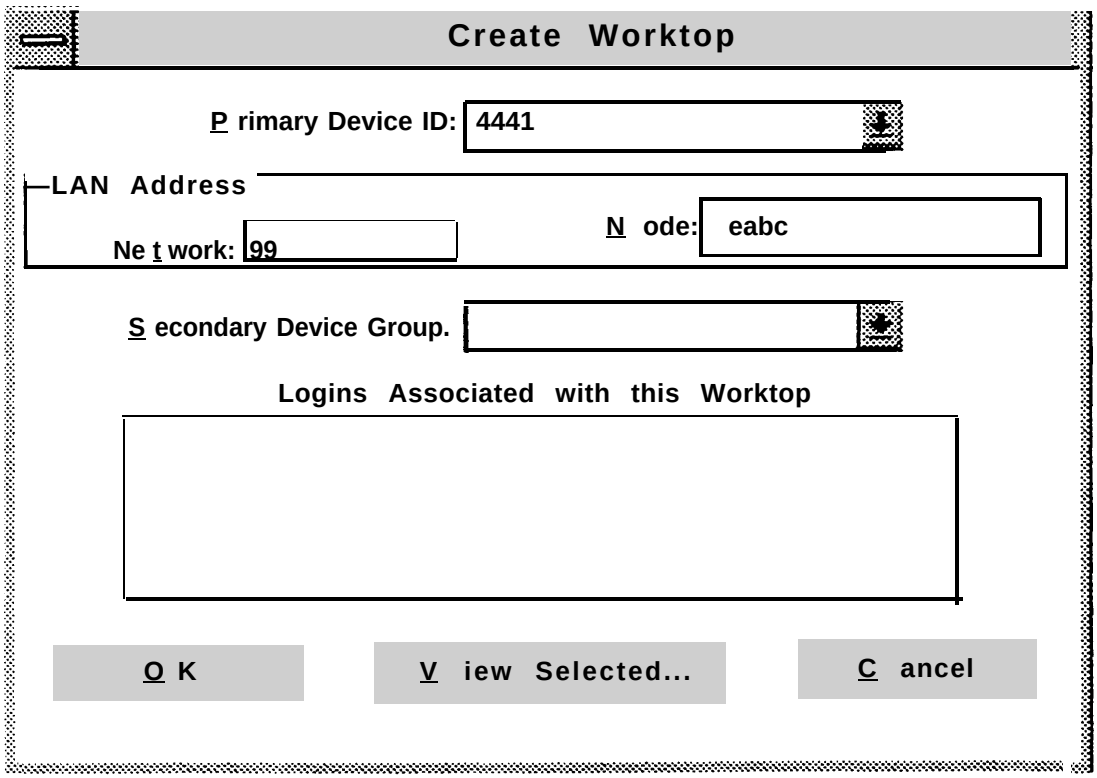
Note these important rules for administering Worktops:

- The identifier for the Worktop is the Device ID of the Primary Device.
- A Primary Device is referred to as "Primary" because it is typically the voice telephone at that Worktop.
- A Secondary Device is referred to as "Secondary" because its name is not that of the Worktop.

Creating a Worktop

1. Choose "C reate" on the "Worktop Information" dialog box to open the "Create Worktop" dialog box.

Figure 7-27
Create Worktop Dialog Box



The fields are:

- **Network** and **Node** are mandatory fields that constitute the NetWare network address. The Node is also known as the Media Access Code (MAC). Together, the network and node comprise a LAN Address that must be unique for each Worktop. Enter the LAN address of the Worktop you wish to create. **Network** defaults to zero.

- **LAN address** is the LAN address of the PC that you want to associate with the Primary Device ID at the user's home worktop. The LAN address becomes an important security check only if a user tries to access a telephone that is not on his or her Worktop.

Note

Certain configurations require the LAN address here for security checks. Other configurations require a unique entry, but do not actually use the field. In the latter case, you may enter unique fields such as

"#?#" followed by the extension number of the telephone at the Worktop or the Primary Device ID.

- **P rimary Device ID.** A mandatory drop-down list showing those Device IDs that are currently not administered as the primary Device at any Worktop. Select a primary Device ID for the Worktop you are creating.

- **S econdary Device Group.** An optional drop-down list showing all Device Groups. Typically, you select the Device Group containing the devices (fax, modem, PC, ACD, etc.) located at this Worktop, thus enabling the user associated with the Worktop to control these Devices.

- **V iew Selected.** Displays the "View" dialog box of whichever field is selected on the-screen. If 'Device ID" is selected, "View Device ID" for that device is displayed.

  For example, if you select an entry in the "Secondary Device Group" drop-down list and then choose "View Selected," the application displays a "View Device Group" dialog box containing information about the selected Device Group.

2. **Choose "O K" to record the addition of the Worktop in the Security Database, or choose "C ancel" to return to the "Device Group Information" dialog box without recording the addition you specified on the screen in the Security Database.**

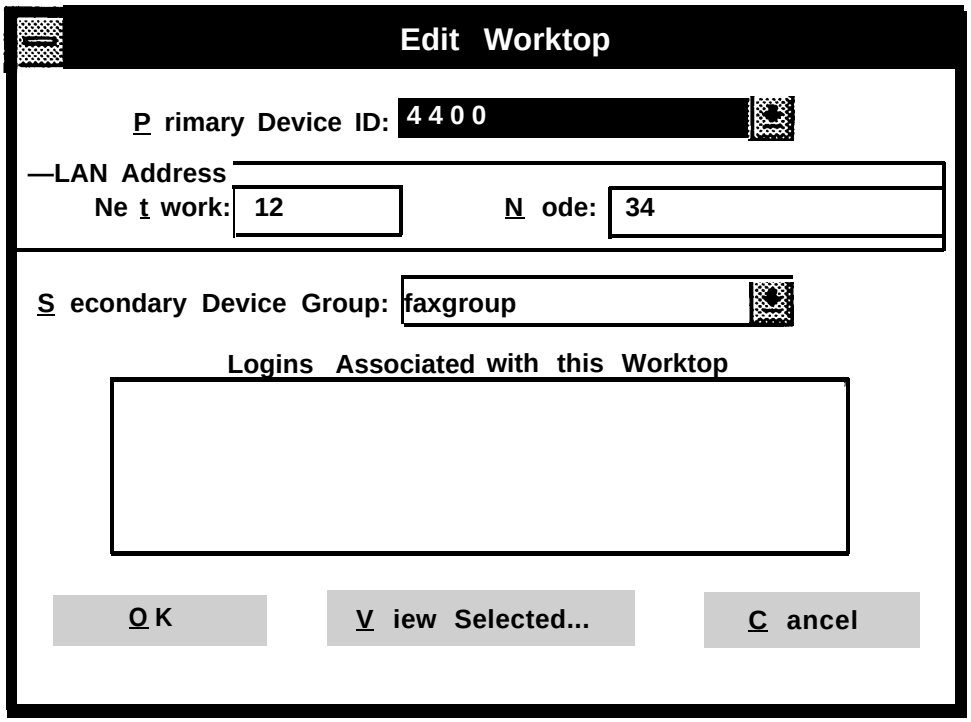
Editing Worktop Information

Procedure 23

1. **Select the Worktop you want to edit from the list on the "Worktop Information" dialog box.**

2. **Choose "E dit" on the "Worktop Information" dialog box to open the "Edit Worktop" diaglog box.**

Figure 7-28
Edit Worktop Dialog Box



3. **Make changes as needed to one or more of the following fields: "Primary Device ID," "Network," "Node," and/or "Secondary Device Group."**

   Both the "Primary Device ID" and "Secondary Device Group" fields are drop-down lists that show additional items.

4. **From the "Edit Worktop" dialog box, choose "OK" to record the editing of the Worktop information in the Security Database, or choose "Cancel" to return to the "Worktop Information" dialog box without recording in the Security Database the changes you specified on the screens.**

Viewing Worktop Information

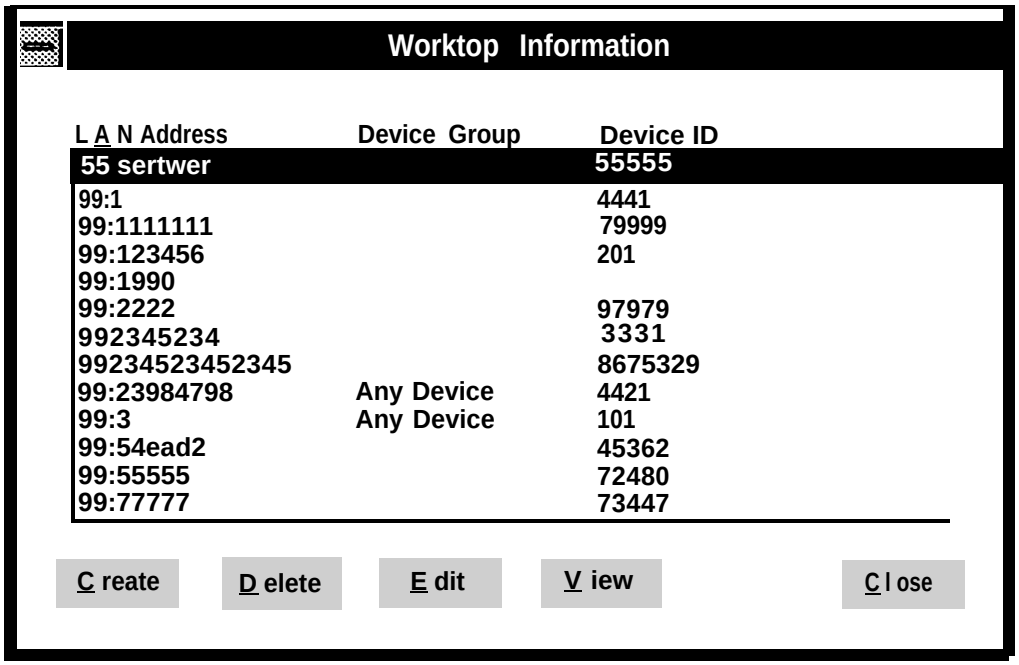
Note

You cannot make any administration changes using this dialog box.

Procedure 2 3

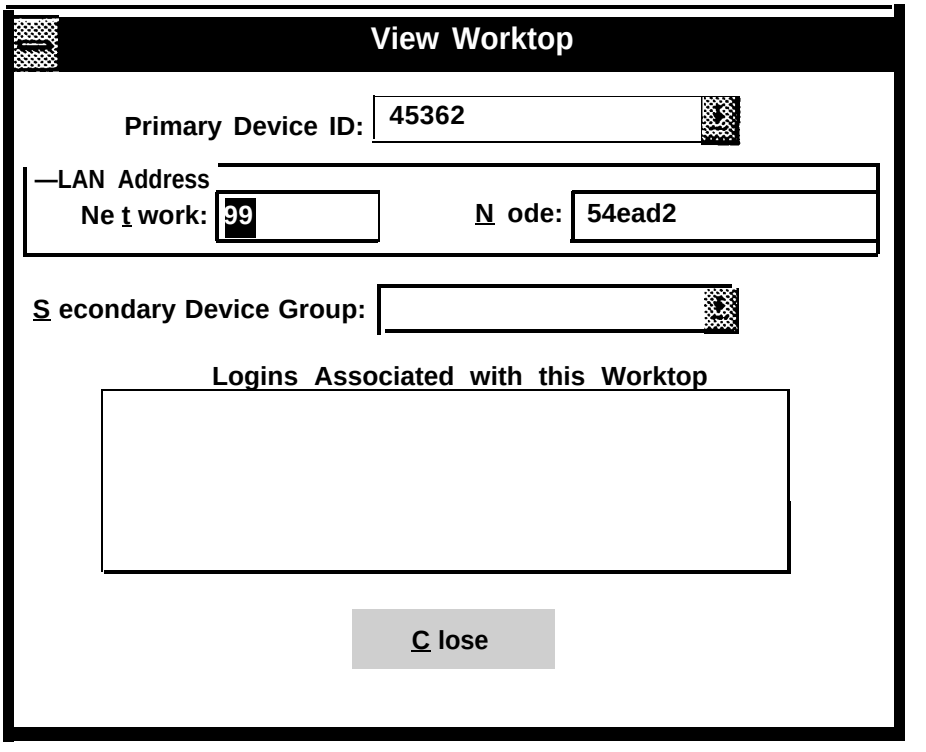
1. **Select the desired Worktop on the “Worktop Information” dialog box.**

Figure 7-29
Worktop Information Dialog Box



2. **The system displays the “View Worktop” dialog box.**

Figure 7-30
View Worktop Dialog Box



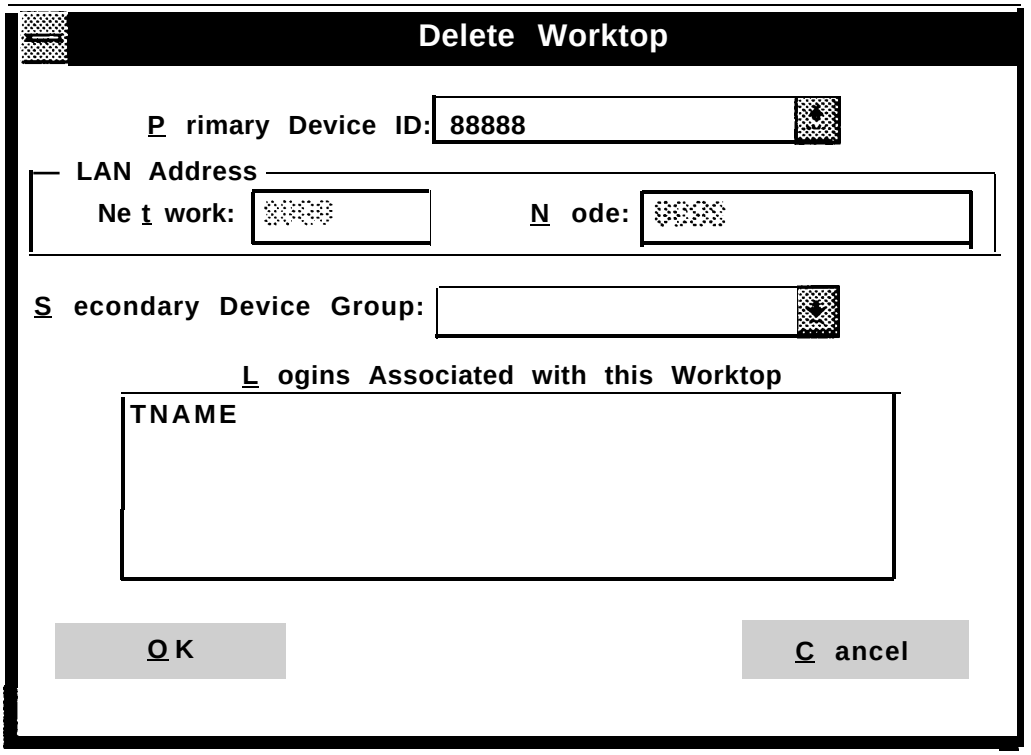
3. Choose "Close" to return to the "Worktop Information" dialog box.

Deleting Worktop Information

Procedure 23

1. Select the Worktop you want to delete from the "Worktop Information" dialog box.
2. Choose "Delete" to open the "Delete Worktop" dialog box.

Figure 7-31
Delete Worktop Dialog Box

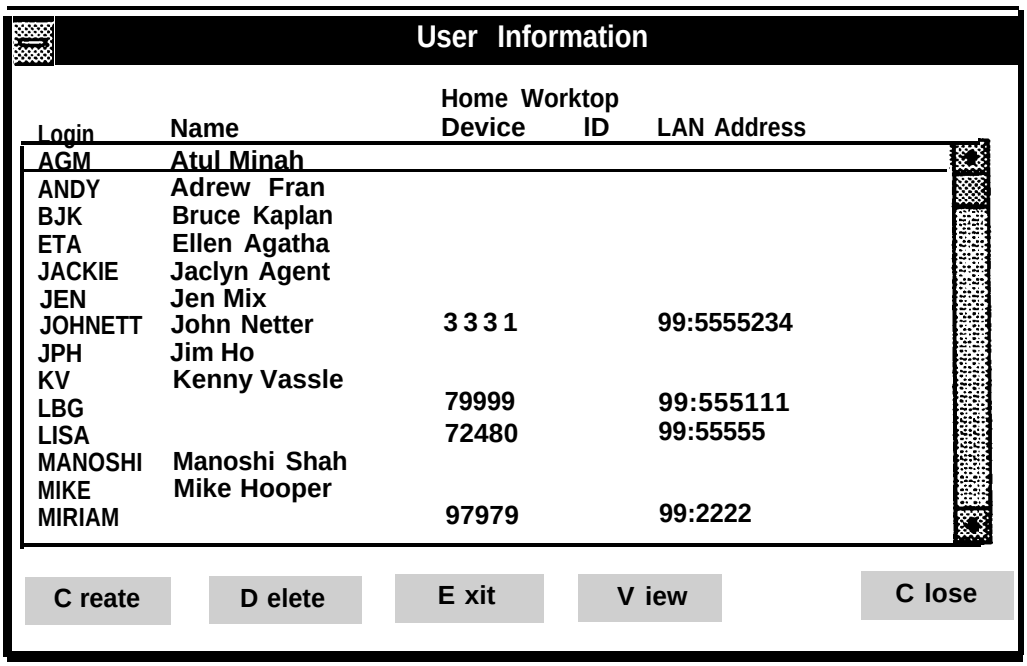


3. Choose "OK" to delete the desired Worktop, or choose "Cancel"

Procedure 23

Select "Users" on the "A dmin" menu to open the "User Information" dialog box.

Figure 7-32
User Information Dialog Box



The fields are:

- **Login** is a mandatory field that contains the user's NetWare login name.
- **Name** is the optional field that contains the administered user name.
- **Home Worktop Device ID** is an optional field that contains the string that the PBX demands to be dialed in order to access that particular device. Refer to your vendor's PBX documentation for detailed information on the required string.
- **LAN Address** is an optional field that contains the administered LAN address of the user's home worktop.

2. Scroll or browse through the list of any administered users. Then, either select an existing user or create a new one.

Suggestion

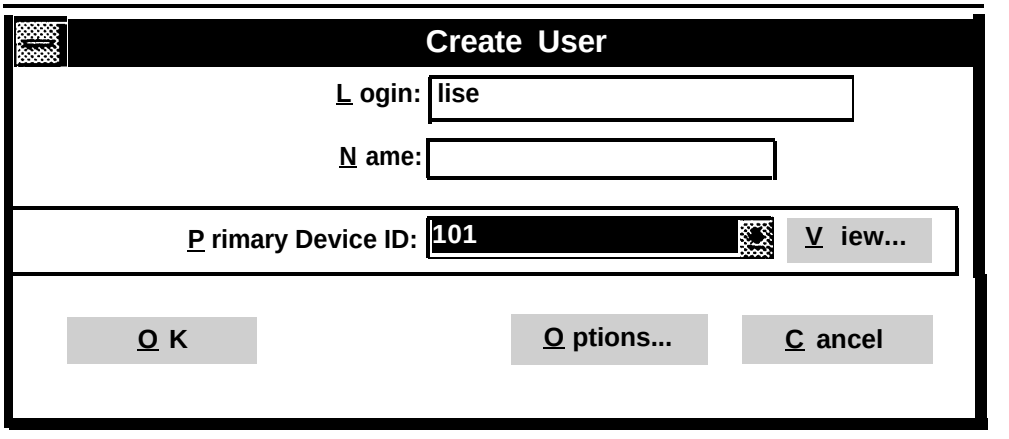
If the contents of a field are too long for the display, choose "E dit" or "V iew" to see the complete field contents.

Creating a User

Procedure

1. Select "Users" in the "Admin" menu to open the "User Information" dialog box.

Figure 7-33
Create User Dialog Box



The fields are:

- **L ogin** is a mandatory field that contains the user's NetWare login name.
- **N ame** is an optional field where you can enter a full user name.
- **P rimary Device ID** is an optional drop-down list showing those devices administered as the primary device ID at all worktops. Select a home worktop for the user from this list. Multiple users may share the same home worktop. A blank entry in the drop down list allows you to specify that the user does not have a home Worktop.

2. Enter the user's login name.

3. **Select the user's Primary Device ID from the drop-down list of administered IDs, and then either:**

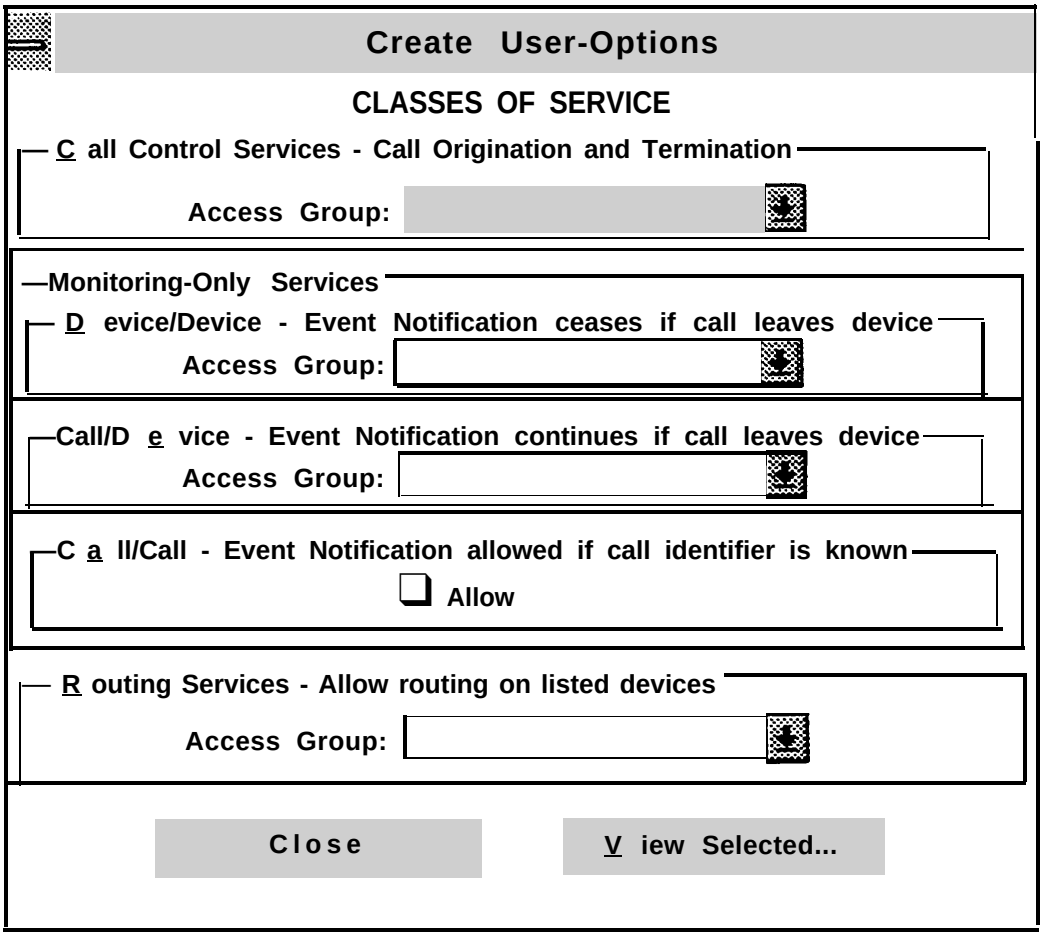
   ♦ Choose "V iew" for additional information on the selected Device, or

   ♦ Choose "C lose" to return to the "Create User" dialog box

4. **If this user is to be administered for "Classes of Service," continue with Step 5. Otherwise, go to Step 7.**

5. **Choose "Op t ions" if you wish to administer Classes of Service for this user.**

Figure 7-34
Create User - Options Dialog Box



The fields are:

♦ **Classes of Service** contains the following options. Each option uses identical single-selection drop-down lists containing all administered Device Groups.

Remember that with Classes of Service options, Device/Device Access Group and Call Control Access Group permissions are used in addition to a user's permissions on Devices at the Home Worktop via the Primary Device ID and the Secondary Device Group.

♦ Call Control Services

♦ Call Control Access Group

Select a Device Group from the drop-down list to give the user permission to execute these CSTA operations on the Devices in the Device Group. A user may have at most one Device list associated with these Classes of Service fields. A blank entry in the drop-down list allows you to specify that the user does not have these permissions for any Device Group.

♦ Monitoring-Only Services

♦ Device/Device Access Group

Select a Device Group from the drop-down list to give the user permission to execute these CSTA operations on the Devices in the Device Group. A user may have at most one Device list associated with these Classes of Service fields. A blank entry in the drop-down list allows you to specify that the user does not have these permissions for any Device Group.

♦ Call/Device Access Group

Select a Device Group from the drop-down list to give the user permission to execute these CSTA operations on the Devices in the Device Group. A user may have at most one Device list associated with these Classes of Service fields. A blank entry in the drop-down list allows you to specify that the user does not have these permissions for any Device Group.

- **Call/Call Monitoring**

  This field is a check box. Check this box if the user is to have CSTA Call/Call Monitoring permissions.

♦ **Routing Services**

- **Routing Access Group**

  Telephony Computing Service can be used by applications to provide the switch with call routing information on a call-by-call basis. These services allow them to determine the destination of a call within the switching domain based on external criteria within the computing domain.

  Select a Device Group from the drop-down list to give the user permission to execute these CSTA operations on the Devices in the Device Group. A user may have at most one Device list associated with these Classes of Service fields. A blank entry in the drop-down list allows you to specify that the user does not have these permissions for any Device Group.

♦ **View Selected** displays any drop-down list selection. Press this button when you have made a drop-down list selection to open a view of only the dialog box describing the selection, or see the contents of that selection. For example, if you select an entry in the "Primary Device ID" drop down list, and then choose "View Selected," the application opens a "View Device" dialog box containing information about the selected device. If a Device Group entry is currently selected, the application opens a "View Device Group" dialog box.

6. **Select one or more of the desired Classes of Service (Call Control Services, Monitoring-only Services, and/or Routing Services).**

7. **(Optional) To see additional information for a drop-down list item, choose "V iew Selected."**

8. **Choose "C lose" to return to the "Create User" dialog box.**

9. Choose "O K" to add the desired user, or choose "C ancel."

Note

Remember the following attributes of the Classes of Service Options:

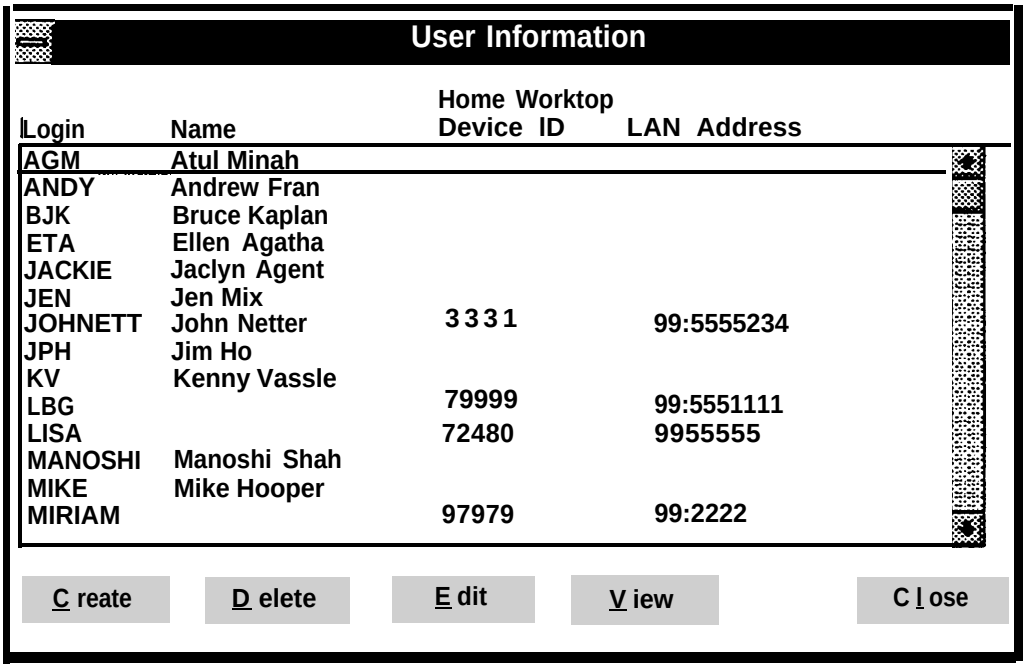
- Device/Device Monitoring and Call Control Access permissions are in addition to a user's permissions on devices at the Home Worktop via the Primary Device ID and the Secondary Device Group.
- In some cases, such as in a "Boss/Secretary" scenario, it would be more practical to place those additional devices that the secretary is to control and/or monitor in his/her Secondary Device Group, rather than administer the Classes of Service attributes.

Editing User Information

Procedure

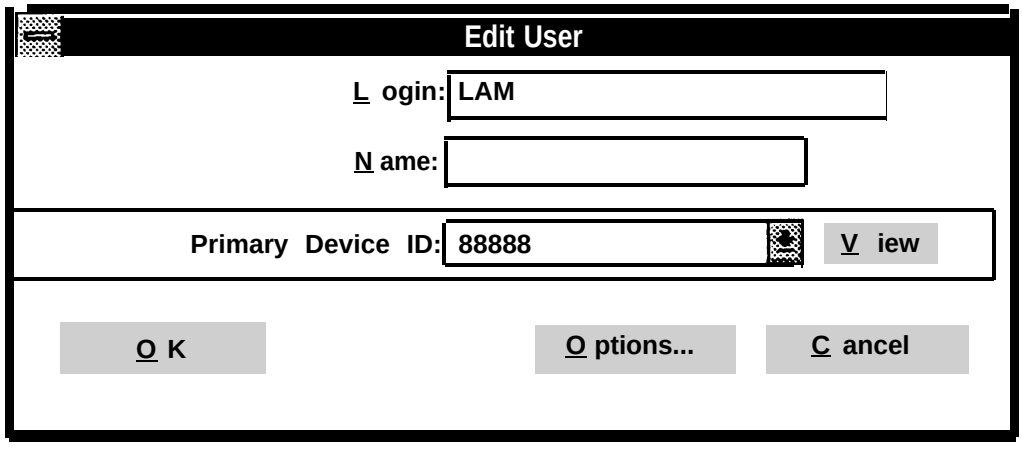
1. Select User from the "User Information" dialog box.

Figure 7-35
User Information Dialog Box



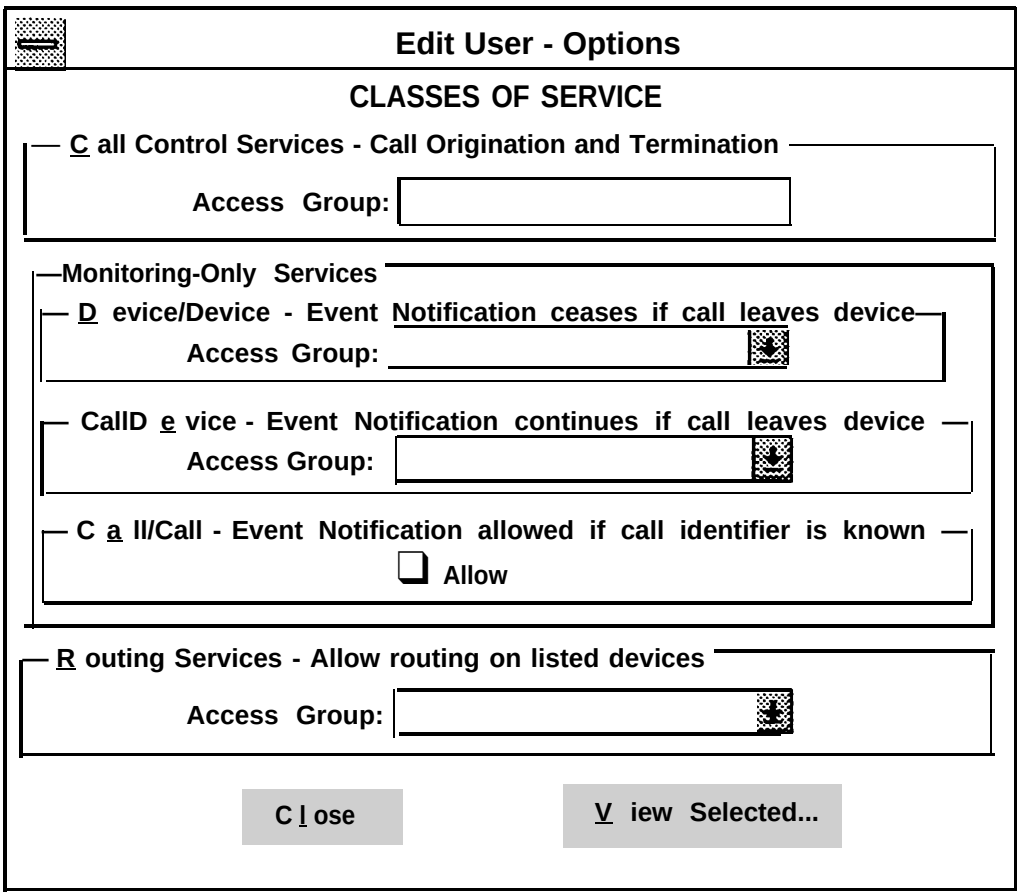
2. Choose "E dit" to open the "Edit User" dialog box.

Figure 7-36
Edit User Dialog Box



3. Choose “Options” to display the “Edit User - Options" dialog box and see if this user has been administered for Classes of Service.

Figure 7-37
Edit User - Options Dialog Box



4. Make any desired changes on the "Edit User-Options" dialog box.

5. (Optional) Choose "V iew Selected" for additional information on one or more of the Classes of Service.

6. Choose "C lose" to return to the "Edit User" dialog box.

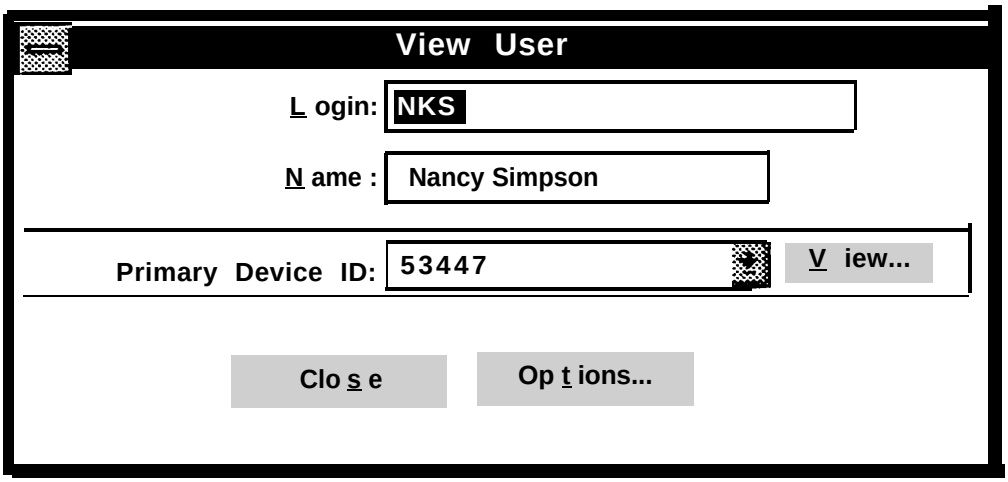
7. Choose "O K" to edit information for the desired user, or choose "C ancel" to exit the "Edit User" dialog without saving any changes.

Viewing User Information

Procedure 23

1. Select a user from the "User Information" dialog box and choose "V iew".

Figure 7-38
View User Dialog Box



2. To show additional device information, Choose "V iew" to bring up the "View Device" dialog box.

   2a. To show information about administered CTI Link Advertised Names, from the "View Device" dialog box, choose "V iew" to display the "View PBX dialog box. Then choose "Clo s e" to get back to the "View Device" dialog box.

3. Choose "Op t ions" to display the "View User - Options" dialog box. Then choose "Clo s e" to return to the "View User" dialog box.

   3a. To show the device's current groups, the LAN address of the Worktops associated with each device, and the login ID of the users associated with each device, choose "V iew Associations" to display the "Device Associations" dialog box. Then choose "C lose" to get back to the "View Device" dialog box and then choose "Clo s e" to return to the "View User" dialog box.

The "View User - Options" dialog box shows the Class of Service Access Groups that are assigned to devices that the user can control.

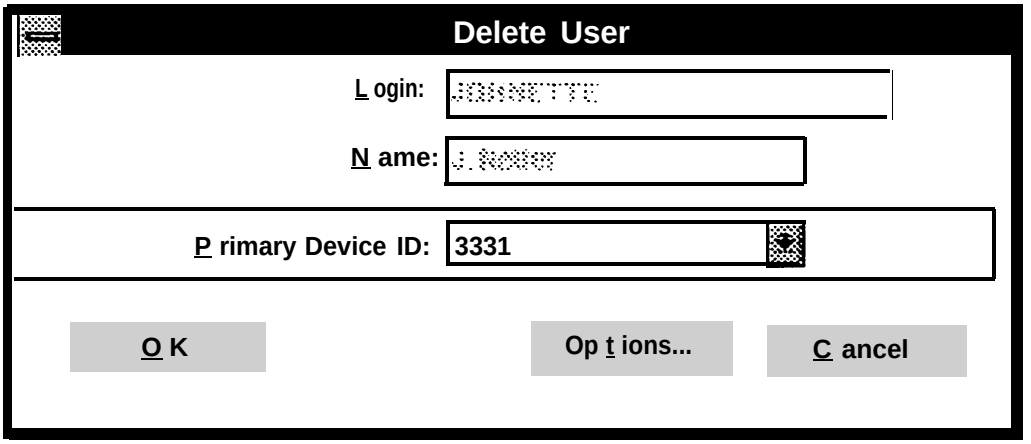
4. **Choose "Clo s e" to return to the "User Information" dialog box.**

Deleting User Information

Procedure

Select "U ser" from the "User Information" dialog box and choose "D elete."

Figure 7-39
Delete User Dialog Box



2. **To show the Class of Service Access Groups that are assigned to devices that the user can control, choose "Op t ions" to display the "Delete User-Options" dialog box. Then choose "C lose" to return to the "Delete User" dialog box.**

3. **Choose "O K" to delete user information, or choose "C ancel" to exit the "Delete User" dialog box without saving any changes.**

Administering Admin Access Groups

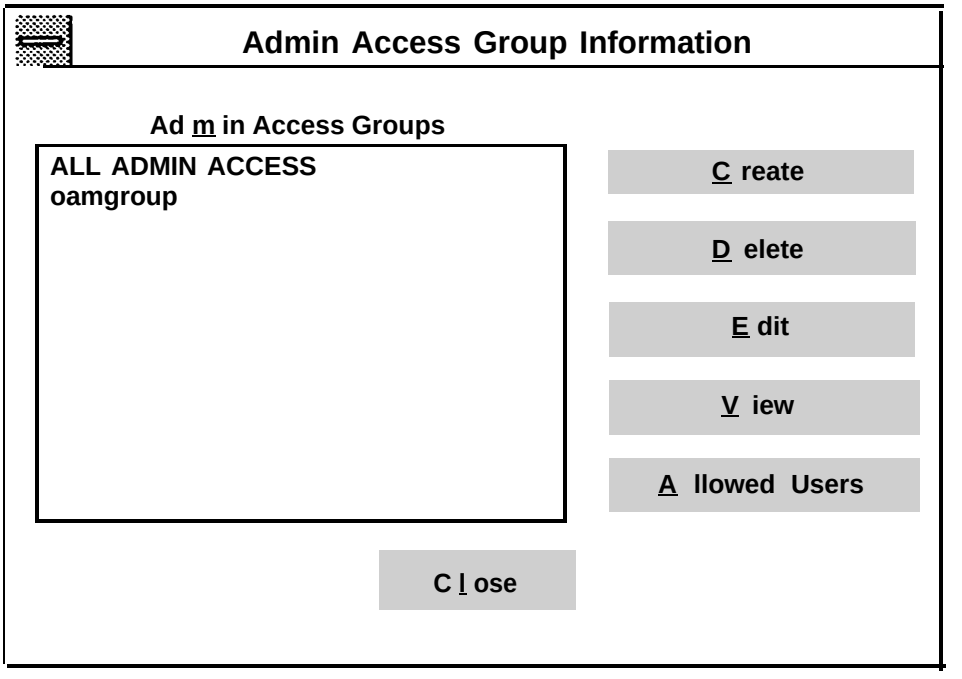
An Admin Access Group is a listing of Tservers, PBX Drivers, or PBX Simulator modules on which users can execute administrative services. While a PBX CTI Link carries CSTA messages from an application through

the Tserver and then through a driver to a PBX (switch), the Tserver Admin Link carries admin messages from the windows application to the PBX driver, a simulator, or a Tserver.

Procedure

1. **At the "A dmin" menu, select "Ad m in Access Groups" to open the "Admin Access Group Information" dialog box.**

Figure 7-40
Admin Access Group Information Dialog Box



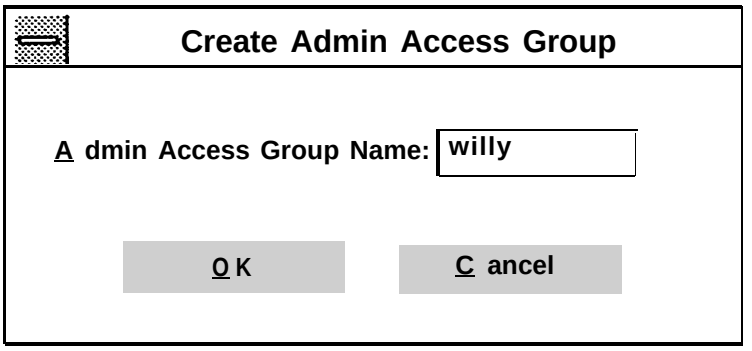
2. **Scroll or browse through the list of any Admin Access Groups. Then either choose an existing Admin Access Group or create a new one.**

Creating an Admin Access Group

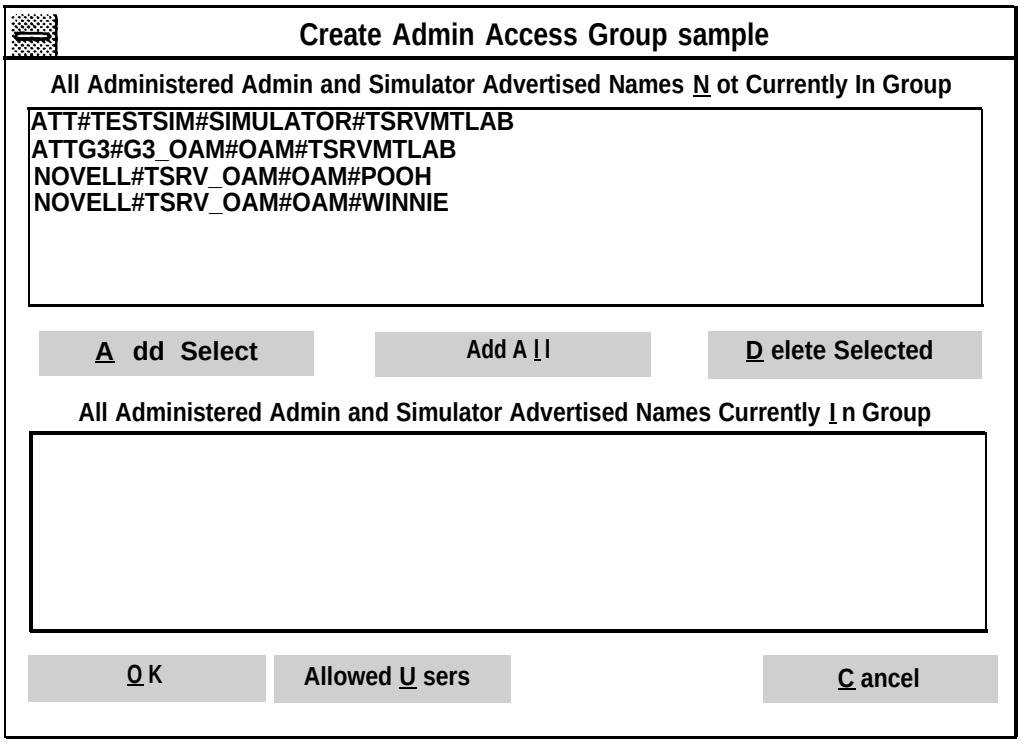
Procedure

1. **Choose "C reate" on the "Admin Access Group Information" dialog box.**

Figure 7-41
Create Admin Access Group Dialog Box



2. Enter the name for the new Admin Access Group and select "OK."



The name of the Admin Access Group appears in the title bar of the "Create Admin Access Group" dialog box. The "Create Admin Access Group" dialog box contains two list boxes:

- Admin Advertised Names Not in Group lists all Admin Link entries of type "Tserver Admin" and/or "TSDRV Admin" that

are not yet included in the selected Admin Access Group. Each of these corresponds to a system component that may be administered and maintained.

- Admin Advertised Names in Group lists all Admin Link entries of type "Tserver Admin" and/or "TSDRV Admin" that are currently included in the selected Admin Access Group. Each of these corresponds to a system component that maybe administered and maintained.

These components may be included in more than one Admin Access Group. However, only components on which Admin service or Simulator is available are listed.

3. **From the available choices in the "Admin Advertised Names...Not in Group" list box, choose one or more entries that you want to add to the previous selected Admin Access Link Group.**

   To select entries within the list, hold down the Control key as you make your selections with the mouse. To select several contiguous entries within the list, hold down the Shift key as you make your selections with the mouse.

4. **Use the appropriate "Add" button ("A dd Selected" or "Add A l l") to move selected items from the "Admin Advertised Names Not in Group" list box to the "Admin Advertised Names in Group" list box.**

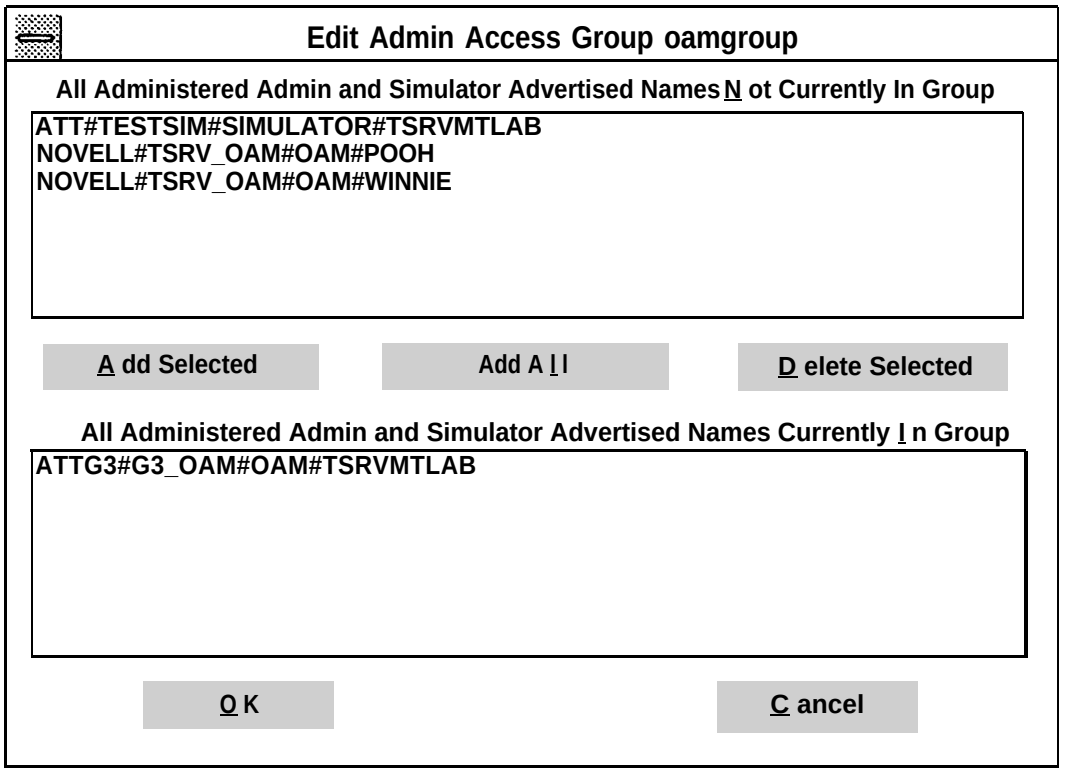
5. **Choose "O K to record the changes in the Security Database, or choose "C ancel" to return to the Admin Access Group dialog box without recording any of the changes you specified on the screen in the official definition of the Admin Access Group in the Security Database.**

Editing an Admin Access Group

Procedure 23

1. **Select "Admin Access Group" from the "Admin Access Group Information" dialog box and choose "E dit."**

Figure 7-42
Edit Admin Access Group Dialog Box



The "Edit Admin Access Group" dialog box contains two list boxes

- **All Administered Admin and Simulator Advertised Names Not Currently In Group.**

  Lists all Admin Link entries of type "Tserver Admin," "TSDRV Admin," and "Simulator" that are not yet included in the designated Admin Access Group. Each type corresponds to a system component that may be administered and maintained.

- **All Administered Admin and Simulator Advertised Names Currently In Group.**

  Lists all Admin Link entries of type "Tserver Admin," "TSDRV Admin," and "Simulator" that are currently included in the designated Admin Access Group. Each type corresponds to a system component that may be administered and maintained.

Note

These components may be included in more than one Admin Access Group. However, only components on which Admin service or Simulator is available are listed.

2. From the available choices in the "All Administered Admin and Simulator Advertised Names Not Currently In Group" box, choose one or more entries that you want to add to the previous selected Admin Access Link Group.

Note

To select entries within the list, hold down the Control key as you make your selections with the mouse. To select several contiguous entries within the list, hold down the Shift key on your keyboard as you make your selections with the mouse.

3. Use the appropriate "Add" button to move selected items from one list box to the other.

4. If you decide that you do not want to add one or more entries that you just moved in the previous step, select the unwanted entries in the "Admin Advertised Names in Group" list box and choose "Delete Selected." The entries are moved back to the "Admin Advertised Names Not in Group" list box.

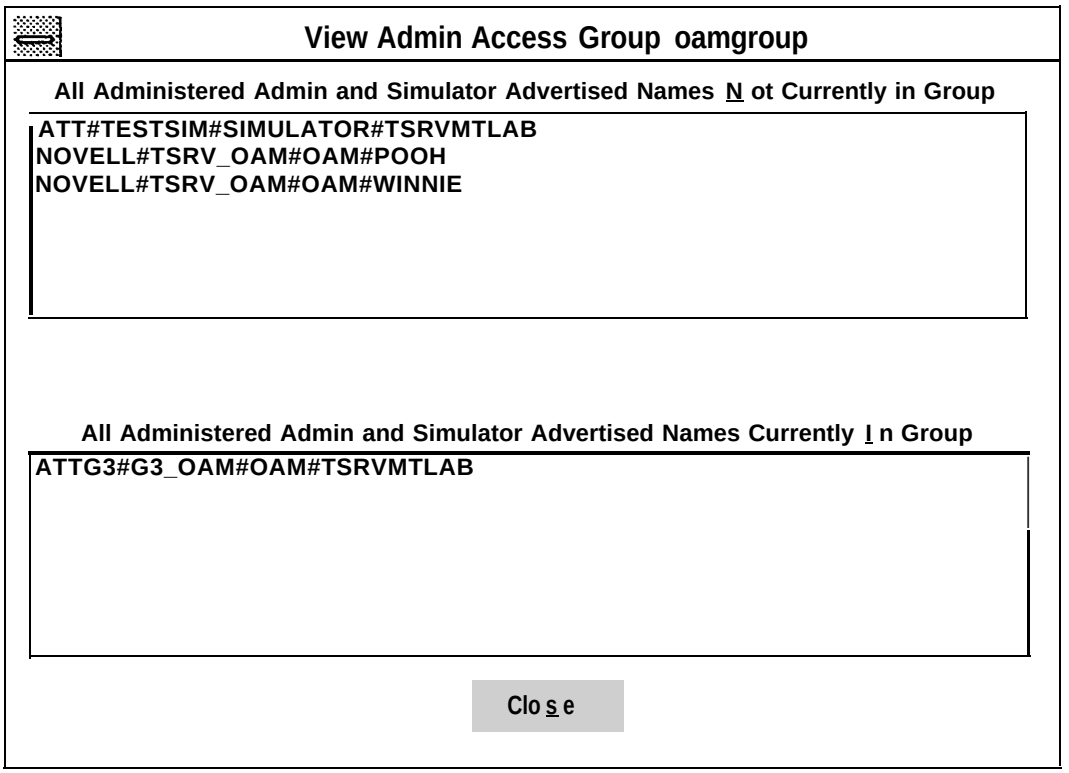
5. Choose "OK" to record the changes in the Security Database, or select "Cancel" to return to the "Admin Access Group" dialog box without recording any of the changes.

Viewing an Admin Access Group

Procedure 23

1. Select Admin Access Group from the "Admin Access Group Information" dialog box and choose "View."

Figure 7-43
View Admin Access Group Dialog Box



The "View Admin Access Group" dialog box contains two list boxes:

- **All Administered Admin and Simulator Advertised Names Not Currently in Group**

  Lists all Admin Link entries of type "Tserver Admin," "TSDRV Admin," or "Simulator" that are not yet included in the designated Admin Access Group. Each type corresponds to a system component that may be administered or maintained.

- **All Administered Admin and Simulator Advertised Names Currently In Group**

  Lists all Admin Link entries of type "Tserver Admin," "TSDRV Admin," or "Simulator" that are currently included in the designated Admin Access Group. Each type corresponds to a system component that may be administered or maintained.

2. **Choose "Clo s e" to return to the "Admin Access Group Information" dialog box.**

Deleting an Admin Access Group

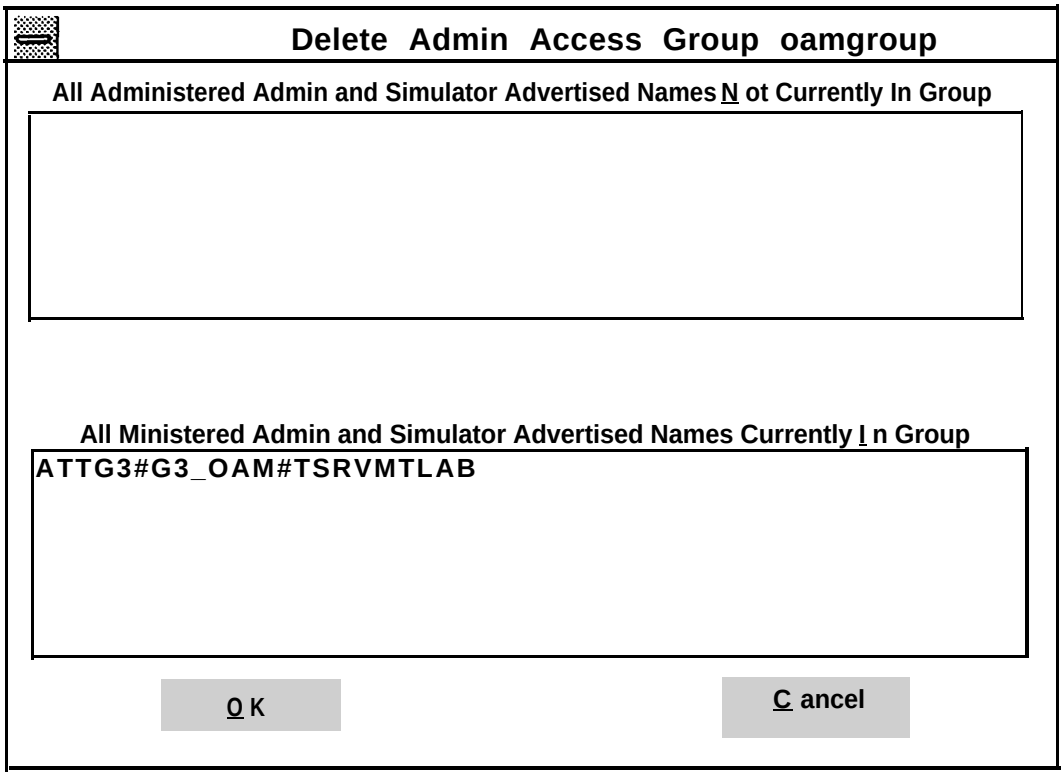
Note

You cannot make administrative changes to field contents from this dialog box.

Procedure

1. **Select Admin Access Group from the "Admin Access Group Information" dialog box and choose "D elete."**

Figure 7-44
Delete Admin Access Group Dialog Box

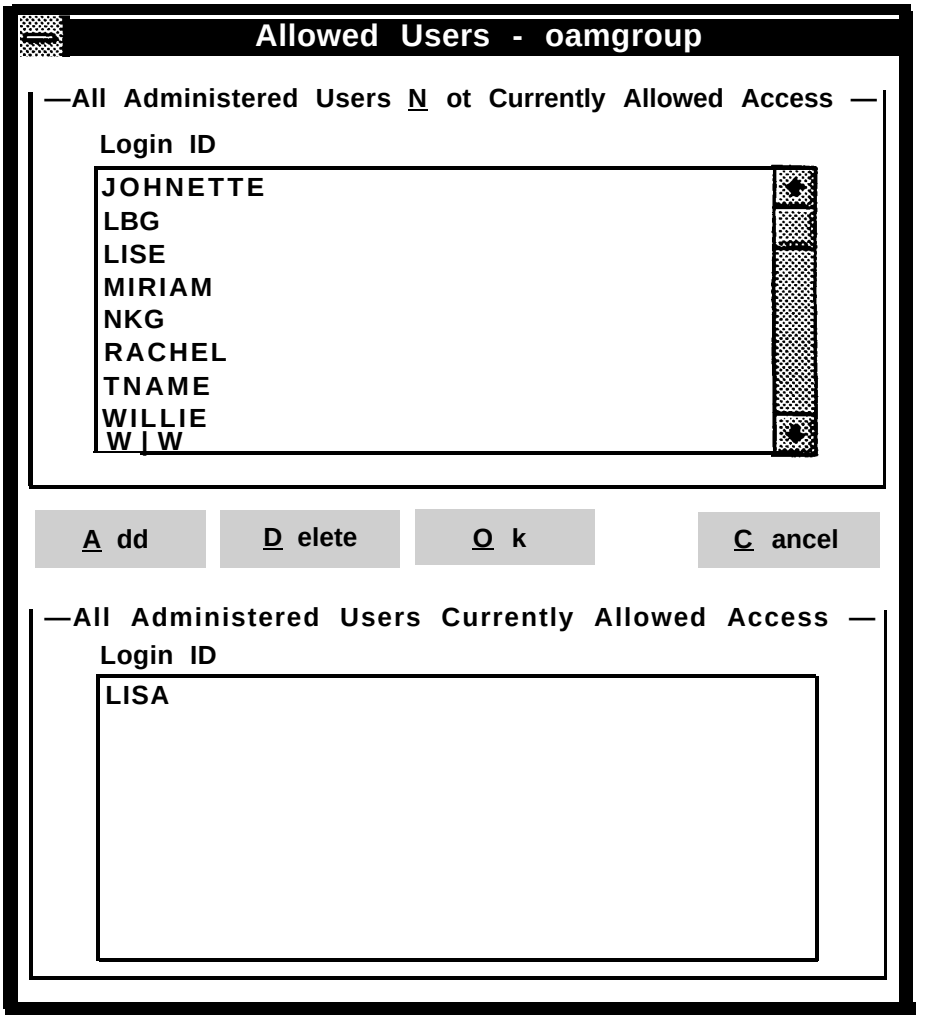


2. **Choose "O K" to delete the Admin Access Group definition from the Security Database or choose "C ancel" to return to the "Admin Access Group Information" dialog box without making any deletions.**

Procedure 23

1. Select an Admin Access Group from the "Admin Access Group Information" dialog box and choose "Allowed users."

Figure 7-45
Allowed Users Dialog Box



The "Allowed Users" dialog box contains two list boxes

♦ **All Administered Users Not Currently Allowed Access**

Lists the login IDs of all users who currently are not authorized to perform administration and maintenance on Admin Link

entries of type “Tserver Admin,” “TSDRV Admin,” and “Simulator.”

♦ **All Administered Users Currently Allowed Access**

Lists the login IDs of all users who currently are authorized to perform administration and maintenance on Admin Link entries of type “Tserver Admin,” “TSDRV Admin,” and Simulator.

2. **To add entries to the “All Administered Users Currently Allowed Access” list box, select entries from the “All Administered Users Not Currently Allowed Access” list box and choose “A dd.”**

The entries are moved from the latter list to the former list.

To select entries within the list, hold down the Control key as you make your selections with the mouse. To select several contiguous entries within the list hold down the Shift key on your keyboard as you make your selections with the mouse.

3. **To delete entries from the “Admin Advertised Names in Group” list box, select entries from the list box and choose “D elete.”**

The entries are moved back to the “Admin Advertised Names Not in Group” list box.

4. **Choose “O K” to record the changes in the Security Database, or “C ancel” to return to the Admin Access Group dialog box without recording any changes.**

Using Quick Add

The “Quick Add” dialog box enables you to create a user and a Primary Device ID from one dialog box. The screen is divided into two sections: “User Information” and “Device and Worktop Information.”

The fields are:

- **L ogin** is a mandatory field that shows the user's NetWare login name.

Note

The NetWare login is not added through this application. Normal NetWare login administration procedures must be used to create the actual NetWare login on the server.

- **N ame** is an optional field that shows the administered user Name.

- **P B X** is a mandatory drop-down list showing all administered PBXs. You associate the Device with the PBX that can monitor and control it. Select a PBX that contains CTI Links to the PBX where the Device is connected. You must ensure that your selection has an interface to the appropriate PBX. This is a single-selection list (that is, you select from one of the choices in the list).

- **P rimary Device ID** is a mandatory field that identifies the primary Device at the Worktop. Typically, this ID is the extension of the primary voice telephone at the Worktop.

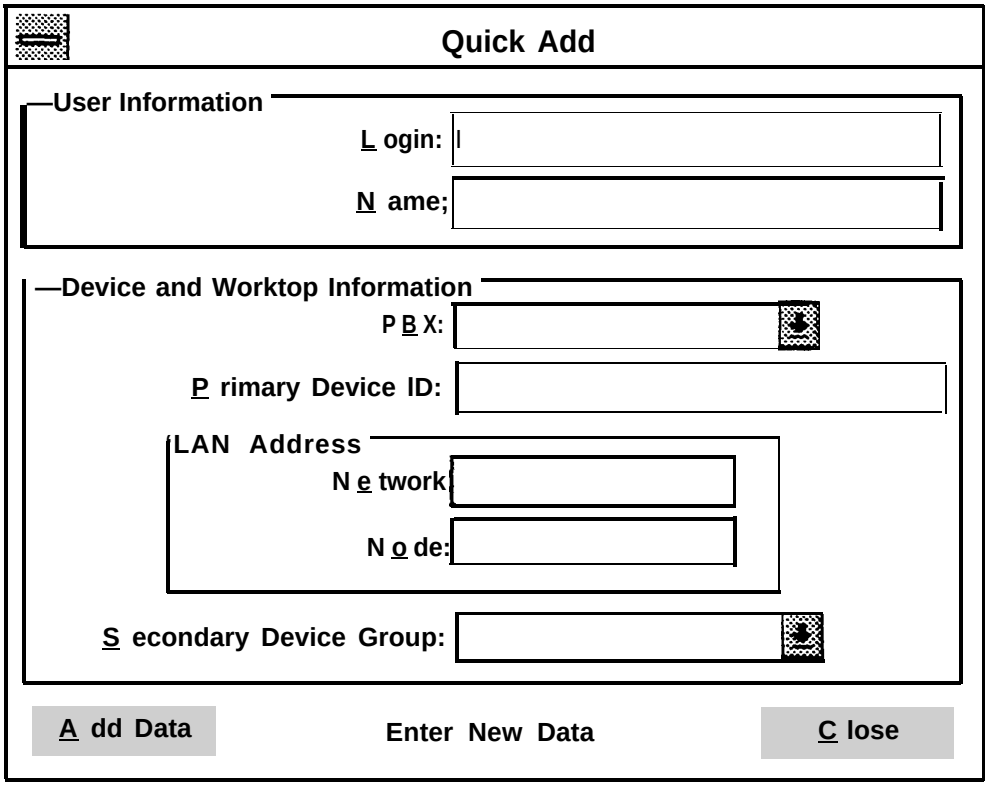
- **N etwork and N o de** are mandatory fields that make up a LAN Address that uniquely identifies the PC to associate with the selected Worktop.

- **S econdary Device Group** is an optional drop-down list showing all Secondary Device Groups in the system. You must have created a Secondary Device Group previously if the user is to be administered with a Secondary Device Group via this screen.

Procedure

1. **Select "Quick Add" from the "A dmin" menu to display the "Quick Add" dialog box.**

Figure 7-46
Quick Add Dialog Box



2 Enter the information for the user.

3. Choose "Add Data" to record the information for the user in the Security Database.

The system confirms that it is processing the new data by displaying the following messages in the following sequence:

- "Processing Data"
- "Processing Device"
- "Processing Worktop"
- "Processing User"
- "Command Successfully Completed"

If the system cannot process the data, it will notify you via an error message.

4. **Choose "C l ose" to close the "Quick Add" dialog box.**

M aint Menu

The Maint menu allows you to control and manipulate information about errors, trace internal Tserver messages, and collect internal Tserver information to help fine-tune Tserver performance.

The Maint menu has the following choices:

- E rror Log
  - S et
  - V iew
- Message T race
  - S et
  - V iew
- TSDRV Resources

You can access all maintenance commands via "M aint" on the Administrator window.

Setting Error log Parameters

By setting error log parameters, you choose which error messages get recorded in the error log, which appear on the screen at the server console,

and which generate alarms. The types of errors include: FATAL; ERROR WARNING; AUDIT TRAIL; CAUTION, AND DEBUG.

Note

You cannot modify the check boxes for logging of “FATAL” and “ERROR” messages to the Error Log File and for Alarm Generation. These destinations are always enabled.

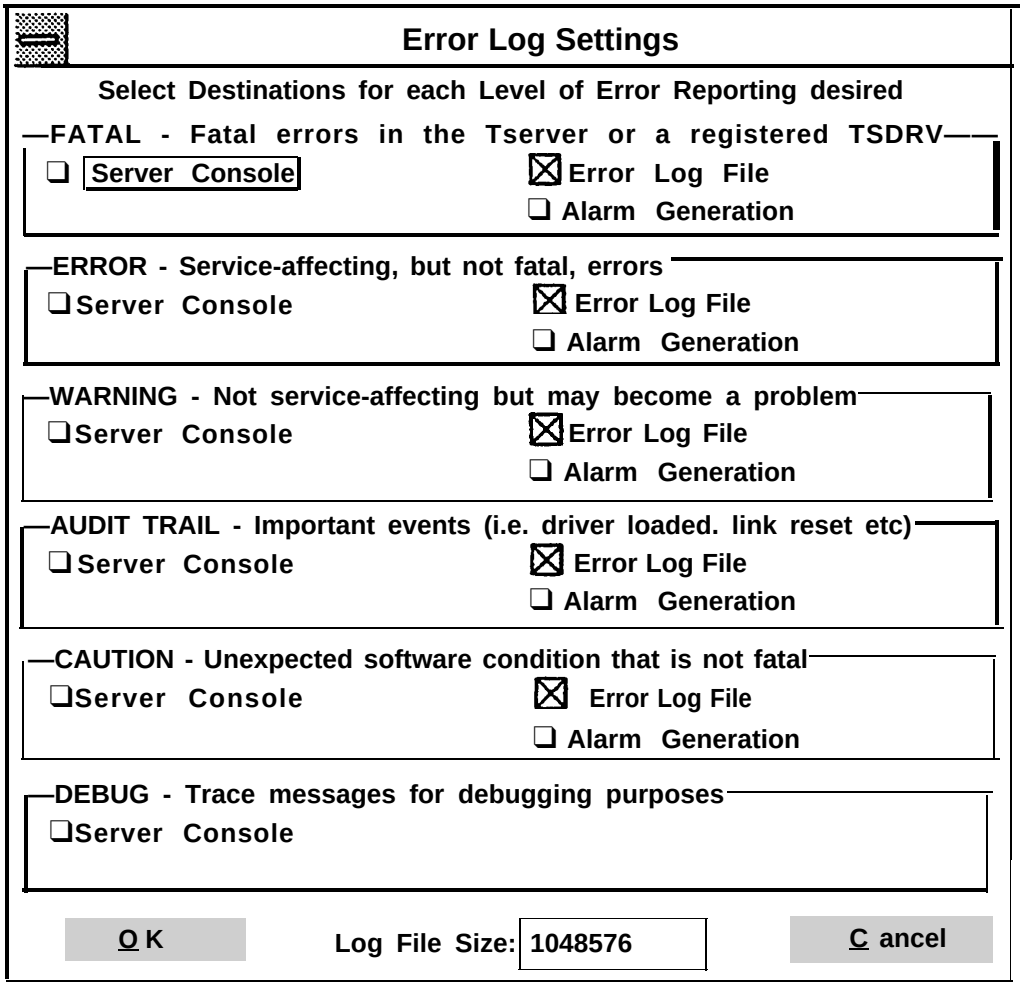
To set error log parameters, use the following procedure:

Procedure

1. **Select “Error Log/Set” on the “Maint” menu to display the “Error Log Settings” dialog box.**

2. **Check the check boxes as desired.**

Figure 7-47
Error Log Settings



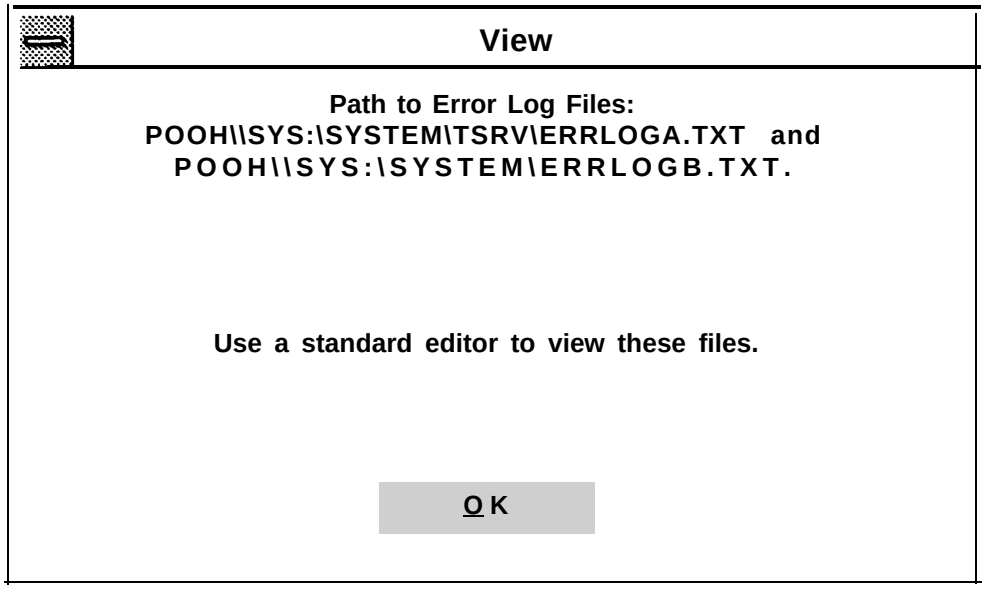
The error log is actually composed of two logs: A and B. Errors flow into log A. When it becomes full, the errors then go into log B. When B becomes full, A is erased and becomes ready to receive more errors. Consequently, you might have to look in both files to find a specific error.

If you find that the error log is not capturing enough information to be useful to you, you can enlarge it from its default of 1 megabyte so that it will hold more data. To increase the size of the error log, enter the number of bytes in the "Log File Size" box and press "OK."

Viewing Error Log Files

To see the path and filenames to access the error log files, choose "View" under "Error Log."

Figure 7-48
Error Log: View



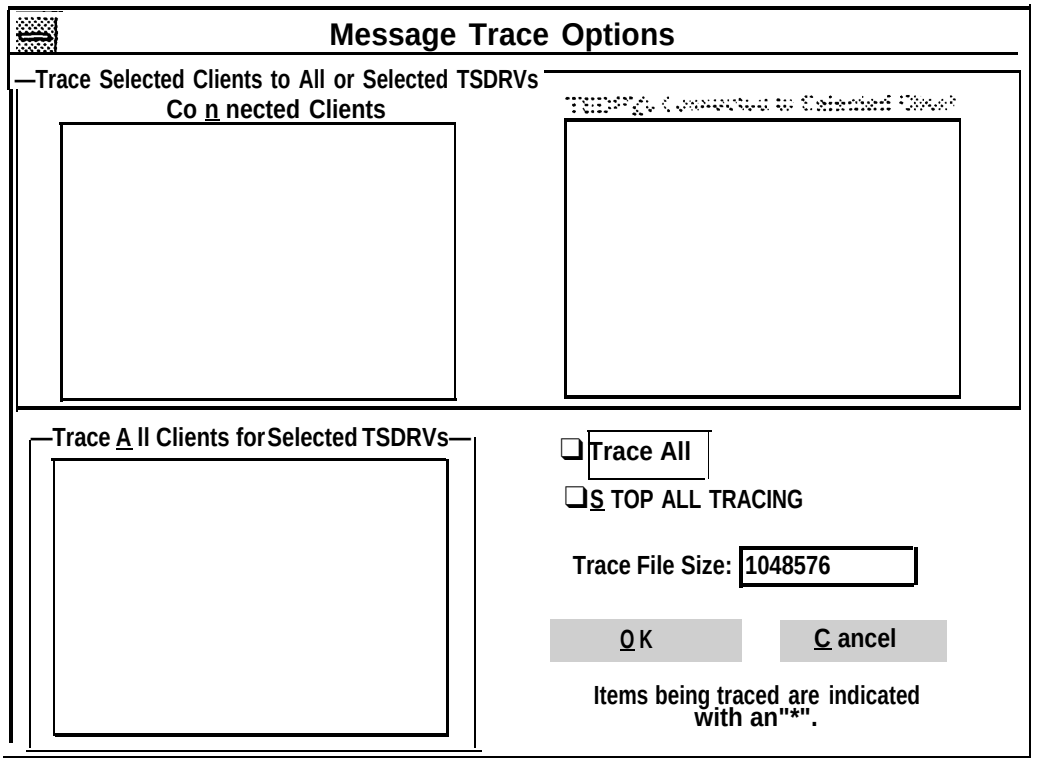
Message Tracing

Message tracing assists in troubleshooting by allowing you to see the flow of messages into and out of the Tserver for a client or set of clients or a driver or set of drivers.

Important

The following procedure is not recommended for use under normal conditions since it causes the system to operate more slowly. Set the message trace parameters only when debugging problems.

Figure 7-49
Message Trace Options



The options are:

- **Trace Selected Clients to All or Selected TSDRVs** traces only TSDRV messages that are done on behalf of the selected clients; only messages from the clients to the selected drivers are traced. To select a client for tracing, double-click on a client listed in the Connected Clients list. All TSDRVs to which the client has streams open are then listed in the **TSDRVs Connected to Selected Client** list. The default is to trace ALL TSDRVs. To deselect a TSDRV, double-click on the selected entry. The **TSDRVs Connected to Selected Client** list

is only populated when a Connected Client is selected that has been marked for tracing.

- **Trace All Clients for Selected TSDRVs** traces only the selected drivers for all client communications (including clients connecting after the tracing is enabled). To select a TSDRV for tracing, double-click on a listed TSDRV.

- **Trace All** traces all current and future registered TSDRVs and clients. When this option is enabled, the other trace options are disabled. To see this option enabled, you must redisplay the Message Trace options dialog box.

- **STOP ALL TRACING** discontinues tracing (after the O K button is pressed). Enabling this option disables all other options in the dialog box. Once tracing is stopped, all entries are cleared and must be reentered to turn on tracing again.

The message trace log is actually composed of two logs: A and B. Messages flow into log A. When it becomes full, the messages then go into log B. When B becomes full, A is erased and becomes ready to receive more messages. Consequently, you might have to look in both files to find a specific message.

If you find that the message log is not capturing enough information to be useful to you, you can enlarge it from its default of 1 megabyte so that it will hold more data. To increase the size of the message log, enter the number of bytes in the "Log File Size" box and choose "OK."

Initiating Message Tracing

1. **Select a client from the "Co n nected Clients" list.**
2. **All TSDRVs for that client will be displayed as selected.**

   To deselect a driver, double-click on it.
3. **Repeat Steps 1 and 2 for each client you are tracing.**
4. **Choose "O K" after you make your selection.**

5. **Select one or more drivers from the "Trace All Clients for Selected TRDRVs" list and choose "OK."**

6. **Select the "Trace All" check box as desired and choose "OK."**

Stopping Message Tracing

Procedure

1. **Deselect each item for which you are stopping message tracing, or select "STOP ALL TRACING".**

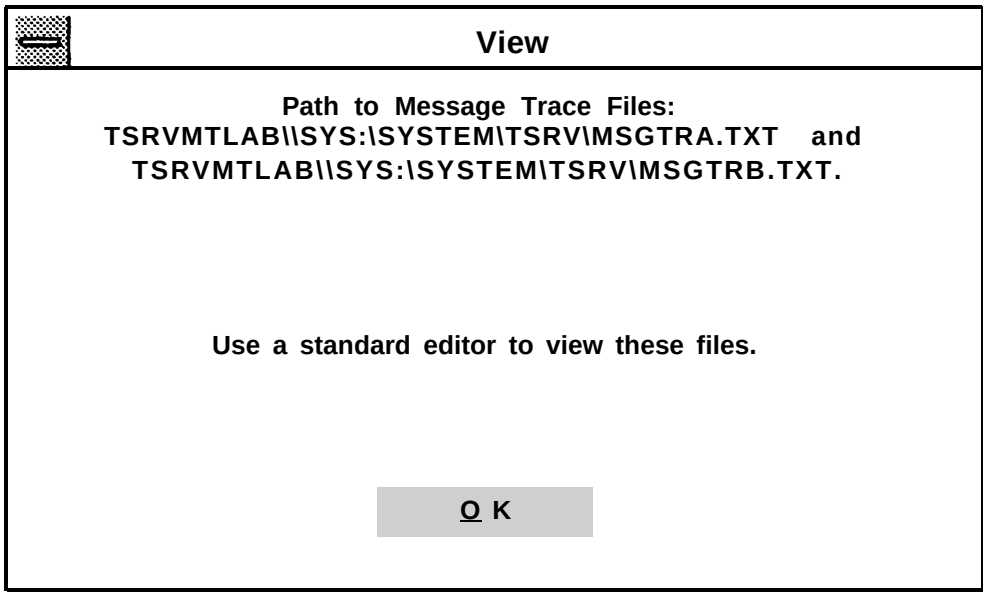
2. **Choose "OK."**

Note

To reenable message tracing, you must select the items you want traced.

Viewing Message Trace Files

Figure 7-50
Message Trace: View



Status Menu

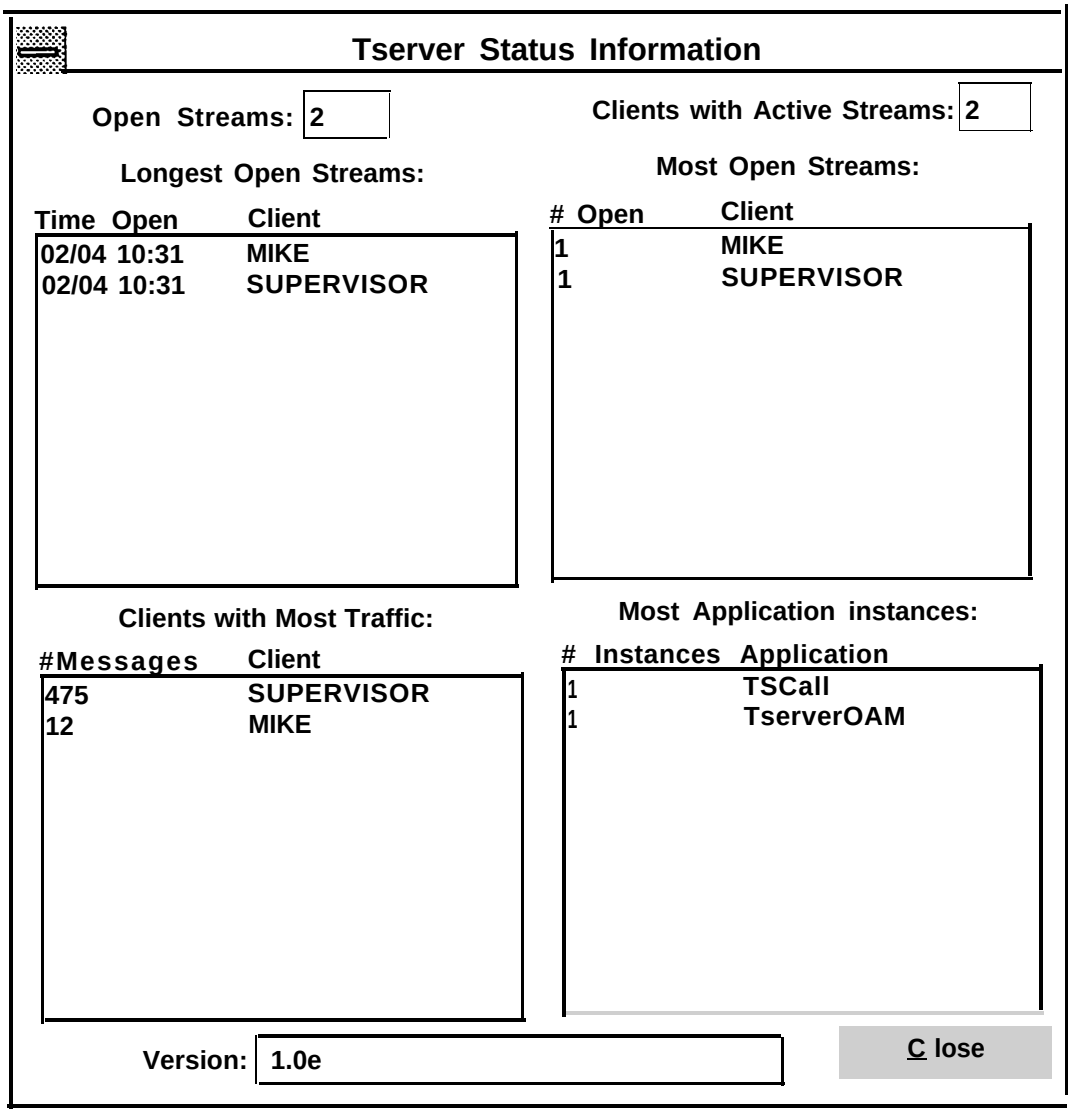
You can access all status commands via "S tatus" on the Administrator window. Status reports are available on the following components: T server, PBX driver (TS D RV), and C lient.

Tserver Status

To obtain status information on the Tserver that is currently being administered, use the following procedure

1. Select "S tatus/ T server" on the Administrator window.

Figure 7-51
Tserver Status Information



The fields are:

- **Open Streams** shows the number of currently open streams to the Tserver.
- **Clients with Active Streams** displays the number of login IDs that currently have open streams to the Tserver.
- **Longest Open Streams** lists the login IDs with the longest currently open streams to the Tserver. This box also indicates the time each stream was opened. The list is in the oldest to

newest order and displays only what can fit in the list box, as it is not a scrollable list box.

- **Most Open Streams** lists the login IDs with the most currently open streams to the Tserver. This box also indicates the number of open streams for each client. The list is in the most open to least open order and displays only what can fit in the list box, as it is not a scrollable list box.

- **Clients with Most Traffic** shows the number of messages transmitted and received, on a per login ID basis, between all applications opened with this login ID and the Tserver, where the number of messages equals the sum of all message types. The list is in the most messages to least messages order and displays only what can fit in the list box, as it is not a scrollable list box.

- **Most Application Instances** lists the applications, such as the Tserver Administrator and TS Call, that are currently most in use to the Tserver. The list is in the most instances to least instances order and displays only what can fit in the list box, as it is not a scrollable list box.

- **Version** refers to the version of the Tserver, not to the version of the Administrator application.

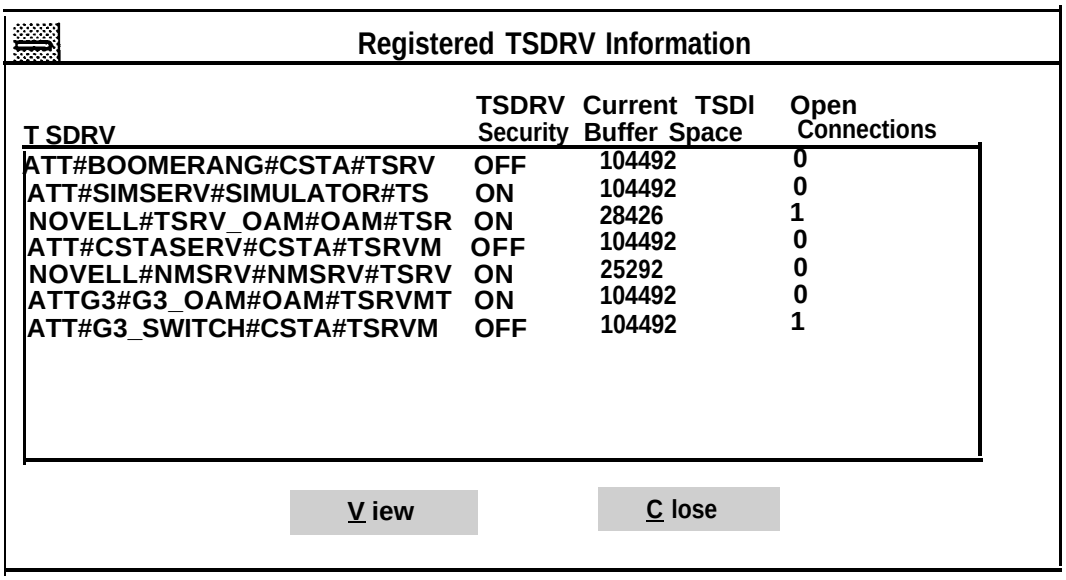
2. Choose "C lose" when you have finished viewing the "Tserver Status Information" dialog box.

TSDRV Status

To obtain status information on all TSDRVs that are currently registered with the Tserver being administered, use the following procedure:

1. Select "S tatus/TS D RV" on the Administrator window. The system displays the "Registered TSDRV Information" dialog box.

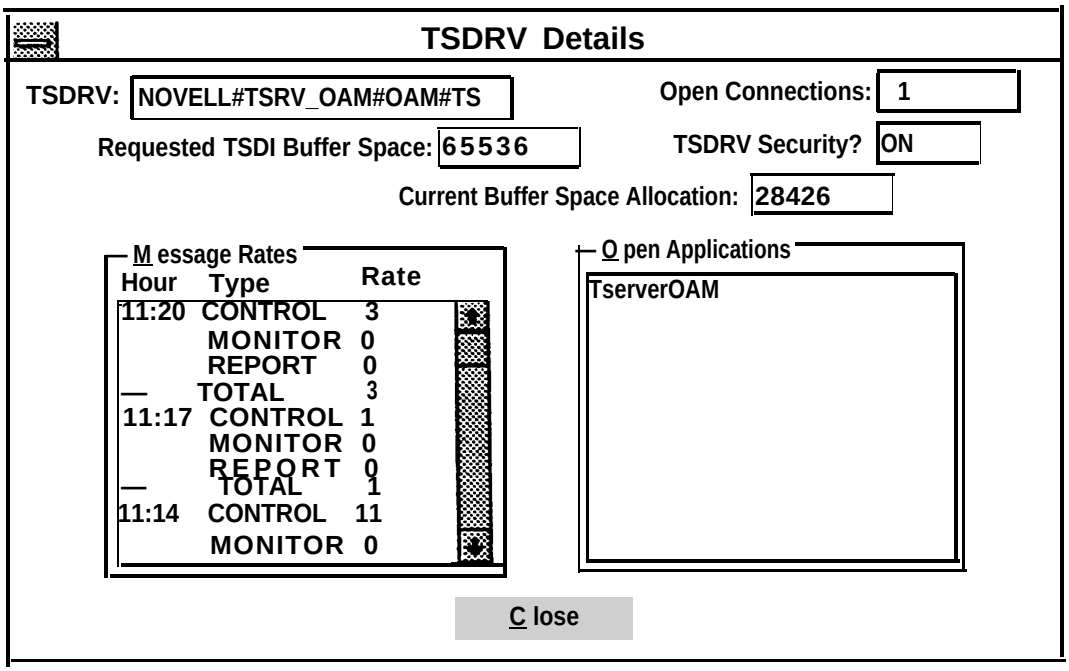
Figure 7-52
Registered TSDRV Information Dialog Box



2. Select a PBX driver from the displayed list.

3. Choose "View" to display more detailed information on the selected PBX driver. The system displays the "TSDRV Details" dialog box.

Figure 7-53
TSDRV Details Dialog Box



The fields are:

- **TSDRV** contains the name of the driver.
- **Requested TSDI Buffer Space** is the amount of memory in the Tserver/TSDRV Interface (TSDI) requested by the driver when it registered. This number is the maximum number of bytes the driver ever expects to need across the TSDI.
- **Current Buffer Space Allocation** is the amount of TSDI memory in use by this driver. The difference between this number and the Requested TSDI Buffer Space is the amount of TSDI memory left available to this driver.
- **O pen Applications** lists all the open applications currently accessing the driver.
- **M essage Rates** summarizes the last 24 hours of traffic information. Whether or not information for each hour is displayed on multiple lines depends on the number of message types being measured. In the above example, three types of messages are being measured. Therefore, there are four lines for each hour. Three of the lines contain the message types and the fourth line contains the total number of messages. The last hour for which information is available is further subdivided into 3-minute internals.

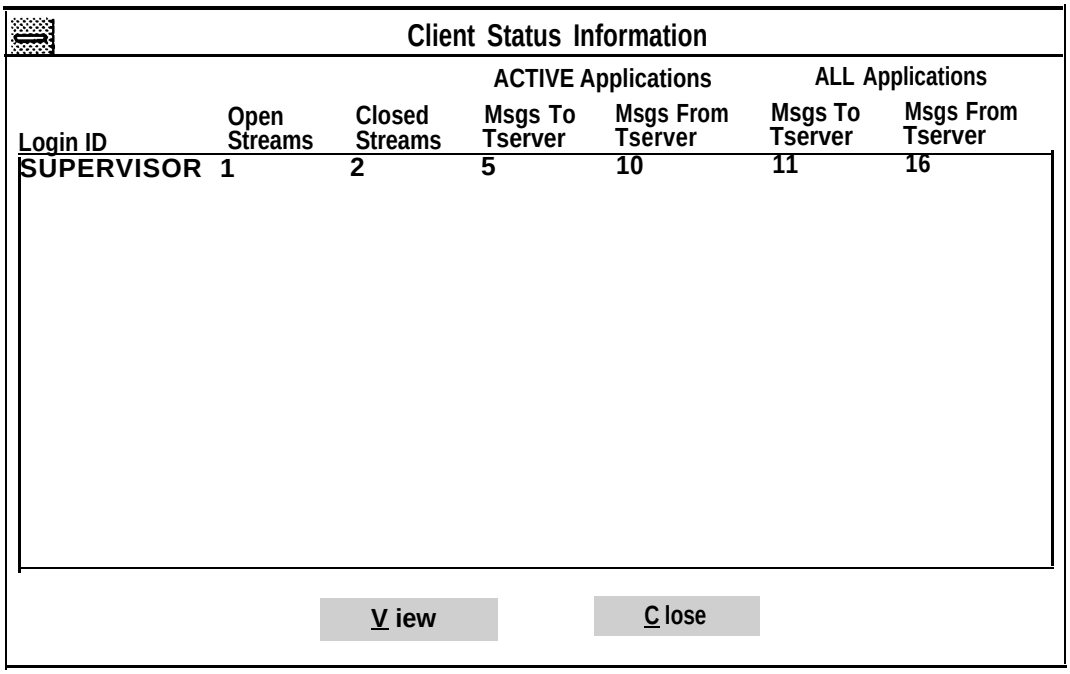
3. Choose "C lose" when you have finished viewing the "TSDRV Details" dialog box.

Client Status

1. To obtain status on a client, select "S tatus/ C lient" on the Administrator window.

The system displays the "Client Status Information" dialog box.

Figure 7-54
Client Status Information Dialog Box



This dialog box lists the current open streams to the Tserver, plus the 50 most recently closed streams.

The fields are:

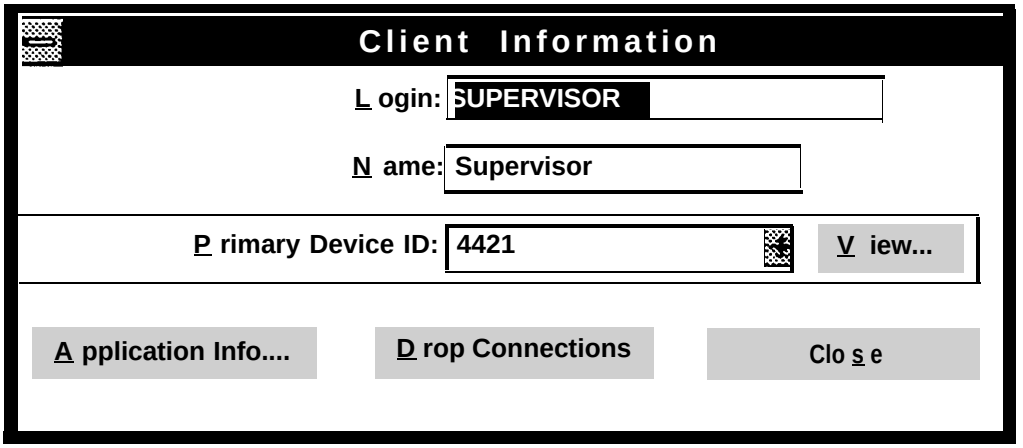
- **Login ID:** The identifier for each login ID with an active or open stream to the **Tserver.**
- **Open Streams:** On a per-client basis, the number of open CSTA message streams to the Tserver.
- **Closed Streams:** On a per-client basis, the number of closed CSTA message streams to the Tserver.
- **Msgs To Tserver:** On a per-client basis, the number of messages sent by the client to the Tserver.
- **Msgs From Tserver:** On a per-client basis, the number of messages sent by the Tserver to the client.

2. Select a client from the displayed list.

3. Choose "View" to display detailed information.

The system displays the "Client Detail Information" dialog box.

Figure 7-55
Client Detail Information Dialog Box



Important

Use the following "Drop Connections" procedure with care since doing so is a destructive action. Valid reasons for dropping connections for a user include the following:

- Suspected breach of security connected with this client and/or client's application.
- Client's application maybe degrading system performance.
- Troubleshooting procedure indicates the client's application may be the source of a problem.

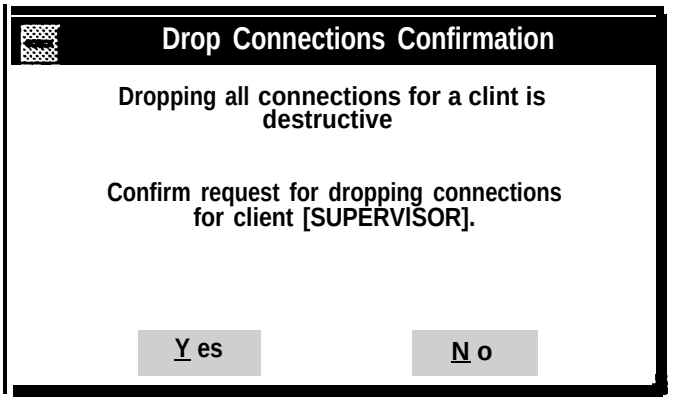
4. (optional) To drop all open streams for a particular user, then, on the "Client Detail Information" dialog box

4a. Select that user from the list.

4b. Choose "Drop Connections."

The system requires that you confirm your request to drop all connections for the specified client since doing so is a destructive action.

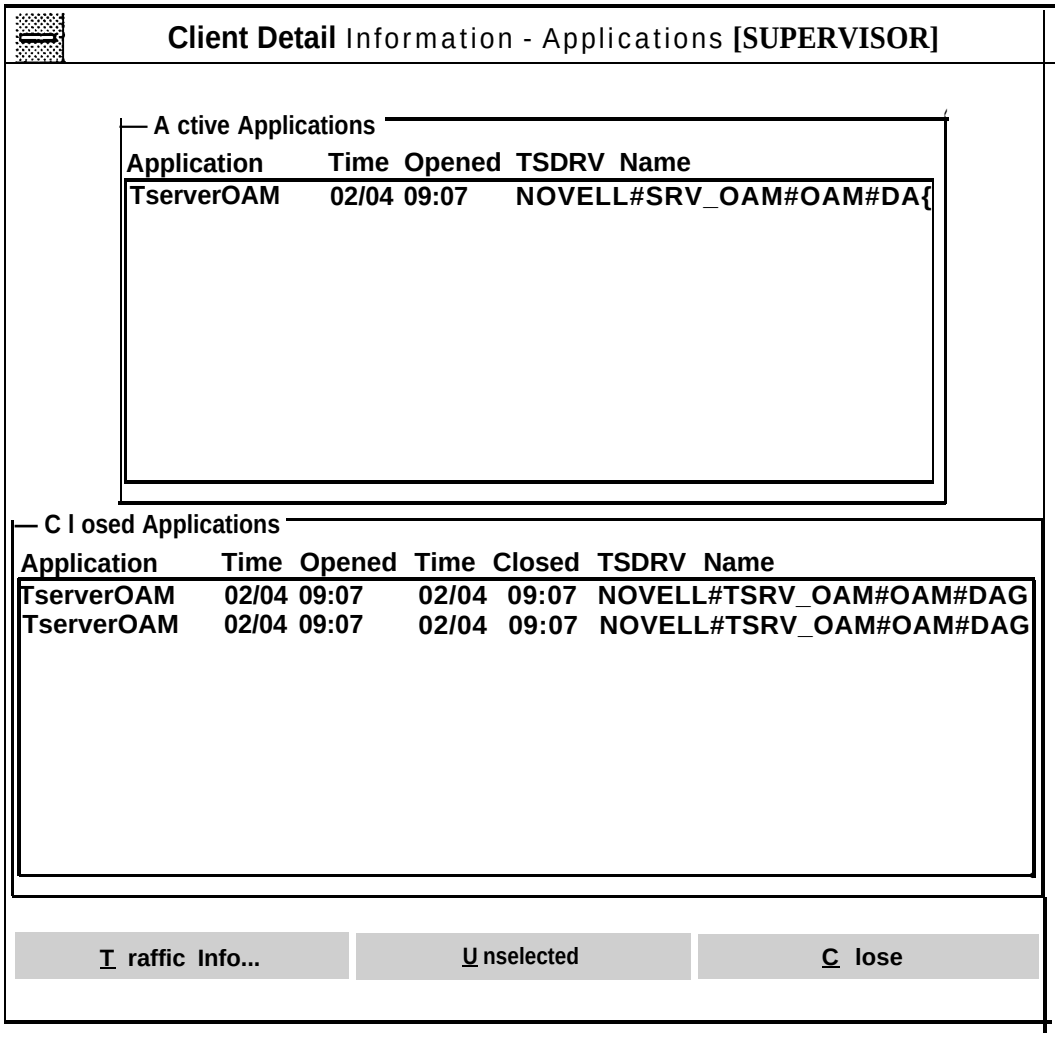
Figure 7-56
Drop Connection Confirmation



5. After the system returns you to the "Client Detail Information" dialog box, choose "Close" to return to the Administrator window.

6. (optional) Choose "Application Info..." to see more details about the client's applications.

Figure 7-57
View Client Detail Information - Applications Dialog Box



This dialog box is divided into two list boxes

- "Active Applications" provides details for all active applications.
- "Closed Applications" provides details for all closed applications, and are determined by the information saved by the Tserver. The Tserver saves information for the 50 most recently closed applications across all users. The number of closed applications displayed for any particular user depends on how recently the applications were in use and how busy the Tserver is. The fields are the same in both list boxes with the

exception of “Time Closed,” which only appears in “Closed Applications.” The fields are:

- **Application:** The name of the application.
- **Time Opened:** The exact time that the application was initially opened by the client.
- **Time Closed:** The exact time that the application was terminated.
- **TSDRV Name:** The name of the PBX driver to which the “open stream” request was sent by the application via a CTI Link.

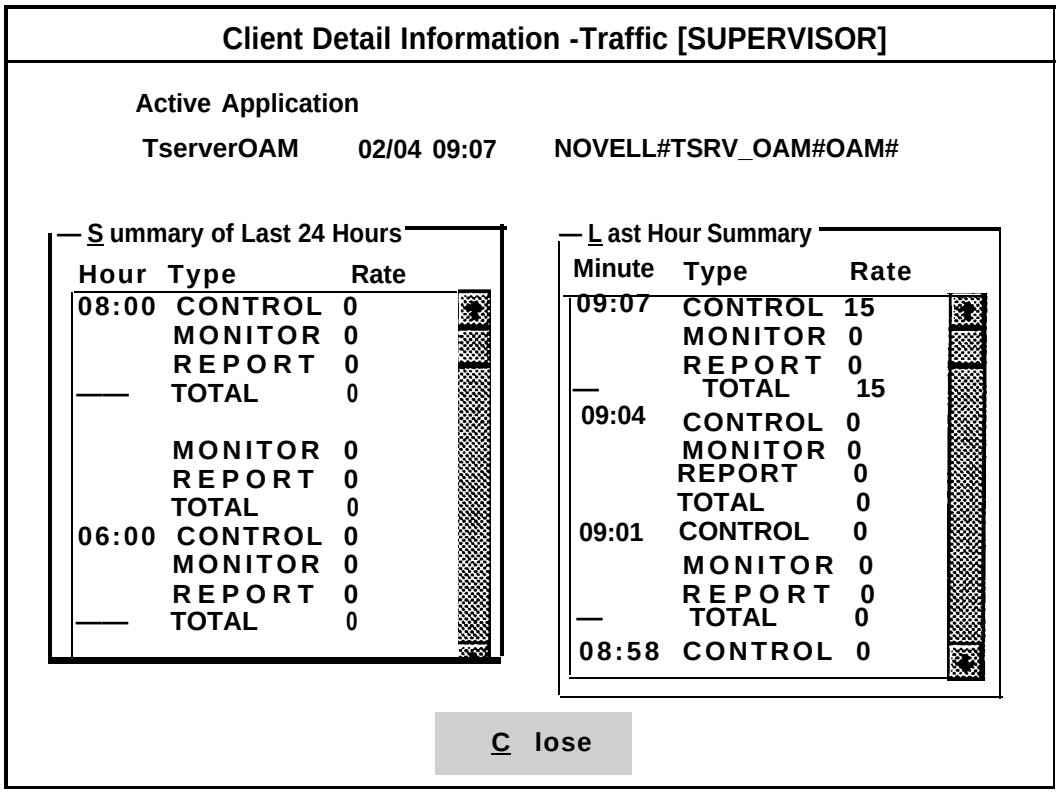
7. (optional) Choose “T raffic Info...” whether or not you have selected an application.

The “Client Detail Information-Traffic” dialog box contains two list boxes. “Summary of Last 24 Hours” summarizes the last 24 hours of traffic information. “Last Hour Summary” subdivides the last hour into 3-minute intervals.

You can select an active or closed application. If you choose “Traffic Info...” without specifying an application, the information displayed is a summary of all active applications. If you select both an active and a closed application, the information displayed is for the active application.

Each Message Type being measured is displayed on a separate line for each interval displayed. Three types of messages are being measured, and there are four lines for each hour: one line for each of the three message types plus a fourth line for the total number of messages.

Figure 7-58
View Traffic Information for a Selected Active Client



Note You may choose "Unselect" any time after you select an application if you change your mind about specifying it.

8. Choose "Close" to return to the "Client Detail Information" dialog box.

TSDRV Resources

Selecting a Driver

TSDRV resources allows the user to view low-level details about the resources used by a driver. These resources include NetWare ECB allocation and status and TSDI allocation and status.

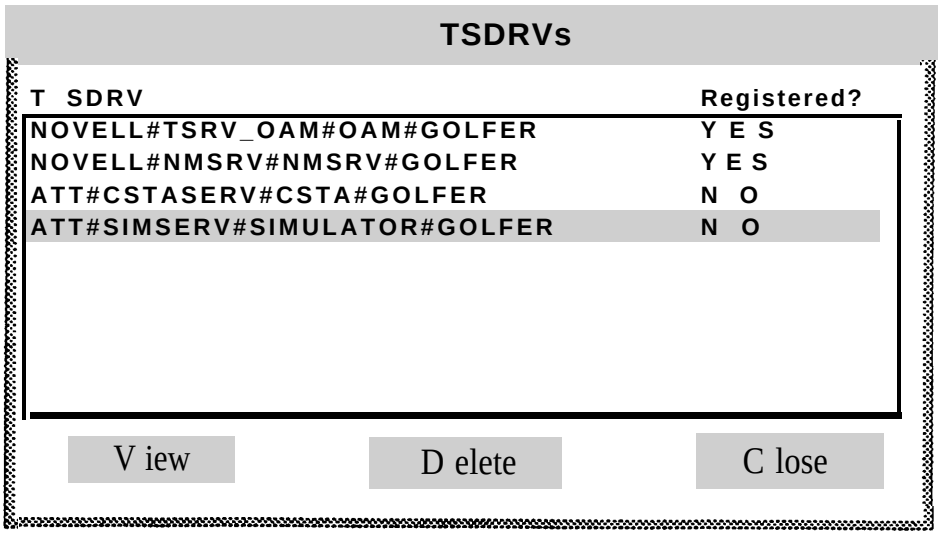
To view the resource parameters of a driver, use the following procedure:

Procedure 23

1. **Select “TSDRV Resources” on the “Maint” menu to display the “TSDRVs” dialog box.**

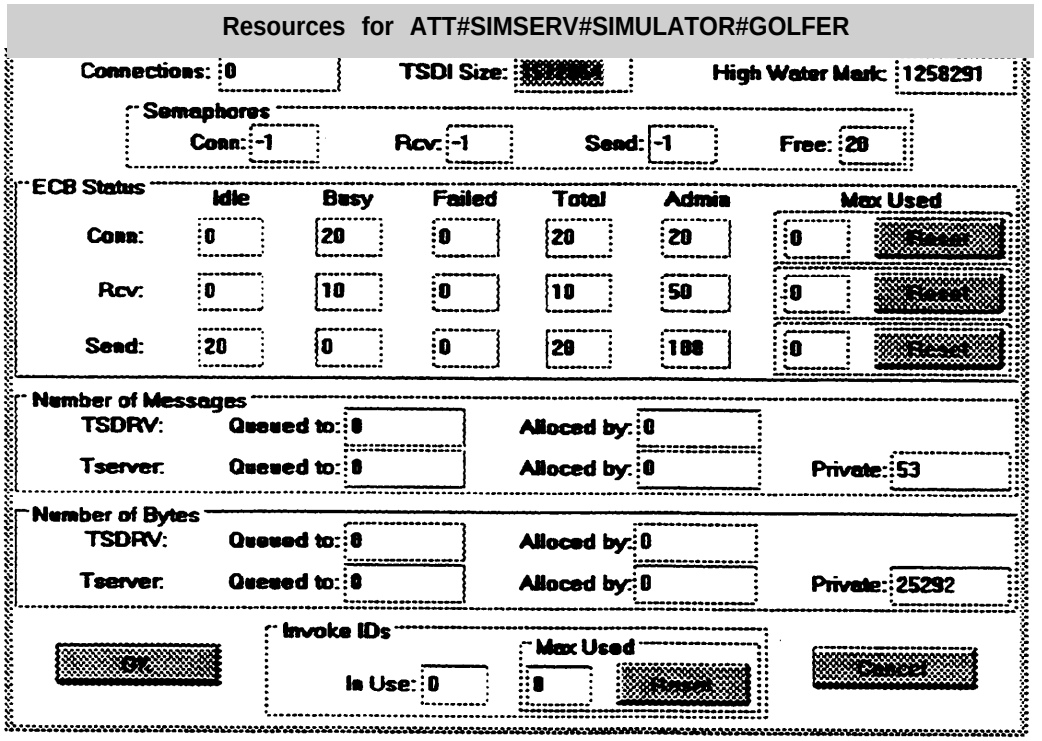
2. **Select the driver whose resources you wish to view.**

Figure 7-59
Select a TSDRV Screen



Viewing Driver Resources

Figure 7-60
TSDRV Resources: View



The fields are:

- **Connections** indicates the number of open streams to this advertised driver name.

- **TSDI Size** is the maximum size of the TSDI buffer space for which this Driver registered. When the amount of memory allocated for this Driver reaches this maximum, further requests to and from this Driver will not be processed until some of this memory has been released. The **Number of Bytes** information shows how close the Driver is to reaching this maximum.

- **High Water Mark** is the amount of memory allocated for this Driver before the TSDI begins to warn the Driver and Tserver that the maximum, TSDI Size, may soon be reached.

- **Semaphores** contains the values of the connect, receive, send, and free ECB semaphores that the Tserver uses for this Driver. ECBs are the mechanism provided by NetWare that an NLM uses (in this case the Tserver NLM) to send and receive packets from clients. These packets can be of two types: packets that indicate a client wishes to establish an SPX connection, and packets that are sent over an established SPX connection that contain actual data.

  - The **connect semaphore (Conn:)** is signaled when a client wishes to establish an SPX connection with the Tserver to send ACS and CSTA messages. A value of -1 indicates that there are no outstanding requests (ECBs) by clients to establish SPX connections to the Tserver. A value of 0 or greater indicates the Tserver has <connect semaphore value plus one> requests (ECBs) to process for this driver. For example, if the semaphore value is 1, then there are two outstanding connect ECBs to be promised by the Tserver for this driver. The connect semaphore value should return to -1 very quickly under normal conditions.

  - The **receive semaphore (Rcv:)** is signaled when a client is sending the actual packets (ECBs) that contain ACS and CSTA messages. A value of -1 indicates that there are no outstanding packets (ECBs) to be processed by the Tserver from clients. A value of 0 or greater indicates the Tserver has <receive semaphore value plus one> receive (ECBs) to process for this driver. For example, if the semaphore value is 0, then there is one outstanding receive ECB to be processed by the Tserver for

this driver. The receive semaphore value should return to -1 very quickly under normal conditions..

- The **send semaphore (Send:)** is signaled when the Tserver sends a packet (ECB) to a client which contains an ACS or CSTA message. A value of -1 indicates that there are no outstanding packets (ECBs) sent by the Tserver to clients that have not been acknowledged by the client. A value of 0 or greater indicates that there are <send semaphore value plus one> unacknowledged packets (ECBs) sent by the Tserver to clients. For example, if the send semaphore value is 5, then there are six outstanding send packets (ECBs) that have not be acknowledged by clients. The send semaphore value should return to -1 very quickly under normal conditions. The Tserver will time out packets (ECBs) sent to clients in approximately 1 minute after first sending the packet to a client. When a packet is acknowledged by a client, the Tserver recovers the ECB used to send the packet and places the ECB on a free list and signals the Free semaphore.

- The **free semaphore (Free:)** is signaled when the Tserver recovers a packet (ECB) sent to a client. When the a driver registers, a certain number of ECBs are allocated by the Tserver for that driver and the semaphore is signaled that many times which means this semaphore is a count of the number of packets (ECBs) that are available for sending events to clients for this driver. The total of the Free and Send semaphores should always be constant (i.e., the send ECBs can be m only one of two states; on the free queue available to send a packet, or in the process of being transmitting data to a client workstation).

♦ **ECB Status** indicates the state of the connect, receive, and send ECBs used for this Driver. The Tserver posts the connect and receive ECBs to NetWare when the Driver registers. These ECBs are used to receive client requests. The send ECBs are used to send messages to clients.

- **Connect ECBs (Conn:)** are created by the Tserver and posted with SPX on behalf of this driver for the purpose of allowing clients to establish SPX connections to the Tserver. When the ECB is posted with SPX, the status of the ECB becomes busy, and SPX uses the ECB to listen for requests from clients to establish an SPX connection between the Tserver and the client

(an SPX connection is used by the client library to then establish an ACS stream between the client and Tserver).

When a client establishes an SPX connection with the Tserver, SPX informs the Tserver by finding a connect ECB with a positive status, populating the ECB with information about the client, and changing the status of the ECB to **idle.** The Tserver is then informed that there is a connect ECB to process by signaling (incrementing) the connect semaphore. After the Tserver processes the ECB (i.e., creates data structures to track this new client), the ECB is reposted back to SPX, the ECB status becomes positive and the connect semaphore is decremented.

- The **Total** field is the sum of the **Idle, Busy,** and **Failed** fields. The total represents that actual total number of this type of ECB at the moment.

- The **Admined** field is the total number of this type of ECB that has been administered via Telephony Services Administrator. When the total number of ECBs is changed via the **TSA** application, the change does not always take effect immediately. If the administered number of ECBs is being increased, then this takes affect immediately. If the administered number of ECBs is being decreased, the Tserver adjusts the total number of ECBs to match the administered number of ECBs as the ECBs come back to the idle state. An ECB can only be deleted when the ECB is in the idle state.

  For clients to establish new SPX connections (ACS streams) to the driver there must be at least one connect ECB with a positive status available. Connect ECBs should only have a negative or zero status for a very short time before being reposted to SPX.

- The **Max Used** field for connect ECBs indicates the largest number of connect ECBs that have been processed at one time by the Tserver for the purpose of establishing SPX connections, since the Tserver was loaded or the max used field was reset to zero by the **Telephony Services Administrator** Application. In other words, this represents that maximum number of new SPX connections (ACS streams) opened to the Tserver

simultaneously. If max used is equal to the total number of connect ECBs available, then there are too few connect ECBs and some client may have failed to open a stream to the Tserver. The number of connect ECBs posted for a driver can be changed by using the **Telephony Services Administrator** Application.

- **Receive ECBs (Rcv:)** are created by the Tserver and posted with SPX on behalf of this driver for the purpose of receiving packets from clients for this driver. When the ECB is posted with SPX, the status of the ECB becomes **busy,** and SPX uses the ECB to listen for packets of data that contain ACS or CSTA messages from clients.

- **Send ECBs (Rcv:)** are created by the Tserver and maintained on a free list until they are needed for sending packets (messages) from the Tserver to a client on behalf of this driver. While the send ECBs are on the free list, their status is **idle.**

♦ **Number of Messages** contains the count of messages in each of the five possible states: queued to the Driver, queued to the Tserver, allocated by the Driver, allocated by the Tserver, and privately allocated by the Tserver. The sum of the first four states equals the total number of messages currently allocated for this TSDI Interface. Messages which are privately allocated by the Tserver are not charged against the total memory allocated for the this TSDI Interface. Currently, the Tserver allocates private TSDI buffers only for keeping track of each new open ACS stream. Because of this, the **number of Tserver Private messages** should always be equal to the Connections field.

♦ **Number of Bytes** contains the count of bytes in each of the five possible states: queued to the Driver, queued to the Tserver, allocated by the Driver, allocated by the Tserver and privately allocated by the Tserver. The sum of the first four fields equals the total number of bytes currently allocated for this TSDI Interface. Compare this total to the **TSDI Size** to determine if the Driver is close to reaching its limit. Messages (i.e., the number of bytes in the message) which are privately allocated by the Tserver are not charged against the total memory allocated for the this TSDI Interface. Currently, the Tserver allocates private TSDI buffers only for keeping track of each new open ACS stream.

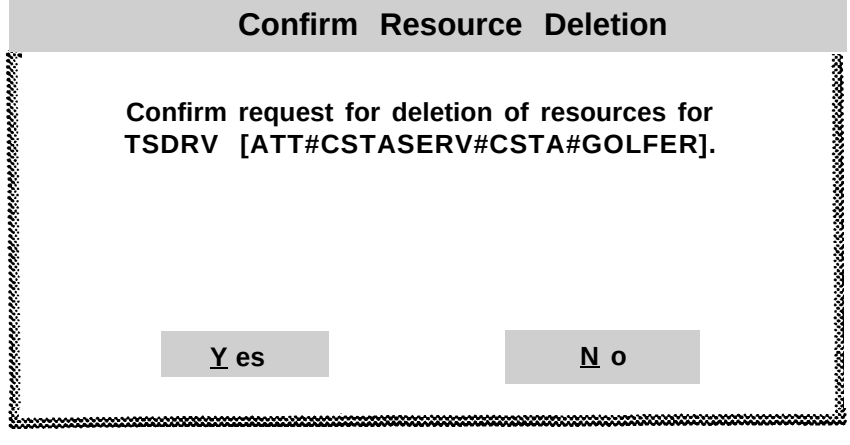
When the Driver registers with the Tserver, memory is allocated by the Tserver for ECBs that it will use for this Driver. Because of this, the **Alloced by Tserver** field in both the **Number of Messages** and **Number of Bytes** display will always have a value. The number of messages depends on the **TSDI Size** a driver uses in the driver registration.

- **Invoke IDs** contains the number of unique invoke IDs currently in use by this Driver. The Tserver guarantees a driver that the invoke IDs on all requests within an ACS stream are unique, so the Tserver saves the invoke ID generated by the application, and passes the driver a unique Invoke ID. A TSDI buffer is used to store this mapping of invoke IDs. When a driver responds to an application request with a confirmation message, the application invoke ID is returned to the application, and the TSDI buffer used to store the application invoke ID is released back to the TSDI. This field indicates how many outstanding client requests a driver is currently processing.

- **Max Used** indicates the largest number of client request messages that have been outstanding at any one time since the Tserver was loaded or the max used field was reset to zero by the **Telephony Services Administrator** Application.

Deleting Driver Resources

Figure 7-61
TSDRV Resources: Delete



Troubleshooting

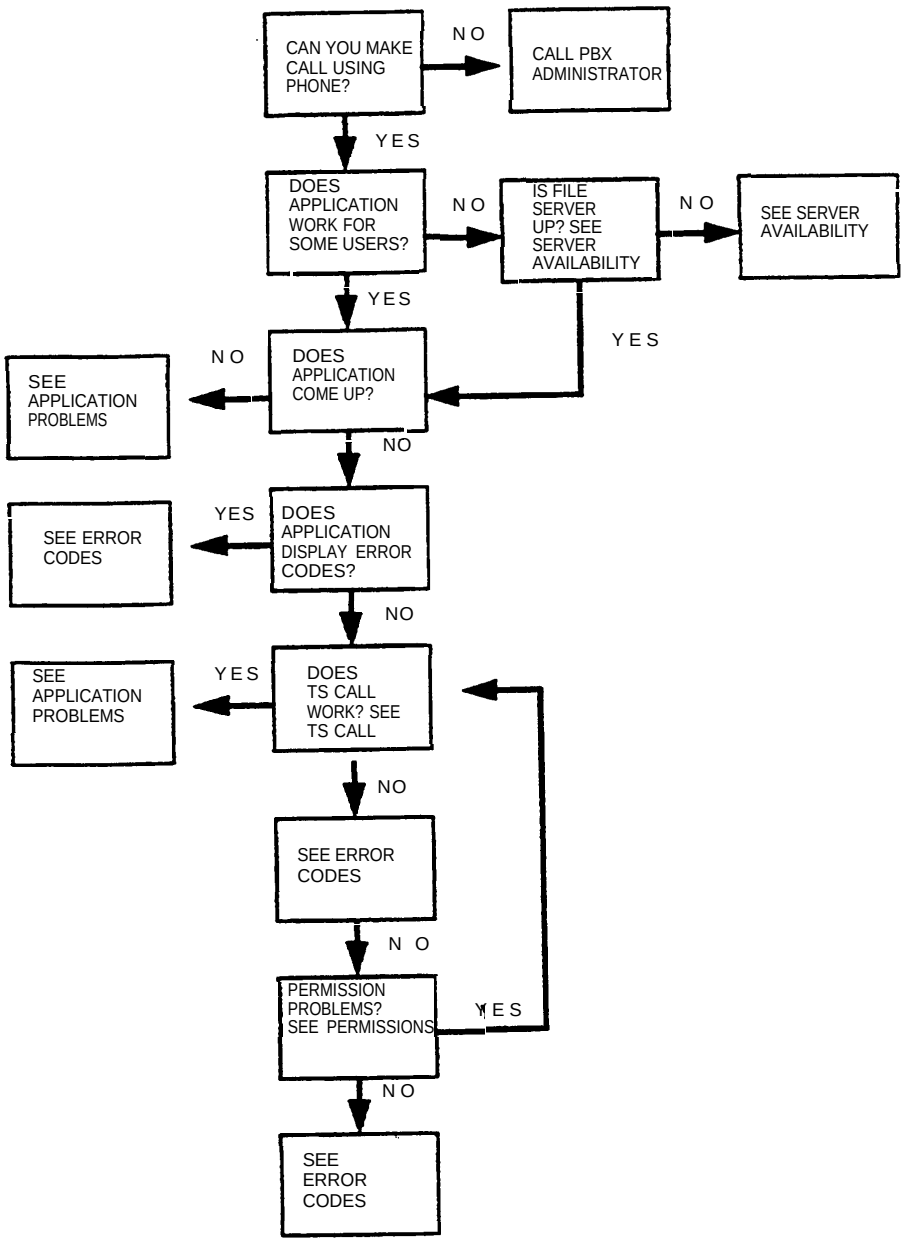
chapter

8 Troubleshooting

This chapter will assist you in resolving system problems or identifying trouble areas so that the correct support organization can be contacted. Three specific areas of potential troubles are presented application problems; server availabity, and permission. TSCall is discussed in terms of how it can be used to assist in troubleshooting. These topics are followed by a table describing all possible error codes.

Figure 8-1 illustrates the normal flow of troubleshooting activity. It will help you isolate the trouble, whether it is in the application, the library, the Telephony Server NLM, the PBX Driver NLM, or the PBX.

Figure 8-1
Troubleshooting Flowchart



Application Problems

If the application does not come up at the client workstation, consult the installation procedures for the specific application. Refer to the appropriate chapters of this manual for detailed information on installation instructions for client and server Telephony Services; versions required for the various files; and minimum requirements for both the client and server (processor, RAM, software versions). Refer to the Novell® documentation for NetWare® installation instructions.

If an application is not working, but had worked previously, a recent change or upgrade could be the cause. If this is the case, backing out the change or upgrade might help identify the cause of the trouble.

If an application is not working for a particular workstation but is working for others, and it appears that the appropriate Telephony Services files are in place, try the following:

- Refer to the application documentation. Are the user parameters administered correctly for the application?
- If the client is using Windows 3.1, the Network parameter in the Windows Setup Control panel must be set to NetWare 3.26 or better.
- To work properly, windows must be running in the enhanced mode, which means that the user needed to have typed “win” to enter windows. The Windows Program Manager Help window displays the operating mode of the client workstation.
- If the application is returning an open stream failure message, verify that the correct version of the IPX module is loaded. Refer to the installation information in this manual for additional information on IPX versions. If the correct version of the IPX module is loaded, then the trouble might be with network connectivity. Consult the appropriate Novell NetWare documentation.
- If the application is being run from the file server, verify that the user has the proper permissions to access the application on the file server. Refer to the NetWare administration documentation for more information.

♦ If the user is authorized to use the Telephony Services Administrator (TSA) capabilities, make sure that the user has the most current shell or VLMs. Refer to the installation information in this manual that deals with the client workstation.

Server Availability

The server must be available and advertising Telephony Services. If you cannot access the file server you want, check to verify that it is up and functioning properly.

From the client workstation, use the "SLIST" utility to display a list of file servers on your network; the file server on which the Tserver resides should be in the list. If it is, then the file server is up and the intervening networks are operating. If it is not, either the file server is down or there is a network problem and you should consult the NetWare documentation. For the "SLIST" command to work from the client workstation, the NEXT.EXE shell or VLMs must be installed on the client. Refer to the Novell utilities documentation for more details on "SLIST".

From the file server console where Telephony Services was installed, use the "MODULES" command to determine if the Tserver and Driver NLMs are loaded. Refer to the installation information in this manual to determine the modules that need to be loaded as well as the correct versions of each. The "MODULES" command displays the name of each module that is loaded on that file server, a descriptive name for each module, and the version number for disk and LAN drivers. Refer to the Novell system administration documentation for more details on the "MODULES" command.

If you use the "MODULES" command from the file server console and the file server displays any of the following error messages on the file server system console screen:

♦ short term allocator failed, out of memory

♦ cache buffers getting low

♦ out of cache buffers

consult your NetWare manuals for further instructions.

If you have performed the “SLIST” and “MODULES’ commands and everything seems to be in order, you must determine that the appropriate telephony services are advertising on the network. From the file server console where NetWare Telephony Services was installed, load the TSRVLIST NLM to generate a list of all Telephony Services that the file server can “see.” The TSRVLIST NLM displays three lists: the CSTA services list, the OAM services list, and the name services list.

The CSTA list displays all of the PBX drivers that have registered with the Tserver(s). If the appropriate PBX driver does not appear in the list, this indicates a PBX driver problem, and the appropriate PBX driver documentation should be consulted.

The OAM list displays all of the drivers that have registered with the Tserver for OAM services as well as the OAM services provided by the Tserver itself. If a particular Telephony Server OAM or a PBX driver OAM does not appear, the appropriate documentation should be consulted. The Tserver OAM application is discussed in this manual; PBX driver OAM applications are discussed in PBX driver documentation.

The Name Services list displays all of the Servers that are advertising themselves with the name services feature. This service should be advertised for every Tserver NLM that is loaded.

These tools help determine the availability of the various Telephony Services components from the view of the file server console. The following checks determine if all Telephony Services are available from a client’s view of the network.

The TSCall application can be used to determine if the appropriate service is advertising and can be seen by the client. To verify this, activate the TSCall application. When the initial screen appears (the Telephony Server Login screen), verify that the appropriate service appears on its server list.

If the client will be performing administration, the client must be attached to the file server that hosts the Telephony Server. Once the client attaches to the correct file server, bring up the Tserver application (NetWare Telephony Services Administrator). This application displays an “Available Tserves” dialog box. If the appropriate TSA modules appear in the list of available Tservers, then the TSA module is advertising and can be seen by the client.

Permissions

If the application is working for others but not for a particular client, there might be a problem with the permissions for that client. To determine this, you need to change the permissions of the client with the problem to full permissions and then determine whether that client's problem has been resolved. If the problem is resolved, then it was a permissions problem. Remember, though, to change the permissions appropriately to conform with the necessary security procedures.

To give a user full permissions, follow this procedure:

1. **Using the NetWare Telephony Services Administrator windows application, select the "User" option on the "Admin" main menu.**

2. **Select the desired user and choose "Edit" to modify this user record.**

3. **Choose "Options" to display the "Classes of Service" form for this user.**

4. **Give this user full telephony permissions to control, monitor, and route any device by:**

   - Selecting "Any Device" under" Call Control Access Group."
   - Selecting "Any Device" under "Device/Device Monitor Access Group"
   - Selecting "Any Device" under the "Call/Device Monitor Access Group."
   - Selecting "Any Device" under "Routing Access Group."
   - Enabling the "Allow Call/Call Monitoring" field.
   - Selecting "Any PBX" for the device.
   - If the user is restricted to his or her home worktop, you must use the application from the user's home worktop or temporarily

remove the “Home Worktop Restriction” on the “Administration Options” screen. Removing the Home Worktop Restriction is global; that is, if you remove the Home Worktop Restriction on the “Administrations Options” screen, the restriction is removed for all users.

If the user performs administrative functions, give the user permission to perform Telephony Services Administration on any PBX driver by:

- Selecting “TSA Access Group” from the “Admin” main menu.
- Select the group “All TSA Access” and select “Allowed Users.”
- Add the user login to the “All Administered Users Currently Allowed Access” box.

TSCall

The TSCall application can be used for troubleshooting in the following ways:

- To determine if the trouble lies within the system or with the application. For example, if TSCall works, then the system administrator knows that NetWare, the Telephony Services software, and an application are successfully communicating. This would indicate that the reported trouble is most likely in another application the user was trying to activate.
- If an applicaiton does not return an error code and display it to the user, TSCall can be used to display the error. This could be useful in certain trouble scenarios, such as inadequate buffers or incompatible file versions.

Before using TSCall, you must know your login ID and password for the Telephony Server, and the name of your Telephony Server. To use the TSCall application, insert the TSCall floppy diskette into the diskette drive of the PC. If the drive is “A” select “a\attcall.exe.”

Note

This is not the standard approach to installing and using TSCall but rather a quick approach to isolate a problem. This approach avoids having to install TSCall on a user's hard drive. To use TSCall correctly with all the available options such as on-line help, follow the installation instructions in the *TSCall User's Guide.*

After you bring up TSCall, the "Telephony Server Login" dialog box appears. The frost time you run TSCall, the box presents sample information. Follow this procedure:

1. **Enter the Advertised Name of the CTI link in the "Server Name" field.**

2. **Enter your telephone extension in the "Phone Extension" field.**

3. **Enter your Telephony Server login ID in the "Login ID" field.**

4. **Enter your password in the "Password" field.**

5. **Choose "OK."**

   If the information you entered in this dialog box is correct, an untitled TSCall window appears.

Click on the dialpad button in the lower right hand corner. The dialpad window will appear. Use your keyboard or click on the number buttons on the dialpad window to enter a valid phone number or extension. Click on the dial button. If you do not have a speakerphone, pickup the handset (within 5 seconds). If you have a speakephone, the speakerphone will activate automatically, unless you have an analog speakerphone, in which case you must manually activate the speakerphone.

If your call completes, the reported trouble is in the user's application; contact the application developer. If the call failed, look up the error code that appears on the screen in the error codes table in this chapter. Some of the more apparent errors, such as "invalid login," will be explained on the screen. However, most errors will produce an error code that you can cross reference in the following table.

Error Codes

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
-1	The API version requested is not supported by the existing API Client Library.	This is an application error; contact the application developer.
-2	One or more of the parameters is invalid	This is an application error; contact the application developer.
-5	This error code indicates the requested Server is not present in the network.	Is the server up? Was the wrong server name used? Are physical connections (wiring) intact?
-6	This return value indicates that there are insufficient resources to open an ACS stream.	Is the correct version of IPX being used? If yes, contact the application developer since the application is trying to open too many streams or is opening streams but not closing them.
-7	The user buffer size was smaller than the size of the next available event	This is an application error; contact the application developer.
-9	The ACS stream has encountered an unspecified error.	This is typically a version mismatch. Has some software been replaced or upgraded recently? If not, call your support number.
-10	The ACS handle is invalid.	This is an application error; contact the application developer.
-11	The ACS stream has failed due to network problems. No further operations are possible on this stream. A connection has been lost.	Is the Tserver down? Is there physical connectivity?
-12	Not enough buffers were available to place an outgoing message on the send queue. No message has been sent. This could be either an application error or an overloaded Tserver.	Use Tserver TSA to check traffic. If traffic reports show no overload, call application developer.
-13	The send queue is full. No message has been sent. This could be either an application error or an overloaded Tserver.	Use Tserver TSA to check traffic. If traffic reports show no overload, call application developer.

0	The Client Library detected that the ACS stream failed.	1. Other errors may have been sent by the Tserver before the ACS stream was taken down. If so, follow the procedures for this error. 2. If no other errors were received from the Tserver first, then verify that the Tserver/Server is still running and look for LAN problems.
9	A NetWare SPX call failed in the Tserver.	There is a serious system problem. These errors will appear in the Tserver error logs. Consult the logs for the NetWare return code.
11	The Tserver was unable to allocate a piece of memory.	1. Verify that the server has enough memory to run the driver and Tserver. 2. If the server has enough memory, then the driver has reached its limit of how much memory the Tserver will allocate. This limit is chosen by the driver when it registers with the Tserver. Call your support number.
13	The Tserver was unable to decode a message from a client workstation.	The application is most likely using an old version of csta.dll. Check the version to ensure that it supports this message. If you have the latest dll then Call your support number.
14	The Tserver tried to process a request with a bad client connection ID number.	1. This error should never be returned to an application. If it appears in the Tserver error logs, it indicates that an application may have been terminated or the client workstation was disconnected from the network while the Tserver was processing messages for it. 2. Determine if either of these two cases is true. 3. If this error occurs repeatedly and these conditions are not true, call your support number.

19	One or more of the files that makeup the Security Database is not present on the server or cannot be opened.	1. It is possible for the Telephony Server to be locked out of the Security Database files for short periods of time while the NetWare Telephony Services TSA Windows application is running. Repeat the operation that caused this error if the TSA application was running at the time the error first occurred. 2. Verify that the files that makeup the Tserver Security Database (SDB) are still present on the NetWare file server the Tserver is loaded. The following files make up the Tserver SDB and should be located in the directory : <file server nam>\sys:system\tsrv\sdb The files are: devices.dta dlist.dta dlistnm.dta indices.dta tlist.dta tlistnm.dta tservers.dta tsrvinfo.dta tsrvrsrc.dta user.dta worktop.dta
22	The Tserver's internal table of API calls indicating which level of security to perform on a specific request is corrupted.	This error should never be returned to an application or appear in the Tserver error logs. If this event is generated by the Tserver, then there is a software problem with the Tserver. Call your support number.
23	The Tserver rejected an ACSOpenStream request because the Server ID in the message did not match a PBX driver supported by this Tserver.	A software problem has occurred with the client csta.dll. Call your support number.
24	The stream type of an ACSOpenStream request was invalid.	A software problem has occurred with the client csta.dll. Call your support number

25	The password, login, or both from an ACSOpenStream request did not match an entry in the Bindery on the server on which the Tserver is running.	1. Validate that the user login and password were entered correctly into the application. 2. Using the syscon command, verify the user has a NetWare login on the NetWare fileserver where the Tserver is running. ● From the “Available Topics” menu in syscon choose “User Information.” ● Validate that the user’s login is in the list of “User Names.” Use the “Insert” key to create a login and associated password for this user if none exists. 3. Verify the user has a user record in the Tserver Security Database by using the NetWare TSA Windows application ● From the Admin option, choose “Users.” ● Validate that the user’s login is in “User Information” and that the login in the security database exactly matches the login on the NetWare Server. Use the Create option to create a login for this user if none exists. Note: Passwords are not kept in the Tserver Security Database.
26	No user record was found in the Security Database for the login specified in the ACSOpenStream request.	Verify the user has a user record in the security database by using the NetWare TSA Windows application. ● Select “Users” from the “Admin” main menu. ● Validate that the user's login in the “User Information“ list and the login in the security database exactly match the login on the NetWare Server. Create a login for this user if none exists. Note: Passwords are not kept in the Tserver security database

27	No device record was found in the security database for the device specified in the API call.	Create the a device record for the device the user is trying to control in the Tserver security database by using the NetWare TSA Windows application • Select “Devices” from the “Admin” main menu. • Use the Create option to create a device record for this device. Note: Make sure the assigned PBX for this device includes the Telephony Server being administered
20	The specified device in an API call was not found on any device list administered for this user.	The Telephony Server translates this error into more specific errors which indicate on which list the device is not listed. If this error is returned to an application, a software problem has occurred in the Telephony Server NLM. Call your support number.
30	The Telephony Server rejected a user’s request to control a device because all of the following are true: • The Primary Device ID of the User's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The fields “Home Worktop Device ID” and “LAN Address” are blank in the user's record indicating the user is not associated with any Worktop. • The Access Group in the “Classes of Service” administration in this user’s record which corresponds to the action being attempted (Call Control, Device/Device Monitoring, Call/Device Monitoring or Routing) is empty. • The user is not sitting at his or her Home Worktop (as defined by the LAN Address in the worktop record associated With this user) and the “Restrict User to Home Worktop” option is enabled.	Change the user’s administration so that the user has permission to control the device through either the user’s worktop reed (worktop administration) or through one of the Classes of Service (user administration).

34	The Tserver read a device record from the Security Database that contained corrupted information. The device record did not contain a PBX index value which is a violation of the SDB structure.	This error should never be returned to an application or appear in the Tserver error logs. If this event is generated by the Tserver, then there is a software problem with the Tserver. Call your support number.
35	The PBX administered for this device does not contain the CTI Link to which the user opened an ACS stream.	1. Validate that the user opened the ACS stream to the correct CTI Link. 2. If the CTI Link to which the stream was opened can support this device, then add this CTI link to the PBX by using the “PBX” option (on the “Admin” main menu) in the NetWare TSA Windows application.
39	The device in the API call is on an exception lit which is administered as part of the information for this user.	1. The Telephony Server translates this error into more specific errors which indicate which list the device is not on. If this error is returned to an application, a software problem has occurred in the Telephony Server NLM. Call your support number.
40	The user login which is attempting to open an TSA stream to a PBX driver does not have that privledge to do so for that driver.	1. If this user is allowed to perform TSA operations on a driver, then in the TSA Windows application, select the TSA Access Groups” option under the “Admin” main menu. 2. Select the TSA Access Group to which this user should be added, or create a new group for this user via the “Create” button. Then, select the new group (you may have to use the “Advertised Names” option on the “Admin” main menu first to administer the CTI Link names that will be added to this CTI Link Group). Add this user to the TSA Access Group via the “Allowed Users” option.

41	An attempt to open a TSA stream to TSA driver name was made but this advertised name is not in the security database.	1. If this user is allowed to perform TSA operations on this PBX driver, then, in the TSA Windows application, select “Advertised Names” under the “Admin” main menu. 2. Create the Tserver TSA or TSDRV TSA advertised name. 3. Use the TSA Access Group option on the “Admin” main menu to select the TSA Access Group to which this user should be added or create a new group for this user with via the ‘Create” button and then select the new group. User the “Allowed Users” option to add this user to the TSA Access Group.
42	The user licenses maximum has been exceeded on this Telephony Server. No new User Licenses may be granted (that is., no new ACS Stream may be open; however, if a user/application has an existing ACS stream open to a driver, they may open another ACS Stream to the same driver from the same Worktop using the same login).	1. Force current users off the system by using the NetWare Telephony Services TSA Windows application and selecting “Client” under the “status” option on the “Admin” main menu. On the “Client Status Information” dialog box, highlight the client you wish to disconnect and select “View.” On the “Client Detail Information” dialog box, use the “Drop Connections” option to drop all current connections for this client. This will free up one or more user licenses. 2. Or, obtain a larger user licensed copy of the NetWare NLM.
43	The TSA Windows application was used to drop the connection for this client.	Determine why the Tserver administrator dropped the client connection.
44	The Tserver could not find a version stamp on the Security Database files.	There is a serious problem with the files that make up the Tserver security database. Call your support number.
45	The Tserver found old, out of date version stamps on the security database files.	There is a serious problem with the files that make up the Tserver security database. Call your support number.
46	The Tserver received a bad SPX packet so the client connection was dropped.	SPX reported a problem on this connection; try again. If this happens repeatedly, call your support number.

47	The Tserver rejected a user's request to open an ACS stream, so the connection was dropped.	An error code should have been returned in response to the ACSOpenStream() request in the ACSUniversalFailureConfEvent. Follow the procedures defined for that error code.
48	An attempt was made to open a second TSA ACS stream to the Tserver TSA driver when there was already an established stream to this driver. The Tserver only allows one open Tserver TSA driver stream at a time. NOTE: Multiple TSA streams to other drivers are allowed.	Determine who else is running the NetWare Telephony Services TSA Windows application. Determining who else is running the TSA application has to be done without the aid of the Tserver.
49	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the device is not a member of the Secondary Device Group of the Home Worktop Record. • The Access Group in the "Classes of Service" administration in this user's record which corresponds to the action being attempted (Call Control or Device/Device Monitoring) is empty or the device is not a member of this access group. • If the user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop) then the Primary Device ID of the "Away" Worktop Record does not match the device and the device is not a member of the Secondary Device Group (or this secondary group is blank) of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through one of the "Classes of Service" (user administration)

50	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any worktop. • The device is not on the Call Control Access Group in the "Classes of Service" administration in this user's record. • If the user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop) then the Primary Device ID of the "Away" Worktop Record does not match the device and the device is not a member of the secondary Device Group (or this secondary group is blank) of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through the Call Control Access Group Classes Of Service (user administration).

51	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device lD of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any worktop • The Access Group in the "Classes of Service" administration in this user's record which corresponds to the action being attempted (Call Control or Device/Device Monitoring) is empty. • The user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop as defined by the LAN Address fields) and the Primary Device ID of the "Away" Worktop Record does not match the device and the device is not a member of the Secondary Device Group of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the user's worktop record (worktop administration) or through one of the "Classes of Service" (user administration).
52	The Telephony Server rejected a user's request to control a device because the device is not a member of the Routing Access Group in the Classes Of Service administration in this user's record.	Change the user's administration so that the user has permission to control the device through the Routing Access Group "Classes of Service (user administration).

53	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any worktop. • The device is not member of the Device/Device Monitoring Access Group in the "Classes of Service" administration in this user's record. • If the user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop) then the Primary Device ID of the "Away" Worktop Record does not match the device and the device is not a member of the Secondary Device Group (or this secondary group is blank) of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through the Device/Device Monitoring Access Group "Classes of Service" (user administration).
54	The Telephony Server rejected a user's request to monitor a device because the device is not a member of the Call/Device Monitoring Access Group in the "Classes of Service" administration in this user's record.	Change the user's administration so that the user has permission to control the device through the Call/Device Monitoring Access Group "Classes of Service" (user administration).
55	The Telephony Server rejected a user's request to monitor a device because the Allow option for Call/Call Monitoring Access Group in the "Classes of Service" administration in this user's record is not enabled.	Enable the Allow option for Call/Call Monitoring Access Group in the "Classes of Service" administration in this user's record (user administration).

56	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group of the Home Worktop Record is empty. • The Access Group in the "Classes of Service" administration in this user's record which corresponds to the action being attempted (Call Control or Device/Device Monitoring) is empty or the device is not a member of this access group. • If the user is not working from his or her Home Worktop (that is, the ACS stream has been opened from an worktop other than the Home Worktop) then the Primary Device ID of the "Away" Worktop record does not match the device and the device is not a member of the Secondary Device Group (or this secondary group is blank) of the "Away" Worktop record.	Change the user's administration so that the user has permission to control the device through either the Worktop record (worktop administration) or through one of the "Classes of Service" (user administration).

57	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any worktop • The Call Control Access Group in the 'Classes of Service" administration in this user's record is empty. • If the user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop) then the Primary Device ID of the "Away Worktop Record does not match the device and the device is not a member of the Secondary Device Group (or this secondary group is blank) of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through the Call Control Access Group 'Classes of Services" (user administration).

58	The Tserver rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any Worktop. • The Access Group in the "Classes of Service" administration in this user's record which corresponds to the action being attempted (Call Control or Device/Devive Monitoring) is empty or the device is not a member of this access group. • The user is not working from his or her home worktop (i.e., the ACS stream has been opened from an "Away" Worktop as defined by the "LAN Address" field) and the Primary Device ID of the "Away" Worktop Record does not match the device and the Secondary Device Group of the "Away" Worktop Record is empty.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through one of the "Classes of Service" (user administration).
59	The Telephony Server rejected a user's request to control a device because the "Routing Access Group" in the "Classes of Service" administration in this user's record is empty.	Change the user's administration so that the user has permission to control the device through the "Routing Access Group" in "Classes of Service" (user administration) by specifying a Device Group for the Routing Access Group.

60	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty. or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any worktop • The Device/Device Monitoring Access Group in the "Classes of Service" (user administration) in this user's record is empty. • If the user is not working from his or her Home Worktop (that is, the ACS stream has been opened from an "Away" Worktop) then the Primary Device ID of the "Away" Worktop Record does not match the device and the device is not a member of the Secondary Device Group (or this Secondary Group is blank) of the "Away" Worktop Record.	Change the user's administration so that the user has permission to control the device through either the worktop record (worktop administration) or through the Device/Device Monitoring Access Group under "Classes of Service" (user administration).
61	The Telephony Server rejected a user's request to control a device because the Call/Device Monitoring Access Group in the "Classes of Service" administration in this user's record is empty.	Change the user's administration so that the user has permission to control the device through the Call/Device Monitoring Access Group under "Classes of Service" (user administration).

62	The Telephony Server rejected a user's request to control a device because all of the following are true: • The Primary Device ID of the user's Home Worktop Record does not match the device and the Secondary Device Group is empty, or The "Home Worktop Device ID" and "LAN Address" fields are blank in the user's record indicating the user is not associated with any Worktop. • The Access Group in the "Classes of Service" administration in this user's record which corresponds to the action being attempted (Call Control, Device/Device Monitoring, Call/Device Monitoring or Routing) is empty. • The user is sitting at his or her home worktop (as defined by the LAN Address in the worktop record associated with this user).	Change the user's administration so that the user has permission to control the device through either the user's worktop record (worktop administration) or through one of the "Classes of Service" (user administration).
63	One of the device lists in a user record is empty. This error is never returned directly in an ACS message, but is translated to a more specific error code.	This error should never be returned to an application or appear in the Tserver error logs. If this event is generated by the Tserver, then there is a software problem with the Tserver. Call your support number.
64	A CSTAGetDeviceList query was made with a bad CSTALevel_t value. Valid CSTALevels are: CSTA_HOME_WORK_TOP 1 CSTA_AWAY_WORK_TOP 2 CSTA_DEVICE_DEVICE_MONITOR 3 CSTA_CALL_DEVICE_MONITOR 4 CSTA_CALL_CONTROL 5 CSTA_ROUTING 6 CSTA_CALL_CALL_MONITOR 7	The application has called CSTAGetDeviceList with an invalid device level. Call the application support number.
65	The ACS stream was torn down because the PBX driver associated with this stream terminated and unregistered with the Tserver.	Verify that the driver unregistered. If it did not, call your support number.

66	The Tserver has received a message from the client or the PBX driver over a stream which has not been confirmed. The PBX driver may have rejected the ACSOpenStream request or violated the protocol by not returning an ACSOpenStreamConfEvent.	1. The Tserver will terminate this stream when this error occurs. Verify that the application waits for an ACSOpenStreamConfEvent before it makes any further requests. 2. If the application is written correctly, Call your support number.
67	The Tserver has dropped the current Tserver TSA application connection per the request of a Tserver administrator.	Determine why the Tserver administrator dropped the connection.
68	The Tserver has determined that NetWare has been trying to retransmit an ECB to a client for an extended period of time. Since the ECB cannot be sent, the Tserver has dropped the client connection.	Something is wrong with the SPX connection. Call your support number.
76	The Tserver TSA application attempted to set the high water mark for the TSDI size to a value that was larger than the TSDI size itself.	The TSA application should have prevented the user from entering a TSDI size that was smaller than the high water mark. This error indicates a problem with the TSA application itself.
77	The Tserver TSA application attempted to set the number of ECBs of a specific type (Connect, Send, or Listen) for a driver below the minimum number allowed for a driver. The minimum allowed number of ECBs of a specific type is 5.	The TSA application should have prevented the user from entering an ECB value that was too low. This error indicates a problem with the TSA application itself.
78	The Tserver TSA application attempted delete driver resource information for a driver which had no record in btrieve file tsrvrsrc.dta. The tsrvrsrc.dta is the btrieve file which stores resource information for drivers.	The TSA application should have prevented the user from trying to delete information for this driver. This error indicates a problem with the TSA application itself.

Index

Index

A

C

D

E

F

H

I

L

M

O

P

Q

R

S

T

U

V

W