

Lucent Technologies Bell Labs Innovations

# PassageWay® Telephony Services for Windows NT® Release 2.22

# Network Manager's Guide Issue 3.0

Lucent Technologies - Formerly the systems and technology units of AT&T

### Copyright © 1997 Lucent Technologies Inc. All Rights Reserved Printed in U.S.A.

#### Notice

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

#### Your Responsibility for Your System's Security

You are responsible for the security of your system. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use. To prevent unauthorized use of this product, it is your responsibility to ensure that you and/or your system administrator read all documents provided with this product to fully understand the features available that may reduce your risk of incurring charges. Lucent Technologies also recommends that you and/or your system administrator refer to the *BCS Products Security Handbook* (555-025-600) for a detailed explanation of security risks and the measures that can be taken to prevent external telecommunications fraud.

#### Trademarks

PassageWay is a registered trademark of Lucent Technologies.

Btrieve is a registered trademark and IPX is a trademark of Novell, Inc.

Microsoft, DOS, Windows, Windows NT, and the Microsoft logo are registered trademarks and Windows 95 is a trademark of Microsoft.

OS/2 is a registered trademark of International Business Machines Corporation.

Pentium is a registered trademark of Intel Corporation.

All products and company names are trademarks or registered trademarks of their respective holders.

#### Lucent Technologies Fraud Intervention

If you *suspect you are being victimized* by toll fraud and you need technical support or assistance, call BCS National Service Assistance Center at **1 800 628-2888**.

#### Warranty

Lucent Technologies provides a limited warranty on this product. Refer to the "Lucent Technologies Network Software License Agreement" provided with your package.

#### Disclaimer

Any reference within this text to American Telephone and Telegraph Corporation or AT&T should be interpreted as reference to Lucent Technologies. The exception is cross-references to books published prior to December 31,1996, which retain their original AT&T titles.

#### Acknowledgment

This document was prepared by the Business Communications Systems Product Documentation Development Group, Lucent Technologies, Middletown, NJ -7748.

# **C**ontents

About This Guide	1
User Responsibilities	1
Customer Support	1
Document Organization	1
Conventions Used in this Document	2
Symbolic Conventions	2
Typographic Conventions	
Online Documentation	
Related Documents	
1 Introducing Telephony Services	5
Computer Telephony Integration	5
Major Components of Telephony Services	8
Running a Telephony Services Application	9
Establishing a Connection	9
Using a Connection	9
Terminating the Connection	10
Telephony Services Terminology	11
2 Telephony Objects and the Security Database	
Security Database Objects	16
The User Object	17
Login	17
Name	17
Worktop Name	
Class of Service	
Administration Privileges	19
The Worktop Object	19
Worktop Name	20
Primary Device ID	20
Secondary Device Group	

LAN Addresses - IP Address	
The Device Object	
Device ID	
Location	
Device Type	
Tlink Group	
The Device Group Object	
The Tlink and Tlink Group Objects	
Tlink Groups	
How Tlinks and Tlink Groups are Used	
Associating a Device with a Particular PBX	
Load Balancing	
Object Administration	
Underlying Database Support	
Using the TSA or TSA32 to Administer Your SDB	
Bulk Administration	
SDB Upgrades	
Version Information	
SDB Logging	
Line Format	
Sample File	
File Wrap-around	
Controlling User Access to Telephony Services	
Terminology	
Granting User Permissions	
Extending User Access to Other Worktops	
Class of Service Options	
Call Control	
Device/Device Monitoring	
Call/Device Monitoring	
Call/Call Monitoring	
Routing	
Sample Configurations	
Users Only Control Devices on Their Own Worktops	46
Manager/Assistant Configuration	47
Call Monitoring Application	40
Portion of User Community Shares Worktops	
Portion of User Community Shares Worktops Prompted Digits	

4 Using the TSA to Administer the Security Database	
Telephony Services Administrator (TSA)	
Starting the TSA Application	
The TSA Menu Bar	
Using Ouick Add	
Administration of System-wide Features	
Controlling SDB Administration Access	
Setting Up an Admin Access Group	
Admin Access Group Rules	
Administering Admin Access Groups	
Creating an Admin Access Group	
Editing an Admin Access Group	
Viewing an Admin Access Group	
Deleting an Admin Access Group	
Administering Allowed Users	74
Order for Administration of Telephony Objects	
Administering Tlinks	77
Accessing Tlink Information	79
Creating a Tlink	
Editing a Tlink	
Viewing a Tlink	
Deleting a Tlink	
Administering Tlink Groups	
Creating a Tlink Group	
Editing a Tlink Group	
Viewing a Tlink Group	
Deleting a Tlink Group	
Administering Devices	
Creating a Device	
Editing a Device	
Viewing a Device	
Deleting a Device	
Administering Device Groups	
Creating a Device Group	
Editing a Device Group	
Viewing a Device Group	
Deleting a Device Group	
Administering Worktops	
Creating a Worktop	
Editing a Worktop	
Viewing a Worktop	

Deleting a Worktop	116
Administering Users	117
Accessing User Information	118
Creating a User	119
Editing a User	121
Viewing a User	122
Deleting a User	123
SDB Logging	124
Using the TSA to Set SDB Log Settings	124
5 Using the TSA32 to Administer the Security Database	125
Telephony Services Administrator (TSA32)	126
Starting the TSA32 Application	127
TSA32 Features	129
The TSA32 Menu Bar	129
The TSA32 Tool Bar	130
The TSA32 SDB Window	131
SDB Tree View	131
SDB Object View	131
Tips for Using the TSA32	132
Creating Objects	132
Selecting Objects	132
Submitting New or Changed Object Information	133
Deleting Objects	134
Using Quick Add	135
Administration of System-wide Features	138
Controlling SDB Administration Access	140
Setting Up an Admin Access Group	141
Admin Access Group Rules	143
Administering Admin Access Groups	143
Creating an Admin Access Group	144
Administering Allowed Users	145
Editing or Viewing an Admin Access Group	147
Deleting an Admin Access Group	149
Order for Administration of Telephony Objects	150
Administering Tlinks	152
Creating a Tlink	154
Viewing a Tlink	155
Deleting a Tlink	156
Administering Tlink Groups	157
Creating a Tlink Group	157

Editing or Viewing a Tlink Group	.158
Deleting a Tlink Group	.161
Administering Devices	.162
Creating a Device	.163
Editing or Viewing a Device	.164
Deleting a Device	.166
Administering Device Groups	.167
Creating a Device Group	.168
Editing or Viewing a Device Group	.170
Deleting a Device Group	.172
Administering Worktops	.173
Creating a Worktop	.174
Editing or Viewing a Worktop	.176
Deleting a Worktop	.177
Administering Users	.178
Creating a User	.179
Editing or Viewing a User	.182
Deleting a User	.184
SDB Logging	.185
Using the TSA32 to Set SDB Log Settings	.185
6 Bulk Administration	.187
Administering Your SDB	.187
Bulk Administration Applications	.187
Adding Telephony Services Objects to your Security Database for the First Time	.188
Making Bulk Changes to an Existing SDB	.189
Printing the Contents of the SDB	.190
Updating Your SDB Automatically	.191
Migrating from a NetWare Telephony Server to a Windows NT Telephony Server	
Examining Bulk Administration Files	192
Examining Duk Administration Thes	192 .193
The Flat File	192 .193 .193
The Flat File	192 .193 .193 .193
The Flat File Section Headers Data Lines	192 .193 .193 .193 .194 .195
The Flat File Section Headers Data Lines Multi-valued Attributes	192 .193 .193 .193 .194 .195 .197
The Flat File Section Headers Data Lines Multi-valued Attributes Flat File Section Types	192 .193 .193 .194 .194 .195 .197 .198
The Flat File     Section Headers     Data Lines     Multi-valued Attributes     Flat File Section Types     The Error File	192 .193 .193 .194 .195 .197 .197 .198 .199
The Flat File Section Headers Data Lines Multi-valued Attributes Flat File Section Types The Error File Correcting Non-Fatal Errors	192 .193 .193 .194 .195 .197 .198 .199 .201
Examining bulk Administration Thes     The Flat File     Section Headers     Data Lines     Multi-valued Attributes     Flat File Section Types     The Error File     Correcting Non-Fatal Errors     Correcting Fatal Errors	192 .193 .193 .194 .195 .197 .197 .198 .199 .201 .202
Examining bulk Administration Thes     The Flat File     Section Headers     Data Lines     Multi-valued Attributes     Flat File Section Types     The Error File     Correcting Non-Fatal Errors     Correcting Fatal Errors     The Simple File	192 .193 .193 .194 .195 .197 .198 .199 .201 .202 .203
Examining bulk Administration Files     The Flat File     Section Headers     Data Lines     Multi-valued Attributes     Flat File Section Types     The Error File     Correcting Non-Fatal Errors     Correcting Fatal Errors     The Simple File     Using the Simple File for Quick Adds	192 .193 .193 .193 .194 .195 .197 .197 .198 .199 .201 .202 .203 .205

Rules For Creating a Simple File	207
Errors Encountered While Processing a Simple File	
Automating the SDB Interface	211
Order of Data Lines in the Flat File	211
Adding Objects to the SDB	213
Modifying Objects in the SDB	213
Deleting Objects from the SDB	214
General Rules	215
Updating from the Flat File	216
Using Bulk Administration	217
Adding Telephony Services Objects to Your SDB for the First Time	217
Making Bulk Changes to Your SDB	218
Printing Data in Your SDB	220
Updating Your SDB Automatically	221
Invoking Bulk Administration	222
Creating Templates	223
Creating Templates Using the TSA	223
Creating Templates Using TSA32	224
Creating a Flat File from the Security Database	225
Backing up the SDB Using the TSA	225
Backing up the SDB Using TSA32	226
Updating the Security Database	227
Updating the SDB Using the TSA	228
Updating the SDB Using TSA32	230
Upgrading the Security Database	232
Upgrading the SDB Using the TSA	232
Upgrading the SDB Using TSA32	233
Object Attribute Tables	234
User Object Attributes	235
Worktop Object Attributes	236
Device Object Attributes	236
Device Group Object Attributes	237
Tlink Object Attributes	237
Tlink Group Object Attributes	237
Admin Group Object Attributes	238
SDB Manual Pages	239
sdbUpdateDataBase()	239
SDBUpdateDataBaseConfEvent	243
sdbBackupDataBase()	245
SDBBackupDataBaseConfEvent	247
SDBUniversalFailureConfEvent	

7 TCP/IP Configuration	
I AN Connectivity	253
Client Software Modules	255
TCP/IP	255
Server Configuration	256
Win16 and Win32 Client Configuration	257
OS/2 Client Setup	258
UnixWare and HP-UX Client Setup	259
TCP/IP and Tserver Feature Interactions	
Extended Workton Access	
Automatic Administration of LAN Addresses	
TCP Preferred Naming Format	
Using the TSA to Administer TCP/IP	
Using TSA32 to Administer TCP/IP	
TCP/IP Status	
Using the TSA to Display TCP/IP Status	
Using TSM32 to Display TCP/IP Status	
User Authentication	
Single Login Authentication	
Local Login Authentication	
Assigning User Rights	
Distinguishing Users In Different Windows NT Domains	
8 The Tserver	
Telephony Server Software	
Telephony Server Modules	
Telephony Server Options	
Pop-Up Alarms	
Using the TSA to Enable Pop-Up Alarms	
Using the TSM32 to Enable Pop-Up Alarms	
Name Server Advertising	
Using the TSA to Enable Name Server Advertising	
Using the TSM32 to Enable Name Server Advertising	
Version and System Status Information	
Using the TSA to View Version Information	
Using the TSA32 to View Version Information	
Using the TSM32 to View Version Information	
Loading and Unloading PBX Drivers	
Driver DLL Information	
Using the TSA to Display Driver DLL Information	298

Using the TSM32 to Display Driver DLL Information	
Adding DLLs	
Removing DLLs	
Loading and Unloading DLLs	
Configuring a DLL for Auto Load	
Tserver Status	
Using the TSA to View Tserver Status Information	
Using the TSA32 to View Tserver Status Information	
Using the TSM32 to View Tserver Status Information	
Resetting the Refresh Rate	
Tlink Status	
Using the TSA to View Resource Information	
Viewing Detailed Information	
Viewing Summary Information	
Using the TSM32 to View Resource Information	
Viewing Detailed Information	
Viewing TSDI Resource Information	
Viewing TCP/IP Information	
User Status	
Using the TSA to View Status Information	
Using the TSM32 to View Status Information	
Dropping a User Connection	
Using the TSA to Drop a User Connection	
Using the TSM32 to Drop a User Connection	
9 Telephony Services Traffic Measurement	
Measuring Traffic	
Telephony Services Traffic Viewer	
System Level Settings	
Tserver Traffic Settings and Reports	
Tserver Settings/Current Report	
Tserver History Report	
Tlink Traffic Settings and Reports	
Tlink Settings	
Tlink Traffic Reports	
Tlink Current Report	
Tlink History Report	
TSDI History Report	
Reset Current Measurements	

Traffic Reports	
Traffic Log	
Sample Traffic Log	
Measurement Alarms	
10 The Cserver	
Flow Control	354
Cserver Status Information	355
Client Statistics	355
CSDI Memory Allocation	358
Buffer Usage	359
Message Traffic	
Semaphores	
Internal Buffer Sizes	
Displaying Cserver Status Information	
Using the TSA to View Cserver Status Information	
Using TSM32 to View Cserver Status Information	
Error Logging	
Cserver Message Tracing	
11 Troubleshooting	
Problem Areas for Troubleshooting	
Common Tserver Problems	
Tserver Authentication Problems	
Tserver Initialization Problems	
Tserver Not Listed as a Service	
Tserver Uninstalled While Still Running	
Tserver Hangs While Trying to Access Novell NT Requester	
Problems Opening a Stream	
Problems Accessing a Device	
Problems Loading a Driver	
Application Problems	
Changing User Permissions	
Using the TSA to Assign Full User Permissions	
Using the TSA32 to Assign Full User Permissions	
Checking Version Information	
Using the TSA to View Version Information	
Using the TSA32 to View Version Information	
Using the TSM32 to View Version Information	
Automatic Administration of LAN Addresses	

SDB Database Engine is not Working Properly	
SDB is Unavailable	
Slow Performance	
Troubleshooting Mechanisms	
General Logging Information	
Maximum Log Size	
Last Log Record	
Current Log Offset and Decreasing the Size of a Log File	
Error Log Entry Format	
Increasing the Size of the Message Trace File	
Message Trace Format	
Viewing the Log Files	
Tserver Error Log	
Selecting the Correct Severity Level	401
Reporting Errors	401
Turning on Error Logging	403
Using the TSA to Select Error Logging Destinations	403
Using the TSM32 to Select Error Levels	404
Tserver Message Tracing	405
Turning On Tserver Message Tracing	
Using the TSA to Enable Message Tracing	407
Using the TSM32 to Enable Message Tracing	
Cserver Message Tracing	410
Turning On Cserver Message Tracing	411
Using the TSA to Enable Cserver Message Tracing	412
Using the TSM32 to Enable Cserver Message Tracing	413
Log File Sizes	414
Using the TSA to Administer Log and Trace File Sizes	414
Using the TSA32 to Administer the SDB Log File Size	414
Using the TSM32 to Administer the Error Log File Size	415
Using the TSM32 to Administer the Tserver Trace File Size	415
Client Message Tracing (TS Spy)	416
Starting TS Spy	416
TS Spy Menu Options	
TS Spy File Logging	
Activating File Logging	
Deactivating File Logging	
TS Spy Individual Connection Tracing	
TS Spy Client Library Model	
TS Spy Trace Records	
TS Spy Error Records	430

Telephony Services Test Application (TSTest)	
Starting the Test Application	
Error Codes	
CSTA Universal Failure Events	
ACS Universal Failure Events	
Security Database Errors	453

# About This Guide

This document provides an overview of the Telephony Services product. The document also describes client and server applications, architecture, software components, and Tserver administration and maintenance operations. The troubleshooting section of this document describes the Tserver error log.

# **User Responsibilities**

You are assumed to be familiar with the operating systems of the server and workstation clients on which you are installing the Telephony Services software. If you are not, refer to the documentation for those systems.

# **Customer Support**

To reach the Lucent Technologies National Customer Care Center by telephone at any time, call:

800-242-2121

and follow the voice prompts for PassageWay Telephony Services.

# **Document Organization**

This guide is organized as follows:

- Chapter 1 introduces PassageWay Telephony Services, and discusses Computer Telephony Integration (CTI) and the Telephony Services components.
- Chapter 2 describes the organization of the SDB: the types of data objects it contains and the database engine used to store the data.
- Chapter 3 describes the permissions checking enforced by the Tserver.
- Chapter 4 describes how to use the TSA for SDB administration and for controlling maintenance and status parameters.

About this Guide 1

- Chapter 5 describes how to use TSA32 for SDB administration.
- Chapter 6 presents an in-depth discussion of the Bulk Administration feature.
- Chapter 7 gives details on TCP/IP configuration.
- Chapter 8 discusses Tserver administration and maintenance.
- Chapter 9 discusses the tools that track Tserver traffic and resource utilization.
- Chapter 10 discusses Cserver administration and maintenance. This chapter also discusses the tools that track Cserver traffic and resource utilization.
- Chapter 11 presents troubleshooting information, including an explanation of errors that users may encounter.

# **Conventions Used in this Document**

# **Symbolic Conventions**



The note symbol provides additional information about the topic currently under discussion. This information is not required in order to run your system.

The checklist symbol indicates a list of items that should be examined.

The important symbol is used to emphasize information that is necessary to correctly install or operate Telephony Services.



The procedure symbol indicates the beginning of a series of steps needed to install Telephony Services on your server or on a client workstation.

## 2 Installation Guide

# **Typographic Conventions**

This guide uses the following typographic conventions:

*italics* Words in italics refer to a document that contains additional information about a topic.
<Enter> Words within angle brackets represent a single key that should be pressed. These include <Enter> , <Insert> and <Delete>.

# **Online Documentation**

The CD-ROM containing the PassageWay Telephony Services for Windows NT software also includes the customer documents and the Adobe Acrobat Reader. If you use Adobe Acrobat to view a document online, set the default magnification to 133% for optimal viewing. (From the "Edit" menu, select "Preferences", then select "General". The "Default Magnification" option is in the "Viewing" area of the dialog box.)

# **Related Documents**

• PassageWay® Telephony Services for Windows Installation Guide

This guide contains information you need to properly install the Telephony Services for NT software on a Windows NT<sup>TM</sup> server and supported client workstations.

 PassageWay® Telephony Services for Windows NT DEFINITY® Enterprise Communications Server Network Manager's Guide

This document describes configuration, maintenance, and troubleshooting of the DEFINITY® G3 PBX Driver (G3PD) for Telephony Services. Information in this document is provided for telephony services administrators and the services organization that assists administrators when they experience problems with the G3PD.

• DEFINITY Communications System Generic 3 Implementation, 555-230-655

This document describes all G3 switch administration and maintenance procedures, including administering the ASAI (adjunct or ADJLK) link and CTI on your DEFINITY system.

 DEFINITY Communications System Generic 3 Installation, Administration, and Maintenance of CallVisor ASAI Over the DEFINITY LAN Gateway, 555-230-223

This document covers the CallVisor ASAI DEFINITY LAN Gateway system that provides ASAI functionality using Ethernet transport. It explains the tasks involved in installing, administering, and maintaining a DEFINITY LAN Gateway system.

♦ Product Security Handbook, 555-025-600

This document provides a detailed explanation of security risks and the measures that can be taken to prevent external telecommunications fraud.

4 Installation Guide

chapter

# **1** Introducing Telephony Services

Telephony Services allows you to integrate telephony monitoring and control with applications on enterprise-wide networks. One or more telephony servers 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."

# **Computer Telephony Integration**

Telephony Services accomplishes the integration of your telephone and PC without the need for special telephones, connectors, PC circuit packs, or new wiring at each client workstation. Client PCs that are already connected to a LAN do not require any new hardware. Hardware at the telephony server provides the physical link between the telephony server and the PBX, to which the users' telephones connect. The server hardware and software are the only incremental expenses required to provide an environment for integrated applications.

As shown in Figure 1-1, the telephone and the PC do not physically connect to each other. Instead, the Tserver logically integrates them.

Introducing Telephony Services 5

Figure 1-1 LAN and Telephony Network with Telephony Services Installed



Your PBX vendor provides three of the pieces in Figure 1-1: a CTI link (wire that physically connects the telephony server and the PBX); a CTI adapter in the telephony server; and the PBX driver (a software module that resides on the telephony server). 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 telephone calls.

The Telephony Services platform provides software modules that reside on the telephony server and on each client workstation. Figure 1-2 shows these modules as shaded areas on the telephony server and client workstation.

6 Network Manager's Guide



Figure 1-2 Telephony Services Components

Applications that you purchase separately may reside on either a server or individual client workstations. These applications use Telephony Services to establish an authorized connection to the telephony server and to send telephony control messages to the PBX. For example, an application running on a client workstation can establish a connection and then request that the PBX place a telephone call from one endpoint to another or monitor call activity at a telephone.

In Telephony Services Release 2.22 for Windows NT, clients and servers use TCP/IP as the transport mechanism.

Introducing Telephony Services 7

# **Major Components of Telephony Services**

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

The major components of Telephony Services are:

- The Tserver This component resides on the telephony server and acts as a conduit from individual client/server applications to the PBX. It routes return messages from the PBX to the client/server that expects them. It also ensures that users log in using a valid login and password and that they have the permissions to do what they are requesting.
- The Security Database (SDB) This is the Telephony Services database that stores information about users and the devices they control. The Tserver uses this information in its permission checking. Administrators can control user access to Telephony Services by placing restrictions on the types of requests users can make. Telephony Services Release 2.22 uses Btrieve for the database engine (the underlying software that controls the data) for the SDB.
- Telephony Services Library (TSLIB) This is a set of functions that acts as an interface between client or server applications and the Tserver. When a user starts a telephony application, the application uses these functions to establish an authorized connection with a particular telephony server and to send telephony control messages to the PBX. The messages sent by the telephony application conform to the Telephony Services Application Programming Interface (TSAPI).

The PBX driver also resides on the telephony server. It receives TSAPI messages from the Tserver and routes them to the PBX over CTI links, performing any necessary conversions in the process. It receives messages from the PBX, reformats them, and sends them back to the Tserver. The PBX driver is supplied by your PBX vendor.

# **Running a Telephony Services Application**

Once you have set up your telephony server, you can run applications on client workstations or on other servers. Before an application can run, it must establish a connection with the Tserver. Once this has been done successfully, the application sends messages to the Tserver using this connection. Messages are forwarded by the Tserver to the PBX driver and ultimately, to the PBX. When you terminate the application, the connection between the Tserver and the application is ended.

## **Establishing a Connection**

When you start your application, it attempts to open a connection to a Tserver. This involves communication between the Tserver and the TSLIB on your workstation. You will be prompted to choose an available service (Tlink) and to provide login and password information. If all security checks pass, a connection is established and your application can send messages to the Tserver and begin processing telephony requests.

# Using a Connection

Suppose your application is designed to let you call people in your personal directory by selecting their name. The application also gives you information about incoming calls. To do this, the application places a device monitor on your telephone, requesting that Telephony Services provide detailed notification of the stages of calls made to and from your phone.

Introducing Telephony Services 9

When you make an outgoing call, the application looks up the destination telephone number and issues a request to make the call. This is sent across the connection you made with the Tserver. The Tserver checks to make sure you are allowed to make calls on this device and, if you are, forwards the call request to the PBX driver. The PBX driver converts the message to the protocol used by your PBX. This message is sent to the PBX over the CTI link. The PBX then sets up the call, sending monitor reports back to the PBX driver as events occur, such as when the destination phone is alerting, when it answers, and so on. The PBX driver reformats messages from the PBX into TSAPI messages and sends them to the Tserver. The Tserver receives these messages from the PBX driver and distributes them to the appropriate clients.

# **Terminating the Connection**

When you exit the application, the connection that you were using is closed and any system resources that you were using become available for others to use.

# **Telephony Services Terminology**

The following terms are used to describe Telephony Services:

- Admin Access Group: A group of Telephony Services users with administration privileges. Group members may have permission to administer either all or only some of the Telephony Server's components.
- ◆ Authentication: The process by which the Tserver determines if a user attempting to establish a connection has provided a valid login ID and password. The login ID and password are always those of a Windows NT Workstation or Server user account (the login IDs must be administered in the Telephony Services Security Database and in the Windows NT user database). See Chapter 7 for details.
- Computer Telephony Integration (CTI): The integration of services provided by a telephone and a computer.
- Computer Supported Telecommunications Applications (CSTA): : A CTI standard established by ECMA, the European Computer Manufacturers' Association.
- CTI Link: The physical connection between a telephony server and a PBX.
- Monitoring: A mechanism for informing clients or applications of events that have occurred on the PBX. Examples of these events include notification of an incoming call, a call being answered, put on hold and so on. Monitor reports include information that allows applications to pop screens or collect statistics.
- **Operation, Administration and Maintenance (OAM)** : The generic term used to describe the administration of Telephony Services information. This includes the administration of SDB objects, Tserver maintenance parameters, and PBX-specific parameters.

Introducing Telephony Services 11

- ◆ **PBX Driver**: A PBX-specific software module that provides the interface between the telephony server and the PBX. The PBX driver receives TSAPI messages from the Tserver on a Tlink, reformats the message into a set of messages understood by the PBX, and sends the reformatted message to the PBX over a CTI link.
- **Private Branch Exchange (PBX)**: The telephone switch that connects users' telephones to the local Central Office.
- Security Database (SDB): The database of information that the Tserver uses to enforce permission restrictions set by the administrator.
- Stream: The logical connection between a client application and a Tserver. A stream is established at the request of the client application. All telephony requests made by the application are sent on this connection.
- **Telephony Server**: A server that has the Telephony Services software installed. More than one telephony server can exist on a LAN.
- **Telephony Services Administrator** (**TSA**): The 16-bit Windows application that allows the system administrator to enter information for the SDB. This application also supports maintenance and status operations for the Tserver.

The functionality of the TSA is equivalent to the combined functionality of the TSA32 plus the TSM32.

- Telephony Services Administrator (TSA32): The 32-bit Windows NT and Windows 95 application that allows the system administrator to enter information for the SDB. On 32-bit platforms, Tserver maintenance and status operations are accessed through the TSM32.
- Telephony Services Maintenance (TSM32): The 32-bit Windows NT and Windows 95 application that allows the system administrator to view and modify maintenance and status parameters (such as Error Logging, Message Tracing, or Tlink Information).
- ◆ Tlink: The name of a service provided by a Tserver. Client applications must connect to the specific service that provides the required functionality. The two types of services are CSTA services (for call control functions) and OAM services (for administrative functions). A Tlink name is made up of four components separated by pound signs. A Tlink name has the following format:

#### VENDOR#DRIVER#SERVICE#SERVERNAME

- Tlink Group: A Tlink Group is a collection of CSTA Tlinks. You can use Tlink Group objects to restrict PBX access.
- **TSAPI (Telephony Services Application Programming Interface)** : The interface used by applications to make telephony requests. These requests include call control requests (make a call, transfer a call), monitor requests (trace a call), and routing requests.
- **Tserver**: The program that resides on a server and receives TSAPI messages from client and server applications. These messages are checked for permissions and, if allowed, forwarded to the PBX driver.
- Worktop: A worktop represents a desktop equipped with a client workstation, a telephone (known as the worktop's Primary Device), and any number of additional telephony devices (such as a fax machine or a modem).

Users can always control and monitor all the devices associated with their worktop, even if they are logged in from a different worktop.

chapter

# **2** Telephony Objects and the Security Database

The Telephony Services Security Database (SDB) stores information about users and the devices they control. The Tserver uses this information in its permission checking. Administrators can control user access to Telephony Services by placing restrictions on the types of requests users can make. Telephony Services Release 2.22 uses Btrieve for the database engine (the underlying software that controls the data) for the SDB.

The purpose of the SDB is to specify the following:

- Who is authorized to use Telephony Services
- Which devices authorized users can access
- The types of telephony requests authorized users can perform on those devices

There are two applications available for administering the SDB. Chapter 4 discusses the Telephony Services Administrator for 16-bit platforms (TSA). Chapter 5 discusses the Telephony Services Administrator for 32-bit platforms (TSA32).

Telephony Objects and the Security Database 15

# **Security Database Objects**

All the information that Telephony Services needs to route messages and control access to the telephony network is stored in the SDB in the form of objects. The object types are Tlink, Tlink Group, Device, Device Group, Worktop, User, and Admin Access Group.

Each object has a set of attributes that describe the object. For example, the Worktop object represents a user's desktop.

The following diagram shows how the basic objects relate to your Telephony Services installation. Users (not shown) are the people who sit at the Worktops.



The following sections describe the object types and give examples of how you can set up your administration to best match the needs of your organization. Chapter 3 discusses controlling access to Telephony Services. Detailed instructions on entering the data can be found in Chapters 4 and 5.

16 Network Manager's Guide

# The User Object

	A user is a person who logs in and runs a Telephony Services application. This user has assigned permissions that control what the user is allowed to do. (Permissions are discussed in detail in Chapter 3.) A worktop is usually associated with each user to indicate that the user is authorized to control the devices on their desktop. Typically, there is one worktop for each Telephony Services user. You can, however, associate more than one user with a worktop. For example, if you have a call center that has three shifts and operates 24 hours a day, you can associate three different users with the same worktop. Each user would have an individual login, and the characteristics of the worktop remain the same. You must create a user object for each person who will use Telephony Services applications.
	The following paragraphs discuss user attributes.
Login Name	The login is the same as a user's Windows NT username. The login must exist in both the SDB and the Windows NT user database.
	This is an optional text field that identifies the user.

#### Worktop Name

The Worktop Name attribute specifies the user's worktop. A user can always control and monitor all the devices associated with this worktop, regardless of which worktop he/she is currently using.

- A worktop may be assigned to more than one user.
- A user does not need to have a worktop. However, a user with no worktop will require Class of Service permissions in order to access Telephony Services.

# **Class of Service**

This collection of attributes allow you to customize permissions for each user. See Chapter 3 for more details. The collection includes:

- Call Control Services
- Monitoring Services
  - Device/Device monitoring
  - Call/Device monitoring
  - Call/Call monitoring
- Routing Services

Call/device monitoring, call/call monitoring, and routing permissions may only be granted through administered Class of Service options.

#### **Administration Privileges**

This collection of attributes contains a user's administration privileges. You can specify whether each user is a member of an Admin Access Group and whether each user is allowed to administer Admin Access Groups.

The default value for these user attributes provides *no* administration privileges. In order to provide privileges, you assign users to an Admin Access Group. The values for the user attributes come from the following fields:

- Administration Access Group: This field is the group of administration modules that the user is allowed to access.
- Allow User to Administer Admin Access Groups: This field indicates whether the user can edit the Admin Access Group information.

For details about these attributes, see the section titled "Administering Admin Access Groups" in Chapter 4 (for TSA information) or Chapter 5 (for TSA32 information).

# The Worktop Object

The Worktop object represents a user's desktop equipped with a client workstation, a telephone (known as the worktop's Primary Device), and any number of additional telephony devices (such as fax machines or modems). These additional devices are specified through the worktop's Secondary Device List. The telephone extension is the Primary Device ID attribute in the Worktop object. Other Worktop attributes include an IPX/SPX and/or TCP/IP network address.

The following paragraphs discuss worktop attributes.

Telephony Objects and the Security Database 19

#### Worktop Name

The worktop name uniquely identifies a worktop. You can name a worktop by its function or by the person who normally uses the worktop. For example, you could name the worktop "Joe's Worktop" or "help desk 1."

#### **Primary Device ID**

The primary device ID is the PBX extension of the telephone on the worktop.

## Secondary Device Group

This is a group of devices (in addition to the primary device) that are associated with the worktop or are shared among several worktops, such as fax machines. Users assigned to this worktop have permission to control and monitor all devices in this group.

## LAN Addresses - IP Address

The network address is the unique identifier of a workstation on the LAN. TCP/IP and IPX/SPX addressing information can be entered in the database. (This release supports only TCP/IP connectivity, although IPX/SPX addresses may be entered in the SDB.).

If you do not want to manually administer the network address for each worktop, you can take advantage of the **Automatic Administration of LAN Addresses**. For more details, refer to the section titled "Administration of System-Wide Features" in Chapter 4 (for TSA information) or Chapter 5 (for TSA32 information).



LAN address information is used **only** when the "Extended Worktop Access" feature is enabled. For more information about this feature, see Chapter 3.
## The Device Object

	The Device Object contains information about a telephony device. Most commonly, a device is a telephone, but devices may also include fax machines, modems, hunt group extensions, or any other device that your PBX controls.
	The following paragraphs discuss device attributes.
Device ID	
	This attribute contains the ID for a device as it is known to your PBX. For example, on most PBXs a telephone uses a 2- to 6-digit number to identify each telephone, modem or other telephony device. (This is not the full 7- or 10-digit number used by the public network.)
Location	
	This is an optional field to identify where the device is located.
Device Type	
	This is an optional field to identify the type of device represented by the object. It is meant to make device identification easier. Valid device types are "PHONE," "FAX," "MODEM," and "ACD." The default value is "PHONE."
Tlink Group	
	This is the list of Tlinks from which users are allowed to access the device. The default value is "Any Tlink." See the section "Tlink and Tlink Group Objects" in this chapter for more details.

Telephony Objects and the Security Database 21

#### The Device Group Object

A device group object contains the name of the group and the devices that make up the group. A device group might be a group of devices:

- in a call center or help desk operation,
- for which an application provides call routing,
- for which an application tracks incoming call statistics, or
- controlled by a user such as a fax or modem.

Device groups may be assigned to either a user or a worktop. You assign a device group to a user when you want to provide the user with permissions for controlling specific devices as well as assign the type of control that the user can exert. This type of control is called Class of Service.

Device groups are used in the worktop object to indicate resources that are shared among the worktop objects that contain the device group.

The attributes for a device group are the devices in the group and whether the device group is an exception group. Devices added to the group are selected from the administered devices for the Tserver.

If the group is designated as an exception group, the Tserver treats the entire group as if it contained every device *except for* those devices in the device group.

#### The Tlink and Tlink Group Objects

A Tlink is the name of a service provided by a Tserver. Client applications must connect to the specific service that provides the required functionality. The most common types of telephony services are:

SERVICE TYPE	SERVICE DESCRIPTION
CSTA	TSAPI services (for Telephony control and monitoring over CSTA links)
OAM	Tserver and PBX driver administration

A Tlink name is made up of four components separated by pound signs, and uses the following format:

#### VENDOR#DRIVER#SERVICETYPE#SERVERNAME

When a PBX driver is loaded, it registers with the Tserver, telling the Tserver what type of services it provides. These are usually CSTA services. Other software modules on the server, such as Telephony Services Administration, also register with the Tserver. These are OAM type services.

#### **Tlink Groups**

A Tlink Group is a collection of CSTA Tlinks. You can use Tlink Group objects to restrict PBX access.

When you associate a device with a Tlink Group, a user can only issue call control requests for that device on a connection set up on a Tlink in the Tlink Group.

If you have no such needs, you can assign the default Tlink Group, "Any Tlink," to all devices as you add them to your Security Database and **skip** the rest of this section. Continue with the section titled "Object Administration."

Telephony Objects and the Security Database 23

#### How Tlinks and Tlink Groups are Used

When a PBX driver is loaded, it tells the Tserver which Tlinks it supports. The Tserver in turn advertises these Tlinks on the network. When a user starts up an application at a client workstation, the application specifies which Tlink it should use. It may present a list of Tlinks to the user and prompt the user for a choice, or it may get the correct Tlink from an initialization file. The application then includes this Tlink in the request to establish a connection.

When the Tserver receives the establish connection request, it saves the Tlink name. Future application requests to control devices using this Tlink are checked by the Tserver. If the device can be accessed by this Tlink, the request goes through. If not, the request is rejected.

If you need the type of checking just described, you need to create groups of Tlinks. Each group is called a Tlink Group. You then associate a particular Tlink Group with each device, thus limiting access to the device to the Tlinks that are in that group. The following sections contain examples of how Tlink Groups are used.

#### Associating a Device with a Particular PBX

The most common use of Tlink Groups is to associate devices with a particular PBX. In this example, a single telephony server handles devices on two different PBXs. Since devices are connected to a specific PBX, you would create two Tlink Groups: "PBX1" and "PBX2." The "PBX1" Tlink Group would contain the Tlink labeled "PBX\_VNDR#CSTA1#CSTA#ALPHA" in Figure 2-1. Similarly, the "PBX2" Tlink Group would contain the Tlink labeled "PBX\_VNDR#CSTA2#CSTA#ALPHA".

You can assign the appropriate Tlink Group to each device. This has two advantages:

- You know by looking at the device object which PBX the device is connected to.
- If a user inadvertently selects the wrong Tlink when opening a connection, the Tserver returns an error immediately indicating that the Tlink cannot control the device. If this control were not in place, the request would be forwarded all the way to the PBX before the error could be detected.

#### Figure 2-1 Associating a Device with a Particular PBX



#### Figure 2-3 Administration for Associating a Device with a Particular PBX

#### **TLINK GROUP OBJECTS:**

TLINK GROUP NAME	TLINK
PBX1	PBX_VNDR#CSTA1#CSTA#ALPHA
PBX2	PBX_VNDR#CSTA2#CSTA#ALPHA

#### **DEVICE OBJECTS:**

DEVICE ID	TLINK GROUP NAME
620	PBX1
621	PBX1
	PBX1
635	PBX1
710	PBX2
711	PBX2
	PBX2
740	PBX2

#### Load Balancing

You can use Tlink Groups to provide load balancing in a single telephony server/single PBX environment. In this example, a company has a telephony server with three CTI links. Two of these links are used by a call center; the third is used by the remaining employees. The goal of this arrangement is to guarantee that the remaining employees are able to use Telephony Services, even if the call center is heavily loaded.

The administrator in this case has set up two Tlink Groups:

The first Tlink Group, "ACD Tlink Group" contains the Tlink labeled "PBX\_VNDR#ACD\_CSTA#CSTA#ALPHA".

The second Tlink Group, "Other Tlink Group" contains the Tlink labeled "PBX\_VNDR#OTHER #CSTA#ALPHA".

The PBX driver distributes requests across the two links and determines how the load is balanced.

The ACD group uses telephones with extensions ranging from 620 to 635. The telephone extensions of the remaining employees range from 710 to 740.

Figure 2-5 Associating a Device with a Particular CTI Link



Telephony Server

Figure 2-7 Administration for Associating a Device with a Particular CTI Link

#### **TLINK GROUP OBJECTS:**

TLINK GROUP NAME	TLINK
ACD Tlink Group	PBX_VNDR#ACD_CSTA#CSTA#ALPHA
Other Tlink Group	PBX_VNDR#OTHER#CSTA#ALPHA

#### **DEVICE OBJECTS:**

DEVICE ID	TLINK GROUP NAME
620	ACD Tlink Group
621	ACD Tlink Group
:	ACD Tlink Group
635	ACD Tlink Group
710	Other Tlink Group
711	Other Tlink Group
:	Other Tlink Group
740	Other Tlink Group

28 Network Manager's Guide

# **Object Administration**

The Security Database (SDB) checks the validity of data as it is administered. The table below describes the checks that are performed by the SDB. For example, when you add a User object, you assign a worktop to the user. The worktop name you supply in the User object must be the name of an existing worktop object.

TO ADD THIS ATTRIBUTE:	TO THIS OBJECT TYPE:	YOU MUST SPECIFY AN EXISTING
Worktop	User	Worktop Name
Device-device Group	User	Device Group Name
Call-device Group	User	Device Group Name
Call Control Group	User	Device Group Name
Routing Group	User	Device Group Name
Admin Access Group	User	Admin Access Group Name
Device ID	Worktop	Device ID
Secondary Device Group	Worktop	Device Group Name
Tlink Group	Device	Tlink Group Name
Device ID	Device Group	Device ID
Tlink	Tlink Group	Tlink Name
Tlink	Admin Group	Tlink Name

If you are adding many new objects to the SDB, you may want to group the objects by object type and add them in the following order:

- **Tlinks**: You may administer these links manually, or load Telephony Services on your server. As each PBX driver is loaded, the Tserver automatically administers all of its Tlinks.
- Tlink Groups: Add any Tlink Groups you may need. A default Tlink Group "Any Tlink" is added to the SDB for you.
- **Devices**: Add device objects for all the telephones, fax machines and modems that are to be controlled by Telephony Services. You can leave the Tlink Group set to the default ("Any Tlink") if you are not using Tlink Groups.
- **Device Groups**: You can make up device groups using the device objects you entered in the previous step.
- Worktops: You can add worktops with primary devices and Secondary Device Groups entered in the previous two steps. You can leave the Secondary Device Group field blank.
- Users: You can add users and assign worktops entered in the previous step to them. You can set up user permissions by assigning device groups created earlier.

## **Underlying Database Support**

A Security Database module within Telephony Services manipulates the objects that make up the Security Database (SDB). This module acts as an interface between Telephony Services and the underlying Btrieve database engine, which is a product of Persuasive Software, Inc. The database engine is installed separately from Telephony Services. (The installation may be done automatically, using the master installer program. For details, refer to the *PassageWay Telephony Services for Windows NT Installation Guide*.)

The Security Database module retrieves object and attribute information from a data dictionary (called DICTNRY.SDB), which resides in the \TSRV\SDB directory. The module uses this information to create and manage the SDB files that reside in the \TSRV\SDB\R2SDB directory. Because of the close relationship between the files and the data dictionary, each file is stamped with the version of the data dictionary that was used to create the file. When Telephony Services is loaded, the database module checks that the version of each file matches the version of the data dictionary. If there is a mismatch, the database module enters and "INCONSISTENT" state, and no database processing can be performed. If you should encounter this problem, examine the error log (refer to Chapter 11, "Troubleshooting").

#### Using the TSA or TSA32 to Administer Your SDB

The SDB is modified using the Telephony Services Administration program (called TSA for 16-bit systems and TSA32 for 32-bit systems). This application is client-based. See Chapter 4 for detailed information on the TSA application or Chapter 5 for detailed information on the TSA32 application. See Chapter 3 for information on how to control user access to the SDB.

Telephony Objects and the Security Database 31

#### **Bulk Administration**

The Bulk Administration feature lets you perform the following functions:

- Initialize your SDB from an existing database
- Administrate your SDB automatically
- Backup your SDB (you can also backup the SDB files using standard backup procedures)
- Print your SDB

For detailed instructions for using the Bulk Administration feature, see Chapter 6.

#### SDB Upgrades

Upgrades to Telephony Services may include a new version of the data dictionary. If this is the case, the installation procedure copies the new data dictionary into the \TSRV\SDB directory. When Telephony Services is started, the SDB module compares the version of the DICTNRY.SDB file with a reference copy of the SDB dictionary, DICTNRY.OLD. When the module examines the .dta files in the \TSRV\SDB\R2SDB directory, it finds that their version matches the DICTNRY.OLD version and concludes that an upgrade is required. It automatically converts the .dta files to the format in the new DICTNRY.SDB file. A copy of the original .dta files is kept in a separate backup directory created in the \TSRV\SDB directory.

The upgrade process is automatic. Most likely, you will be unaware that an upgrade has occurred. In the unlikely event that the upgrade is not successful, refer to Chapter 11 for recovery instructions.

32 Network Manager's Guide

#### Version Information

Version information can be obtained from the "About Telephony Services Administrator" screen (from the Help/About menu) in TSA or from the "Components" tab (from the Tserver Properties menu) in TSA32. Refer t o the Version Information section of Chapter 8, "The Tserver," for more details.

#### SDB Logging

You can keep a log of all the changes made to your Security Database. When you enable this feature, all successful updates that are made are saved in a file, *sdblog.txt*, in the \Program files\Telephony Services\tsrv\logfiles directory on the telephony server where the changes were made. This file is a comma-separated, ASCII file and may be viewed with a standard spreadsheet.

Changes are logged as they are made. The file grows until it reaches the allowed maximum size. At this point, it starts at the beginning of the file, overwriting data that was there previously. If you make many changes during the day, you may want to expand the size of the file.

#### Line Format

Each line in the sdblog.txt file contains the following fields:

Time: The date and time that the change was made.

**Application**: The application that made the change. If you use the TSA, this field contains "TSA16." If you used the TSA32, this field contains "TSA32." If you used Bulk Administration, the field contains "Bulk add."

Telephony Objects and the Security Database 33

**Login**: The login of the user making the change. If you used Bulk Administration to initiate an update of the SDB, the word "console" appears in this field.

**Opcode**: The type of change made to the SDB. The possible values are:

ADD	A new object was added to the SDB
MODIFY	The attributes of an existing object were modified
DELETE	An existing object was deleted from the SDB
ADD MEMBER	A member was added to a group. You would see this opcode if you added a device to a device group or a Tlink to a Tlink or admin access group.
DELETE MEMBER	A member was deleted from a group. You would see this opcode if you deleted a device from a device group or a Tlink from a Tlink or admin access group.

**Object Type**: The type of object that was added/modified/deleted. The valid object names are User, Worktop, Device, Device Group, Tlink, Tlink Group, and Admin Access Group.

Attribute: The name of the attribute in the object that was modified. For example, if the name of a user object was modified, this field would read "name."

**Original Attribute Value**: The current value of the attribute you are modifying or deleting. If you are adding a new object or a new member to an existing group, this column is empty.

New Attribute Value: The new value of the attribute.

#### Sample File

The following is a sample SDBLOG.TXT file. The file contains a header indicating when the file was created. The file also contains the text "Last SDB Log Record" after the last addition to the log. If your file has wrapped around, look for this text to indicate where the latest information ends. (You should also notice that the entries after this text have an earlier timestamp.)

#### Figure 2-9 Sample Telephony Services SDB Log File

	TELEPHONY SERVICES SDB LOG						
	File Created at:	: 10-13-96 4:42:41p	m				
TIME	APPLICATION	LOGIN	OPCODE	OBJECT TYPE	KEY ATTRIBUTE	ORIG ATTRIBUTE VALUE	NEW ATTRIBUTE VALUE
10-13-96 4:43:08pm	TSA32	ADMINISTRATOR	ADD	DEVICE	Device ID		4401
·					Tlink Group		Any Tlink
					Device Type		PHONE
					Location		NYC
10-13-96 4:43:48pm	TSA32	ADMINISTRATOR	ADD	WORKTOP	Worktop Name		Help desk 1
·					Primary Device		4401
					IPX Address		
					IP Address		
					IP Name		
					Secondary Device Grp		
10-13-96 4:44:11pm	TSA32	ADMINISTRATOR	MODIFY	USER	Login		joe
					Name	Joe Smith	Joe Smythe
Last SDB Log	Record						

Telephony Objects and the Security Database 35

#### File Wrap-around

If the file reaches its maximum size, any data beyond the last valid log entry is erased. A new header is then placed at the beginning of the file. This header contains the date and time the file wrapped around. The example below shows the new header after the file has wrapped around.

Figure 2-11

Sample Telephony Services SDB Log File Wrap Around

	TELEPHONY SERVICES SDB LOG						
	File Wrapped Around at: 10-13-96 5:22:14pm						
TIME	APPLICATION	I LOGIN	OPCODE	OBJECT TYPE	KEY ATTRIBUTE	ORIG ATTRIBUTE VALUE	NEW ATTRIBUTE VALUE
10-13-96 5:22:14pm	TSA32	ADMINISTRATOR	ADD	USER	Login	WILCE	TDL
·					Name		t lac
					Worktop Name		WKTP 30
					Call-Dev Monitor Grp		DLIST 1
					Call Monitoring		TRUE
					Call Control Group		DLIST 5
					OAM Group		ADMIN GROUP 4
					Super Admin User		FALSE

chapter

# **3** Controlling User Access to Telephony Services

Typically, users receive permissions to access Telephony Services from their assigned worktop. These default permissions allow every Telephony Services user to control and monitor the devices associated with their own worktop, but not any other devices.

Telephony Services allows for users to be granted additional permissions by assigning Class of Service options to the user object. Also, the "Extended Worktop Access" feature allows user permissions to be assigned based on the worktop where a user is running an application (users can log in from any worktop and control the devices on that worktop).

If each of your users has an assigned desk and does not use any other desks, you can use the default settings and ignore the rest of this chapter.

# Terminology

Call Control	Call control permissions for a device allow a user to run an application that originates calls from that device, transfers or conferences calls at that device, etc.
Device	A device can be anything that can originate or terminate a telephone call. Examples are telephones, fax machines, modems, trunks, trunk groups, and incoming call groups. In examples given in this document, a device is a telephone.
Monitor	A monitor placed on a device or a call causes reports of changes in the status of the device or call to be sent to the client requesting the monitor. If your application places a device monitor on your phone, your application is notified of any change in your phone's status (e.g., an incoming call has been received, a call ended, etc.). Many applications rely on monitors to provide this type of information.
Worktop	A worktop represents a desktop equipped with a client workstation, a telephone (known as the worktop's Primary Device), and any number of additional telephony devices (such as a fax machine or modem). These additional devices are specified through the worktop's Secondary Device Group. Users can always control and monitor all the devices associated with their worktop.
	When a user logs in from a worktop other than their assigned worktop, that user can also control and monitor devices on that other worktop (provided the "Extended Worktop Access" option is enabled and the other worktop is administered in the Security Database). The worktop object must include the LAN address of the worktop.

## **Granting User Permissions**

There are three ways in which a user may be granted permissions:

- 1. The user may be assigned a worktop in the Security Database. This gives the user call control and device/device monitoring permissions for any of the devices associated with that worktop.
- 2. The user may have Class of Service options administered in the Security Database. This provides permission to access specific devices for each of the following types of requests:
  - Call control
  - Device/Device monitoring
  - Call/Device monitoring
  - Call/Call monitoring
  - Routing

Call/device monitoring, call/call monitoring, and routing permissions may only be granted through administered Class of Service options.

3. The system may be administered to allow us ers to access any of the devices associated with the client workstations wherever they are working. This type of access is controlled through the "Extended Worktop Access" option. When this feature is enabled, the Telephony Server checks the Security Database for a worktop with the same LAN address as the workstation where the user is working. If a match is found, then the user is given call control and device/device monitoring permissions for any of the devices associated with that worktop.



If you make changes to a user's permissions, the user must close any active applications and restart them before the changes take effect. This is because user permission information is saved in memory when the user's application first opens a connection to the Tserver. Any subsequent changes to the SDB are not reflected in the saved information.

Controlling User Access to Telephony Services 39

#### **Extending User Access to Other Worktops**

Users can always control all the devices on their worktop and in their own call control Class of Service device group. "Extended Worktop Access" is a system-wide administration field that affects all users. If this field is enabled, a user can log in from any worktop and control the devices on that worktop.



LAN address information is used when the "Extended Worktop Access" feature is enabled, so that the Telephony Server can determine from which worktop the user is logged in and which devices are associated with that worktop.

If the "Extended Worktop Access" option is **disabled**, then a user can control only the following devices:

- The primary device on their worktop
- Any device in the secondary device group associated with the user's worktop
- Any device in the call control Class of Service group in his/her user object

If a user logs in from another worktop while this option is disabled, he/she cannot control the devices on that worktop. The user can still control the devices on his/her own worktop and the devices in their call control Class of Service.

If most users should be restricted to the devices associated with their assigned worktop but some specific users must control other devices, you can still disable the "Extended Worktop Access" feature. For those users who need additional access you can employ the user level Class of Service permissions structure described below. Even with the "Extended Worktop Access" system option disabled, these users will be able to control the necessary devices.

#### **Class of Service Options**

Applications that use Telephony Services vary widely from simple directory functions to call routing centers. Depending on the application you want to run, you may need to administer different types or levels of permission. Class of service permissions can be categorized as follows: call control services, device/device monitors, call/device monitors, call/call monitors, and routing services.

The Class of Service permissions in the User object dictate which type of requests each user can make. The entry in each field is a group of devices on which the user can make a request. For example, the ACME Corporation has a help desk that is staffed by three users, Michael, Sue and Tom, each of whom has an assigned desk. The device IDs (telephone extensions) on these desks are 750, 751 and 752. Their supervisor, Edward, runs an application that generates productivity statistics for the help desk by monitoring all of the user's extensions. The supervisor's device ID is 760. For security reasons, the "Extended Worktop Access" option is disabled.

To enable this operation, you need to make one device group, HELP DESK, of the devices in the help center: 750, 751, and 752. You would then assign this group to the Device Monitor and Call/Device Monitor Class of Service options in the supervisor's User object. The following tables summarize the types of administration you can set up.

#### **Device Group Administration**

Device Group Name	Device IDs
HELP DESK	750, 751, 752

#### **User Administration**

Login	Worktop	Call Control	Device/Device Monitor	Call/Device Monitor
Edward	ACD SUPV		HELP DESK	HELP DESK
Michael	Michael's worktop			
Sue	Sue's worktop			
Tom	Tom's worktop			

#### Worktop Administration

Worktop Name	Primary Device ID
Michael's worktop	750
Sue's worktop	751
Tom's worktop	752
ACD SUPV	760

#### **Call Control**

A user's call control class of service specifies the devices that a user can control. Basically, call control permissions include any operation that the user could perform manually, using their telephone. The application can originate calls, activate features such as call forwarding and so on, for this set of devices.

42 Network Manager's Guide

#### **Device/Device Monitoring**

An application places a device monitor on a specific device so it can receive an event report any time an event occurs at that device. For example, if the device receives an incoming call or originates an outgoing call, the application receives an event report. Device monitors are the most commonly used monitor. By default, all users have this permission for the devices associated with their worktop.

#### **Call/Device Monitoring**

Call/device monitors are placed to track events for a call once it reaches the device being monitored. Unlike device/device monitors, events for a call continue to be received even after the call leaves the device. A common usage of this monitor is to place it on the extension that incoming calls to a call center reach before being distributed to an agent. Once the call reaches this first extension, all further events (such as transfers to queues and disconnects) are sent to the application that requested the monitor.

This type of monitor is commonly used by applications that track the efficiency of a call center operation. Supervisors may use this type of application to decide how to best allocate inbound call agents. In the Help Desk example, only users who are supervisors need this level of permission; individual agents who receive the calls do not.

#### **Call/Call Monitoring**

Call/call monitors work differently from the device and call/device monitors previously mentioned. Those monitors are based on a device ID. Call control monitors are tracked based on a call ID (a unique identifier of the call being handled by the PBX). Users either have or do not have this permission; you do not need to create a device group for this class of service.

Controlling User Access to Telephony Services 43

#### Routing

When a routing application is started, it sends route registration requests to the PBX, each containing a device ID. This instructs the PBX to send all incoming calls to these devices to the Tserver (and then on to the application) for routing. The PBX does not route these calls.

Before the route registration request is passed to the PBX, the Tserver checks that the user (in this case, the routing application) has permission to route calls for this device. The Device Group in the Routing Class of Service of the user object must contain the device IDs of all the devices the application can route. If the user is allowed to route calls for all devices, you can use the default device group, "Any Device." If you do not enter anything in the routing attribute, all routing requests are rejected by the Tserver.

Note that the user in this case does not need to be a real person. It can be an application that logs into Telephony Services with its own login and password.

## **Sample Configurations**

This section describes operations at a fictional organization, the ACME company. It is a mail order company that sells seeds and garden equipment. Each of the following sections explores part of the operation and describes the administration required to implement it.

The ACME corporation has disabled the "Extended Worktop Access" feature. This limits each user to their own worktop, but as you will see, some users are given permission to monitor other devices or control calls at those devices. This is accomplished by creating device groups for these devices and associating those groups with each user.



The type of permissions you need to give each user depends on the applications that the user is running. Before you assign permissions, check your applications to see what permissions they require to work properly.

#### **Users Only Control Devices on Their Own Worktops**

The ACME corporation has two inbound call groups: one group handles calls for the seed catalog and the second group handles calls for the tools catalog. Members of each group have their own desks and do not run Telephony Services applications from any desk other than their own.

The basic permissions granted to a user are enough for these users, even with the "Extended Worktop Access" option disabled.

#### Table 3-1 Basic Permissions – Worktop Administration

Worktop Name	Device ID	Secondary Device Group
Tools1	7701	
Tools2	7702	
Seeds1	7711	
Seeds2	7712	

#### Table 3-2

**Basic Permissions – User Administration** 

Login	Worktop	Call Control	Device Monitoring	Call/Device Monitoring	Routing
Michael	Tools1				
Sally	Tools2				
Juan	Seeds1				
Marie	Seeds2				

46 Network Manager's Guide

#### Manager/Assistant Configuration

ACME has a president, two vice presidents, and a single assistant who handles all incoming calls to the executives (the president and vice presidents). The president and vice presidents handle only their own phones.

Since the president and vice presidents use only the phones at their desks, you do not need to grant additional access to these users. However, in order for their assistant to be able to control and monitor their phones, you must create a device group containing the device IDs of their telephones and assign this group to the assistant.

The following tables summarize the types of administration you can set up.

#### Table 3-3 Manager/Assistant – Device Group Administration

Device Group Name	Device IDs	
EXEC LIST	7911, 7912, 7913	

Table 3-4

Manager/Assistant – Worktop Administration

Worktop Name	Device ID	Secondary Device Group
PRESIDENT WKTP	7911	
VP WKTP1	7912	
VP WKTP2	7913	
ASSISTANT WKTP	7914	

Controlling User Access to Telephony Services 47

# Table 3-5 Manager/Assistant – User Administration

Login	Worktop	Call Control	Device Monitoring	Call/Device Monitoring	Routing
President	PRESIDENT WKTP				
VP1	VP WKTP1				
VP2	VP WKTP2				
Exec Assistant	ASSISTANT WKTP	EXEC LIST	EXEC LIST		

You can get the same results as the above example by assigning the EXEC LIST to the secondary device group on the assistant's worktop:

# Table 3-6 Manager/Assistant – Assistant Worktop Administration

	Worktop Name		Device ID	) Secon	dary Device	Group	
	ASSISTANT WK	TP	7914	EXEC	LIST		
Table 3-7 Manager/Assistant – /	Assistant User	r Adr	ninistrat	ion			
	Login	Wor	ktop	Call control	Device Monitori ng	Call/Device Monitoring	Routing
	Exec Assistant	ASS WK1	ISTANT IP				

#### **Call Monitoring Application**

The inbound call agents are monitored by their supervisor, Martha. Martha has one application that collects call handling statistics and a second application that lets her join a call in progress at an agent's desk. To run these applications, Martha must be given call control privileges and device/device monitor, call/device monitor and call/call monitor privileges on the phones used by the agents. A device group containing the device IDs of the agents is created and entered in Martha's user object.

### Table 3-8

**Call Monitoring – Device Group Administration** 

Device Group Name	Device IDs
ACD AGENTS	7701, 7702, 7711, 7712

Table 3-9 Call Monitoring – User Administration

Login	Worktop	Call Control	Device Monitoring	Call/Device Monitoring	Call/Call Monitoring
Martha	ACD SUPV	ACD AGENTS	ACD AGENTS	ACD AGENTS	Enabled

These permissions might also be required by applications that bill based on telephone usage.

#### Portion of User Community Shares Worktops

Two regular employees, Tom and Lalitha, normally sit at their own desks to perform their job, but may occasionally act as an in-bound call agent when a regular agent is out sick or on vacation. ACME handles this situation by creating a device group, ACD Substitutes, and assigning it to the worktops used by Tom and Lalitha.

Table 3-10

#### Shared Worktop – Device Group Administration

Device Group Object	Device IDs
ACD Substitutes	7701, 7702, 7711, 7712

Table 3-11

Shared Worktop – Worktop Administration

Worktop Name	Device ID	Secondary Device Group	
WKTP1	7801	ACD Substitutes	
WKTP2	7802	ACD Substitutes	

#### Table 3-12

#### Shared Worktop – User Administration

Login	Worktop	Call Control	Device Monitoring	Call/Device Monitoring	Routing
Tom	WKTP1	_			
Lalitha	WKTP2				

As an alternative, you could allow Michael, Sally, Juan, and Marie (the inbound call agents) to switch desks by assigning the ACD Substitutes list to the secondary device group on each worktop or by assigning the list to the Call Control and Device groups in each user object.

ACME also shares a worktop in its shipping department where Louise, Frank, and Susan work. There is only one worktop in this department and all three share it.

#### 50 Network Manager's Guide

#### Table 3-13 Shared Worktop – Secondary Device Worktop Administration

	Worktop Name	Device ID	Secondary Device Group			
	SHIPPING	7810				
Table 3-14 Shared Worktop – Secondary Device User Administration						

Login	Worktop	Call Control	Device Monitoring	Call/Device Monitoring	Routing
Louise	SHIPPING				
Frank	SHIPPING				
Susan	SHIPPING				

#### **Prompted Digits**

ACME has a telephony-enabled application that can "pop-up" information about a customer using the customer's account number. Customers call a vector directory number (VDN), where a recorded announcement prompts them to enter their account number on their touch tone phone. The call is then directed to a customer service representative. By monitoring the VDN, ACME's application is able to retrieve the collected digits and display the customer information at the customer service representative's PC.

The extension associated with the VDN is 7800. The application must perform both device/device monitoring (on the customer service representative's phone) and call/device monitoring (on the VDN). Therefore, the customer service representatives must be given call/device monitoring permissions. (Note: Because collected digits are not part of the CSTA model and can only be implemented using private data, your PBX driver may require a different configuration.)

A device group, "CSR VDN," is created containing the VDN. This device group is then assigned to the customer service representatives in their Class of Service options.

Controlling User Access to Telephony Services 51

# Table 3-15 Prompted Digits – Device Group Administration

Device Group Name	Device IDs
CSR VDN	7800

Table 3-16 Prompted Digits – User Administration

Login	Worktop	Call Control	Dev/Device Monitoring	Call/Device Monitoring	Routing
Beth	WKTPA			CSR VDN	
Sally	WKTPB			CSR VDN	
Dave	WKTPC			CSR VDN	

#### **Call Routing**

ACME has a server application that routes all calls to the call center based on the number called, the availability of agents and other criteria. The extension of the incoming calls are 7700 (seeds) and 7710 (tools).

The user in this case is the routing application - not a person. The routing application logs in to Telephony Services just as a person would and has the same types of privileges. When the routing application begins, it sends a routing registration request to the PBX, requesting that incoming calls to extensions 7700 and 7710 be directed to it (the routing application). When the routing application determines which agent should get the call, it tells the PBX where to connect the call.

The routing application must be given routing permissions for devices 7700 and 7710. Notice that the user, RoutingAppl, has no associated worktop.

Table 3-17 Call Rou

Table 3-18 Call Routing

I	Routing –	Device	Group	Admin	istration
---	-----------	--------	-------	-------	-----------

RoutingApp

Device Gro	oup Name	Device IDs				
ACD ROUTE		7700, 7710				
Administrat	tion					
Login	Worktop	Call-control	Dev/ Device Monito	Call/ Device Monito	Routing	

Controlling User Access to Telephony Services 53

ACD ROUTE

chapter

# **4** Using the TSA to Administer the Security Database

This chapter describes the basic operation of the 16-bit Telephony Services Administration application (TSA). It describes how you can add Telephony Services objects easily to the SDB using "Quick Add." Following the "Quick Add" section you will find instructions on how to administer system-wide features as well as instructions for controlling SDB administration access by administering Admin Access Group objects. If you do not require any additional access restrictions, these three sections describe all of the administration you need to do.



In order to properly administer your SDB, you should be familiar with the SDB concepts covered in Chapter 2.

The remaining sections of this chapter discuss the order to follow for administering Telephony objects, and the TSA procedures that administer the Tlink, Tlink Group, Device, Device Group, Worktop, and User objects. The last section describes how to log SDB transactions to a log file.

Additional procedures that enable maintenance and performance tuning are described in other chapters:

**Chapter 6:** Administering the SDB in bulk (for automating certain aspects of SDB administration)

Chapter 7: Connecting your telephony server and clients to the LAN

Chapter 8: Tserver status and maintenance functions

Using the TSA to Administer the Security Database 55

Chapter 9: Telephony Services traffic measurements

Chapter 10: Cserver administration, status, and maintenance functions

Chapter 11: Enabling troubleshooting functions



The administrative changes you make do not affect current applications. Users must end the application and restart it before changes take effect. This is because the Tserver stores much of the user's information in its memory when it sets up a connection. This makes subsequent permissions checking much faster.

## **Telephony Services Administrator (TSA)**

The Telephony Server Administrator (TSA) client application provides an MS Windows 95 "look and feel" for administering your Telephony Servers. Using the TSA menus, you can perform administration tasks and get on-line help.

After installation, only the Administrator login can access and administer the Tserver.



If you also have Telephony Services for NetWare, you cannot use the TSA application to administer those Telephony Servers. Use the TSA or NWAdmin tools provided with the NetWare product when administering those Telephony servers.



Since two users can access the Tserver at the same time, one user can make changes that are not immediately visible to another user. If the second user attempts to edit the same information, an error appears. To view current edits, redisplay the screen (close the dialog box, then open it again).

56 Network Manager's Guide
## Starting the TSA Application

1.



From the "TS Win16 Client" program group, double-click on the "Telephony Services Admin" icon to execute the TSA16 application. The "Available Tservers" dialog box is displayed:

Figure 4-1 Available Tservers Dialog Box

Available Tservers	
Choose a <u>I</u> server to access: ACME_NY	
Login: ADMINISTRATOR	
Password:	
OK Exit Application	

- 2. From the "Choose a Tserver to access" list, select the Tserver you want to administer.
- 3. Fill in the "Login" and "Password" fields.

Immediately after installation, only the Administrator login ID is authorized to administer the Tserver.

# 4. Select "OK" to access that Tserver, or "Exit Application" to terminate the application.

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 4-2 Administrator Window

## The TSA Menu Bar

The TSA menu bar contains File, Admin(istration), Maint(enance), Status, and Help menus.

- The "File" menu allows you to change to a different Tserver by closing the existing Tserver connection and opening another one, and allows you to exit from Telephony Services Administrator.
- The "Admin" menu allows you to add, change, and delete objects in the Security Database, to use "Quick Add" to create objects, or to invoke Bulk Administration commands.
- The "Maint" menu allows you to administer system-wide options, to monitor Tserver-PBX driver resource utilization, and to view and configure Driver DLL information.
- The "Status" menu allows you to monitor connection status with the Tserver, registered Tlinks, and Users.
- The "Help" menu provides access to on-line help for the TSA and version information for various Tserver software modules.

# **Using Quick Add**

"Quick Add" enables you to create a user, a worktop and a device using one simple procedure. The Quick Add dialog box has two sections where you can enter data: "User Information" and "Device and Worktop Information." Quick Add also has a section for "Previously Administered Logins, Devices, and Worktops," which allows you to retrieve information that was recently entered using Quick Add.

The User Information section contains two attributes: Login and Name. The login is a mandatory field that shows the user's login name. (You are not creating the login on the server here. You must use the Windows NT User Manager to create the login.) The Name is the user's name and is optional.



In order to access Telephony Services, users must have a Windows NT account. A Telephony Services user may access Telephony Services by using their own Windows NT login ID (in which case they are not required to provide their Windows NT password), or they can access Telephony Services using any other Windows NT login ID for which they can supply a password. In either case, the Windows NT login ID must exist in the Telephony Services Security Database.

Windows NT logins are administered through the Windows NT User Manager. If users wish to access Telephony Services using a Windows NT login ID other than their own, they must have the **Log on as a service** user right assigned to their account on the Windows NT machine that is running Telephony Services. For more details, refer to the "User Authentication" section in Chapter 7.

The **Device and Worktop Information** section contains three attributes: **Tlink Group**, **Primary Device ID**, and **Worktop Name**. The **Tlink Group** attribute is a drop-down list showing all administered Tlink Groups. You can select the default Tlink Group, "Any Tlink" if you do not want to restrict the user's device. See Chapter 2 for more details. **Primary Device ID** identifies the primary device at the user's worktop. Typically, this is the extension of the telephone on the worktop. **Worktop Name** is the name of the user's worktop. You can use any naming convention you want, but each worktop must have a different name. By default, the **Previously Administered Logins, Devices, and Worktops** section displays all the users, worktops and devices you added using "Quick Add" since the dialog box was opened. If you select "Retrieve Information," all administered logins, devices, and worktops are displayed.



1. From the "Admin" menu, select "Quick Add." The "Quick Add" dialog box is displayed:

Figure 4-3 Quick Add Dialog Box

User Information		Beth	
<u>N</u> ame:		Beth Fitzpatrick	
☐ Device and Worktop Info	ormation —		
Tlink <u>G</u> roup:		Any Tlink	<u>+</u>
Primary Device ID:		7706	
Worktop Name:		Service 2	
Add Data	Enter No	ew Data	<u>C</u> lose
Previously Administered Logins, Devices, and Worktops			
Re <u>t</u> rieve Information	on		
Login	Primary Device ID	Work Name	top
RGG	7705	Servi	ice 1

2. Enter the user information and the device and worktop information.

# 3. Select "Add Data" to save the information in the Security Database.

From the "Enter New Data" status line of the dialog box, the system confirms that it is processing the new data by rapidly displaying the following messages in the following sequence:

Processing Data (the TSA is validating input data)

**Processing Device** (the TSA is adding a device object to your SDB)

**Processing Worktop** (the TSA is adding the worktop object to your SDB)

**Processing User** (the TSA is adding the user object to your SDB)

**Command Successfully Completed** (the TSA has added all the necessary objects for this user)

When the system redisplays "Enter New Data," you may enter new information for the next user. If the system cannot process the data, it displays an error message indicating the problem it encountered. These errors are explained in the "SDB Error Codes" section in Chapter 11, "Troubleshooting."

#### 4. Select "Close" to close the "Quick Add" dialog box.

# **Administration of System-wide Features**

The "Tserver Options" dialog box is used to administer system-wide parameters. These parameters include the following:

- Enable Pop-Up Alarm Notification: Enabling this feature causes a pop-up window to be displayed whenever an alarm occurs. You may want to enable this feature if you are running a mission critical application. See Chapter 8 for details on when this option should be enabled.
- ♦ Advertise Telephony Services Name Server: This field is provided for compatibility with future releases. It should always be enabled.
- Extended Worktop Access: If you check this box, users who log in from a worktop other than their assigned worktop will be able to monitor and control the devices associated with that worktop, as well as monitor and control the devices on their assigned worktop and in their classes of service. See Chapter 3 for more details on this feature.
- Enable Automatic Administration of LAN Addresses: If the LAN address is not already assigned for the user's worktop and you enable this feature, the Tserver automatically fills in the LAN address information the next time a user logs on. (LAN addresses are only necessary if you are using the "Extended Worktop Access" feature.)

The Tserver checks the worktop object whenever a client opens a connection to the Tserver. If the worktop object does not contain the network address, it sets the address attribute of the worktop object to the network address it received in the open stream connection. You should use this feature only if users are going to log in from their own worktop for the first time.



If you are using Dynamic Host Configuration Protocol (DHCP), automatic administration of LAN addresses will not produce the desired results unless the TCP Preferred Naming Format is set to Host Name and Windows Internet Name Service (WINS) is also available. • **Transport Layer Options:** These fields are used to specify the transport method between client and server. The supported method is TCP/IP.

For TCP/IP connections, the format of the saved address is based on the setting of the "TCP Preferred Naming Format" field. The format can be set to either "Host Name" or "IP Address." See Chapter 7, "Client Connectivity," for a complete discussion of these fields.



From the "Maint" menu, select "Tserver Options." The "Tserver Options" dialog box is displayed.

Figure 4-4 Tserver Options Dialog Box

Enable Pop-Up Alarm Notification
Advertise Telephony Services <u>N</u> ame Server
Extended Worktop Access
Enable Automatic Administration of LAN Addresses
Transport Layer Options   IPX/ <u>S</u> PX   ICP/IP   TCP Port: 450
IP <u>A</u> ddress: 135.20.70.5
TCP Preferred Naming Format
<u> </u>

- 2. Select the desired options.
- 3. Select "OK" to save the information in the Security Database.

# **Controlling SDB Administration Access**

Telephony Services restricts administration access to the SDB. Each user who will be administering Telephony Services is assigned a level of security; this level is kept in the SDB. Telephony Services has three levels of security: no SDB administration permissions; regular SDB administration permissions; and privileged users. Regular SDB administrators are allowed to add, change, and delete data in the SDB. Privileged users can modify data in the SDB and can also grant or revoke administrative privileges to other users.

One admin access group object is created when you install Telephony Services on a server: "ALL ADMIN ACCESS." Members of this group can administer all available modules; you do not need to explicitly add OAM Tlinks to this group. If all your administrators have permission to administer every administration module, you can assign each administrator to this group and skip the rest of this section. You do not need to create additional admin access groups.

When you install Telephony Services on a server, the Administrator user is added to the SDB with privileged user permissions.

You must add the User objects for each administrator to your SDB before you can assign them administration privileges. You can use either the "Quick Add" method described above or the mor e detailed User administration procedure described later in this chapter.

The TSA does not allow you to get into a situation where no one has administration privileges. The "ALL ADMIN ACCESS" group cannot be deleted and you cannot remove the last user from the group. Also, Telephony Services ensures that at least one user in this group will always have the ability to administer admin access groups.

Using the TSA to Administer the Security Database 65

## Setting Up an Admin Access Group

Giving administration access rights to a group of users is a two-step process. First, you must identify the Tlinks that will be in the admin access group. Second, you must assign the users with the corresponding administration responsibilities to the appropriate admin access group(s).

An admin access group contains a list of OAM-type advertised services, or Tlinks. (OAM is the service type for administration.) When adding Tlinks to an admin access group, consider the following:

- Administrators who will be administering the SDB using the TSA32 require SDB\_OAM permissions.
- Administrators who will be performing maintenance tasks using the TSM32 require TSRV\_OAM permissions.
- Administrators who will be administering the SDB using the TSA require both SDB\_OAM and TSRV\_OAM permissions.
- Administrators who will be administering options provided by the PBX vendor require the PBX driver OAM Tlink permissions.

The following example explains how you can set up several admin access groups and control which telephony servers the administrators can access. Suppose your organization has three administrators: Judy can administer the SDB data; Mike can perform PBX driver administration; and Luis can perform all administration. You would perform the following:

1. Create a "SDB ADMIN" group. Put the SDB\_OAM Tlink for the Tserver in this group:

TSERVER#SDB\_OAM#OAM#ACME\_NY

2. Add Judy to the SDB ADMIN group.

3. Create a "PBX ADMIN" group. Put the PBX\_OAM Tlink for the server in this group:

PBX\_VENDOR#PBX\_OAM#OAM#ACME\_NY

- 4. Add Mike to the PBX ADMIN group.
- 5. Add Luis to the ALL ADMIN ACCESS group. (You may also make a third admin access group containing all OAM Tlinks and add Luis to it.)

## **Admin Access Group Rules**

The following rules apply when administering admin access groups:

- A Tlink may appear in more than one admin access group.
- A user may be associated with only one admin access group.
- The Tlinks in an admin access group may be from different vendors.

## Administering Admin Access Groups

Admin access group administration allows you to create new groups or modify an existing group. When you select the "Admin Access Group" option from the "Admin" menu, a list is displayed containing all the ad min groups on the server. If you highlight an existing group, you can edit the OAM Tlinks that make up the group, edit the list of "Allowed Users" who are given this permission, view the group or delete the entire group.

Each dialog box has an "Allowed Users" button. By pressing this button, you can see all the users who are currently assigned to this admin access group and you can make changes as needed. If you delete an admin access group, the users who were allowed to administer OAM type Tlinks in the group can no longer administer anything.



From the "Admin" menu, select "Admin Access Groups." The "Admin Access Group Information" dialog box is displayed.

Figure 4-5 Admin Access Group Information Dialog Box

1.

🛥 🛛 📥 Admin Access Gr	oup Information
Admin Access Groups: ALL ADMIN ACCESS	Create
LA Admin NY Admin	<u> </u>
	<u>⊻</u> iew
	Delete
Close	Allowed Users

2. Scroll or browse through the list of any admin access groups. Then either select an existing admin access group or create a new one.

#### Creating an Admin Access Group

1.

Procedure 23

From the "Admin Access Group Information" dialog box, select "Create." The "Create Admin Access Group" dialog box is displayed:

Figure 4-6 Create Admin Access Group Dialog Box

🛥 Create Admir	n Access Group
<u>A</u> dmin Access Group Name:	NY Admin <u>C</u> ancel

2. Enter the name for the new admin access group and select "OK." The "Create Admin Access Group" dialog box is displayed:

Figure 4-7 Create Admin Access Group Dialog Box

🛥 Crea	te Admin Access Group N	Y Admin	
All Admin Tlinks <u>N</u> ot Currently	All Admin Tlinks <u>N</u> ot Currently In Group:		
LUCENT#SDB_OAM#OAM#AC	:ME_LA		
Add Selected	Add A <u>l</u> l	Delete Selected	
All Admin Tlinks Currently In G	roup:		
LUCENT#SDB_OAM#OAM#AC	ME_NY		
TSERVER#CSRV_UAM#UAM	FACME_NY FACME_NY		
	<u>-</u>		
<u> </u>		<u>L</u> ancel	

#### 3. Add Tlinks to the admin access group as desired:

To add specific Tlinks to the admin access group, highlight the Tlink(s) in the top list box and select the "Add Selected" button.

To add all of the Tlinks in the top list box to the admin access group, select the "Add All" button.

- 4. To remove Tlink(s) from the admin access group, highlight the Tlink(s) in the bottom list box and select the "Delete Selected" button.
- 5. Select "OK" to record the changes in the Security Database or "Cancel" to return to the "Admin Access Group Information" dialog box without recording any of the changes.
- 6. You are now able to assign users to this group. See the section "Administering Allowed Users" later in this chapter.

#### **Editing an Admin Access Group**

1.

Procedure 23

From the "Admin Access Group Information" dialog box, select an admin access group and select "Edit." The "Edit Admin Access Group" dialog box is displayed.

Figure 4-8 Edit Admin Access Group Dialog Box

- Edit	Admin Access Groun	nimbA YN
All Admin Tlinks <u>N</u> ot Currently I LUCENT#SDB_0AM#0AM#AC LUCENT#SIMSERV#SIM#ACM	n Group: ME_LA E_NY	
<u>A</u> dd Selected All Admin Tlinks Currently <u>I</u> n Gr LUCENT#SDB_0AM#0AM#AC TSERVER#CSRV_0AM#0AM#	Add A <u>ll</u> oup: ME_NY ACME_NY ACME_NY	Delete Selected
	ALME_NT Allowed Users	<u>C</u> ancel

#### 2. Add Tlinks to the admin access group as desired:

To add specific Tlinks to the admin access group, highlight the Tlink(s) in the top list box and select the "Add Selected" button.

To add all of the Tlinks in the top list box to the admin access group, select the "Add All" button.

- 3. To remove Tlink(s) from the admin access group, highlight the Tlink(s) in the bottom list box and select the "Delete Selected" button.
- 4. Select "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

1.



From the "Admin Access Group Information" dialog box, select an admin access group and select "View." The "View Admin Access Group" box is displayed.

Figure 4-9 View Admin Access Group Dialog Box

View Admin Access Group NY Admin
All Admin Tlinks Not Currently In Group:
All Admin Tlinks Currently In Group:
LUCENT#SDB_OAM#OAM#ACME_NY
TSERVER#CSRV_OAM#OAM#ACME_NY
ISERVER#ISRV_UAM#UAM#ACME_NY
Allowed Users Llose

2. Select "Close" to return to the "Admin Access Group Information" dialog box.

#### **Deleting an Admin Access Group**

Before deleting an Admin Access Group, the Tlinks administered by the group and the users in the group are displayed. Select the "Allowed Users" button to view these users because, once you have deleted an admin access group, the allowed users in the group no longer have administrative permissions. If you still want them to be administrators, you should add them to another admin access group.

The TSA guarantees that you will always have at least one person who can administer your SDB object and give this permission to other users. You cannot remove the "ALL ADMIN ACCESS" group and you cannot delete the last user in this group



From the "Admin Access Group Information" dialog box, select the admin access group and select "Delete." The "Delete Admin Access Group" dialog box is displayed.

Figure 4-10 Delete Admin Access Group Dialog Box

1.

Delete Admin Access Group NY Admin	
All Admin Tlinks <u>N</u> ot Currently In Group:	
All Admin Thinks Course do to Course	
All Admin Tlinks Currently In Group: THEFNT#SDR_DAM#AAM#ACMF_NY	
TSERVER#CSRV_OAM#OAM#ACME_NY	
ISERVER#ISRV_UAM#UAM#ACME_NY	
<u>OK</u> Allowed <u>U</u> sers <u>C</u> ancel	

Using the TSA to Administer the Security Database 73

2. Select "OK" to delete the admin access group from the Security Database or "Cancel" to return to the "Admin Access Group Information" dialog box without deleting the admin access group.

## Administering Allowed Users

Users are given administration permissions by including them in the "Allowed Users" list for a specified Admin Access Group.

To view the list of "Allowed Users," either select this option after you have highlighted an admin access group from the "Admin Access Group Information" dialog box, or view a highlighted access group and then select "Allowed Users" from the "View Admin Access Group" dialog box.

The "Allowed Users" dialog box contains two list boxes:

• All Users Not Currently In any Admin Access Group

This box lists the login IDs of all users who currently are not authorized to perform administration and maintenance on any admin Tlink entries.

• All Users Currently In Group

This box lists the login IDs of all users who currently are authorized to perform administration and maintenance on the OAM Tlink entries in the selected admin access group.



 From the "Admin Access Group Information" dialog box, select an admin access group, then select "Allowed Users." (Alternatively, you can select an admin access group, select "Edit," and then select "Allowed Users" to edit the allowed users for the highlighted group.)

Figure 4-11 Allowed Users Dialog Box

Allowed Osers for NT Autility	
All Users Not Currently In any Admin Access Group	٦
Login ID	-
LCHEN	
LUIS	
LYNN	
PAIM	
RGG	41
<u>A</u> dd <u>D</u> elete <u>D</u> K <u>C</u> ancel	
← All Users Currently In Group	
Login ID	
BJ₩	
MARTHA	

- 2. To add entries to the "All Users Currently in Group" list box, select entries from the "All Users Not Currently In any Admin Access Group" list box and select "Add."
- 3. To delete entries from the "Allowed Users" list box, select entries from the "All Users Currently In Group" list box and select "Delete."
- 4. Select "OK" to record the changes in the Security Database or "Cancel" to return to the admin access group dialog box without recording any changes.

# **Order for Administration of Telephony Objects**

If you do not use "Quick Add" to add your User, Worktop and Device objects to the SDB, you must add individual objects in a certain order. This is because the TSA validates some attributes as you enter the object and prohibits you from entering invalid information. For example, if you are adding a Worktop object that has a device "4401" associated with it, you must have first added the "4401" Device object to the SDB.

A Tserver should be administered in the following order:

#### 1. System-wide features for the Tserver

Administer the options described in the "Administration of Systemwide Features" section of this chapter.

#### 2. Tlinks

Administer the CSTA and OAM Tlinks if they have not been added automatically.

#### 3. Tlink Groups

If necessary, create the groups of Tlinks that devices are allowed to use. See Chapter 2 for details. The default group "Any Tlink" is provided for you automatically.

#### 4. Devices

Create an object for each device (telephone) that will be controlled by Telephony Services applications. Valid device IDs are needed to create Device Group and Worktop objects.

#### 5. Device Groups

Create groups of devices for user classes of service and worktop secondary device groups. See Chapter 3 for details. The group "Any Device" is provided for you. If you plan to assign device groups to either the Worktop or User objects, you must add them to the SDB first.

#### 6. Worktops

Create a worktop object for each telephone-workstation pair that is to use Telephony Services. You must create the Worktop object before you can assign a worktop to a User object.

#### 7. Users

Create a user object for each person who will be using Telephony Services. These users must exist on the Windows NT system (they must have a Windows NT login to the operating system, which must be added through the Windows NT User Manager).

#### 8. Admin Access Groups

If necessary, create admin access groups to give users administration permissions.

# Administering Tlinks

Tlinks are the services offered by Tservers and PBX drivers. (See the section titled "The Tlink and Tlink Group Objects" in Chapter 2 for a complete description of Tlinks.) Tlinks can be added to the SDB in two ways:

- ♦ You can install and load the Tserver and PBX drivers on your telephony server, causing all the Tlinks on that Tserver to be created automatically for you.
- You can create the Tlinks using the TSA.

In most cases, you can rely on the automatic administration and **skip the rest of this section**. You may choose to administer Tlinks if your telephony server configuration is incomplete and you want to get a head start on your system administration.

The following are the fields that make up the Tlink name:

- **Tserver:** The name of the server where the CSTA link, Tserver or PBX driver administrative module is located. The string you enter may not exceed 19 characters and may not contain the pound sign (#).
- **Tlink Type:** The kind of service provided by a PBX driver or a Tserver. The following kinds of service may be advertised:
  - **CSTA:** This type of link provides call control, monitoring, and routing functionality.
  - **Driver Admin:** This type of link provides administration and maintenance of a PBX driver. You can include this Tlink type in an admin access group to give users administration permissions for that PBX driver.
  - Simulator: This type of link is used when the PBX is not available. You should only use this type of Tlink when you are testing a Telephony Services application in a simulated environment.
  - **Tserver Admin:** This type of link provides administration and maintenance of the Tserver module. You can include this Tlink in an admin access group to give users maintenance privileges for this server.
  - **Cserver Admin:** This type of link provides administration and maintenance of a CSTA server. You can include this Tlink type in an admin access group to give users administration permissions for the CSTA server.
  - **SDB Admin:** This type of link provides administration and maintenance of the SDB driver. You can include this Tlink type in an admin access group to give users administration permissions for accessing the SDB.

- **Driver Name**: Fill in the driver name with the name provided by your PBX vendor, if applicable.
- Vendor: Fill in the vendor name with the name provided by your PBX vendor, if applicable.

## **Accessing Tlink Information**

1.



From the "Admin" menu, select "Tlinks." The "Tlink Information" dialog box is displayed:

Figure 4-12 Tlink Information Dialog Box

🛥 Tlink Information	
<u>I</u> links: LUCENT#CSTASERV#CSTA#ACME_NY LUCENT#SDB_OAM#OAM#ACME_LA	<u>C</u> reate
TSERVER#CSRV_DAM#DAM#ACME_NT TSERVER#NSRV#CSTA#ACME_NY TSERVER#NSRV#CSTA#ACME_NY TSERVER#TSRV_DAM#DAM#ACME_NY	Edit
	<u>⊻</u> iew Delete
<u>Cl</u> ose	

2. Scroll or browse through the list of all administered Tlinks. Then either select an existing Tlink or create a new one.

Using the TSA to Administer the Security Database 79

# **Creating a Tlink**



1.

From the "Tlink Information" dialog box, select "Create." The "Create Tlink" dialog box is displayed:

Figure 4-13 Create Tlink Dialog Box

-	Create Tlink
<u>T</u> server:	
Tlink Type	
● C <u>S</u> TA	○ Ts <u>e</u> rver Admin
O <u>D</u> river Admin	○ Cse <u>r</u> ver Admin
○ Si <u>m</u> ulator	○ SD <u>B</u> Admin
Driver <u>N</u> ame:	
<u>V</u> endor:	
<u>0</u> K	<u>C</u> ancel

- 3. Enter the name of the Tserver for which you want to create the Tlink in the "Tserver" field.
- 4. Select the desired Tlink Type.
- 5. Enter the appropriate values in the "Driver Name" and "Vendor" fields (if applicable).
- 6. Select "OK" to add the new Tlink information to the Security Database, or "Cancel" to return to the "Tlink Information" dialog box without creating the Tlink.

# **Editing a Tlink**

You cannot change a registered, or active, Tlink. To determine if a Tlink is active, select the "Tlink Information" option from the "Maint" menu. Each Tlink and its registration status is displayed.



1. From the "Tlink Information" dialog box, select the Tlink that you want to modify and select "Edit." The "Edit Tlink" dialog box is displayed:

Figure 4-14 Edit Tlink Dialog Box

1	Edit Tlink
<u>T</u> server:	ACME_NY
Tlink Type	
● C <u>S</u> TA	○ Ts <u>e</u> rver Admin
O Driver Admin	Cse <u>r</u> ver Admin
⊖ Si <u>m</u> ulator	○ SD <u>B</u> Admin
Driver <u>N</u> ame:	CSTASERV
<u>V</u> endor:	LUCENT
<u>0</u> K	<u>C</u> ancel

- 2. Make the desired modifications to the displayed Tlink information. You cannot edit an active Tlink.
- 3. Select "OK" to record the changes in the Security Database, or "Cancel" to return to the "Tlink Information" dialog box without recording any of the changes.

# Viewing a Tlink

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



1. From the "Tlink Information" dialog box, select the Tlink that you want to view and select "View." The "View Tlink" dialog box is displayed:

Figure 4-15 View Tlink Dialog Box

3	View Tlink
<u>T</u> server:	ACME_NY
┌ Tlink Type	
● C <u>S</u> TA	○ Ts <u>e</u> rver Admin
O <u>D</u> river Admin	Cse <u>r</u> ver Admin
⊖ Si <u>m</u> ulator	○ SD <u>B</u> Admin
Driver <u>N</u> ame:	CSTASERV
<u>V</u> endor:	LUCENT
	<u>C</u> lose

2. Select "Close" when you have finished viewing the information for the selected Tlink.

# **Deleting a Tlink**



1.

From the "Tlink Information" dialog box, select the Tlink that you want to delete and select "Delete." You cannot delete an active Tlink.

Figure 4-16 Delete Tlink Dialog Box

-	Delete Tlink
<u>T</u> server:	ACME_NY
Tlink Type	
● C <u>S</u> TA	○ Ts <u>e</u> rver Admin
O <u>D</u> river Admin	Cse <u>r</u> ver Admin
⊖ Si <u>m</u> ulator	○ SD <u>B</u> Admin
Driver <u>N</u> ame:	CSTASERV
<u>V</u> endor:	LUCENT
OK	<u>C</u> ancel

2. Select "OK" to delete the selected Tlink from the Security Database, or "Cancel" to return to the "Tlink Information" dialog box without deleting the Tlink.

# **Administering Tlink Groups**

1.

Tlink Group objects are groups of CSTA-type Tlinks. This Tlink type is used for call control, monitoring and routing. See Chapter 2 for details on Tlink Group object usage.



From the "Admin" menu, select "Tlink Groups." The "Tlink Group Information" dialog box is displayed:

#### Figure 4-17 Tlink Group Information Dialog Box

-	Tlink Group Information
<u>T</u> link Groups:	
Sales Service	<u>C</u> reate
	<u>E</u> dit
	<u>⊻</u> iew
	Delete
	Close

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

# **Creating a Tlink Group**

Procedure **1**23

1.

From the "Tlink Group Information" dialog box, select "Create." The "Create Tlink Group" dialog box is displayed:

Figure 4-18 Create Tlink Group Dialog Box

- Create	Tlink Group
<u>T</u> link Group Name:	Sales
<u>D</u> K	<u>C</u> ancel

2. Enter the name of the new Tlink Group and select "OK." The "Create Tlink Group" dialog box is displayed:



🛥 Create Tlink Group Sales		
All CSTA Tlinks <u>Not</u> Current LUCENT#CSTASERV#CST TSERVER#NSRV#CSTA#A	ly In Group: A#ACME_NY CME_NY	
Add Selected	Add A <u>l</u> l	Delete Selected
All CSTA Tlinks Currently In	Group:	
<u>         0</u> K		<u>C</u> ancel

#### 3. Add Tlinks to the Tlink Group as desired:

To add specific Tlinks to the Tlink Group, highlight the Tlink(s) in the top list box and select the "Add Selected" button.

To add all of the Tlinks in the top list box to the Tlink Group, select the "Add All" button.

# 4. To remove Tlinks from the Tlink Group, highlight the Tlink(s) in the bottom list box and select the "Delete Selected" button.

5. Select "OK" to record the changes in the Security Database, or "Cancel" to return to the "Tlink Group Information" dialog box without adding the Tlink Group to the Security Database.

# **Editing a Tlink Group**



1.

From the "Tlink Group Information" dialog box, select the Tlink Group that you want to modify and select "Edit." The "Edit Tlink Group" dialog box is displayed:

Figure 4-20 Edit Tlink Group Dialog Box

-	💳 Edit Tlink Group Sales		
All CSTA Tlinks <u>N</u> ot Current	All CSTA Tlinks <u>N</u> ot Currently In Group:		
TSERVER#NSRV#CSTA#A	TSERVER#NSRV#CSTA#ACMENY		
Add Selected		Delete Selected	
<u>A</u> dd Joneoled		Delete Solotto	
All CSTA Tlinks Currently In	Group:		
LUCENT#CSTASERV#CST	A#ACME_NY		
<u> </u>	L L	<u>C</u> ancel	

#### 2. Add Tlinks to the Tlink Group as desired:

To add specific Tlinks to the Tlink Group, highlight the Tlink(s) in the top list box and select the "Add Selected" button.

To add all of the Tlinks in the top list box to the Tlink Group, select the "Add All" button.

3. To remove Tlinks from the Tlink Group, highlight the Tlink(s) in the bottom list box and select the "Delete Selected" button.

4. Select "OK" to record the changes in the Security Database or "Cancel" to return to the "Tlink Group Information" dialog box without changing the data in the Security Database.

## **Viewing a Tlink Group**

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



1.

From the "Tlink Group Information" dialog box, select the Tlink Group that you want to view and select "View." The "View Tlink Group" dialog box is displayed:

Figure 4-21 View Tlink Group Dialog Box

View Tlink Group Sales
All CSTA Tlinks Not Currently In Group:
TSERVER#NSRV#CSTA#ACME_NY
All CSTA Tlinks Currently In Group:
LUCENT#CSTASERV#CSTA#ACME_NY
Clo <u>s</u> e

2. Select "Close" when you have finished viewing the selected Tlink Group.

## **Deleting a Tlink Group**

You can only delete a Tlink Group if there are no devices currently associated with it.



1.

From the "Tlink Group Information" dialog box, select the Tlink Group that you want to delete and select "Delete." The "Delete Tlink Group" dialog box is displayed:

#### Figure 4-22 Delete Tlink Group Dialog Box

Delete Tlink Group Sales
All CSTA Tlinks Not Currently In Group:
All CSTA Tlinks Currently In Group:
LUCENT#CSTASERY#CSTA#ACME_NY
0K Cancel

If this Tlink Group is used by one or more devices, the "Unable to Delete [group]" dialog box is displayed instead, containing the following message: "Deletion of a Tlink Group is not allowed while there are devices associated with the Tlink Group." A list of all devices currently associated with the Tlink Group is provided.

#### Figure 4-23 Unable to Delete Tlink Group Dialog Box

- Unable to Delete -	Sales
Deletion of a Tlink Group is not allowed while there are devices associated with the group.	
Devices associated with this Tlink Group:	
7701 7702 7703	<u>E</u> dit Selected
7704	<u> </u>

To delete the Tlink Group, do the following for each device in the list:

- a) Highlight the device.
- b) Choose "Edit Selected." The "Edit Device" dialog box is displayed.
- c) Change the Tlink Group attribute for the device.
- d) Select "OK" on the "Edit Device" dialog box.



When using the TSA32 to delete a Tlink Group, any devices that are currently associated with the group will automatically be changed to "Any Tlink." See Chapter 5 for details.

	Edit Device
Device <u>I</u> D:	7710
Location:	NY Room 506
Device <u>T</u> ype:	PHONE <u>±</u>
Tlink <u>G</u> roup:	Any Tlink <b>±</b> ⊻iew Group
View Associations	
<u>D</u> K <u>C</u> ancel	

Once all the device references to this Tlink Group are removed, you can close the dialog box and return to the "Tlink Group Information" dialog box. The device previously selected for deletion is still highlighted. Select "Delete" and continue.

2. Select "OK" to remove the Tlink Group from the Security Database or "Cancel" to return to the "Tlink Group Information" dialog box without deleting the Tlink Group.

# **Administering Devices**

These procedures allow you to create, edit, and delete Device objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these procedures to add the same devices. You may edit or delete those devices using these procedures.

The attributes that make up the Device object are administered using these procedures. Each attribute is briefly described below. For more details, see the "Device Attributes" section of Chapter 2.

- Device ID is the exact string of numbers that the PBX uses to identify a particular device (e.g., the extension of the telephone on your desk). Refer to your vendor's PBX documentation for detailed information on the required string.
- Location is an optional field. You can use it to indicate where the device is located.
- Device Type (PHONE, FAX, MODEM, ACD) is an optional entry that shows the administered type for the device. The default type is "PHONE." This field is not used by the telephony server; it is provided for information only.
- **Tlink Group** is the list of Tlinks that are allowed to control the device. "Any Tlink" is the default value.


1.

From the "Admin" menu, select "Devices." The "Device Information" dialog box is displayed:

Figure 4-24 Device Information Dialog Box

_		De	vice Information		
	Device ID	Device Type	Location	Tlink Group	
	7701	PHONE	NY Room 404	Sales +	
	7702	PHONE	NY Room 405	Sales	
	7703	PHONE	NY Room 407	Sales	
	7704	PHONE	NY 4th fl sec	Sales	
	7705	PHONE		Any Tlink	
	7706	PHONE		Any Tlink	
	7710	PHONE	NY Room 506	Any Tlink	
	7711	PHONE	NY Room 507	Any Tlink	
	7712	PHONE	NY Room 508	Any Tlink	
	7713	PHONE	NY 5th fl recept	Any Tlink 🗌	
	7720	PHONE	NY Shipping Do	c Any Tlink 🛛 🖬	
	<u>C</u> reate	<u>E</u> dit	<u>⊻</u> iew <u>D</u>	elete C <u>l</u> ose	
	<u>C</u> reate	<u>E</u> dit	<u>V</u> iew <u>D</u>	elete C <u>l</u> ose	_

2. Scroll or browse through the list of devices. Either select an existing device or create a new one.

## **Creating a Device**



1.

From the "Device Information" dialog box, select "Create." The "Create Device" dialog box is displayed:

Figure 4-25 Create Device Dialog Box

	Create Device
Device <u>I</u> D:	7710
Location:	NY Room 506
Device <u>T</u> ype:	PHONE <u>+</u>
Tlink <u>G</u> roup:	Any Tlink 👱 View Group
	View <u>A</u> ssociations
	<u>O</u> K <u>C</u> ancel

- 2. Enter the Device ID. Enter other values as desired.
- 3. Select "OK" to add the device to the Security Database, or "Cancel" to return to the "Device Information" dialog box without adding the new device to the Security Database.

#### **Editing a Device**



1.

From the "Device Information" dialog box, select the device you want to edit and select "Edit." The "Edit Device" dialog box is displayed:

Figure 4-26 Edit Device Dialog Box

	Edit Device
Device <u>I</u> D:	7710
Location:	NY Room 506
Device <u>T</u> ype:	PHONE <u>+</u>
Tlink <u>G</u> roup:	Any Tlink <u>±</u> <u>V</u> ie <del>w</del> Group
	View Associations <u>D</u> K <u>C</u> ancel

- 2. Change device attributes as desired.
- 3. Select "View Group" to view all administered Tlinks currently associated with the selected Tlink Group.

Select "Close" when you have finished viewing the Tlink Group information in the dialog box.

4. Select "View Associations" to display both the device groups to which this device belongs and worktops and users associated with this device.



1		Device Associations					
	Current <u>G</u> roups Device is in:						
	Worktons and Us	ers Associated with Device					
	Worktop Name	Login ID					
	President	LCHEN					
		<u>C</u> lose					

The "Device Associations" dialog box displays a list of the device groups that contain the chosen device, and a list of worktops and users associated with that device. Select "Close" when you are done viewing this dialog box.

5. Select "OK" to save the new device information in the Security Database, or "Cancel" to return to the "Device Information" dialog box without changing the data in the Security Database.

#### **Viewing a Device**

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



1. From the "Device Information" dialog box, select the device that you want to view and select "View." The "View Device" dialog box is displayed:

Figure 4-28 View Device Dialog Box

1	View Device
Device <u>I</u> D:	7710
Location:	NY Room 506
Device <u>T</u> ype:	PHONE <b>±</b>
Tlink <u>G</u> roup:	Any Tlink 🛨 View Group
	View Associations
	Close

2. Select "View Group" to view all administered Tlinks currently associated with the selected Tlink Group.

Select "Close" when you have finished viewing the Tlink Group information in the dialog box.

- 3. Select "View Associations" to display both the device groups to which this device belongs and worktops and users associated with this device.
- 4. Select "Close" when you have finished viewing the information for the selected device.

#### **Deleting a Device**



1.

From the "Device Information" dialog box, select the device you want to delete and select "Delete." The "Delete Device" dialog box is displayed.

Figure 4-29 Delete Device Dialog Box

- Delete Device				
Device <u>I</u> D:	7710			
Location:	NY Room 506			
Device <u>T</u> ype:	PHONE <b>±</b>			
Tlink <u>G</u> roup:	Any Tlink 👱			
View Associations				
	<u>O</u> K <u>C</u> ancel			

If a worktop is associated with this device, you cannot delete the device. The "Unable to Delete Device" dialog box is displayed instead, containing the following message: "Deletion of a Device ID is not allowed while there are worktops associated with the Device ID." A list of all worktops currently associated with the Tlink Group is provided.



Unable to Delete Device				
Deletion of a Device ID is not allowed while there are worktops associated with the Device ID.				
Worktops associated with this Device ID:				
President				
	Edit Selected			
	<u>C</u> lose			
	]			

To delete the device, do the following for each worktop in the list:

- a) Highlight the worktop.
- b) Choose "Edit Selected." The "Edit Worktop" dialog box is displayed.
- c) Change the primary device ID entry for the worktop
- d) Select "OK" on the "Edit Worktop" dialog box.



When using the TSA32 to delete a device, any worktops that are currently associated with the device will updated automatically. See Chapter 5 for details.

1	Edit Wor	ktop
	Worktop Name:	President
	Primary Device ID:	7710 <u>+</u>
	LAN <u>A</u> ddress	85
	Secondary Device Group:	(none) ±
	Logins Associated with this We	orktop:
	LCHEN	
	<u>O</u> K <u>V</u> iew Selecte	d <u>C</u> ancel

Once all worktop references to this device are removed, you can close the dialog box and return to the "Device Information" dialog box. The device previously selected for deletion is still highlighted. Select "Delete" and continue.

2. Select "OK" to delete the device, or select "Cancel" to return to the "Device Information" dialog box without deleting the device.

# **Administering Device Groups**

Device Groups are lists of devices. When assigned to a user's worktop or service class of permissions, they give or restrict user control over all the devices in the group. See Chapter 2, Device Group Objects, for more details.

The attributes for a device group are the devices in the group and whether the device group is an exception group. Devices added to the group are selected from the administered devices for the Tserver.

If the group is designated as an exception group, the Tserver treats the entire group as if it contained every device *except for* those devices in the device group. For example, suppose Robert is a supervisor with permission to control all of the phones in the company except for those belonging to the president and vice president. Rather than setting up a device group that contains all of the devices except for those belonging the president and the vice president, you could set up an exception group and assign it to Robert. This exception group would only contain the devices of the president and vice president.

Once you have selected a device group, a dialog box containing two list boxes is displayed.

#### All Administered Devices Not Currently In Group

#### All Administered Devices Currently In Group

It is likely that the list of devices not currently in any group exceeds the available room in the list box. You can quickly find any existing device by entering the device ID you are looking for in the "Find Device ID" box. The device ID you enter becomes the first device in the list box.



From the "Admin" menu, select "Device Groups." The "Device Group Information" dialog box is displayed.

Figure 4-31 Device Group Information Dialog Box

1.

	Device Group Infor	mation
Device <u>G</u> roups	:	
Execs LA Sales		Create
NT Sales		<u>E</u> dit
		<u>⊻</u> iew
		Delete
	C <u>l</u> ose	

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

#### **Creating a Device Group**

1.

Procedure

From the "Device Group Information" dialog box, select "Create." The "Create Device Group" dialog box is displayed:

Figure 4-32 Create Device Group Dialog Box

Create Device Group				
<u>D</u> evice Group Name:	Help Desk <u>C</u> ancel			

- 2. Enter the name for the new device group.
- 3. Select "OK" to display the "Create Device Group" dialog box, or select "Cancel" to return to the "Device Group Information" dialog box without creating the device group.



Figure 4-33 Create Device Group Dialog Box

- 4. To make the device group an exception group, set the "Exception Group" check box.
- 5. To add a device to the device group, highlight the device in the top list box. (You can also select multiple devices by using the Shift and Control keys.) Select the "Add" button.

- 6. To remove a device from the device group, highlight the device in the bottom list box. (You can also select multiple devices by using the Shift and Control keys.) Select the "Delete" button.
- 7. When finished, select the "OK" button to add the device group to the Security Database, or select the "Cancel" button to return to the "Device Group Information" dialog box without creating the device group.

#### **Editing a Device Group**



1.

From the "Device Group Information" dialog box, select a device group and select "Edit." The "Edit Device Group" dialog box is displayed:

Figure 4-34 Edit Device Group Dialog Box

⇒ Edit Device Group Help Desk						
All Administered Devices Not Currently In Group						
Find Device ID:						
	Device					
Device <u>I</u> D	Туре	Location	Tlink Group			
7704	PHONE	NY 4th fl sec	Sales 🔸			
7705	PHONE		Any Tlink			
7706	PHONE		Any Tlink			
7708	FAX	4th fl sales	Sales			
7710	PHONE	NY Room 506	Any Tlink			
7711	PHONE	NY Room 507	Any Tlink 📃			
7712	PHONE	NY Room 508	Any Tlink 🛛 🛨			
<u>A</u> dd	<u>D</u> elete	<u><u> </u></u>	<u>C</u> ancel			
All Administered Devices Currently In Group						
All Administered A	Devices Curre	ntly In Group 💳				
All Administered I	Devices Curre Device	ntly In Group	Group			
⊤All Administered I De <u>v</u> ice ID	Devices Curre Device Type	ntly In Group <u>E</u> xception Location	Group Tlink Group			
⊤All Administered I De <u>v</u> ice ID  7702	Devices Curre Device Type PHONE	ntly In Group <u>Exception</u> Location NY Room 405	Group Tlink Group Sales			
<sup>∼</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE	ntly In Group Exception Location NY Room 405 NY Room 407	Group Tlink Group Sales Sales			
<sup>∼</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE PHONE	ntly In Group Exception Location NY Room 405 NY Room 407	Group <u>Tlink Group</u> Sales Sales			
<sup>∼</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE	ntly In Group <u>Exception</u> Location NY Room 405 NY Room 407	Group <u>Tlink Group</u> Sales Sales			
<sup>~</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE	ntly In Group Exception Location NY Room 405 NY Room 407	Group Tlink Group Sales Sales			
<sup>~</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE	ntly In Group <u>Exception</u> Location NY Room 405 NY Room 407	Group Tlink Group Sales Sales			
<sup>~</sup> All Administered I De <u>v</u> ice ID 7702 7703	Devices Curre Device Type PHONE PHONE	ntly In Group Exception Location NY Room 405 NY Room 407	Group <u>Tlink Group</u> Sales Sales			

The system displays a scroll box containing information about the devices in the device group, one per line.

2. To add devices to the device group, highlight the devices in the top list box and select the "Add" button.

- 3. To delete devices from the "All Administered Devices Currently In Group" box, highlight one or more devices and select "Delete."
- 4. To make the device group an exception group, set the "Exception Group" check box.
- 5. Select "OK" to save the changes in the Security Database or "Cancel" to return to the "Device Information Group" dialog box without changing any data in the Security Database.

## Viewing a Device Group

1.



From the "Device Group Information" dialog box, select the desired device group and select "View." The "View Device Group" dialog box is displayed:

Figure 4-35 View Device Group Dialog Box

_	View Devi	ice Group Help D	esk		
All Administered Devices Not Currently In Group					
<u>Find Device ID:</u>					
	Device				
Device <u>I</u> D	Туре	Location	Tlink Group		
7704	PHONE	NY 4th fl sec	Sales		
7705	PHONE		Any Tlink		
7706	PHONE		Any Tlink		
7708	FAX	4th fl sales	Sales		
7710	PHONE	NY Room 506	Any Tlink		
7711	PHONE	NY Room 507	Any Tlink		
7712	PHONE	NY Room 508	Any Tlink	+	
		<u>C</u> lose			
All Administered D	evices Curre	ntly In Group			
	Device	<u>Exception</u>	Group		
De <u>v</u> ice ID	Туре	Location	Tlink Group		
7702	PHONE	NY Room 405	Sales		
7703	PHONE	NY Room 407	Sales		
[					

2. Select "Close" to return to the "Device Group Information" dialog box.

#### **Deleting a Device Group**

This procedure allows you to delete a device group. If the group is assigned to the class of service fields in any User objects or if it is assigned as a secondary device group for any Worktop objects, the device group entry is removed from these objects.



1.

From the "Device Group Information" dialog box, select the desired device group and select "Delete." The "Delete Device Group" dialog box is displayed:

Figure 4-36 Delete Device Group Dialog Box

Delete Device Group Help Desk						
All Administered Devices Not Currently In Group						
Find Device ID:						
Device <u>I</u> D	Device Type	Location	Tlink Group			
		<u>K</u>	<u>C</u> ancel			
All Administered Devices Currently In Group						
Device ID	Device Tune	Location	Tlink Groun			
7702	PHONE	NY Room 405	Sales			
7703	PHONE	NY Room 407	Sales			

2. Select "OK" to delete the device group from the Security Database, or select "Cancel" to return to the "Device Group Information" dialog box without deleting the device group from the Security Database.

# **Administering Worktops**

These procedures allow you to create, edit, and delete Worktop objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these procedures to add the same worktops. However, you can edit or delete worktops created by "Quick Add" using these procedures.

The attributes that make up the Worktop object are briefly described below. See "The Worktop Object" section in Chapter 2 for more details.

- Worktop Name: A unique name that identifies the worktop.
- **Primary Device ID**: The primary device on the worktop, usually the extension of the telephone.
- LAN Addresses: A button that brings up the LAN Addresses dialog box listing the addressing options for the workstation. If you wish to use the "Extended Worktop Access" feature, you must either
  - Let the system fill in the fields automatically by enabling the "Automatic Administration of LAN Addresses" feature (available from the Maint/Tserver Options menu), or
  - Supply the TCP/IP address of the workstation on the worktop. Enter either the host name or the IP address, depending on the TCP Preferred Naming Format you have chosen for Telephony Services. (See Chapter 7 for details about TCP Preferred Naming Format.)

- Secondary Device Group: A drop-down list showing all device groups. If applicable, select the device group containing ant additional devices located at this worktop, thus enabling the user associated with the worktop to control these devices. See Chapter 2 for details on the uses of this device group. This is an optional field.
- Logins Associated with this Worktop. Users that have been associated with this worktop.

A **View Selected** button is available on the create, edit, and view worktop dialog boxes. This button allows you to get additional information about a device ID, a secondary device group, or a login from the worktop dialog box. To view the attributes for that object, highlight the object you are interested in and select the "View Selected" button. The appropriate dialog box is displayed, containing the attributes for that object.



1.

# From the "Admin" menu, select "Worktops." The "Worktop Information" dialog box is displayed:

Figure 4-37 Worktop Information Dialog Box

ice ID	
5 1	
2	Create
3	
0	
0	<u>E</u> dit
0	<u>_</u>
1	
0	<u><u>v</u>iew</u>
1	
4	Delete
5 🗕	
	2 3 0 0 1 1 0 1 4 5 ↓

2. Scroll or browse through the list of administered worktops. Then either select an existing worktop or create a new one.

## Creating a Worktop

Procedure 123

1.

From the "Worktop Information" dialog box, select "Create." The "Create Worktop" dialog box is displayed:

Figure 4-38 Create Worktop Dialog Box

🛥 Creat	e Worktop
<u>W</u> orktop Name:	Service 3
<u>P</u> rimary Device ID:	7708 🛨
LAN <u>A</u> d	dresses
<u>Secondary Device Group:</u>	(none) 👤
Logins Associated with th	nis Worktop:
OK <u>V</u> iew Se	elected <u>C</u> ancel

- 2. Fill in the name of the worktop and select the primary device from the drop-down list.
- 3. If you want to enter LAN address information for the worktop, select the "LAN Addresses" button. The "LAN Addresses" dialog box is displayed:

Figure 4-39 LAN Addresses Dialog Box

-	LAN Addresses
□IPX/SPX Ne <u>t</u> work:	<u>N</u> ode:
TCP/IP Host Name:	
IP Address:	137.94.11.251
	Close

- 4. When you have finished entering the LAN Address information, select "Close" to return to the "Create Worktop" dialog box.
- 5. Select "OK" to save the worktop information in the Security Database or select "Cancel" to return to the "Worktop Information" dialog box without creating the worktop.

#### **Editing a Worktop**



1.

From the "Worktop Information" dialog box, select the worktop you want to edit and select "Edit." The "Edit Worktop" dialog box is displayed:

Figure 4-40 Edit Worktop Dialog Box

📥 Edit	Worktop
<u>W</u> orktop Name:	Service 3
<u>P</u> rimary Device ID:	7708 🛨
LAN <u>A</u> do	tresses
Secondary Device Group:	(none) <u>+</u>
Logins Associated with th	is Worktop:
N	
<u>O</u> K <u>V</u> iew Se	lected <u>C</u> ancel

#### 2. Make changes as needed to the worktop's attributes.

If you want to change the LAN address for the workstation, select the "LAN Addresses" button.

3. Select "OK" to record the changes the Security Database, or "Cancel" to return to the "Worktop Information" dialog box without changing data in the Security Database.

## **Viewing a Worktop**

This option lets you display information about a worktop; you cannot make any changes using this dialog box.



1.

From the "Worktop Information" dialog box, select the worktop you want to view and then select "View." The "View Worktop" dialog box is displayed:

#### Figure 4-41 View Worktop Dialog Box

🛥 View	Worktop
Worktop Name:	Service 3
Primary Device ID:	7708 <u>+</u>
LAN <u>A</u> dd	lresses
<u>S</u> econdary Device Group:	(none) 🛓
Logins Associated with th	is Worktop:
View Se	ected

2. Select "Close" to return to the "Worktop Information" dialog box.

## **Deleting a Worktop**



From the "Worktop Information" dialog box, select the worktop you want to delete and select "Delete." The "Delete Worktop" dialog box is displayed:

Figure 4-42 Delete Worktop Dialog Box

- Delete	Worktop
<u>W</u> orktop Name:	Service 3
<u>P</u> rimary Device ID:	7708 <u>+</u>
LAN <u>A</u> dd	resses
Secondary Device Group:	(none) 👤
Logins Associated with thi	s Worktop:
	<u>C</u> ancel

2. Select "OK" to delete the worktop from the Security Database, or select "Cancel" to return to the "Worktop Information" dialog box without deleting the worktop.

116 Network Manager's Guide

# **Administering Users**

These procedures allow you to create, edit and delete User objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these procedures to add the same users. However, you can edit or delete users created by "Quick Add" using these procedures.



In order to access Telephony Services, users must have a Windows NT login ID and password. In addition, they must have the "Log on as a service" user right assigned to their account on the Windows NT Machine that is running Telephony Services. This information is administered through the Windows NT User Manager. For more details, refer to the "User Authentication" section in Chapter 7.

The attributes that make up the User object are briefly described below. See "The User Object" section of Chapter 2 for more details about the attributes.

- Login: the user's login as administered through the Windows NT User Manager.
- Name: the user's name.
- Worktop Name/Primary Device ID: a drop-down list showing the administered worktops along with the primary device assigned to the worktop. Select a worktop for the user from this list. Multiple users may share the same worktop. Choose "(none)" to specify that the user does not have a worktop.

Each user dialog box allows you to view the details about the individual worktop or device you have currently selected by choosing either the "View Worktop" or "View Device" option.

- ◆ Admin Access Group Information : indicates whether or not a user has administration permissions. You can grant these permissions to a user by checking the "Allow User to Administer Admin Access Groups?" box in the "Create User" option, or by including the user in the "Allowed Users" list for an Admin Access Group.
- **Options:** a separate dialog box that is displayed when you select the "Options" button on any of the Create, Edit, View, or Delete user dialog boxes. When you select "Options," the user's Class of Service attributes are displayed. For a complete discussion of Class of Service attributes, see Chapter 3.

#### **Accessing User Information**

1.

Procedure

User Information Dialog Box

Figure 4-43

From the "Admin" menu, select "Users." The "User Information" dialog box is displayed:

ogin	Name	Home Worktop Name	Home Worktop Device ID	
3J₩	Brian Wallis	Help Desk 2	7703	+
30B	Robert Martinez	Loading Dock	7720	
EGKEENE	Edward Keene	Sales 1	7700	
ESTHER	Esther Cohen	Loading Dock	7720	$\square$
FRANK	Frank Fuller	Sales 4	4401	
FRR	Frances Reese	Exec Secretary	7713	-   !
HJG	Harry Gardner	VP 2	7712	
LALITHA	Lalitha Harris	VP 1	7711	-   !
LCHEN	Lee Chen	President	7710	
LSM	Leslie Kuhn	Sales sec/admin	7704	
LUIS	Luis Munoz	Sales 2	7701	+

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

If the contents of a field are too long for the display, select "Edit" or "View" to see the complete field contents.

## **Creating a User**



1.

From the "User Information" dialog box, select "Create." The "Create User" dialog box is displayed:

Figure 4-44 Create User Dialog Box

	Create User					
<u>L</u> ogin:	Alice	<u>N</u> ame:	Alice Katz			
<b>₩orktop</b>	Information					
Worktop	Name / <u>P</u> rimary Device ID:	S	ales 3 / 4400	<b>±</b>		
	View Worktop		⊻iew Device…	]		
Admin Ac	cess Group Information User to Administer Admin Admin Admin Admin Adminiater	ccess Groups?				
Current A	dmin Access <u>G</u> roups User is	s in:		<u>+</u> +		
	<u> </u>	Options	<u>C</u> ancel			

- 2. Enter the user's login as administered through the Windows NT User Manager.
- 3. Select the user's worktop name/primary device ID pair from the drop-down list of administered IDs.
- 4. If you want the user to be able to administer admin access groups, set the "Allow User to Administer Admin Access Groups?" checkbox.
- 5. If this user is to be administered with "Classes of Service" options, continue with Step 6. Otherwise, continue with Step 9.
- 6. Select "Options" if you wish to administer classes of service for this user. The "Create User Options" dialog box is displayed.



- Create	User - Options					
CLASSES OF SERVICE						
<u>Call Control Services - Call Origination</u>	Call Control Services - Call Origination and Termination					
Device Group:	(none) ±					
「Monitoring-Only Services 	eases if call leaves device					
Device Group:	(none) ±					
Call/D <u>e</u> vice - Event Notification conti	nues if call leaves device					
Device Group:	(none) <u>±</u>					
Call/Call - Event Notification allowed if call identifier is known						
∟ <u>⊢ R</u> outing Services - Allow routing on list	ed devices					
Device Group:	(none) 👱					
Close	<u>⊻</u> iew Selected					

#### 7. Assign one or more of the desired classes of service.

For each class of service (except Call/Call monitoring), you can use the drop-down lists of all the currently administered device groups to select a group for this user. The Call/Call monitoring is either enabled or disabled. See Chapter 3 for details about classes of service.

The **View Selected** button displays the members of a device group for a selected group. Highlight a device group and press "View Selected."

You may administer some, none, or all of the classes of service.

- 8. Select "Close" to return to the "Create User" dialog box.
- 9. Select "OK" to add the user to the Security Database, or select "Cancel" to return to the "User Information" dialog box without adding the new user to the Security Database.

## **Editing a User**



1.

From the "User Information" dialog box, select a user and select "Edit." The "Edit User" dialog box is displayed:

Figure 4-46 Edit User Dialog Box

	Edit	User		
<u>L</u> ogin:	ALICE	<u>N</u> ame:	Alice Katz	
<b>∵</b> Worktop Info	rmation			
Worktop Nam	ie / <u>P</u> rimary Device ID:	Sales 3 / 4	400	ŧ
	View <u>W</u> orktop	 ⊻iew De	vice	
Admin Acces	s Group Information r to Administer Admin Access Group	ps?		
Current Admir	) Access <u>G</u> roups User is in:			+
	<u>O</u> K Op <u>t</u> ion	s	<u>C</u> ancel	

- 2. Make any user attribute changes you desire.
- 3. To view the worktop that is currently displayed for this user, select "View Worktop."
- 4. To see the attributes of the device associated with the worktop name, select "View Device."

- 5. Select "Options" to display the "Edit User Options" dialog box to see if this user has been administered for Classes of Service.
  - 5a. Make any desired changes on the "Edit User Options" dialog box.
  - 5b. Select "Close" to return to the "Edit User" dialog box.
- 6. Select "OK" to save the changes in the Security Database or "Cancel" to return to the "User Information" dialog box without changing any data in the Security Database.

#### Viewing a User

View User Dialog Box

Figure 4-47



1. From the "User Information" dialog box, select a user and select "View." The "View User" dialog box is displayed:

The View User					
<u>L</u> ogin:	ALICE	<u>N</u> ame	e:	Alice Katz	
<b>₩orktop</b>	Information				
Worktop	Name / <u>P</u> rimary Device ID:	[	Sales 3	/ 4400	1
	View <u>W</u> orktop		<u>V</u> iew	Device	
<sup>∼</sup> Admin Ad 	ccess Group Information User to Administer Admin Acce Admin Access <u>G</u> roups User is in	ss Groups?			-
	Close	Op <u>t</u> ions	ר		

- 2. To view the worktop that is currently displayed for this user, select "View Worktop."
- 3. To see the attributes of the device associated with the worktop name, select "View Device."

- 4. Select "Options" to display the "Edit User Options" dialog.
- 5. Select "Close" to return to the "User Information" dialog box.

#### **Deleting a User**

To ensure that at least one user is always able to perform administration, you cannot delete the last user from the "All Admin Access" group.



1. From the "User Information" dialog box, select a user and select "Delete." The "Delete User" dialog box is displayed:

#### Figure 4-48 Delete User Dialog Box

-		Delete	User				
<u>L</u> ogin:	ALICE		<u>N</u> ame:	Alice Katz			
└ Worktop Information							
Worktop Name / Primary Device ID:			Sales 3 / 4400 ±		±		
Admin Access Group Information							
Current Admin Access <u>G</u> roups User is in:							
	<u>0</u> K	Option	s	<u>C</u> ancel	]		

- 2. To show the Class of Service groups assigned to the user, select "Options." The "Delete User - Options" dialog box is displayed. Select "Close" to return to the "Delete User" dialog box.
- 3. Select "OK" to delete the user from the Security Database, or select "Cancel" to return to the "User Information" dialog box without deleting the user.

# **SDB Logging**

You can choose whether you want SDB transactions to be logged and if so, to set the size of the Security Database log file. For more information about logging and log files, refer to the section "General Logging Information" in Chapter 11.

#### Using the TSA to Set SDB Log Settings

1.

Procedure

From the "Maint" menu, select "SDB Logging." The "SDB Logging" dialog box is displayed:

Figure 4-49 SDB Log Settings

SDB Logging					
Log Changes to SDB					
<u>S</u> DB Log File Size (bytes):	100000				
SDB Log <u>F</u> ile:	\\acme_ny\progra~1\teleph~1\tsrv\logfiles\sdblog.tx				
<u></u> K	<u>C</u> ancel				

2. Set the log size and enable logging by setting the "Log Changes to SDB" checkbox. Then select "OK" for your choices to take effect.

124 Network Manager's Guide

chapter

# **5** Using the TSA32 to Administer the Security Database

This chapter describes the basic operation of the 32-bit Telephony Services Administrator application (TSA32). It describes how you can add Telephony Services objects easily to the SDB using "Quick Add." Following the "Quick Add" section you will find instructions on how to administer system-wide features as well as instructions for controlling SDB administration access by administering Admin Access Group objects. If you do not require any additional access restrictions, these three sections describe all of the administration you need to do.



In order to properly administer your SDB, you should be familiar with the SDB concepts covered in Chapter 2.

The remaining sections of this chapter discuss the order to follow for administering Telephony objects, and the TSA32 procedures that administer the Tlink, Tlink Group, Device, Device Group, Worktop, and User objects. The last section describes how to log SDB transactions to a log file.

Additional procedures that enable maintenance and performance tuning are described in other chapters:

**Chapter 6:** Administering the SDB in bulk (for automating certain aspects of SDB administration)

Chapter 7: Connecting your telephony server and clients to the LAN

Chapter 8: Tserver status and maintenance functions

Using the TSA32 to Administer the Security Database 125

Chapter 9: Telephony Services traffic measurements

Chapter 10: Cserver administration, status, and maintenance functions

Chapter 11: Enabling troubleshooting functions



The administrative changes you make to a particular user's permissions will not affect applications currently in use by that user. Users must end the application and restart it before changes take effect. This is because the Tserver stores much of the user's information in its memory when it sets up a connection. This makes subsequent permissions checking much faster.

# **Telephony Services Administrator (TSA32)**

The Telephony Server Administrator (TSA32) client application provides an MS Windows 95 "look and feel" for administering your Telephony Servers. Using the TSA32 menus, you can perform administration tasks and get online help. The TSA32 also allows you to have simultaneous connections to multiple Telephony Servers.

Immediately after installation, only the Administrator login can access and administer the Tserver.



If you also have Telephony Services for NetWare, you cannot use the TSA32 application to administer those Telephony Servers. Use the TSA or NWAdmin tools provided with the NetWare product when administering those Telephony servers.



Since two users can access the Tserver at the same time, one user can make changes that are not immediately visible to another user. If the second user attempts to edit the same information, an error appears. To view current edits, redisplay the screen (close the dialog box, then open it again).

#### Starting the TSA32 Application

1.



From the "TS Win32 Client" program group, double-click on the "Telephony Services Admin" icon. The "Open Tserver" dialog box is displayed:

Figure 5-1 Open Tserver Dialog Box

-	Open Tserver	
<u>T</u> server:		
ACME_NY	ŧ	OK
		Cancel
		Help
<u>L</u> ogin:	Ism	
Password:	*******	

2. From the "Tserver" drop-down list, select the Tserver you want to administer.

#### 3. Fill in the "Login" and "Password" fields.

Immediately after installation, only the Administrator login ID is authorized to administer the Tserver.

If you are already logged in to the Windows NT machine for the selected Tserver, you will not be prompted to enter a password.

4. Select "OK" to access that Tserver, or "Cancel" to close the "Open Tserver" dialog box without logging in to a Tserver.




### **TSA32** Features

When you first start the TSA32 application, the TSA32 main window is displayed. Once you connected to a Tserver, the title bar displays the name of that Tserver. The main window includes a menu bar, a tool bar, and the SDB window. The SDB window is split into a tree view (on the left-hand side of the window) and an object view (on the right-hand side of the window). The SDB tree view displays several icons, each of which represents an SDB object type.

The SDB icon appears at the top of the tree view. The name of the Tserver you are connected to appears in the object view (below the tool bar).

#### The TSA32 Menu Bar

The TSA32 menu bar contains File, Admin(istration), View, Window, and Help menus.

- The "File" menu allows you open another Tserver connection, close the current Tserver connection, or exit the Telephony Services Administrator.
- The "Admin" menu allows you to create objects in the Security Database, to use "Quick Add" to create objects, or to invoke Bulk Administration commands. This menu also allows you to display object properties and to remove objects from SDB.
- The "View" menu allows you to change the presentation of information in the object view. There are four different formats: Large Icon View, Small Icon View, List View, and Detailed View. The "View" menu also gives you the option of displaying the tool bar and the status bar.
- The "Window" menu allows you to add a new window, cascade, tile, or arrange icons. This menu also allows you to switch between different Tservers, if you have open connections to more than one Tserver.
- The "Help" menu provides access to on-line help and version information for the TSA32.

#### The TSA32 Tool Bar

The TSA32 tool bar gives you access to many of the menu items without having to work your way through all the menus or having to remember any keyboard accelerators. The tool bar provides "tool tips" whenever the cursor is over an icon on the tool bar (a small pop-up window appears, telling you the purpose of the icon).

Figure 5-3 presents a summary of the tool bar icons and the tool tip that is displayed for each icon. For details of the operations described, see the appropriate section in this chapter.

#### Figure 5-3 The TSA32 Tool Bar



130 Network Manager's Guide

#### The TSA32 SDB Window

The SDB window is divided into two parts: a tree view and an object view. The views are divided by a separator bar (the SDB tree view is to the left of the bar; the object view is to the right of the bar).

#### **SDB Tree View**

The tree view items in the SDB window are fixed, and the icons appear in the following order: SDB, Users, Worktops, Devices, Device Groups, Tlinks, Tlink Groups, and Admin Access Groups. To view the administered objects for an object type, click on the icon for that object type. The information appears in the object view box, on the right-hand side of the window.

#### SDB Object View

The object view displays all of the administered objects for the type selected in the tree view, and can be displayed four different ways:

- Detailed View is the only view that includes the "List" title bar. It also includes more information than just the names of the objects and their corresponding icons. The "List" title bar consists of a set of columns with labels. For each object type, the number of columns and the labels on each column are different. (There is one row for each object, and many of the object's attributes are displayed along with the object name.)
- **List View** lists items in multiple columns that fit the view vertically, and allows you to scroll horizontally through the list.
- Small Icon View lists items in as many columns as fit the view horizontally, and allows you to scroll vertically through the list.
- Large Icon View is similar to the Small Icon View in that the view is filled in horizontally until no full items fit. You can then scroll vertically to see the remainder of the items.

### Tips for Using the TSA32

The TSA32 provides several methods for creating an object and for selecting an object in order to view or edit information for the object. The application also provides a number of ways for submitting changes. In addition, the TSA32 provides several quick methods for deleting objects from the database.

#### **Creating Objects**

The TSA32 provides three methods you can use to create objects:

- Select the appropriate "Create" option from the "Admin" menu.
- Click on a "Create" icon from the toolbar.
- Select an object type from the SDB tree view, then press the "Insert" key.

#### Selecting Objects

To select an object in order to view or edit information for the object, use one of the following methods:

- Select the object type from the tree view, then double-click on the object name in the object view.
- Highlight an object name in the object view, then select the "Display Properties" button on the tool bar.
- Highlight an object name in the object view, then select "Properties" from the "Admin" menu.
- Select an object type from the SDB tree view, then select "Properties" from the "Admin" menu. When the "Display Object Properties" dialog box is displayed, enter the name of the object and select "OK" (or press the "Enter" key).

Select an object type from the SDB tree view, then press "Ctrl/Enter" (hold down the "Ctrl" key while you press the "Enter" key). When the "Display Object Properties" dialog box is displayed, enter the name of the object and select "OK" (or press the "Enter" key).

#### Submitting New or Changed Object Information

If you are creating or changing information for an object, the TSA32 presents three options for submitting the information: the "OK" button, the "Cancel" button, and the "Apply" button.

"OK" and "Apply" provide equivalent functions: both will send the information you entered to the database. However, if you select "OK," the information is sent to the database and the dialog box is dismissed. If you select "Apply," the information is also sent to the database, but the dialog box is not dismissed. This can save time when you are creating multiple objects of the same type.

If you are **creating** information and you select "Apply," the fields on the dialog box are cleared after the information has been logged to the database. This allows you to continue to enter information for a number of objects consecutively. When you are done entering object information, select the "Cancel" button to dismiss the dialog. (If you select "OK" after the screen has been cleared, you will see an error message.)

If you are **editing** information and you select "Apply," the fields on the dialog box are not cleared after the information has been logged to the database. When you are done editing object information, you can select either "Cancel" or "OK." (If you select "OK" to accept changed information, you should not see any error messages.)

#### **Deleting Objects**

To delete objects from the SDB, use one of the following methods:

- Select the object(s) you want to delete, then press the "Delete" key.
- Select the object(s) you want to delete, then select "Remove Object" from the "Admin" menu.
- Select the object(s) you want to delete, then select the "Remove Object" button on the tool bar (represented by the large "X").

When you use any of these methods, the "Remove SDB Objects" dialog box is displayed, requesting confirmation for removing the object you selected. (The list of objects that will be deleted and a matching icon appear in the dialog box.)

E_NY 🔽
靋
ОК
Cancel
Help

Select "OK" to remove the object. Select "Cancel" to close the dialog box.

## **Using Quick Add**

"Quick Add" enables you to create a user, a worktop and a device using one simple procedure. The Quick Add dialog box has two sections where you can enter data: "User Information" and "Device and Worktop Information."

The User Information section contains two attributes: Login and Name. The login is a mandatory field that shows the user's login name. (You are not creating the login on the server here. You must use the Windows NT User Manager to create the login.) The Name is the user's name and is optional.



In order to access Telephony Services, users must have a Windows NT account. A Telephony Services user may access Telephony Services by using their own Windows NT login ID (in which case they are not required to provide their Windows NT password), or they can access Telephony Services using any other Windows NT login ID for which they can supply a password. In either case, the Windows NT login ID must exist in the Telephony Services Security Database.

Windows NT logins are administered through the Windows NT User Manager. If users wish to access Telephony Services using a Windows NT login ID other than their own, they must have the **Log on as a service** user right assigned to their account on the Windows NT machine that is running Telephony Services. For more details, refer to the "User Authentication" section in Chapter 7.

The **Device and Worktop Information** section contains three attributes: **Tlink Group**, **Primary Device ID**, and **Worktop Name**. The **Tlink Group** attribute is a drop-down list showing all administered Tlink groups. You can select the default Tlink group, "Any Tlink" if you do not want to restrict the user's device to a particular Tlink group. See Chapter 2 for more details. **Primary Device ID** identifies the primary device at the user's worktop. Typically, this is the extension of the telephone on the worktop. **Worktop Name** is the name of the user's worktop. You can use any naming convention you want, but each worktop must have a different name.



1. From the "Admin" menu, select "Quick Add." The "Quick Add" dialog box is displayed:

Figure 5-4 Quick Add Dialog Box

— Quic	:k Add - ACME_NY					
Enter New Data						
User Information						
Login:	Charlotte					
<u>N</u> ame:	Evans					
Device and Worktop Information						
Tlink <u>G</u> roup:	Sales 👱					
Primary Device ID:	7709					
Worktop Name:	NY Sales 3					
	<u>C</u> lose Help					

2. Enter the user information and the device and worktop information.

# 3. Select "Apply" to save the information in the Security Database.

The status line at the top of the screen indicates the progress of the Quick Add command by displaying the following messages:

Processing Data (The TSA32 is validating input data)

**Processing Device** (The TSA32 is adding a device object to your SDB)

**Processing Worktop** (The TSA32 is adding the worktop object to your SDB)

**Processing User** (The TSA32 is adding the user object to your SDB)

**Command Successfully Completed** (The TSA32 has added all the necessary objects for this user)

When the system redisplays "Enter New Data," you may enter new information for the next user. If the system cannot process the data, it displays an error message indicating the problem it encountered. These errors are explained in the "SDB Error Codes" section in Chapter 11, "Troubleshooting."

4. Select "Close" to close the "Quick Add" dialog box.

## **Administration of System-wide Features**

The "Tserver Options" dialog box is used to administer system-wide parameters. These parameters include the following:

- Extended Worktop Access: If you check this box, users who log in from a worktop other than their assigned worktop will be able to monitor and control the devices associated with that worktop, as well as monitor and control the devices on their assigned worktop and in their classes of service. See Chapter 3 for more details on this feature.
- Enable Automatic Administration of LAN Addresses: If the LAN address is not already assigned for the user's worktop and you enable this feature, the Tserver automatically fills in the LAN address information the next time the user logs on. (LAN addresses are only necessary if you are using the "Extended Worktop Access" feature.)

The Tserver checks the worktop object whenever a client opens a connection to the Tserver. If the worktop object does not contain the network address, it sets the address attribute of the worktop object to the network address it received in the open stream connection. You should use this feature only if users are going to log in from their own worktop for the first time.



If you are using Dynamic Host Configuration Protocol (DHCP), automatic administration of LAN addresses will not produce the desired results unless the TCP Preferred Naming Format is set to Host Name and Windows Internet Name Service (WINS) is also available.

◆ **TCP Preferred Naming Format:** The format of the LAN address saved for worktop objects is based on the setting of the "TCP Preferred Naming Format" field. The format can be set to either "Host Name" or "IP Address." See Chapter 7, "TCP/IP Configuration," for a complete discussion of these fields.



- 1. Select the SDB icon from the tree view of the SDB wind ow.
- 2. From the "Admin" menu, select "Properties" to open the "Tserver Properties" dialog box.

Figure 5-5 Tserver Properties Dialog Box

Tserver Properties - ACME_NY
Options SDB Log Settings Components
Enable Automatic Administration of LAN Addresses
TCP Preferred Naming Format
O Host Name   PAddress

- 3. From the "Options" tab, select the desired options.
- 4. Select "OK" to save the information in the Security Database.

## **Controlling SDB Administration Access**

Telephony Services restricts administration access to the SDB. Each user who will be administering Telephony Services is assigned a level of security; this level is kept in the SDB. Telephony Services has three levels of security: no SDB administration permissions; regular SDB administration permissions; and privileged users. Regular SDB administrators are allowed to add, change, and delete data in the SDB. Privileged users can modify data in the SDB and can also grant or revoke administrative privileges to other users.

One admin access group object is created when you install Telephony Services on a server: "ALL ADMIN ACCESS." Members of this group can administer all available modules; you do not need to explicitly add OAM Tlinks to this group. If all your administrators have permission to administer every administration module, you can assign each administrator to this group and skip the rest of this section. You do not need to create additional admin access groups.

When you first install Telephony Services, the Administrator user is added to the SDB with privileged permissions.

You must add a User object for each administrator to your SDB before you can assign them administration privileges. You can use either the "Quick Add" method described above or the more detailed User administration procedure described later in this chapter.

The TSA32 does not allow you to get into a situation where no one has administration privileges. The "ALL ADMIN ACCESS" group cannot be deleted and you cannot remove the last user from the group. Also, Telephony Services ensures that at least one user in this group will always have the ability to administer admin access groups.

140 Network Manager's Guide

#### Setting Up an Admin Access Group

Giving administration access rights to a group of users is a two-step process. First, you must identify the Tlinks that will be in the admin access group. Second, you must assign the users with the corresponding administration responsibilities to the appropriate admin access group(s).

An admin access group contains a list of OAM-type advertised services, or Tlinks. (OAM is the service type for administration.) When adding Tlinks to an admin access group, consider the following:

- Administrators who will be administering the SDB using the TSA32 require SDB\_OAM permissions.
- Administrators who will be performing maintenance tasks using the TSM32 require TSRV\_OAM permissions.
- Administrators who will be administering the SDB usi ng the TSA require both SDB\_OAM and TSRV\_OAM permissions.
- Administrators who will be administering options provided by the PBX vendor require the PBX driver OAM Tlink permissions.

The following example explains how you can set up several admin access groups and control which telephony servers the administrators can access. Suppose your organization has three administrators: Judy can administer the SDB data; Mike can perform PBX driver administration; and Luis can perform all administration. You would perform the following:

1. Create a "SDB ADMIN" group. Put the SDB\_OAM Tlink for the Tserver in this group:

TSERVER#SDB\_OAM#OAM#ACME\_NY

- 2. Add Judy to the SDB ADMIN group.
- 3. Create a "PBX ADMIN" group. Put the PBX\_OAM Tlink for the server in this group:

PBX\_VENDOR#PBX\_OAM#OAM#ACME\_NY

- 4. Add Mike to the PBX ADMIN group.
- 5. Add Luis to the ALL ADMIN ACCESS group. (You may also make a third admin access group containing all OAM Tlinks and add Luis to it.)

#### Admin Access Group Rules

The following rules apply when administering admin access groups:

- A Tlink may appear in more than one admin access group.
- A user may be associated with only one admin access group.
- The Tlinks in an admin access group may be from different vendors.

### **Administering Admin Access Groups**

Admin access group administration allows you to create new groups or modify an existing group. When you click on the "Admin Access Groups" icon in the SDB tree view, the names of all the admin groups on the server appear in the object view. If you highlight an existing group, you can edit the OAM Tlinks that make up the group, edit the list of "Allowed Users" who have access to the group, view the group, or delete the entire group.

Each dialog box has an "Allowed Users" tab. By selecting this tab, you can see all the users who are currently assigned to this admin access group and you can make changes as needed. If you delete an admin access group, the users who were allowed to administer OAM type Tlinks in the group will lose their administration permissions.

#### Creating an Admin Access Group

1.



From the "Admin" menu, select "Create Admin Access Group." The "Create Admin Access Group" dialog box is displayed, showing "Information" and "Allowed Users" tabs.

Figure 5-6 Create Admin Access Group Dialog Box

-	- Create Admi	n Access Grouj	p - ACME_NY
	Information Allowed Users		
	<u>G</u> roup Name:	LA Admin	
	Admin Tlinks <u>N</u> OT in Group:		Admin Tlinks <u>I</u> N Group:
	LUCENT#SDB_OAM#OAM#ACME_NY TSERVER#CSRV_OAM#OAM#ACME_ TSERVER#TSRV_OAM#OAM#ACME		LUCENT#SDB_OAM#OAM#ACME_LA
		>> A00 2>	
		< <u>&lt;</u> Delete <<	
	•		•
		OK Ca	ancel <u>A</u> pply Help

- 2. Enter the name for the new admin access group.
- 3. To add Tlinks to the admin access group, highlight the Tlink(s) in the "Admin Tlinks NOT in Group" list box and select the "Add" button.
- 4. To remove Tlinks from the admin access group, highlight the Tlink(s) in the "Admin Tlinks IN Group" list box and select the "Delete" button.

144 Network Manager's Guide

5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating an admin access group.

You are now able to assign users to this group. See the following section for details.

#### Administering Allowed Users

You can allow users to have administration permissions by including them in the "Allowed Users" list for a specified Admin Access Group, or by checking the "Allow User to Administer Admin Access Groups?" box on the "Admin Access Groups" tab, accessible from the "Create User" dialog box.

To view the list of "Allowed Users," select this tab from the "Admin Access Group Properties" dialog box.

The "Allowed Users" tab contains two list boxes:

• Users NOT in any Group

This box lists the login IDs of all users who currently are not authorized to perform administration and maintenance on any admin Tlink entries.

• Users IN Group

This box lists the login IDs of all users who currently are authorized to perform administration and maintenance on the OAM Tlink entries in the selected admin access group.



1.

Select the "Allowed Users" tab.

Figure 5-7 Allowed Users Tab

🗕 🛛 🗖 🗖 🗖 🗖 🗖	ess Group Properties - ACME_NY 📃 🔽
Information Allowed Users Group Name: LA Admin	
Users <u>N</u> OT in any Group: BETH BJW BOB CHARLOTTE EGKEENE ESTHER FRANK FRR HJG LALITHA LCHEN LUIS LYNN MARTHA PATM	Users _N Group: → Add >> << Delete <<
	OK Cancel Apply Help

- 2. To add entries to the "Users IN Group" list box, select entries from the "Users NOT in any Group" list box and select "Add."
- 3. To delete entries from the "Users IN Group" list box, select entries from the list box and select "Delete."
- 4. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

Editing or Viewing an Admin Access Group

1.



In the SDB tree view, click on the "Admin Access Groups" icon. The names of previously administered admin access groups appear in the object view.



2. Double-click on an Admin Access Group name. The "Admin Access Group Properties" dialog box shows "Information" and "Allowed Users" tabs for the group name you selected.

Select the "Information" tab to view Tlink information for this group, or select the "Allowed Users" tab to view all the users who are currently assigned to this group.

Figure 5-8 Admin Access Group Properties - Information Tab

🗖 📃 🗖 Admin Access	Group Properti	es-ACME_NY
Information Allowed Users		1
<u>G</u> roup Name:	NY Admin	
Admin Tlinks <u>N</u> OT in Group: LUCENT#SDB_OAM#OAM#ACME_LA		Admin Tlinks <u>I</u> N Group: LUCENT#SDB_OAM#OAM#ACME_NY TSERVER#CSRV_OAM#OAM#ACME_ TSERVER#TSRV_OAM#OAM#ACME_
+	>> Add <u>&gt;</u> > < <u>&lt;</u> Delete <<	•
	OK Ca	ncel Apply Help

- 3. To add Tlinks to the admin access group, highlight the Tlink(s) in the "Admin Tlinks NOT in Group" list box and select the "Add" button.
- 4. To remove Tlinks from the admin access group, highlight the Tlink(s) in the "Admin Tlinks IN Group" list box and select the "Delete" button.
- 5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

#### **Deleting an Admin Access Group**

This feature allows you to delete an entire admin access group. Before deleting the group, select the "Allowed Users" tab to view the users assigned to this group. This is recommended because, once you delete an admin access group, the allowed users in the group no longer have administrative permissions. If you still want these users to be administrators, you should add them to another admin access group.

The TSA32 guarantees that you will always have at least one person who can administer your SDB object and give this permission to other users. You cannot remove the "ALL ADMIN ACCESS' group and you cannot delete the last user in this group.



- 1. In the SDB tree view, click on the "Admin Access Groups" icon. The names of previously administered admin access groups appear in the object view.
- 2. Select the group name you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

## **Order for Administration of Telephony Objects**

If you do not use "Quick Add" to add your User, Worktop and Device objects to the SDB, you must add individual objects in a certain order. This is because the TSA32 validates some attributes as you enter the object and prohibits you from entering invalid information. For example, if you are adding a Worktop object that has a device "4401" associated with it, you must have first added the "4401" Device object to the SDB.

A Tserver should be administered in the following order:

#### 1. System-wide features for the Tserver

Administer the options described in the "Administration of Systemwide Features" section of this chapter.

#### 2. Tlinks

Administer the CSTA and OAM Tlinks if they have not been added automatically.

#### 3. Tlink Groups

If necessary, create the groups of Tlinks that devices are allowed to use. See Chapter 2 for details. The default group "Any Tlink" is provided for you automatically.

#### 4. Devices

Create an object for each device (telephone) that will be controlled by Telephony Services applications. Valid device IDs are needed to create Device Group and Worktop objects.

#### 5. Device Groups

Create groups of devices for user classes of service and worktop secondary device groups. See Chapter 3 for details. The group "Any Device" is provided for you. If you plan to assign device groups to either Worktop or User objects, you must add them to the SDB first.

#### 6. Worktops

Create a worktop object for each telephone-workstation pair that will be using Telephony Services. You must create the Worktop object before you can assign a worktop to a User object.

#### 7. Users

Create a User object for each person who will be using Telephony Services. These users must exist on the Windows NT system (they must have a Windows NT login, added through the Windows NT User Manager).

#### 8. Admin Access Groups

If necessary, create admin access groups to give users administration permissions.

## **Administering Tlinks**

Tlinks are the services offered by Tservers and PBX drivers. (See the section titled "The Tlink and Tlink Group Objects" in Chapter 2 for a complete description of Tlinks.) Tlinks can be added to the SDB in two ways:

- ♦ You can install and load the Tserver and PBX drivers on your telephony server, causing all the Tlinks on that Tserver to be created automatically for you.
- You can enter the Tlinks using the TSA32.

In most cases, you can rely on the automatic administration and skip the rest of this section. You may choose to administer Tlinks if your telephony server configuration is incomplete and you want to get a head start on your system administration.

You cannot change or view any properties for a Tlink.

The fields on the "Create Tlink" dialog box are described briefly in the following text. See "The Tlink and Tlink Group Objects" section in Chapter 2 for more details.

- **Tserver:** The name of the file server where the CSTA link, Tserver or PBX driver administrative module is located. The string you enter may not exceed 19 characters and may not contain the pound sign (#).
- **Tlink Type:** The kind of service provided by a PBX driver or a Tserver. The following kinds of service may be advertised:
  - **CSTA:** This Tlink type provides call control, monitoring, and routing functionality.
  - **Driver Admin:** This Tlink type provides administration and maintenance of a PBX driver. You can include this Tlink type in an admin access group to give users administration permissions for that PBX driver.

- **Simulator:** This Tlink type is used when the PBX is not available. You should only use this Tlink type when you are testing a Telephony Services application in a simulated environment.
- **Tserver Admin:** This Tlink type provides administration and maintenance of the Tserver module. You can include this Tlink in an admin access group to give users maintenance privileges for this Telephony Server.
- **Cserver Admin:** This Tlink type provides administration and maintenance of a CSTA server. You can include this Tlink type in an admin access group to give users administration permissions for the CSTA server.
- **SDB Admin:** This Tlink type provides administration and maintenance of the SDB driver. You can include this Tlink type in an admin access group to give users administration permissions for accessing the SDB.
- **Driver Name**: Fill in the driver name with the name provided by your PBX vendor, if applicable.
- **Vendor:** Fill in the vendor name with the name provided by your PBX vendor, if applicable.

## **Creating a Tlink**



1. From the "Admin" menu, select "Create Tlink." The "Create Tlink" dialog box is displayed:

Figure 5-9 Create Tlink Dialog Box

Create Tlink - ACME_NY				
Information				
<u>I</u> server: Tlink Type ● C <u>S</u> TA ● <u>D</u> river Admin ● Si <u>m</u> ulator	ACME_NY O Tserver Admin O Cserver Admin O SDB Admin			
Driver <u>N</u> ame: <u>V</u> endor:	CSTASERV			
<u>IOK</u>	Cancel Apply Help			

- 2. Enter the name of the Tserver for which you want to create the Tlink in the "Tserver" field.
- 3. Select the desired Tlink Type.
- 4. Enter the appropriate values in the "Driver Name" and "Vendor" fields (if applicable).
- 5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the Tlink.

### Viewing a Tlink



1.

In the SDB tree view, click on the "Tlinks" icon. The names of current Tlinks appear in the object view. There are no "Properties" to view for Tlinks.

Figure 5-10 SDB Window (Tlink Information)



## **Deleting a Tlink**



- 1. In the SDB tree view, click on the "Tlinks" icon. The names of current Tlinks appear in the object view.
- 2. Select the Tlink you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

## **Administering Tlink Groups**

1.

Tlink Group objects are groups of CSTA-type Tlinks. This Tlink type is used for call control, monitoring and routing. See Chapter 2 for details on Tlink Group object usage.

### **Creating a Tlink Group**



From the "Admin" menu, select "Create Tlink Group." The "Create Tlink Group" dialog box is displayed:

Figure 5-11 Create Tlink Group Dialog Box

Create Tlink Group - ACME_NY				
Information				
<u>G</u> roup Name:	Service			
CSTA Tlinks <u>N</u> OT in Group:	CSTA Tlinks <u>I</u> N Group:			
	>> Add ≥> << Delete <<			
	OK Cancel Apply Help			

2. Enter the name of the new Tlink group in the "Group Name" field.

Using the TSA32 to Administer the Security Database 157

- 3. To add Tlinks to the Tlink group, highlight the Tlink(s) in the "CSTA Tlinks NOT in Group" list box and select the "Add" button.
- 4. To remove Tlinks from the Tlink group, highlight the Tlink(s) in the "CSTA Tlinks IN Group" list box and select the "Delete" button.
- 5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the Tlink group.

### **Editing or Viewing a Tlink Group**



1. In the SDB tree view, click on the "Tlink Groups" icon. The names of current Tlink Groups appear in the object view.

Figure 5-12 SDB Window (Tlink Groups)



2. Double-click on a Tlink Group name. The "Tlink Group Properties" dialog box is displayed:

Figure 5-13 Tlink Group Properties Dialog Box

- Tlink Grou	ip Properties	ACME_NY	-
Information			
<u>G</u> roup Name:	Sales		
CSTA Tlinks <u>N</u> OT in Group:		CSTA Tlin <u>I</u> N Group	iks p:
LUCENT#CSTASERV#CSTA#ACME2_		LUCENT#CSTASERV4	#CSTA#ACME_N
	< <u>&lt;</u> Delete <<		
+		•	•
	OK Ca	ncel Apply	Help

- 3. To add Tlinks to the Tlink group, highlight the Tlink(s) in the "CSTA Tlinks NOT in Group" list box and select the "Add" button.
- 4. To remove Tlinks from the Tlink group, highlight the Tlink(s) in the "CSTA Tlinks IN Group" list box and select the "Delete" button.
- 5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

### **Deleting a Tlink Group**



- 1. In the SDB tree view, click on the "Tlink Groups" icon. The names of current Tlink groups appear in the object view.
- 2. Select the Tlink group you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

## **Administering Devices**

These procedures allow you to create, edit, and delete Device objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these procedures to add the same devices. You may edit or delete those devices using these procedures.

The attributes that make up the Device object are administered using these procedures. Each attribute is briefly described below. For more details, see the "Device Attributes" section of Chapter 2.

- Device ID is the exact string of numbers that the PBX uses to identify a particular device (e.g., the extension of the telephone on your desk). Refer to your vendor's PBX documentation for detailed information on the required string.
- Location is an optional field. You can use it to indicate where the device is located.
- **Device Type** (PHONE, FAX, MODEM, ACD) is an optional entry that shows the administered type for the device. The default type is "PHONE." This field is not us ed by the telephony server; it is provided for information only.
- **Tlink Group** is the list of Tlinks that are allowed to control the device. "Any Tlink" is the default value.

## **Creating a Device**



1.

From the "Admin" menu, select "Create Device." The "Create Device" dialog box is displayed:

Figure 5-14 Create Device Dialog Box

🗕 Create	Device - ACME_NY
Information	
<u>D</u> evice ID:	4402
Location:	LA Sales
Device <u>T</u> ype:	PHONE
Tlink <u>G</u> roup:	Any Tlink 👤
OK	Cancel <u>A</u> pply Help

- 2. Enter the Device ID. Enter other values as desired.
- 3. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the device.

## Editing or Viewing a Device

1.

- Procedure
- In the SDB tree view, click on the "Devices" icon. The names of current devices appear in the object view.

Figure 5-15 SDB Window (Devices)

Telephony Serv	ices Administr	ator 32-bit - [ACME_I	NY Devices]	<b>•</b>	
<mark>– E</mark> ile <u>A</u> dmin ⊻iew ⊻	/indow <u>H</u> elp			\$	
	🛎 🖻 🖄		% <b>⊮</b> ?		
⊡ 🔤 SDB	Device ID	Tlink Group	Device Type	Location 🛨	
🛛 🔒 Users	<del>හි</del> 4400	Any Tlink	PHONE	LA Room	
Worktops	會 4401	Any Tlink	PHONE	LA Room	
Devices	<b>55</b> 4402	Any Tlink	PHONE	LA Sales	
Device Groups	窗 441	Any Tlink	PHONE		
Section 1 Section 1	<del>හි</del> 442	Any Tlink	PHONE		
Admin Access Crowns	<del>හි</del> 443	Any Tlink	PHONE		
Admin Access Groups	☎ 444	Any Tlink	PHONE		
	<del>හි</del> 445	Any Tlink	PHONE		
	<del>හි</del> 446	Any Tlink	PHONE		
	☎ 447	Any Tlink	PHONE		
	<del>හි</del> 448	Any Tlink	PHONE		
	<del>හි</del> 449	Any Tlink	PHONE		
	<del>හි</del> 450	Any Tlink	PHONE		
	<u>ප 75553</u>	Any Tlink	PHONE	+	
	+			<b>&gt;</b>	
For Help, press F1					

2. Double-click on a device ID. The "Device Properties" dialog box shows the "Information," "Device Groups" and "Worktops" tabs.


- Device	Properties - ACME_NY
Information Device Group	s   Worktops
<u>D</u> evice ID:	4402
Location:	LA Sales
Device <u>T</u> ype:	PHONE
Tlink <u>G</u> roup:	Any Tlink 👤
	Cancel <u>Apply</u> Help

- 3. To change the Device Type or Tlink Group associations, select the appropriate device type or Tlink Group using the drop-down lists.
- 4. To display the device groups to which this device belongs, select the "Device Groups" tab. To display the worktops associated with this device, select the "Worktops" tab.
- 5. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

## **Deleting a Device**

You can delete device objects using the following procedure. The "Worktops" tab shows you which worktops are associated with this device. If the device is a member of a device group or if it is assigned to a worktop, it is deleted from the group; you do not have to explicitly remove it from the group.



1.

- In the SDB tree view, click on the "Devices" icon. The names of current devices appear in the object view.
- 2. Select the device ID of the device you want to remove.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

# **Administering Device Groups**

Device Groups are lists of devices. When device groups are assigned to a user's worktop or class of service permissions, they give or restrict user control over all the devices in the group. (Device groups can also be assigned to a worktop.) See Chapter 2, the "Device Group Objects" section, for more details.

The attributes for a device group are the devices in the group and whether the device group is an exception group. Devices added to the group are selected from the administered devices for the Tserver.

If the group is designated as an exception group, the Tserver treats the entire group as if it contained every device *except for* those devices in the device group. For example, suppose Robert is a supervisor with permission to control all of the phones in the company except for those belonging to the president and vice president. Rather than setting up a device group that contains all of the devices except for those belonging the president and the vice president, you could set up an exception group and assign it to Robert. This exception group would only contain the devices of the president and vice president.

# **Creating a Device Group**

1.

- Procedure
- From the "Admin" menu, select "Create Device Group." The "Create Device Group" dialog box is displayed:

Figure 5-17 Create Device Group Dialog Box

🗕 Create	Device Group - ACME_N	Y 🔽
Information		
<u>G</u> roup Name:	NY Sales	
	Exception Group?	
Devices <u>N</u> OT in Group:		Devices IN Group:
4402 441 442 443 444 445 446 447 448 449 450 75553 7702 7703 7704 ↓	7700 7701 >> Add ≥> <≤ Delete <<	
ОК	Cancel <u>A</u> pply	Help

- 2. Enter the name for the new device group.
- 3. To add devices to the device group, highlight the device(s) in the "Devices NOT in Group" list box and select the "Add" button.

- 4. To remove devices from the device group, highlight the device in the "Devices IN Group" list box and select the "Delete" button.
- 5. To make the device group an exception group, set the "Exception group?" checkbox.
- 6. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the device group.

## **Editing or Viewing a Device Group**

1.



In the SDB tree view, click on the "Device Groups" icon. The names of current device groups appear in the object view.

Figure 5-18 SDB Window (Device Groups)



2. Double-click on a device group name. The "Device Group Properties" dialog box is displayed:



- Device G	Group Properties - ACME_NY
Information	
<u>G</u> roup Name:	NY Sales
	<u>Exception Group?</u>
Devices <u>N</u> OT in Group:	Devices <u>I</u> N Group:
400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 •	>> Add >>   << Delete <<
<u> </u>	Cancel Apply Help

The TSA32 application displays a list box containing information about the devices in the device group, one per line.

- 3. To add devices to the device group, highlight the device(s) in the "Devices NOT in Group" list box and select the "Add" button.
- 4. To remove devices from the device group, highlight the device in the "Devices IN Group" list box and select the "Delete" button.
- 5. You can make the "Devices IN Group" list an "Exception Group" list by checking the "Exception Group?" box.

6. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

#### **Deleting a Device Group**

This procedure allows you to delete a device group. If the group is assigned to the class of service fields in any User objects, the device group entry is removed from the user objects. Similarly, if a device group is assigned as a secondary device group for a worktop object, deleting the device group removes the entry from the worktop object.



- 1. In the SDB tree view, click on the "Device Groups" icon. The names of current device groups appear in the object view.
- 2. Select the device group you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

# **Administering Worktops**

These procedures allow you to create, edit, and delete Worktop objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these dialog boxes to add the same worktops. However, you can edit or delete worktops created by "Quick Add" using these procedures.

The attributes that make up the Worktop object are briefly described below. See "The Worktop Object" section in Chapter 2 for more details.

- Worktop Name: A unique name that identifies the worktop.
- **Primary Device ID**: The primary device on the worktop, usually the extension of a telephone.
- Secondary Device Group: A drop-down list showing all device groups. Typically, you select the device group containing the devices located at this worktop, thus enabling the user associated with the worktop to control these devices. See Chapter 2 for details on the uses of this device group. This is an optional field.
- LAN Addresses: A listing of the addressing options for the workstation, available on the LAN Addresses tab. If you wish to use the "Extended Worktop Access" feature, you must either
  - Let the system fill in the fields automatically by enabling the "Automatic Administration of LAN Addresses" feature (available on the "Options" tab from the SDB "Admin/Properties" menu),

or

- Supply the TCP/IP address of the workstation on the worktop. Enter either the host name or the IP address, depending on the TCP Preferred Naming Format you have chosen for Telephony Services.
- Users: Users that are associated with this worktop.

## **Creating a Worktop**



1.

From the "Admin" menu, select "Create Worktop." The "Create Worktop" dialog box is displayed, showing tabs for "Information" and "LAN Addresses."

Figure 5-20 Create Worktop Dialog Box

- Create W	/orktop - ACME_NY
Information LAN Addresses	
Worktop Name:	Sales 5
Primary Device ID:	4402
Ennaly before ib.	
Secondary Device Group:	(none)
	Cancel <u>A</u> pply Help

- 2. Fill in the name of the worktop on the "Information" tab.
- 3. Select a Primary Device ID from the drop-down list (if desired).
- 4. Select a Secondary Device Group from the drop-down list (if desired).
- 5. Select the "LAN Addresses" tab to enter LAN address information for the worktop.



Create Worktop - ACME_NY
Information LAN Addresses
TCP/IP Heat Name:
IP Address: 137 . 28 . 11 . 269
IPX/SPX
Node:

Enter a TCP/IP host name or an IP address.



If you are using Dynamic Host Configuration Protocol (DHCP), LAN addresses should be entered in Host Name format and Windows Internet Name Service (WINS) must be available.

6. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the worktop.

# Editing or Viewing a Worktop

1.



In the SDB tree view, click on the "Worktops" icon. The names of current worktops appear in the object view.

Figure 5-22 SDB Window (Worktops)

🗖 🛛 Telephony Serv	ices Administrator	32-bit - [ACME_N	VY Worktops]	
<mark> <u>F</u>ile    <u>A</u>dmin    <u>V</u>iew   <u> </u></mark>	<u>M</u> indow <u>H</u> elp			\$
	🔌 😫 🖻 🗡		? №?	
E⊡ 🛃 SDB	Worktop Name	Device ID	Device Group	+
	🚭 Exec Secretary	7713		
Worktops	🚭 Help Desk 1	7702		
	- Help Desk 2	7703		
Bevice Groups		7720		
Section 1995	- NY Sales 3	7709		
Advis Access	🚭 President	7710		
Admin Access Groups	🞝 Sales 1	7700		
	🞝 Sales 2	7701		
	🞝 Sales 3	4400		
	🞝 Sales 4	4401		
	🞝 Sales 5	4402		
	🚭 Sales sec/admin	7704		
	🞝 Service 1	7705		
	🞝 Service 2	7706		
	Service 3	7708		-
For Help, press F1				14

2. Double-click on a worktop name. The "Worktop Properties" dialog box shows tabs for "Information," "LAN Addresses," and "Users."

Worktop Properties - ACME_NY			
Information I AN Addresses I Users			
Worktop Name:	NY Sales 3		
Dimen Device ID:	7700		
Frimary Device ID:	7703		
Secondary Device Group:	(none) 👤		
	Cancel Apply Help		

#### 3. Make changes as needed to the worktop's attributes.

If you want to change the LAN address for the workstation, select the "LAN Addresses" tab. If you want to view the users who are associated with this worktop, select the "Users" tab.

4. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

#### **Deleting a Worktop**

- Procedure **23**
- 1. In the SDB tree view, click on the "Worktops" icon. The names of current worktops appear in the object view.
- 2. Select the worktop you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

Using the TSA32 to Administer the Security Database 177

# **Administering Users**

These procedures allow you to create, edit and delete User objects in your Security Database. If you have used "Quick Add" to create Users, Worktops, and Devices, you do not need to use these procedures to add the same users. However, you can edit or delete users created by "Quick Add" using these procedures.



In order to access Telephony Services, users must have a Windows NT login ID and password. In addition, they must have the "Log on as a service" user right assigned to their account on the Windows NT Machine that is running Telephony Services. This information is administered through the Windows NT User Manager. For more details, refer to the "User Authentication" section in Chapter 7.

The attributes that make up the User object are briefly described below. See "The User Object" section of Chapter 2 for more details about the attributes.

- Login: the user's login as administered through the Windows NT User Manager.
- Name: the user's name.
- Worktop Name: a drop-down list showing the administered worktops along with the primary device assigned to the worktop. Select a worktop for the user from this list. Multiple users may share the same worktop. Choose "(none)" to specify that the user does not have a worktop.
- Class of Service: displays the different Class of Service attributes for this user. For a complete discussion of Class of Service attributes, see Chapter 3.
- Admin Access Groups: a separate tab indicating whether or not a user has administration permissions. You can grant these permissions to a user by setting the "Allow User to Administer Admin Access Groups?" checkbox on this tab, or by including the user in the "Allowed Users" list for an Admin Access Group.

# **Creating a User**



1.

From the "Admin" menu, select "Create User." The "Create User" dialog box is displayed, showing tabs for "Information," "Class of Service," and "Admin Access Groups."

Figure 5-23 Create User Dialog Box

Create User - ACME_NY			
Information Class of Service Admin Access Groups			
Login:	Manuel		
Manar	Manual Direct		
<u>N</u> ame:	Manuel Filvera		
Worktop Name:	Sales 3 👤		
OK	Cancel <u>A</u> pply Help		

2. On the "Information" tab, enter the user's login and name. Select a worktop name from the drop-down list.

If this user is to be administered for "Class of Service," continue with Step 3. Otherwise, select "OK."

3. Select the "Class of Service" tab.

Figure 5-24 Create User - Class of Service Tab

-	Cre	ate User - ACME_N	١Y	•
Information	Class of Service	Admin Access Groups		
<sub>E</sub> Call Contro	ol Services - Call Ori	gination and Termination		
A	<u>c</u> cess Group:	LA Sales		<b>±</b>
Monitoring	-Only Services			
Device/	Device - Event Not	ification ceases if call lea	ves device	
A	ccess <u>G</u> roup:	LA Sales		<u>+</u>
Call/Dev	vice - Event Notifica	ation continues if call leav	es device	
A	cce <u>s</u> s Group:	(none)		<b>±</b>
Call/Call	- Event Notification	n allowed if call identifier is	s known	
		🗖 Allo <u>w</u>		
Routing S	ervices - Allow routi	ng on listed devices		
A	ccess G <u>r</u> oup:	(none)		<b>±</b>
	OK	Cancel	Apply	Help

#### 4. Assign one or more of the desired classes of service.

For each class of service (except Call/Call monitoring), you can use the drop-down lists of all the currently administered device groups to select a group for this user. The Call/Call monitoring is either enabled or disabled. See Chapter 3 for details about classes of service.

You may administer some, none, or all of the classes of service.

5. If you want the user to be able to administer admin access groups, select the "Admin Access Groups" tab and set the "Allow User to Administer Admin Access Groups?" checkbox.

Figure 5-25 Create User - Admin Access Groups Tab

Create User - ACME_NY	-
Information Class of Service Admin Access Groups	
Allow User to Administer Admin Access Groups?	
OK Cancel <u>A</u> ppl	y Help

6. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without creating the user.

# Editing or Viewing a User

1.



In the SDB tree view, click on the "Users" icon. The names of current users appear in the object view.

Figure 5-26 SDB Window (Users)

📼 🛛 Telephony Services Administrator 32-bit - [ACME_NY Users] 🔹 💌					
<mark>- E</mark> ile <u>A</u> dmin ⊻iew Y	<u>W</u> indow <u>H</u> elp			\$	
	* # * ×	<u>□</u> <u></u>	₩?		
⊡ 🛃 SDB	Login ID	User Name	Worktop Name	÷	
Users	🚨 BETH	Beth Fitzpatrick	Service 2		
	🚨 BJW	Brian Wallis	Help Desk 2		
	🚨 BOB	Robert Martinez	Loading Dock		
Device Groups	🚨 CHARLOTTE	Evans	NY Sales 3		
Section 1 and 1 a	🚨 EGKEENE	Edward Keene	Sales 1		
Tink Groups	🚨 ESTHER	Esther Cohen	Loading Dock		
Admin Access Groups	🚨 FRANK	Frank Fuller	Sales 4		
	🚨 FRR	Frances Reese	Exec Secretary		
	🚨 HJG	Harry Gardner	VP 2		
	🚨 LALITHA	Lalitha Harris	VP1		
	🚨 LCHEN	Lee Chen	President		
	🚨 LSM	Leslie Kuhn	Sales sec/admin		
	🚨 LUIS	Luis Munoz	Sales 2		
	ALYNN	Lunn Johnson	Sales 3	┛	
	+		+		
For Help, press F1				/1.	

2. Double-click on a Login ID. The "User Properties" dialog box shows tabs for "Information," "Class of Service," and "Admin Access Groups."

Figure 5-27 User Properties - Information Tab

User Properties - ACME_NY				
Information Class of Service Admin Access Groups				
Login:		CHARLOTTE		_
<u>N</u> ame:		Charlotte Eva	ans	
) (orktop Name:		MY Salas 2		
		Int Jales J		
	OK	Cancel	Apply	Help

#### 3. Make changes to the user's attributes as desired.

If you want to change the class of service for the user, select the "Class of Service" tab. If you want to give the user permission to administer admin access groups, select the "Admin Access Groups" tab and set the "Allow User to Administer Admin Access Groups?" checkbox.

4. Select "OK" to save the information in the Security Database or "Cancel" to close the dialog box without saving any changes.

# **Deleting a User**

To ensure that at least one user is always able to perform administration, you cannot delete the last user from the "All Admin Access" group.



- 1. In the SDB tree view, click on the "Users" icon. The names of current users appear in the object view.
- 2. Select the user you want to delete.
- 3. Press the "Delete" key.
- 4. Select "OK" to confirm the deletion.

# **SDB Logging**

You can choose whether you want SDB transactions to be logged and if so, to set the size of the Security Database log file. For more information about logging and log files, refer to the section "General Logging Information" in Chapter 11.

## Using the TSA32 to Set SDB Log Settings



 In the SDB tree view, click on the SDB icon. Then, from th e "Admin" menu, select "Properties." The "Tserver Properties" dialog box is displayed, showing tabs for "Options," "SDB Log Settings," and "Components." Select the "SDB Log Settings" tab.

Figure 5-28 SDB Log Settings

Tserver Properties - ACME_NY
Options SDB Log Settings Components
I Log Changes to SDB
SDB Log File Size (bytes): 100000
SDB Log File: \\acme_ny\progra~1\teleph~1\tsrv\logfiles\sdblog.txt
OK Cancel Apply Help

2. Set the log size and enable logging by setting the "Log Changes to SDB" checkbox. Then select "OK" for your choices to take effect.

chapter

# 6 Bulk Administration

This chapter discusses the Bulk Administration feature, which allows you to set up your SDB from information in your corporate directory. It also describes ways you can automate further updates to the SDB.

# **Administering Your SDB**

Bulk administration allows you to administer your SDB in bulk rather than by editing individual objects in the SDB. If you prefer to use the TSA or TSA32 to maintain your Security Database, you may skip the rest of this chapter.

The Bulk Administration feature also provides a mechanism that allows you to migrate from a NetWare telephony server to a Windows NT telephony server. If you need to perform this migration, you must first convert the Telephony Services Security Database to a format understood by the NT server. This can be accomplished using the Bulk Administration feature.

## **Bulk Administration Applications**

This section describes ways you can use bulk administration. Each subsection includes a diagram of the process and/or a list of sections you should read before using bulk administration.

Bulk Administration 187

#### Adding Telephony Services Objects to your Security Database for the First Time

Suppose your company has just purchased Telephony Services and an application that will be used by all 500 people in your company. Most likely, you already have a computerized database, such as payroll or a telephone directory, that contains a record for each Telephony Services user. Each record contains the user's login, name and telephone number. If you have a computer programmer who can extract the data from your database and create an ASCII file, you can use bulk administration to add these users to your SDB, rather than adding them individually.

#### Figure 6-1

Adding Telephony Service Objects to the SDB



Security Database Files

If you wish to use this application, read the following sections in this chapter:

Examining Bulk Administration Files The Flat File The Error File The Simple File Using Bulk Administration: Adding Telephony Services Objects to Your SDB for the First Time Invoking Bulk Administration: Updating the Security Database

188 Network Manager's Guide

#### Making Bulk Changes to an Existing SDB

Suppose your company of 500 users has been using Telephony Services for 6 months. You have recently purchased a new application that requires you to give each user a certain set of permissions. With bulk administration you can extract all the data from your SDB, modify it using a standard spreadsheet, and reinsert the updated information.

Figure 6-2 Making Bulk Changes to An Existing SDB



Bulk Administration 189

If you wish to use this application, read the following sections in this chapter:

Examining Bulk Administration Files The Flat File The Error File Using Bulk Administration: Making Bulk Changes to Your SDB Invoking Bulk Administration: Backing Up the Security Database Upgrading the SDB

#### Printing the Contents of the SDB

You can generate a file containing all the information in your SDB. This file can be viewed, edited, and printed using a standard spreadsheet.

### Figure 6-3

Printing the Contents of the SDB



190 Network Manager's Guide

If you wish to use this application, read the following sections in this chapter:

Examining Bulk Administration Files The Flat File Using Bulk Administration: Printing Data in Your SDB Invoking Bulk Administration: Backing Up the Security Database

#### **Updating Your SDB Automatically**

Suppose your company has ten sites across the country and each site has its own telephony server. You want to centralize the administration of these telephony servers at the same location that handles all data input for your company. With the help of a programmer, you can create bulk administration update files that add new users and modify or delete existing users.

Figure 6-4 Updating Your SDB Automatically



If you wish to use this application, read the following sections in this chapter:

Examining Bulk Administration Files The Flat File The Error File Using Bulk Administration: Updating Your SDB Automatically Invoking Bulk Administration: Updating the SDB Bulk Administration Manual Pages Object Attribute Tables

#### Migrating from a NetWare Telephony Server to a Windows NT Telephony Server

If you want to migrate from a NetWare telephony server to a Windows NT telephony server, you need to convert the Telephony Services Security Database to a format understood by the NT server. This can be easily accomplished using the Bulk Administration feature.

This procedure is described in detail in Appendix A of the *PassageWay Telephony Services for Windows NT Installation Guide*. If you have already completed your conversion, you can skip this section.

If you wish to use this application, read the following sections in this chapter:

Examining Bulk Administration Files The Flat File The Error File Using Bulk Administration: Invoking Bulk Administration: Backing Up the Security Database Upgrading the SDB

#### **Examining Bulk Administration Files**

Bulk Administration uses three different files to perform the features just described: the flat file, simple file, and error file. You can view any of these files using a standard spreadsheet. You should open the file as a text file using commas as the field delimiters. This displays each attribute in the correct column and is easier to edit.

These files can also be examined with an editor, but you must be careful in choosing which editor or word processor you use to examine the file. Some editors automatically insert a new line character when a line exceeds a certain length. This looks like two lines to bulk administration; the second line will cause problems because it is not formatted correctly.

#### The Flat File

The flat file is central to the bulk administration of your SDB. This file is created when you "back up" your SDB and is the input to the "update" of your SDB. It is an ASCII file.

Data retrieved from the SDB is grouped into sections. There is one section for each object type:

User Worktop Device Device Group Tlink Tlink Group Admin Access Group

Each section contains one line for each instance of that object type in your SDB. The attributes that make up the object are separated from each other by commas allowing you to view the data with a spreadsheet. When you open the file, specify that the text has commas as delimiters.



You must save the file in the same format. Do not replace the commas with tabs. If you do, the file cannot be used to update the SDB.

#### **Section Headers**

The following table illustrates the User section in the flat file when viewed with a spreadsheet program.

#### Figure 6-5 Flat File - User Section

INFORM1	1	100	101	102	103	105	108	109
INFORM2	User	Login	Name	Worktop Name	Device Monitor Group	Call-Dev Monitor Grp	OAM Group	Super Admin User
ADD	1	JOE	Joe Smith	W401		FALSE		FALSE
ADD	1	LUIS	Luis Gonzales	W410		FALSE		FALSE
ADD	1	SUE	Sue Ferraro	W402		FALSE		FALSE
ADD	1	ТОМ	Tom Chen	W403		FALSE		FALSE

The first two lines are informational and are referred to as the section header. The first line in the header has the keyword "INFORM1" in the first column. It is used by bulk administration to figure out the object type for the section and the attributes associated with that object type. The second line, "INFORM2," contains the same information as the first, but is in text format so that you can understand what is in each column. Bulk administration does not use the information in the INFORM2 line.

If the column header is surrounded by asterisks, the field is for information only and cannot be updated using bulk administration. These fields occur only with the TLINK objects.

#### **Data Lines**

Below the section header are data lines - typically, one per object instance. The first column of each data line has a keyword telling bulk administration what to do with this line. The allowed keywords are:

- **ADD**: add this object to the SDB.
- **MODIFY**: update an existing object with these new attribute values.
- **DELETE**: delete this object from the SDB.
- **IGNOREON**: ignore all the data lines from here until a subsequent IGNOREOFF.
- **IGNOREOFF**: start processing the data lines from now on.
- **COMMENT**: ignore this line. An empty entry in the first column is also considered a comment line.

Column 2 of each data line contains the object type. This must be the same object type as in column 2 of the INFORM1 line. The example in the figure above is a user object. In this example, the number "1" must be in column 2 of each data line.

Column 3 of each data line contains the primary key of the object. This is the attribute that uniquely identifies that object. In this example, "Login" is the primary key for the User object.

If you are adding an object, an object of the same type with this name (primary key) must not already exist in the SDB. If you are modifying or deleting an object, then an object of that type with that primary key must already exist in the SDB. You will receive an error if this is not the case.

Bulk Administration 195

The remaining columns contain the attribute information for the objects. Information contained in these columns depends on the object type of the section. You can get a template of all the section headers by invoking the "Create Templates" command of bulk administration. It creates an output file that looks like the following table when you view it with any standard spreadsheet.

#### Figure 6-6 Flat File - Object Information

INFORM1	16	500	510				
INFORM2	Tlink	Tlink Name	*Service Type*				
INFORM1	32	600	601	601	601	601	601
INFORM2	Tlink Group	Tlink Group Name	Tlink	Tlink	Tlink	Tlink	Tlink
INFORM1	64	700	701	701	701	701	701
INFORM2	Admin Group	Admin Group Name	OAM Tlink	OAM Tlink	OAM Tlink	OAM Tlink	OAM Tlink
INFORM1	4	300	301	302	303	304	
INFORM2	Device	Device ID	Device Type	Tlink Group	Location	Telephone Number	
INFORM1	8	400	401	402	402	402	402
INFORM2	Device Group	Device Group Name	Exception	Device ID	Device ID	Device ID	Device ID
INFORM1	2	200	201	202	203	204	205
INFORM2	Worktop	Worktop Name	Primary Device	IPX Address	IP Address	IP Name	Secondary Device Grp
INFORM1	1	100	101	102	103	104	105
INFORM2	User	Login	Name	Worktop Name	Device Monitor Group	Call-Dev Monitor Group	Call Monitoring

Note that this table has only eight columns. The actual file contains more columns since the user object has a large number of attributes. The file has been truncated to make it easier to view.

196 Network Manager's Guide

#### **Multi-valued Attributes**

A multi-valued attribute can be assigned to an object more than once. There are only three multi-valued attributes in the Telephony Services SDB. In each case, multi-valued attributes are used to represent the members of a group:

- Devices in a Device Group
- CSTA Tlinks in a Tlink Group
- OAM Tlinks in an Admin Access Group

Since the number of members in a group is unlimited, Bulk Administration uses multiple lines per object, each line containing up to five group members. In the example below, there are eight devices in the device group "Help Desk." Bulk Administration would create one device group with eight members of the group.

#### Figure 6-7 Flat File - Device Group Information

INFORM1	8	400	401	402	402	402	402	402
INFORM2	Device Group	Device Group Name	Exception	Device ID				
ADD	8	Help Desk	FALSE	410	411	412	413	414
ADD	8	Help Desk	FALSE	415	416	417		

You cannot modify the members of a group (multi-valued attributes). You can only add or delete them.

#### **Flat File Section Types**

As mentioned earlier, there is one section per object type: Tlink, Tlink Group, Admin Group, Device, Device Group, Worktop, and User.

The sections are in the same order in which you would have to add objects to the SDB:

- **Tlink:** An object exists for all Tlinks registered by the PBX driver and for any Tlinks you administered. You should not modify any data in this section.
- Tlink Group: This contains all of the Tlink Groups you have administered plus the default value "Any Tlink." If you are not using Tlink Groups, the only data line in this section is the default value.
- ♦ Admin Access Group: This section contains the administration access groups you have created plus the one default data line for the "ALL ADMIN ACCESS." If all your administrators have the default permission, you should have only the "ALL ADMIN ACCESS" record in this section.
- **Device:** This section contains information about device objects.
- **Device Group:** This section contains information about the device groups. These groups are used to assign user permissions. The default device group "Any Device" is automatically added to the SDB.

INFORM1	8	400	401	402	402	402	402	402
INFORM2	Device Group	Device Group name	Exception	Device ID				
ADD	8	Any Device	FALSE					
ADD	8	DEVICE GROUP 1	FALSE	75553	75551	75555	75560	75561
ADD	8	DEVICE GROUP 1	FALSE	75562	75563	75564	75565	75566
ADD	8	DEVICE GROUP 1	FALSE	75567	75568	75569	75570	75571
ADD	8	DEVICE GROUP 1	FALSE	75572	75573	75574	75575	75576
ADD	8	DEVICE GROUP 1	FALSE	75577	75578	75579		
ADD	8	DEVICE GROUP 2	FALSE	75562	75563			

#### Figure 6-8 Flat File - Device Group Section

• Worktop: This section contains information about the worktop objects in the SDB.

• User: This section contains information about the user objects in the SDB.

#### **The Error File**

Errors that occur while you are updating your SDB from a flat file are logged in an error file. Errors can be of two levels of severity: non-fatal and fatal. A non-fatal error applies to a single data line. It could be caused by invalid data on that line. The line causing the error is written to an error log, the SDB is not updated and processing continues unless you have enabled the "Stop Processing on Non-Fatal Errors?" option.

A fatal error is caused by a problem that affects more than one data line. For example, there is no available disk space or the file contains an illegal attribute in the INFORM1 line. If the update encounters a fatal error, it writes the line that generated the error to the error file and stops processing.

The format of the error file is similar to that of the flat file. It is a commaseparated ASCII file that can be examined using a standard spreadsheet.

Bulk Administration 199

The file is organized by section; each section header contains two INFORM lines.

#### Figure 6-9 Error File - Format

Error Description	Line Number	Attribute In Error	INFORM1	4	300	301	302		
Error Description	Line Number	Attribute In Error	INFORM2	Device	Device ID	Device Type	Tlink Group		
Error Description	Line Number	Attribute In Error	INFORM1	8	400	401	402		
Error Description	Line Number	Attribute In Error	INFORM2	Device Group	Device Group Name	Exception	Device ID		
Error Description	Line Number	Attribute In Error	INFORM1	2	200	201	202		
Error Description	Line Number	Attribute In Error	INFORM2	Worktop	Worktop Name	Primary Device	IPX Address		
Error Description	Line Number	Attribute In Error	INFORM1	1	100	101	102		
Error Description	Line Number	Attribute In Error	INFORM2	User	Login	Name	Worktop Name		
Invalid Primary key	143	102	ADD	1	joe	Joe Smith	W401		
	Total lines in error: 1								

There are three extra columns at the beginning of each line. These columns provide the following information:

- Error Description: a brief description of why the update failed. For a more complete discussion of the error and what may have caused it, refer to the SDB errors section of Chapter 11, "Troubleshooting."
- Line Number: the number of the line in error. If you read the input file with a spreadsheet, this is the number on the left-hand side of the spreadsheet.
- ◆ Attribute In Error: the attribute that caused the error. The number that is in this column should match one that is in the INFORM1 line. Sometimes the update fails because the data for a particular attribute value is invalid. In the example above, the worktop name in the user object is not the name of an existing worktop object. The input line for the user is rejected and the attribute in error is 102, the "Worktop Name."
An attribute ID does not always appear in this column. For example, if "joe" already existed in the SDB, the error would have been "DUPLICATE KEY" and no attribute ID would have been supplied.

You should check the error file each time you update your SDB. A line at the bottom of the file tells you how many errors occurred. If a fatal error occurs before the entire file has been processed, the last line in the file should be an indication of the line that caused the problem. The line including the error count is not present.

### **Correcting Non-Fatal Errors**

Examine each line and correct the errors. Once all the lines have been fixed, you can remove the first three columns and use this file as input to the update process. You do not need to remove the section headers for sections with no data lines. After performing these steps, the error file from the example above would look like this:

## Figure 6-10 Error File - Correcting Non-Fatal Errors

INFORM1	4	300	301	302	
INFORM2	Device	Device ID	Device Type	Tlink Group	
INFORM1	8	400	401	402	
INFORM2	Device Group	Device Group Name	Exception	Device ID	
INFORM1	2	200	201	202	
INFORM2	Worktop	Worktop Name	Primary Device	IPX address	
INFORM1	1	100	101	102	
INFORM2	User	Login	Name	Worktop Name	
ADD	1	joe	Joe Smith	W402	

This is a small sample section of the file. Several columns have been removed from the right side of the preceding figures so that the examples fit on the page.

#### **Correcting Fatal Errors**

If a fatal error occurs on a line, the previous lines in the file have been processed; none of the later lines have been processed. Once you have fixed the problem, you should remove the lines that were successfully processed and resubmit the file for update. Do not remove the INFORM lines for sections that still contain data lines.

You can remove lines by deleting them with the spreadsheet program or by using the IGNOREON and IGNOREOFF keywords. These keywords can be used to surround lines that have been processed. Bulk administration ignores all the data lines inside the keywords. (It does use the INFORM lines). For example, suppose you have a flat file with only device and worktop object updates. All the devices were correctly updated, but the INFORM1 line for the worktop objects was corrupted, causing the update to stop. You can either remove the device object data line from the flat file, or add a line containing the keyword "IGNOREON" at the beginning of the device object data lines and another line containing "IGNOREOFF" at the end of the device object data lines.

INFORM1	4	300	301	302
INFORM2	Device	Device ID	Device Type	Tlink Group
IGNOREON				
ADD	4	401	PHONE	Any Tlink
ADD	4	402	PHONE	Any Tlink
ADD	4	403	PHONE	Any Tlink
ADD	4	410	PHONE	Any Tlink
IGNOREOFF				
INFORM1	2	200	201	202
INFORM2	Worktop	Worktop Name	Primary Device	IPX Address
ADD	2	W401	401	
ADD	2	W402	402	
ADD	2	W403	403	
ADD	2	W410	410	

#### Figure 6-11 Error File - Correcting Fatal Errors

## 202 Network Manager's Guide

### The Simple File

The simple file is used to add new users to the SDB. It is made up of information that is likely to be available in an existing corporate database. The simple file cannot be used to modify information in existing SDB objects.

The simple file is an abbreviated version of the flat file. It, too, is a commaseparated ASCII file. It contains only one section. This section header has two INFORM lines; each having the same format as INFORM lines in the flat file. There is one data line for each user to be added to the SDB. You can use the simple file format to add users, worktops, and devices to your SDB. You cannot use the simple file to modify or delete these objects once they have been added to the SDB.

Column 1 always contains the keyword "ADD." Column 2 always contains the filename "Simple." Like the flat file, column 3 contains a unique identifier for the user - the Login ID. The attributes that follow the Login ID are information you are likely to have in a computerized database. These attributes are:

# Table 6-1 Simple File Information

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION	TELEPHONY SERVICES OBJECT TYPE
Device ID	The extension of the primary device associated with the user's worktop. This is the PBX extension. It is usually the last two to five digits of the telephone number. If not supplied, no device object is created.	Worktop/Device
IP Address	For TCP/IP, you can supply either this IP address or the IP name, depending on the naming format you have chosen. See Chapter 7, "TCP/IP Configuration," for more information. You can also use the "Auto Administration of LAN Addresses" feature to supply this information. The IP LAN address format is four one- to three-decimal character fields, each separated by a period, that is: xxx.xxx.xxx.	Worktop
IP Name	For TCP/IP, you can supply either this IP name or the IP address, depending on the naming format you have chosen. See Chapter 7, "CTCP/IP Configuration," for more information. You can also use the "Auto Administration of LAN Addresses" feature to supply this information.	Worktop
IPX LAN Address	Although this release supports only TCP/IP connectivity, IPX/SPX addresses may be entered in the SDB. You can insert the IPX LAN address in the simple file. You can also use the "Auto Administration of LAN Addresses" feature to supply this information. The format is 8 hex characters, a colon, 12 hex characters, a colon, and 4 hex characters (that is, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Worktop
Location	The location of the telephone. This field is for information only.	Device
Login	Login ID of the user.	User
Name	The name of the user. The SDB uses this field for information only.	User
Telephone Number	The full number of the telephone on the user's worktop. This is usually a 7- or 10-digit number. This field is for your information only.	Device

204 Network Manager's Guide

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION	TELEPHONY SERVICES OBJECT TYPE
Tlink Group Name	This is the group of Tlinks that supports the user's telephone. You can use the value "Any Tlink." This means that the user's telephone is supported by any Tlink Group.	Device/Tlink Group
Worktop Name	A unique identifier of the worktop; if not supplied, no worktop or device object is created for this user.	User/Worktop

#### Using the Simple File for Quick Adds

By using this feature of bulk administration, you are performing a series of "Quick Adds" to the SDB. For each data line in the simple file, you create a Device, Worktop and User object if you have provided the primary key for each object.

If you provide

A Login ID, Worktop Name, and Device ID, you create all three objects.

A Login ID and Worktop Name, you create a user and worktop object.

A Login ID, you create only a user object.

If you do not provide a primary key for an object, even though you have given attributes that are in that object, no object is created. For example, if you have a device ID and an IP address for a worktop but you do not provide a worktop name, no worktop object is created.

#### Simple File Format

You can create a simple file by writing a computer program, report, or query that extracts data from an existing database and formats the information in the simple file format. You can create a template for this file by using the bulk administration feature, "Create Templates."

#### Figure 6-12 Simple File Format

	SIMPLE	FILE T	EMPLA	TE							
	File Cre	ated: 3	-29-95 1	:51:35pm							
	File Nar	ne: smp	letmpl.t	ĸt							
	Server N	Name: A	CME_N	IY							
	SDB So	ftware 7	Type: Bti	rieve							
	SDB So	ftware \	/ersion:	2.22.30.1							
	Dictiona	ry Versi	ion: 2.0.	0.3							
INFORM1	Simple	100	101	200	202	203	204	300	303	304	600
INFORM2	Simple	Login	User Name	Worktop Name	IPX Address	IP Address	IP Name	Device ID	Location	Telephone	Tlink Group Name

The program you write to create the simple file may need to generate some of the attribute values if they do not exist in your corporate database. For example,

- A worktop name could be generated from existing data. For example, you could generate a worktop name by adding the letter "W" to the device ID.
- A telephone extension can be generated from the last 2, 3, 4, or 5 digits of the telephone number.
- A Tlink Group entry can be defaulted to "Any Tlink."
- LAN addresses may be left blank and populated later using the Automatic Administration of LAN Addresses feature.

When you are done, the simple file may look like this:

INFORM1	Simple	100	101	200	202	203	204	300	303	304	600
INFORM2	Simple	Login	User Name	Worktop Name	IPX Address	IP Address	IP Name	Device	Location	Telephone	Tlink Group Name
ADD	Simple	Joe	Joe Smith	W401				401	NYC		Any Tlink
ADD	Simple	Sue	Sue Ferraro	W402				402	NYC		Any Tlink
ADD	Simple	Tom	Tom Chen	W403				403	NYC		Any Tlink

## Figure 6-13 Simple File - Sample Template

Notice that the program has taken the telephony extension, added a "W" and put the result in the "Worktop Name" field. It has also set the Tlink Group Name to "Any Tlink."

### **Rules For Creating a Simple File**

- 1. All characters must be printable, ASCII characters. If you use a comma as a character within a field, you must surround the entire field with double quotes. Otherwise, Bulk Administration will interpret the single field as two fields separated by a comma.
- 2. Do not change the format of the file by adding or deleting fields/columns.
- 3. Once you have created a simple file, you must move it to the \TSRV\SDB\BULK\_ADD directory on the telephony server where bulk administration will be run.
- 4. The two INFORM lines must precede all the data lines in the file. These lines indicate what type of information is stored in each column of the file.
- 5. If you want to add comments to the simple file, leave the first column blank. This is the same as starting the line with a comma. For example, ", comment here."
- 6. Each column represented by an entry in an INFORM1 line has its attribute ID at the head of the column. Each piece of data in a column must be of the type reflected by the column heading.

- 7. The first two columns of each data line following the INFORM lines must contain the words "ADD" and "Simple."
- 8. Spaces are considered valid characters. If you want to leave a field blank, leave no space between the commas (,,). If you put a space between the commas, the attribute is thought to contain a space.
- 9. Except for the login, data is case-sensitive. "Mary" is not the same as "MARY" or "mary."
- 10. The only valid keywords in column 1 are "INFORM1," "INFORM2," and "ADD." All other keywords are treated as comment lines. The keywords "MODIFY" and "DELETE" are not valid in a simple file.

#### **Errors Encountered While Processing a Simple File**

The process of converting a simple file into a flat file does not create a separate error file. Any errors that occur during the conversion are logged in **errlog.txt**, the error log maintained by the Tserver. See Chapter 11, "Troubleshooting," for information on reading the error log.

Two types of errors may be logged. The first type includes general errors (for example, an invalid simple file name was provided or an error occurred while writing data to the disk). The second type of error is caused by invalid data in the simple file. These errors are identified by the phrase "Bulk Admin: error occurred while processing <the name of the simple file>...." Following this phrase is text identifying the type of error and the line on which the error occurred. These errors are listed in the following table.

## Table 6-2 Simple File - Processing Errors

Error Text	Description and Recovery Procedures
No INFORM1 line in the file	The simple file does not contain an INFORM1 line. No lines of data have been processed. You must add this line. (This error would also occur if the file is not a simple file.)
Invalid file name in column 2 of INFORM1 line	Column 2 of the INFORM1 line does not contain the text "Simple." No lines in the file have been processed.
	You should change the entry in column 2 of the INFORM1 line to "Simple."
Primary key attribute missing on INFORM1 line	Column 3 of the INFORM1 line does not contain valid data. No data in the file has been processed.
	You should create a template of the simple file and make sure the column headings in your simple file are the same as those in the template file.
Invalid attribute ID on INFORM1 line	Column 3 or greater in the INFORM1 line contains an entry that is not a valid attribute ID. No data in the file has been processed.
	You should create a template of the simple file and make sure the column headings in your simple file are the same as those in the template file.
Invalid file name in column 2 on line X	Column 2 of line X does not contain the text"Simple." Data on this line has not been processed.
	You should change the entry in column 2 of the appropriate line to "Simple."
Invalid primary key on line X, attribute ID = Y	Column 3 of line X is empty. Any other data on the line is ignored.
	You should provide the data in column 3 of this line.

Error Text	Description and Recovery Procedures
Invalid opcode in column 1 on line X	The first column of line X does not contain a valid opcode. INFORM1, INFORM2, ADD, IGNOREON, IGNOREOFF and comment lines are valid. This may occur when a new line is accidentally inserted in the middle of the preceding line, so that attribute data is in column 1.

If an error is encountered while processing the INFORM1 line, none of the data in the file is updated. Errors that occur on individual data lines in the simple file prevent only those lines from being processed. Once you have completed the conversion process you should check the error log and make sure all the data lines in the simple file have been processed. If errors have occurred on individual lines, remove all the lines that were successfully updated, leaving only the lines in error. Fix the errors and restart the conversion process.

## Automating the SDB Interface

If you want to automate all your SDB administration, you must use the flat file format. This is the only way you can modify or delete existing objects from the SDB. You should be familiar with the section on the Flat File before reading this section.

## Order of Data Lines in the Flat File

One important principle that applies to all updates is that Telephony Services does not allow you to make the database inconsistent. That is, you cannot delete an object if it is referenced by another object and you cannot add information if it references another object and that object is not in the SDB. For example, if you are adding a worktop object to the SDB, the device object associated with that worktop must already be in the SDB before you can add the worktop object. You also cannot delete the device object if a worktop object references it.

Since bulk administration updates occur line by line, you must make sure your updates are done in the correct order. The order provided in the flat file template is appropriate for additions to the SDB because objects are added to the SDB before being referenced by other objects appearing later in the file. In the following example, the worktop and device sections appear in reverse order. Therefore, the attempt to ADD the worktop "W4401" will fail because the Device it refers to, "4401," has not been added to the SDB yet.

## Figure 6-14 Flat File - Order of Data Lines (Attempted Add)

INFORM1	2	200	201	202
INFORM2	Worktop	Worktop Name	Primary Device	IPX Address
ADD	2	W4401	4401	
INFORM1	4	300	301	302
INFORM2	Device	Device ID	Device Type	Tlink Group
ADD	4	4401	PHONE	Any Tlink

This order is inverted for deletions which require that references be removed before an object is deleted. In the following example, the device "4401" cannot be deleted because worktop "W4401" still refers to it.

## Figure 6-15 Flat File - Order of Data Lines (Attempted Delete)

INFORM1	4	300	301	302
INFORM2	Device	Device ID	Device Type	Tlink Group
DELETE	4	4401		
INFORM1	2	200	201	202
INFORM2	Worktop	Worktop Name	Primary Device	IPX Address
DELETE	2	W4401	4401	

You can get around this by adding a second set of INFORM lines in the same flat file. If you want to both ADD and DELETE objects, the flat file can contain a set of INFORM lines in the original order for ADDs and a second set in inverted order for DELETEs for a total of 14 sets of INFORM lines.

212 Network Manager's Guide

## Adding Objects to the SDB

You can add objects to the SDB by creating an ADD line in the appropriate section. Column 2 must contain the object type (the value that is in column 2 of the INFORM1 line). Column 3 must contain a unique primary key. This key must be unique within the object type.

You can fill in from columns 4 on with the appropriate data. If you do not provide data in a column, one of two things will happen. If the attribute has an assigned default value, that value is assigned to the attribute in the new object. If there is no default, the attribute is empty. See the object attribute tables at the end of this section for information about each attribute.

If you want to add new members to an existing group, create an ADD line and give the primary key for the group. List only the new members to be added; you should not include existing members of the group. If you want to add more than five new members, you must use multiple ADD lines.

## Modifying Objects in the SDB

To modify an existing object in the SDB, use the MODIFY keyword. Column 3 must contain the primary key of the object to be changed. All columns that contain a non-blank character(s) are changed to the new value in the column, subject to the validations described in the attribute tables. Only the columns that contain a value are updated.



You cannot change the primary key of an object. To change a primary key, you must delete the existing object and add it back with the new key value.

To blank out an attribute in an object (but not delete the object), use the DELETE keyword, not MODIFY. See the section on deleting attributes below.

You cannot modify multi-valued attributes (members of a group); the old attribute value must be deleted and the new value added.

## **Deleting Objects from the SDB**

To delete an existing object in the SDB, set the keyword in column 1 to DELETE. Column 2 must be set to the value of Column 2 of the INFORM1 line. Column 3 must contain the primary key of the object to be deleted. If only the primary key is entered, the entire object is deleted. If any other attribute column is not blank, then only that attribute is deleted (or blanked out) but the object itself is not deleted. Before an object can be deleted, all references to that object must be changed to something else or blanked out.

If you want to delete an entire group, you can just provide the name of the group (the primary key) in column 3 and set the keyword in column 1 to DELETE. You do not need to delete all the members before deleting the entire group.

To delete members from a group, set the keyword in column 1 to DELETE and put the name of the group (the primary key) in column 3. List the members to be deleted in the appropriate columns. If you want to delete more than five members, you must use multiple DELETE lines.

If you want to delete a single attribute in an object, you must put some character in the appropriate column; you do not need to put in the current contents. Bulk Administration only looks for some indication that this field is to be deleted. Be careful; if you do not indicate at least one attribute to be deleted, the entire object is deleted.

## **General Rules**

The following rules apply when creating simple or flat files:

- 1. Each field in either the simple file or flat file may contain any printable ASCII characters.
- 2. In the examples in this chapter, the extension ".txt" has been used for all flat, simple, and error files. You should actually use the extension that your spreadsheet uses to indicate that the file is in a comma-separated text format. This varies among spreadsheet vendors.
- 3. If you want to include a comma in a field, you must surround the entire field by double quotes. For example, if user name fields are formatted as

Last name, first name

the field value should be specified as

"Last name, first name"

If it is not, the last name and the first name look like separate fields to bulk administration. If you have unbalanced double quotes (you only have one double quote), the results are uncertain. Most likely, the entire line is included in the single field.

- 4. Each object has a primary key that uniquely identifies it. Some attributes in an object may refer to the primary key of another object. These attributes are called *foreign keys*. For example, the worktop name in a User object refers to a Worktop object with that worktop name. You cannot remove an object if its primary key is referred to by a foreign key in another object.
- 5. Most attributes are case-sensitive. If you use the worktop name "Mary's Worktop," it is different than the worktop name "mary's worktop."
- 6. If you do not want to assign a value to an attribute, do not ent er a space in the field. It will be considered a valid entry. An empty attribute is

represented by two consecutive commas in both the flat and simple files.

## Updating from the Flat File

Once you have created the Flat File, you have two ways to use it to update the SDB. First, you can use the Bulk Administration menu and invoke the "Update SDB" option. Second, the program that you wrote to create the Flat File can invoke the update directly. Several functions [*sdbUpdateDataBase()* and *sdbBackupDataBase()*] are included in the TSLIB for Windows. Manual pages describing each function are included at the end of this chapter.

## **Using Bulk Administration**

This section describes the high-level procedures for each of the Bulk Administration scenarios described at the beginning of this chapter. Detailed procedures for invoking the bulk administration commands are found later in this chapter.

## Adding Telephony Services Objects to Your SDB for the First Time

You can create the basic telephony objects in your SDB from data that is available in an existing computer database.



#### 1. Create a set of template files.

Use the "Create Templates" command to create a set of template files on the telephony server in the \TSRV\SDB\BULK\_ADD directory.

## 2. Write a software program to extract data from your existing database in the format given in the simple file template.

See the section on the simple file for more details.

## 3. Move the file you created to the BULK\_ADD directory on the server.

The simple file you created must be in the \TSRV\SDB\BULK\_ADD directory on the server where bulk administration will be run.

#### 4. Update the Security Database with the simple file.

Use the "Update SDB" command to initiate the update. At the "Simple File Name" prompt, enter the name of the file you created in step 2. You can use the default values for the "Flat File Name" and "Error File Name" or you can provide your own file names. Set the "Convert Simple File to Flat File" and "Convert Flat File to SDB" checkboxes.

- 5. Check the error log (errlog.txt) to see if any errors occurred during the conversion of the simple file to the flat file.
- 6. Check the bulk administration error file for any errors that may have occurred during processing.

The error file is also an ASCII file, similar to the flat file. You can examine it with a spreadsheet. See the section on the Error File for instructions on how to resolve errors.

## Making Bulk Changes to Your SDB

Use this process if you already have Telephony Services administered and want to make a number of changes. Suppose you have 30 users who have previously worked in a group that shared a set of phones. Now these users may use these phones plus another set of 20 phones. You have made up a new device group, "Joint group" and you want to assign it to the 30 users. Their previous permissions allowed them access to the "Sales group" of phones.



1. Use the TSA or TSA32 to create the "Joint Group" in your SDB.

### 2. Back up your Security Database to a file - jointgrp.txt

Use the "Create Flat File From SDB" command to create the "jointgrp.txt" file. This file is created on the telephony server in the \TSRV\SDB\BULK\_ADD directory. You should leave the file in this location.

### 3. Read the "jointgrp.txt" file using a standard spreadsheet.

Read the file as an ASCII (text) file with commas as the field delimiters. Notice that all the data lines have an opcode of "ADD."

#### 4. Remove data lines for objects you do not want to change.

In this example, you are only changing User objects, so you can remove all the Tlink, Tlink Group, Admin Group, Device, Device Group, and Worktop objects.

# 5. Change the keyword in column 1 from "ADD" to "MODIFY" for all data lines.

If you want, you can remove the data lines of users that you are not updating. This is not necessary since you are modifying objects with the same data as they had before, but you will minimize processing time.

#### 5. Make the necessary changes to the data lines.

Change the data in the correct row and column. In this example, you are changing the text "Sales group" to "Joint group."

When saving your file, be sure to save it as a comma-separated file, not a text file. If you save it as a text file, tabs are substituted for the commas, causing any subsequent updates to fail.

## 6. Use the upgrade feature of bulk administration to make the changes in the SDB

Invoke the "Upgrade SDB" command. When you are prompted for a flat file name, enter the name "jointgrp.txt." When asked for an error file name, supply a valid name that does not exist in the \TSRV\SDB\BULK\_ADD directory on the server. Clear the checkboxes for both Run-Time options: "Stop processing on non-fatal errors" and "Should ADD overwrite existing records?."

## 7. Check the error file for errors.

The error file is also an ASCII file, similar to the flat file. You can examine it with a spreadsheet. See the section on the Error File for instructions on how to resolve errors.

## Printing Data in Your SDB

You can print the data in your Security Database at any time by generating a flat file and using a spreadsheet to format and print the information.



# 1. Back up your Security Database to a file (for example, printsdb.txt)

Use the "Create Flat File from SDB" command to create the "printsdb.txt" file. When you are prompted f or a flat file name, use a name that does not exist on the telephony server in the \TSRV\SDB\BULK\_ADD directory. Comments you enter at this time are saved in the header of the file that is created. Since you are only using this file for printing purposes, you can move it anywhere you like once it is created.

## 2. Read the "printsdb.txt" file using a standard spreadsheet.

Read the file as an ASCII (text) file with commas as the field delimiters. Notice that the file has a header that includes your comments, the date, and time the file was created and the name of the server.

### 3. Remove sections you do not want.

Remove sections that are of no interest. If you only want Device, Worktop and User objects, you can remove the rest. You can also remove the INFORM1 lines from the remaining section headers because you are not using this file for subsequent updates. (Without the INFORM1 lines, the bulk administration will not work.)

## 4. Add any formatting of data and print.

## Updating Your SDB Automatically

Bulk Administration allows you to automate some or all of the administration process. The procedure described below assumes you are creating a flat file with additions, modifications, and deletions of objects in the SDB and then you are manually invoking Bulk Administration. A description of how you automate everything follows the procedure.



#### 1. Create a set of template files.

Use the "Create Templates" command to create a set of template files on the telephony server in the \TSRV\SDB\BULK\_ADD directory.

2. Modify your administration program to generate a flat file as changes are made to your corporate database.

See the section on "Automating the SDB Interface" for more details.

3. Move the file you created to the BULK\_ADD directory on the server.

The flat file you created must be in the \TSRV\SDB\BULK\_ADD directory on the server so that it can be accessed by Bulk Administration.

#### 4. Use the Update Security Database function.

Use the "Update SDB" command to initiate the update. You do not need to enter a simple file name. At the prompt for the "Flat File Name," enter the name of the flat file you created in step 2. You can use the default file for the "Error File Name" or you can provide your own file name. Clear the "Convert Simple File to Flat File" checkbox and set the "Convert Flat File to SDB" checkbox. The remaining options can be cleared.

# 5. Check the error log file for any errors that may have occurred during processing.

The command should complete successfully. If it does not, refer to Chapter 11 for an explanation of the error that was returned or the errors that appear in the error file.

To achieve an even higher level of automation, you can modify your administration program to perform steps 2, 3 and 4 in one step in your software update program. It must create the flat file, copy it to the correct directory and invoke the update command using the functions described at the end of this chapter.

## **Invoking Bulk Administration**

The Bulk administration commands appear under the "Bulk Admin" option of the "Admin" menu. Each command involves reading and/or creating files. Bulk administration creates files in the \TSRV\SDB\BULK\_ADD directory on the telephony server where the bulk admin command has been run.

If you are prompted for the name of an output file and that file already exists in the BULK\_ADD directory, it is overwritten. If not, it is created. You may wish to pick an extension (.xxx) that represents a comma-separated ASCII file for your spreadsheet program (for example, Microsoft Excel uses ".csv").

## **Creating Templates**

This command can be used to create a template of both the flat and simple files used for bulk administration. Each template includes only the section headers for each object type. You can then add data lines and populate each column with the type of data required by the column's heading. You should not modify the data in the INFORM1 lines.

The default names are:

- SMPLTMPL.TXT for the simple file template
- FLATTMPL.TXT for the flat file template

You must enter names for both files or use the default names provided. Both files are always created.

## **Creating Templates Using the TSA**

1.



From the "Admin" menu, select "Bulk Admin," then "Create Templates." The "Create Templates" dialog box is displayed:

Figure 6-16 Create Templates Dialog Box (TSA)

😑 Create T	emplates					
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.						
<u>F</u> lat File Name: <u>S</u> imple File Name:	flattmpl.txt smpltmpl.txt					
OK	<u>C</u> ancel					

2. Fill in the flat file name and/or the simple file name if you do not wish to use the default names, and select "OK."

The file templates are created for you containing the INFORM lines required by each file type.

## Creating Templates Using TSA32

1.



From the Admin menu, select "Bulk Admin," then "Create Templates." The "Create Templates" dialog box is displayed:

Figure 6-17 Create Templates Dialog Box (TSA32)

Create Templates	ACME_NY
All file names should NOT include a path located in \\acme_ny\progra~1\teleph~	. All Bulk Admin files are 1\tsrv\sdb\bulk_add.
<u>F</u> lat File Name:	flattmpl.txt
<u>S</u> imple File Name:	smpltmpl.txt
OK Cancel	Help

2. Fill in the flat file name and/or the simple file name if you do not wish to use the default names, and select "OK."

The file templates are created for you containing the INFORM lines required by each file type.

## Creating a Flat File from the Security Database

This command creates a flat file from the SDB. You are prompted for the name of a file to be created containing the Telephony Services objects from the SDB on that telephony server. If you do not provide a name, a default name, BCKUPSDB.TXT, is used.

You can also enter comments that are placed in the beginning of the flat file. A maximum of 40 characters is allowed. The flat file header will also include the date and time the file was created and the name of the server that contained the SDB.

## Backing up the SDB Using the TSA

1.



From the Admin menu, select "Bulk Admin," then "Back Up SDB." The "Create Flat File From SDB" dialog box is displayed:

#### Figure 6-18 Create Flat File From SDB Dialog Box (TSA)

Create Flat File From SDB			
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.			
<u>F</u> lat File Name: Co <u>m</u> ments for File Header:	bckupsdb.txt		
<u>0</u> K	<u>C</u> ancel		

- 2. You are prompted for the name of the flat file where the data is to be stored. If you choose, you may enter additional information for the file header at this time.
- 3. Select "OK."

## Backing up the SDB Using TSA32



1. From the Admin menu, select "Bulk Admin," then "Create Flat File From SDB." The "Create Flat File From SDB" dialog box is displayed:

Figure 6-19 Create Flat File From SDB Dialog Box

Create Flat File From SDB - ACME_NY			
All file names should NOT include a path. located in \\acme_ny\progra~1\teleph~1	All Bulk Admin files are  \tsrv\sdb\bulk_add.		
<u>F</u> lat File Name:	bokupsdb.txt		
Comments for File Header:			
OK Cancel	Help		

- 2. You are prompted for the name of the flat file where the data is to be stored. If you choose, you may enter additional information for the file header at this time.
- 3. Select "OK."

## **Updating the Security Database**

This command is used to initialize the SDB, or to update it periodically. It uses a simple file you created from your existing corporate database to create objects in the SDB.

Usually, this task is performed as a single process that converts a Simple File (created from the corporate database) to a flat file and then, using the flat file, updates the SDB. You can, for reasons described earlier in this chapter, break this process into its two individual steps.

You are prompted for the name of the simple file, flat file, and error file. If you do not supply names, the default names, "SMPLESDB.TXT," "FLATSDB.TXT," and "ERRORSDB.TXT" are used. If a file already exists with the name you chose, it is overwritten.

## Updating the SDB Using the TSA

1.



From the Admin menu, select "Bulk Admin," then "Update SDB." The "Update SDB" dialog box is displayed:

Figure 6-20 Update SDB Dialog Box (TSA)

- Update SDB				
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.				
<u>S</u> imple File Name:	smplesdb.txt			
<u>E</u> rror File Name:	errorsdb.txt			
Run Time Options				
Should <u>A</u> DD overwrite existing records?				
Advanced Options				
<u>OK</u>	<u>C</u> ancel			

- 2. Fill in the names of the simple file and the error file.
- 3. Choose the run time options.
- 4. To run only part of the update or to change the flat file name, select "Advanced Options." The "Advanced Update Options" dialog box is displayed:

#### Figure 6-21 Advanced Update Options Dialog Box (TSA)

Advanced Update Options			
Convert <u>S</u> imple File to Flat File			
Convert <u>Flat</u> File to SDB			
Flat File <u>N</u> ame:	flatsdb.txt		
Liuse			

This dialog box allows you to break the update process into two steps: converting from the simple file to the flat file and from the flat file to the security database. By default, both steps are performed.

If you want to update your SDB in two stages, set the appropriate checkbox at this dialog box, then select "Close."

5. Select "OK."

## Updating the SDB Using TSA32



1. From the Admin menu, select "Bulk Admin," then "Update SDB." The "Update SDB" dialog box is displayed, showing tabs for the "Basic" and "Advanced" options:

Figure 6-22 Update SDB Dialog Box (TSA32)

Update SDB - ACME_NY				
Basic Advanced				
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.				
Simple File Name: smplesdb.txt				
Error File Name: errorsdb.txt				
Run Time Options				
Stop processing on non-fatal errors?				
Should ADD overwrite existing records?				
OK Cancel Apply Help				

- 2. Fill in the names of the simple file and the error file on the "Basic" tab.
- 3. Choose the run time options.
- 4. To run only part of the update or to change the Flat File Name, select the "Advanced" tab.

### Figure 6-23 Update SDB Dialog Box (TSA32)

🗝 Update	SDB - ACME_NY
Basic Advanced	
🔽 Convert Simple File t	o Elat File
Convert <u>a</u> imple hie t	
Convert <u>F</u> lat File to S	iDB
Flat File <u>N</u> ame:	flatsdb.txt
	Cancel Apply Help

The "Advanced" options tab allows you to break the update process into two steps: converting from the simple file to the flat file and from the flat file to the security database. By default, both steps are performed.

If you want to update your SDB in two stages, set the appropriate checkbox from this tab.

5. Select "OK."

## **Upgrading the Security Database**

This command allows you to complete the upgrade of an SDB from an earlier release of Telephony Services to the current release. This command is also used to migrate and SDB from a NetWare Telephony server.

## Upgrading the SDB Using the TSA

1.



From the Admin menu, select "Bulk Admin," then "Upgrade SDB." The following dialog box is displayed:

Figure 6-24	
Upgrade SDB	<b>Dialog Box (TSA)</b>

SDB Upgrade - Stage 2				
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.				
<u>F</u> lat File Name:	upgrdsdb.txt			
<u>E</u> rror File Name:	errorsdb.txt			
Run Time Options Stop processing on non-fatal errors? Should <u>A</u> DD overwrite existing records?				
<u>O</u> K	<u>C</u> ancel			

# 2. Enter the Flat File Name and Error File Name that should be used for the upgrade.

If you are migrating the SDB from NetWare Telephony Service, enter the name of the output file generated by MIGRATE.EXE in the "Flat File Name" field. Refer to the *PassageWay Telephony Services for Windows NT Installation Guide* for details.

3. Select the desired run time options, and select "OK."

## Upgrading the SDB Using TSA32

1.



From the Admin menu, select "Bulk Admin," then "Upgrade SDB." The following dialog box appears:

Figure 6-25 Upgrade SDB Dialog Box (TSA32)

Upgrade SDB - ACME_NY				
All file names should NOT include a path. All Bulk Admin files are located in \\acme_ny\progra~1\teleph~1\tsrv\sdb\bulk_add.				
<u>F</u> lat File Name:	upgrdsdb.txt			
Error File Name:	errorsdb.txt			
Run Time Options				
Stop processing on non-fatal errors?				
Should ADD overwrite existing records?	?			
<u>OK</u> Cancel	Help			

# 2. Enter the Flat File Name and Error File Name that should be used for the upgrade.

If you are migrating the SDB from NetWare Telephony Service, enter the name of the output file generated by MIGRATE.EXE in the "Flat File Name" field. Refer to the *PassageWay Telephony Services for Windows NT Installation Guide* for details.

3. Select the desired run time options, and select "OK."

## **Object Attribute Tables**

This section contains the following information about each attribute in the SDB:

- The type of data: numeric, alphanumeric, true/false .
- Attribute validations: which checks are made on each attribute value before it can be stored in the SDB.
- Primary key/Foreign Key Relationships: which attributes are foreign keys; that is, which attributes in one object refer to the primary key in another object. Data in these foreign keys must refer to a valid primary key.

Flat file column headings surrounded by asterisks cannot be used to update the database. For example, the "Service Type" column heading for the Tlink object is "\*\*Service Type\*\*," and cannot be updated.

In the following tables, the attributes preceded by an asterisk cannot be modified using bulk administration

## **User Object Attributes**

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS
Login	100	Login name	49 char max. Must be unique.
Name	101	Name of user	32 char max.
Worktop Name	102	Worktop name	20 char max. Must be the name of an existing worktop object.
Device Monitor Group	103	Name of device/device monitoring group	32 char max. Must be the name of an existing device group.
Call-Dev Monitor Grp	104	Name of call/device monitoring group	32 char max. Must be the name of an existing device group.
Call Monitoring	105	Call/call monitoring permission	true/false. (Default: false)
Call Control Group	106	Name of call control device group	32 char max. Must be the name of an existing device group.
Routing Group	107	Name of routing device group	32 char max. Must be the name of an existing device group.
OAM Group	108	Name of admin access group	32 char max. Must be the name of an existing admin access grp.
Super Admin User	109	Does this user have super set of permissions?	true/false. (Default: false)

## Worktop Object Attributes

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS
Worktop Name	200	Worktop name	20 char max.
Primary Device	201	Device identifier of phone on worktop	10 char max. Must be the name of an existing device object.
IP Address	203	IP LAN address xxx.xxx.xxx where x is a decimal digit 0-9	32 char max. Must be the name of an existing IP address: XXX.XXX.XXX.XXX where each X is decimal and each set of 3 Xs range from 0 to 255.
IP Name	204	IP domain name	100 char max.
Secondary Device Grp	205	Name of device group to which the worktop has access	32 char max. Must be the name of an existing Device Group object.

## **Device Object Attributes**

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS
Device ID	300	Device identifier (unique). This is a PBX extension	10 char max.
Device Type	301	Type of device	PHONE, FAX, MODEM, ACD.
Tlink Group	302	Name of PBX that supports this device	32 char max. Must be the name of an existing Tlink Group. (Default: Any Tlink)
Location	303	Location of device	20 char max.
Telephone Number	304	Full telephone no. (for bulk administration only)	20 char max.

236 Network Manager's Guide
ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS
Device Group Name	400	Name of device group	32 char max.
Exception	401	Is this an exception group?	true/false. (Default: false)
Device ID	402	Device identifier of devices in group (multi-valued)	10 char max. Must be the Device ID of an existing device object.

# **Device Group Object Attributes**

# **Tlink Object Attributes**

The attributes in the following table are stored in the Tlink object by the Tserver. They are included for completeness, but you do not need to maintain them. The attributes that are preceded by an asterisk cannot be modified.

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS		
Tlink Name	500	Name of Tserver link	49 char max; periods not allowed		
*Service Type	510 Tlink Type		2 - CSTA 5 - TSRV_OAM 6 - CSRV_OAM 7 - SDB_OAM		

# **Tlink Group Object Attributes**

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS	
Tlink Group Name	600	PBX name	32 char max.	
Tlink	601	Name of CSTA Tlink (multi-valued)	49 char max. Must be the name of an existing CSTA Tlink object.	

Bulk Administration 237

ATTRIBUTE NAME	ID	DESCRIPTION	ATTRIBUTE RESTRICTIONS
Admin Group Name	700	Name of admin access group	32 char max.
OAM Tlink	701	Name of OAM Tlink (multi-valued)	49 char max. Must be the name of an existing OAM Tlink object.

# Admin Group Object Attributes

238 Network Manager's Guide

# **SDB Manual Pages**

The functions described below can be used to automate the administration of the Security Database. These functions are only available on Windows, Windows NT, and Windows 95 clients. Refer to the TSAPI reference manual for a discussion of the TSAPI programming model.

# sdbUpdateDataBase()

The **sdbUpdateDataBase(**) service is used to update a Btrieve SDB from data contained in the flat or simple file. This function may be used in lieu of the Bulk Administration feature to automate SDB administration.

The interface can be used in two modes:

Mode 1: You have created a simple file from data contained in a corporate database and wish to initialize the SDB with this information. You must supply the name of this simple file and set the options field to include SDB\_CONVERT\_SIMPLE and SDB\_CONVERT\_FLAT. You may specify the name of the error file to be created; if none is specified, the default file name, *errorsdb.txt*, is used. You may also choose to enable two additional options, SDB\_NON\_FATAL and SDB\_OVERWRITE.

SDB_NON_FATAL	If set, the update stops when a non-fatal error occurs. This error is saved in the error log along with information about the line in error. Fatal errors always cause processing to stop.
SDB_OVERWRITE	If set, the update overwrites an existing record with a new record with the same primary key. A copy of the original record is saved in the error log, flagged as a warning.

The conversion process involves two steps: converting from simple file to flat file and then from the flat file to the SDB. The name of the flat file may be specified or the default name, *flatsdb.txt*, may be used.

Mode 2: You have created a flat file and wish to update the SDB. This option allows you to automate the entire administration of the SDB. You must provide the name of the flat file containing the update information and set the options field to SDB\_CONVERT\_FLAT. You do not need to set the name of the simple file and must NOT set the SDB\_CONVERT\_SIMPLE option. The two additional options described in mode 1 also apply here.

#### Syntax

```
#include <acs.h>
#include <csta.h>
#include <sdb.h>
RetCode_t
              sdbUpdateDataBase(
   ACSHandle_t
                                      acsHandle,
   InvokeID_t
                              invokeID,
   SDBFlatFileName_t
                              *flatFile,
   SDBSimpleFileName_t
                              *simpleFile,
   SDBErrorFileName_t
                                      *errorFile,
                              *options);
   SDBOptions_t
```

#### Parameters

#### acsHandle

This is the value of the unique handle to the opened ACS stream. The stream must be opened to a Tserver SDB\_OAM service. The stream must be opened with at least TSAPI version 4.

#### invokeID

A handle provided by the application to be used for matching a specific instance of a function service request with its associated confirmation event. This parameter is only used when the invoke ID mechanism is set for application-generated IDs in the **acsOpenStream()** request. The parameter is ignored by the ACS library when the stream is set for library-generated invoke IDs.

#### flatFile

The name of the flat file to be used in the update. If no name is entered, the default name *flatsdb.txt* is used. For mode 1, this file is created in the \tsrv\sdb\bulk\_add directory on the server which is to be upgraded. This file name is required for mode 2 and must be placed in the bulk\_add directory prior to invoking the update function.

#### simple File

The name of the simple file that is to be used in the update. This field is required for mode 1 and not used in mode 2. If no *simpleFile* name is given, the default name, *smplesdb.txt*, is used. This file must already exist in the \tsrv\sdb\bulk\_add directory on the telephony server.

#### errorFile

The name of the error file to be created during the update. If no name is entered, the default name *errorsdb.txt* is used. This file is created in the **\tsrv\sdb\bulk\_add** directory on the server which is to be upgraded.

#### options

The set of options that apply to this upgrade. Options may be selected by "OR"ing them together in the options variable. The valid options are:

- 1. SDB\_CONVERT\_FLAT
- 2. SDB\_CONVERT\_SIMPLE
- 3. SDB\_NON\_FATAL
- 4. SDB\_OVERWRITE

Mode 1 requires that options (1) and (2) be set; mode 2 requires that only option (2) is set. Options (3) and (4) apply to both modes (1) and (2).

#### **Return Values**

This function returns the following values depending on whether the application is using library or application-generated invoke identifiers:

*Library-generated Identifiers* — if the function call completes successfully, it returns a positive value, i.e., the invoke identifier. If the call fails, a negative (<0) value is returned. For library-generated identifiers, the return value is never zero (0).

Application-generated Identifiers — if the function call completes successfully, it returns a zero (0) value. If the call fails, a negative (<0) value is returned. For library-generated identifiers, the return value is never positive (>0).

The application should always check the **SDBUpdateDataBaseConfEvent** message to ensure that the service request has been acknowledged and processed by the Telephony Server.

Bulk Administration 241

The following are possible negative error conditions for this function:

ACSERR_BADHDL	This return value indicates that a bad or unknown <i>acsHandle</i> was provided by the application.
ACSERR_STREAM_FAILED	This return value indicates that a previously active ACS stream has been abnormally terminated.

## Comments

This function can be called from a Windows client running a custom program developed by corporate programmers.

All SDB update requests and file creation occur on the server to which the stream has been opened. If either the flat file or the error file already exists, the file is overwritten without notice: all previous data is lost. All files are created in the \tsrv\sdb\bulk\_add directory on the telephony server.

# **SDBUpdateDataBaseConfEvent**

The *SDBUpdateDataBase* confirmation event provides the positive response from the server for a previous update request. No additional information is returned in the confirmation events.

#### Syntax

The following structure shows only the relevant portions of the unions for this message.

```
typedef struct
{
   ACSHandle_t
                              acsHandle;
   ACSHandle_t
EventClass_t
EventType_t
CSEventHeader_t;
                              eventClass;
                              eventType;
} ACSEventHeader_t;
typedef struct
   ACSEventHeader_t eventHeader;
   union
   ł
    struct
    {
      InvokeID_t
                     invokeID;
      union
       {
       SDBUpdateDataBaseConfEvent_t updateDatabase;
typedef struct SDBUpdateDataBaseConfEvent_t {
Nulltype null;
} SDBUpdateDataBaseConfEvent_t;
```

## Parameters

# acsHandle

This is the handle for the ACS stream.

# *eventClass*

This is a tag with the value **SDBCONFIRMATION**, which identifies this message as an SDB confirmation event.

# eventType

This is a tag with the value **SDB\_UPDATE\_DATA\_BASE\_CONF**, which identifies this message as an **SDBUpdateDataBaseConfEvent**.

# invokeID

This parameter specifies the function service request instance for the service which was processed at the telephony server or at the switch. This identifier is provided to the application when a service request is made.

# sdbBackupDataBase( )

The **sdbBackupDataBase(**) service copies all the information in the security database to a flat file.

#### Syntax

#### Parameters

#### acsHandle

This is the value of the unique handle to the opened ACS stream. The stream must be opened to a Tserver SDB\_OAM service. The stream must be opened with at least TSAPI version 4.

#### invokeID

A handle provided by the application to be used for matching a specific instance of a function service request with its associated confirmation event. This parameter is only used when the invoke ID mechanism is set for application-generated IDs in the **acsOpenStream()** request. The parameter is ignored by the ACS library when the stream is set for library-generated invoke IDs.

## flatFileNm

The name of the flat file to be created. If no name is entered, the default name *flatsdb.txt* is used. This file is placed in the \TSRV\SDB\BULK\_ADD directory on the server that is to be backed up. If the name is the same as an existing file in this directory, the existing file is overwritten without warning that this will occur.

#### comments

A 255 character field that is included in the header of the backed-up file. This is a user specified field.

#### **Return Values**

This function returns the following values depending on whether the application is using library or application-generated invoke identifiers:

*Library-generated Identifiers* — if the function call completes successfully, it returns a positive value, i.e., the invoke identifier. If the call fails, a negative (<0) value is returned. For library-generated identifiers, the return value is never zero (0).

Application-generated Identifiers — if the function call completes successfully, it returns a zero (0) value. If the call fails, a negative (<0) value is returned. For library-generated identifiers, the return value is never positive (>0).

The application should always check the **SDBBackupDataBaseConfEvent** message to ensure that the service request has been acknowledged and processed by the Telephony Server.

The following are possible negative error conditions for this function:

ACSERR_BADHDL	This return value indicates that a bad or unknown <i>acsHandle</i> was provided by the application.
ACSERR_STREAM_FAILED	This return value indicates that a previously active ACS stream has been abnormally terminated.

## Comments

This function can be called from a client running the TSA or TSA32 bulk administration menu or from a custom program developed by corporate programmers.

All data collection and file creation occurs on the server where the SDB to be backed up resides. If the backup file already exists, the file is overwritten without notice: all previous data is lost. All backup files are created in the \tsrv\sdb\bulk\_add directory.

# **SDBBackupDataBaseConfEvent**

The **SDBBackupDataBase** confirmation event provides the positive response from the server for a previous backup request. There is no additional information returned in the confirmation event.

#### Syntax

The following structure shows only the relevant portions of the unions for this message.

```
typedef struct
{
    ACSHandle_t
    ACSHandle_t acsH
EventClass_t eventClass;
EventType_t even
CSEventHeader t.
                                   acsHandle;
                                   eventType;
} ACSEventHeader_t;
typedef struct
   ACSEventHeader_t eventHeader;
   union
    ł
    struct
    {
       InvokeID_t
                         invokeID;
       union
    SDBBackupDataBaseConfEvent_t
                                           backupDatabase;
    }u;
} SDBConfirmationEvent;
} event;
} SDBEvent_t;
typedef struct SDBBackupDataBaseConfEvent_t {
Nulltype null;
} SDBBackupDataBaseConfEvent_t;
```

## Parameters

# acsHandle

This is the handle for the ACS stream.

# *eventClass*

This is a tag with the value **SDBCONFIRMATION**, which identifies this message as an SDB confirmation event.

# eventType

This is a tag with the value **SDB\_BACKUP\_DATA\_BASE\_CONF** which identifies this message as an **SDBBackupDataBaseConfEvent**.

# invokeID

This parameter specifies the function service request instance for the service which was processed at the telephony server or at the switch. This identifier is provided to the application when a service request is made.

# **SDBUniversalFailureConfEvent**

The SDB universal failure confirmation event provides a generic negative response from the server for a previously requested service. The **SDBUniversalFailureConfEvent** is sent in place of any confirmation event described in this section when the requested function fails. The confirmation events in this section are only sent when that function completes successfully.

#### Syntax

The following structure shows only the relevant portions of the unions for this message.

```
typedef struct
{
    ACSHandle_t
                                       acsHandle;
                               eventClass;
    EventClass_t
    EventType_t
                                       eventType;
ACSEventHeader_t;
typedef struct
   ACSEventHeader_t
                                eventHeader;
   union
    {
        struct
        {
           InvokeID_t invokeID;
           union
           {
               SDBUniversalFa ilureConfEvent_t
                                                         failure;
           }u;
        } SDBConfirmationEvent;
   } event;
} SDBEvent_t;
typedef struct
UniversalFailure_t
} SDBUniversalFailureConfEvent_t;
                                                error;
```

Bulk Administration 249

#### Parameters

# acsHandle

This is the handle for the ACS Stream.

# *eventClass*

This is a tag with the value **SDBCONFIRMATION** which identifies this message as an SDB confirmation event.

## eventType

This is a tag with the value **SDB\_UNIVERSAL\_FAILURE\_CONF** which identifies this message as an **SDBUniversalFailureConfEvent** 

#### invokeID

This parameter specifies the function service request instance that has failed at the server. This identifier is provided to the application when a service request is made.

#### error

This parameter contains the error returned by the function. See the section titled "Security Database Errors" in Chapter 11 for more details.

Error Code	Error Name	Description
504	SDB_INVALID_STATE	The SDB is not in a NORMAL state. Check the version information and correct the problem.
553	SDB_READ_FAILURE	The specified name of the simple/flat/error file is not a valid format
554	SDB_FILE_NOT_PRESENT	Could not find the simple/flat file name requested.
552	SDB_WRITE_FAILED	Could not write to the flat/error file. This is not a failure to write to the SDB.
544	SDB_INVALID_OPCODE	The first column of a line in the simple/flat file contained an invalid opcode. This may occur if the editor used to create the file inserted a new line <cr> on lines that exceeded a preset maximum.</cr>
	Attribute specific errors	If the user has selected the STOP ON NON FATAL ERRORS option, errors on an individual attribute cause processing to stop.

Bulk Administration 251

# chapter **7 TCP/IP Configuration**

This chapter describes TCP/IP configuration for the Tserver and Telephony Services clients. It discusses the interaction of TCP/IP with Telephony Services features.

This chapter also describes the authentication methods used by telephony services to check that a user attempting to establish a connection is an authorized user.

# LAN Connectivity

Figure 7-1 shows the LAN architecture for Telephony Services. Both servers and clients are included in this diagram; each has a transport module using TCP/IP that is responsible for setting up a connection between a Telephony Services Library (TSLIB) client and a Windows NT machine running Telephony Services.

Figure 7-1 Telephony Services LAN Architecture



254 Network Manager's Guide

# **Client Software Modules**

The TSLIB for each client platform uses a configuration file to identify the telephony servers available on a network. A summary of the TSLIB modules and configuration files for the different platforms is provided in Table 7-1.

# Table 7-1

## **TSLIB Modules and Configuration Files**

CLIENT TYPE	NAME OF TSLIB MODULE	CONFIGURATION FILE
Windows	CSTA.DLL	TSLIB.INI
Windows NT	CSTA32.DLL	TSLIB.INI
Windows 95	CSTA32.DLL	TSLIB.INI
OS/2	CSTA.DLL	TSLIB.INI
UnixWare	libcsta.so	/usr/lib/tslibrc
HP-UX	libcsta.sl	/usr/lib/tslibrc

# TCP/IP

With Telephony Services Release 2.22 for Windows NT, clients connect to your telephony server using TCP/IP. During installation, each telephony server is assigned a unique IP address that is used to bind Telephony Services to TCP/IP. This must be a fixed IP address. (DHCP cannot be used to assign this address). Telephony Services has been assigned TCP Port 450; this is used as the default value if you do not explicitly select a different port number. Both the IP address and port number are specified in a configuration file on the client workstation. When an application wants to establish a connection to a telephony server, TSLIB reads the configuration file and retrieves the IP address and port information.

TCP/IP Configuration 255

# **Server Configuration**

If you need to change the Tserver's IP address, you can do so in the "Telephony Services for Windows NT" program group. Use the following procedure to change the IP address:



- 1. From the "Telephony Services for Windows NT" program group, double-click on "TSAPI Telephony Services Controller."
- 2. Select the "Advanced" button and then select "Change IP Address."
- 3. Enter a new address in the "Enter New IP Address" dialog box, then select "OK."
- 4. Select "Close" to return to the "TSAPI Telephony Services Controller" dialog box. Select "Close" when done.

You should not need to change the TCP port number to something other than 450 unless you have an application that is using port number 450. If you do need to change the port number, you must modify the \SYSTEM32\DRIVERS\ETC\SERVICES file on the server. Lines in this

file have the following format:

service\_name port\_number/protocol\_name [alias [...]]
# Comments

The following is a sample SERVICES file with a line for Telephony Services added:

#
#
#
#
#
#
#
#
#
Network service mappings. Maps service names to transport
# protocol and transport protocol ports.
ftp 21/tcp
telnet 23/tcp
#
# Host specific functions
# Assign port 3000 to Telephony Services
telephony\_server 3000/tcp #Telephony Services

# Win16 and Win32 Client Configuration

Each Windows 3.1, Windows for Workgroups 3.11, Windows NT, or Windows 95 client that uses TCP/IP to connect to the telephony server must have a TSLIB.INI file. This file has a standard Windows ".INI" format.

The first section of this file is labeled "[Telephony Servers]." Each line in this section identifies a Tserver's host name or IP address. The line may also contain a port number; if the Tserver's port number is a value other than "450" (the assigned port for Telephony Services), you must provide the Tserver's port number.

Each line in the "[Telephony Servers]" section of TSLIB.INI must adhere to the following format:

 $host\_name=port\_number$ 



Spaces are not valid in host names.

The following is a sample of a TSLIB.INI file on a client workstation that identifies two telephony servers:

```
[Telephony Servers]
;list of Telephony Servers
acmehost1=450
172.16.80.21=3000
```

If you prefer, you can create a single TSLIB.INI file on a server and direct all clients to use this shared file. The TSLIB.INI file on the server must have a "[Telephony Servers]" section that identifies the telephony serv ers in your network, as described above.

In addition to creating a TSLIB.INI file on the server, you must create a TSLIB.INI file on each client. In the "[Shared Admin]" section, you must provide a pointer to the TSLIB.INI file on the server.

TCP/IP Configuration 257

This pointer has the following format:

tslib.ini= shared\_path\_name

where *shared\_path\_name* is the path name of the shared TSLIB.INI file on the server.

The following is an example of a client TSLIB.INI file that references a server TSLIB.INI file.

[Shared Admin] ;file option allows administrator to point to ;a shared .ini file that lists the servers tslib.ini=h:\tsrv\admin\tslib.ini

To edit this file, use the "Edit TSLIB.INI" icon in the "TS Win16 Client" or the "TS Win32 Client" program group.

# **OS/2 Client Setup**

Each OS/2 client that uses TCP/IP to connect to the telephony server must have a TSLIB.INI file located in the C:\CSTA directory. This file has a binary format, and contains information concerning the communications protocols that will be active for this client. The file also contains the Internet domain names or IP addresses and port numbers of the TCP/IP Tserver listings (if using TCP/IP as the communications protocol).

Since the TSLIB.INI file is a binary file which you cannot edit directly, you must use the OS/2 configuration application to change the address and port number in the file to match the address and port number of the server you want to access.

To use the OS/2 configuration application, access the "Configure Telephony Servers" dialog box. Enter the IP name or address for the server. The default port number is 450; it should appear on the screen. If there is no port number, enter 450 or the specific port number you want to access. Select "Add" to enter the address and port number in the TCP/IP Servers list box. Then select "Save" to update the TSLIB.INI file with the new information.

258 Network Manager's Guide

# UnixWare and HP-UX Client Setup

Each Unix-based client that uses TCP/IP to connect to the telephony server must be able to locate a configuration file containing address information for the Tservers the client needs to access. You can specify the pathname for this file by setting the shell environment variable TSLIBRC. If the TSLIBRC variable is not set, then the client library searches your \$HOME directory for a file named .tslibrc. If the client library cannot locate a configuration file after looking in both TSLIBRC and .tslibrc, it then looks for the file /usr/lib/tslibrc.

Each line of the configuration file must have the following format:

host\_name port\_number # this is a comment

where *host\_name* is an Internet domain name or IP address, and *port\_number* is the TCP port for the Tserver's name server. If the *port\_number* is omitted, a default value of 450 is assumed.



Spaces are not valid in host names.

Also, since the HP-UX client does not support IPX/SPX, the TCP/IP transport layer option must be enabled on the server.

The following is a sample .tslibrc file:

#	list	o£	the	servers	that	а	re	runn	ing	Tele	phony	Servic	es
t۵	srvhos	st				#	ass	ume	defa	ault	port	number	
17	72.16.	.8.2	21	300	00	#	use	por	ct 30	000			

A template file, /usr/lib/tslibrc, is created during installation. However, this file contains only sample names and addresses. You must edit it to change the sample information to the actual Telephony Server host name (or IP address) and port information for the servers your Unix-based client needs to access.

TCP/IP Configuration 259

The template for the /usr/lib/tslibrc file looks like this:

#### # /usr/lib/tslibrc

# Blank lines and text beginning with "#" are ignored.

# This is a list of one or more hosts offering Telephony Services via TCP/IP. # Either domain name or IP address may be used; default port number is 450 # The form is: host\_name [port\_number] For example:

tserver.mydomain.com	450	# domain name style
127.0.0.1	450	# dotted-decimal IP address

# replace the above samples with the actual Telephony Server address(es).

# Individual users may override the contents of this file by setting # the TSLIBRC environment variable to the pathname of an alternate # server list (in this same format) or by creating a ".tslibrc" file # in their \$HOME directory.

Replace the "tserver.mydomain.com" and "127.0.0.1" lines with the names (or IP addresses) and port numbers of the Telephony Servers you want to access.

# **TCP/IP and Tserver Feature Interactions**

The Tserver has several features whose operation depends upon how TCP/IP is configured on your network. These features are:

- Extended Worktop Access If you check this box, users who log in from a worktop other than their assigned worktop will be able to monitor and control the devices associated with that worktop, as well as monitor and control the devices on their assigned worktop and in their classes of service.
- Automatic Administration of LAN Addresses If a LAN address is not already assigned to a user's worktop and you enable this feature, the Tserver automatically fills in the LAN address information the next time the user logs on.
- TCP Preferred Naming Format Lets you choose either Host Name or IP address as the format for workstation LAN addresses.

The TCP Preferred Naming Format is only used if you have enabled "Extended Worktop Access" or "Automatic Administration of LAN Addresses." If both of the above features are disabled, the TCP Preferred Naming Format setting does not matter. However, for performance reasons, it is recommended that this field remain at the default setting, "IP Address."

#### **Extended Worktop Access**

If "Extended Worktop Access" is enabled, then the TCP Preferred Naming Format is used to check User and Worktop object information. The Tserver uses the TCP Preferred Naming Format field to determine if the user is logging in from his/her own worktop.

If you have chosen "Host Name" format, the Tserver converts the IP address in the connection request message to a host name. It then looks up the User and Worktop object for the person logging in. If the host name in the Worktop matches the converted host name, the user is at his/her own worktop. If the two names do not match but the "Extended Worktop Access" feature is **enabled**, the user has logged into another worktop and can also control the devices on that worktop. If the two names do not match and "Extended Worktop Access" is **disabled**, then the user can control only the devices on his/her own worktop.

# Automatic Administration of LAN Addresses

If "Automatic Administration of LAN Addresses" is enabled, then the TCP Preferred Naming Format is used to determine how the LAN address is stored on the telephony server.

If you select "IP Address" as your naming format and have enabled "Automatic Administration of LAN Addresses," the Tserver will use the client workstation IP Address when assigning a LAN Address to a user's worktop (if that field is empty).

#### **TCP Preferred Naming Format**

If you use the Host Name format, the Tserver must be able to resolve the host name using some form of host-name resolution, such as Domain Name Services (DNS) or Windows Internet Name Services (WINS). Enter the IP addresses you want to use for host-name resolution in a local HOSTS file, a DNS HOSTS file, or a WINS HOSTS file.



Do not use a LAN Manager Hosts (LMHOSTS) file. This is because the Tserver only searches for addresses in files with the specific name of HOSTS (no extension). If no HOSTS files are found, slow performance or a time out failure will result.



If you are using DHCP for your clients, you must also have WINS and must use Host Names as the TCP Preferred Naming Format. If you specify aliases for host names, you must use the primary host name in the "Host Name" field of the Worktop object.

If you use the "IP Address" format, the Tserver compares the IP address in the open connection request to the IP address in the user's Worktop object. The Tserver uses the address in the Worktop object to decide if the user is at their own worktop or another worktop. It does not require any host-name resolution.

# Using the TSA to Administer TCP/IP

1.



From the TSA, select "Tserver Options" from the "Maint" menu. The "Tserver Options" dialog box is displayed:

## Figure 7-2 Tserver Options

	Tserver Options	
Enable Pop-Up Ala	rm Notification	
Advertise Telephor	ny Services <u>N</u> ame Server	
Extended Worktop	Access	
🗌 🗌 Enable Automatic A	Administration of LAN Addresses	
Transport Layer Option □ IPX/ <u>S</u> PX ◎ <u>I</u> CP/IP	ns TCP Port: 450	
IP <u>A</u> ddress:	135.20.70.5	
TCP Preferred Naming Format         O       Host Name         IP Address		
	<u>OK</u> <u>C</u> ancel	

- 2. Use this screen to set the TCP Preferred Naming Format.
- 3. Select "OK" when done.

# Using TSA32 to Administer TCP/IP

1.



From the TSA32, select "Properties" from the "Admin" menu. The "Tserver Properties" dialog box is displayed, showing tabs for "Options," "SDB Log Settings," and "Components."

#### Figure 7-3 Tserver Properties

- 2. Use the "Options" tab to set the TCP Preferred Naming Format.
- 3. Select "OK" when done.

# **TCP/IP Status**

You can use the TSA or the TSM32 display information about the TCP/IP transport protocol for a particular Tlink. The information displayed includes the total number of pending connection requests that are active at the current time. The "Max Used" field indicates the highest number of establish connection requests active at one time and allows you to reset the value to zero.

# Using the TSA to Display TCP/IP Status

1.



To view TCP/IP information for a specific Tlink using the TSA, select the "Tlink Information" option from the "Maint" menu. The "Tlink Information" dialog box is displayed:

Figure 7-4 Tlink Information

Tlink Information	
Ilinks: LUCENT#CSTASERV#CSTA#ACME_NY LUCENT#SDB_OAM#OAM#ACME_LA LUCENT#SDB_OAM#OAM#ACME_NY TSERVER#CSRV_OAM#OAM#ACME_NY TSERVER#NSRV#CSTA#ACME_NY TSERVER#TSRV_OAM#OAM#ACME_NY	<u>C</u> reate <u>E</u> dit
C <u>l</u> ose	<u>D</u> elete

2. Select the Tlink you are interested in and select "View." The "Tlink Information Details" dialog box is displayed:

Figure 7-5 Tlink Information Details

Tlink Information Details for LUCENT#CSTASERV#CSTA#ACME_NY								
TSDI <u>S</u> ize (bytes):	1572864	<u>H</u>	igh Water Mark (bytes):	1258291				
IPX/SPX Info		C	onnections:	20				
		S	tream Type:	CSTA				
<u> </u>	•	S	upported Protocols:	TS2				
		v	ersion:	2.22.29.0				
Flow Control (TSDI B	Flow Control (TSDI Buffers)							
			Disabled					
<b>∏Number of Messages</b>								
Queued to Tlink:		1	Allocated by Tlink:	0				
Queued to Tserver:		0	Allocated by Tserver:	1				
Tserver Private:		107						
Number of Bytes		170	Aller at the TE-te	0				
Queued to Tlink:		172	Allocated by Tlink:	0				
Queued to I server:		U	Allocated by 1 server:	172				
Tserver Private:		36460						
Invoke IDs								
		_		Caract				
<u> </u>	In Use:	2	20 <u>R</u> eset	Lancel				
			L]					

TCP/IP Configuration 267

3. Select the "TCP/IP Info" button. The "TCP/IP Information" dialog box is displayed:



Figure 7-6 TCP/IP Information

4. Select "Close" when done.

# Using TSM32 to Display TCP/IP Status

1.

Procedure **123** 

To view TCP/IP information for a specific Tlink using TSM32, select "Tlink Status" from the "Options" menu. The "Tlink Status" dialog box is displayed, showing tabs for "Information," "TSDI," and "TCP/IP."

Figure 7-7 Tlink Status

	Tlink Status	- ACME_NY	-
Information TSDI TCP	/IP]		
<u>I</u> link: LUCENT	#SDB_OAM#OAM	#ACME_NY	<u>±</u>
Registered? Open Connec Stream Type: Version: Supported Pro Tlink Security Flow Control ( Invoke IDs In Use:	tions: otocols: : TSDI Buffers):	Yes 2 OAM 2.22.27.0 TS4-5 Login Disabled	
Max Used:		1	<u>R</u> eset
Applications: TSA16 TSA32			Re <u>f</u> resh Delete
	OK	Cancel	Apply Help

2. Select the Tlink you want from the "Tlink" drop-down list (on the "Information" tab). Then select the "TCP/IP" tab.



	Tlink S	tatus - AC	ME_NY		-
Information TSDI	TCP/IP				
Tlink:	LUCENT#SDB_OAM	#OAM#ACM	E_NY		
	-Outstanding Connec	tions			
	Current:	0			
	Current.	U			
	Max Used:	1	<u> </u>	et	
	I				
	<u>lok</u>	Ca	ncel	Apply	Help

3. Select "OK" when done.

# **User Authentication**

Authentication is the process by which the Tserver determines if a user attempting to establish a connection has provided a valid login ID and password. The login ID and password are always those of a Windows NT Workstation or Server user account (the login IDs must be administered in the Telephony Services Security Database **and** in the Windows NT user database). Telephony Services authenticates a user against Windows NT user accounts in one of the following ways:

- If a user has already authenticated themselves to Windows NT, Telephony Services will allow the user to establish a connection by supplying only a login ID. This is known as Single Login Authentication. Only Windows-based TSLIB clients with support for Microsoft networking can interact with the Telephony Server to establish the identity of a client for Single Login Authentication.
- 2. If Single Login Authentication cannot be used to validate a client connection request, then Local Login Authentication is used. In Local Login Authentication, a login ID and password are always required by Telephony Services in order to establish a connection.



Even though a user has authenticated themselves with Windows NT and is running a Windows-based application (for example, they are using a Windows-based TSLIB client), this does not guarantee that an application will not ask the user for their Windows NT password. The application must have taken advantage of TSAPI calls which allow it to ask the Tserver for the login and password requirements.

If all requirements for Single Login Authentication are met, then the application is told that only a login ID is required. If the requirements are not met, then the application is told that both login ID and password are required. The application must then display appropriate dialog boxes which ask only for the needed information. However, if the application is told that only a login ID is required and the application still asks for a password, the password will be ignored by the Telephony Server. In the following discussions, "Windows NT Machine" refers to a computer running either Windows NT Workstation software or Windows NT Server software (where the Windows NT Server is configured as either a Windows NT Server, a Windows NT Backup Domain Controller, or a Windows NT Primary Domain Controller [PDC]). Telephony Services can run on any Windows NT Machine which is part of a Windows NT Workgroup or Domain.

It is recommended that users who will be using Telephony Services have a single Windows NT user account. For a single account, the following conditions apply:

- If Telephony Services is running on a Windows NT workstation which is not a member of a domain, then all user accounts must exist on the Windows NT Workstation.
- ◆ If Telephony Services is running on a Windows NT machine which is a member of a domain, then it is suggested that all user accounts exist on a single Primary Domain Controller (PDC). The PDC can exist in either the domain containing the Windows NT machine that is running Telephony Services, or in a Trusted Domain that is part of the domain containing the Windows NT machine which is running Telephony Services. (Microsoft documentation on Windows NT also makes similar recommendations about having a single user account.)
- If you have a network configuration which requires the same user login to exist on different Windows NT machines and/or domains, Telephony Services SDB administration allows you to qualify a user record's login ID with the name of the Windows NT machine or domain. For more information, refer to the section titled "Distinguishing Users In Different Windows NT Do mains" later in this chapter.
## Single Login Authentication

The following TSLIB clients have the ability to interact with the Telephony Server to perform Single Login Authentication:

- I6-bit Windows TSLIB (CSTA.DLL), which operates on Windows for Workgroups (Single Login Authentication is not possible on Windows 3.1). Windows for Workgroups must be set up so that you are able to log in to the NT server in order for Single Login Authentication to work from a Windows for Workgroups machine running a Telephonyenabled application. (If your Windows for Workgroups client can access files on the server, then Single Login Authentication should work.)
- 32-bit Windows TSLIB (CSTA32.DLL), which operates on Windows NT and Windows 95. The user must already be authenticated with Windows NT prior to trying to establish a connection to the Tserver. (The login ID must be administered on the NT server and on the client.) The connection can be established by mapping a drive to a Windows NT machine.

The following methods are available for logging into or mapping drives to Windows NT and Windows 95 systems:

- 1. Logging into a Windows NT machine, which means:
  - Logging into the Windows NT Machine that is running Telephony Services, or
  - Logging into the Windows NT Primary Domain Controller for which the Windows NT machine (which is running Telephony Services) is a domain member, or
  - Logging into a Windows NT Primary Domain Controller in a Trusted Domain where the Windows NT machine (which is running Telephony Services) is a domain member

- 2. Logging into a Windows 95 machine, which means:
  - Providing a login ID and password for "Microsoft Networking" that matches a login ID/password combination on the Windows NT Machine that is running Telephony Services, or
  - Providing a login ID and password for "Microsoft Networking" that matches a login ID/password combination on the Windows NT Primary Domain Controller for which the Windows NT machine (which is running Telephony Services) is a domain member, or
  - Providing a login ID and password for "Microsoft Networking" that matches a login ID/password combination on a Windows NT Primary Domain Controller in a Trusted Domain where the Windows NT machine (which is running Telephony Services) is a domain member
- 3. Mapping a Drive to a Windows NT machine, which means:
  - Mapping a drive to the Windows NT Machine that is running Telephony Services, or
  - Mapping a drive to the Windows NT Primary Domain Controller for which the Windows NT machine (which is running Telephony Services) is a domain member, or
  - Mapping a drive to a Windows NT Primary Domain Controller in a Trusted Domain where the Windows NT machine (which is running Telephony Services) is a domain member

## Local Login Authentication

If the requirements for Single Login Authentication are not met, then the Tserver and TSLIB client together revert to using Local Login Authentication. In this method of authentication, the user must always supply a login ID and a password, both of which are used by Telephony Services in a Windows NT login attempt. If the login is successful, Telephony Services determines where the login occurred (either on a Windows NT machine or in a particular domain), then logs the user out. This method requires at least one Windows NT client license to be available at the time of the login attempt. Telephony Services processes all Local Login Authentication attempts in a serial manner, so that no more than one available Windows NT license is required.

When attempting a Windows NT login, Windows NT performs a search for a matching login ID and password, in the following order:

#### If the Tserver is not a domain member:

1. The local Windows NT machine running Telephony Services

#### If the Tserver is a domain member:

- 1. The Primary Domain Controller for a Windows NT Machine running Telephony Services
- 2. The Primary Domain Controller in Trusted Domains for the domain in which the Tserver is running

If more than one user account in this search path exists with the same login ID and password, then the Telephony Services user is authenticated against the first user account encountered. If this first user account has a password different from the one supplied, Telephony Services will fail the authentication even if there is a user account with the same login ID and password further along in the search path.

TCP/IP Configuration 275

In addition to having an existing user account for Local Login Authentication, the user account must also have the following properties:

- 1. The account must be enabled.
- 2. The account must have the **Log on as a service** User Right assigned to the account on the Windows NT Machine that is running Telephony Services.

If a Windows NT Workstation (which is part of a domain) is running Telephony Services and the user account exists on the Primary Domain Controller, the Primary Domain Controller user account must be given the **Log on as a service** User Right on the Windows NT Workstation, *not on the Primary Domain Controller*. It is suggested that you create a new group (such as "Telephony Users") and that you add to this group every user account which will be using Telephony Services. You would then assign the **Log on as a service** right to this new group on the Windows NT Machine running the Telephony Server.



The **Log on as a service** right is a more advanced right in Windows NT and is not one that the Windows NT administrator may wish to grant to every Windows NT user who will be accessing Telephony Services. The following are ways to limit the granting of this right while still allowing access to Telephony Services.

 It is not required that all users of Telephony Services be granted the Log on as a service right. Only those users who will access Telephony Services using a login ID that is different from the one they normally log into Windows NT with will need to be given this right. In most cases, the login ID a user uses on a daily basis to gain access to Windows NT will be the same login ID the user should use to gain access to Telephony Services. For these users, Single Login Authentication will allow them access to Telephony Services without their Windows NT password or the Log on as a service right. 2. If the Telephony Server is run on a Windows NT Machine in a domain other than the Primary Domain Controller, then the following technique can be used to limit the granting of the Log on as a service right. Maintain all user accounts on the Primary Domain Controller and create a global group on the PDC which contains users who need to access Telephony Services via Local Login method. Then assign the Log on as a service right to this group on the machine running the Telephony Server, not on the PDC. This limits the ability of the Windows NT user to exercise this right to only the case when accessing Telephony Services.

In Windows NT, the following procedure is used to assign User Rights to accounts.

## **Assigning User Rights**



1.

## Start the "User Manager"

On a Windows NT Workstation, run "User Manager" (on a Windows NT Server, run "User Manager For Domains"). This program is normally found in the **Administrative Tools** Program group.

#### 2. Select "User Rights"

From the "Policies" menu, select **User Rights**. The **Users Rights Policy** dialog box is displayed.

#### 3. Enable "Show Advanced User Rights"

Set the "Show Advanced User Rights" checkbox. Then, from the pull down list labeled "Right," select "Log on as a service."

#### 4. Add users or groups

Use the **Add** option to add users or groups to this right as appropriate.

5. Select "OK."

TCP/IP Configuration 277

## **Distinguishing Users In Different Windows NT Domains**

Although not recommended, if the Windows NT configuration (in which Telephony Services is operating) calls for multiple Windows NT user accounts with the same user name, the Telephony Services Security Database can be administered to distinguish between these accounts.



If these accounts actually represent different users requiring different Telephony Services access permissions, then distinguishing between different user accounts with the same user name would be appropriate. If different Windows NT user accounts represent the same user, then there is no need to distinguish between the accounts in the Telephony Services SDB.

You can enter a user name into the SDB using one of the following formats:

- Windows NT User Account Name
- Windows NT machine Name\Windows NT User Account Name
- Windows NT machine Domain Name\Windows NT User Account Name

When entering a Windows NT machine or Domain name before the user name, be sure to separate the two parts with a backward slash ( "\"). Do not use spaces.

When Telephony Services authenticates a user's request to establish a connection, the Windows NT machine or Domain that the account was authenticated against is known to Telephony Services. Telephony Services will first attempt to find a user record in the SDB which includes the authenticating Windows NT machine or Domain name. If such a user record does not exist, then Telephony Services looks for a user record with just the user account name. A user record in one of these formats must always exist in the SDB in order for a user to establish a connection with Telephony Services.

The following examples help clarify this concept. In the examples, the Windows NT Primary Domain Controller machine is called "SALES-PDC," and it exists in the Windows NT Domain "SALES." A Windows NT Workstation called "STAFF" also exists, and is a member of the domain SALES. Sally has a Windows NT account on both machines (SALES-PDC and STAFF). Telephony Services is running on the machine STAFF.

#### Example 1

If Sally is logged into the domain SALES from a different Windows NT workstation within the domain, when she attempts to establish a connection to Telephony Services she is authenticated against her Windows NT user account which exists in the domain SALES. Telephony Services first looks for a user account with the name "SALES/SALLY." If this account does not exist, Telephony Services then looks for a user account with the name "SALLY."

#### Example 2

If Sam is logged into his own Windows NT Workstation and has mapped a drive to the Telephony Services machine STAFF, when he attempts to establish a connection to Telephony Services he is authenticated against his Windows NT user account which exists on the Windows NT Workstation (STAFF). Telephony Services first looks for a user account with the name "STAFF\SAM." If this account does not exist, Telephony Services then looks for a user account with the name "SAM."

When a user is authenticated against a domain, the domain name, **not the name of the Primary Domain Controller**, is used to qualify the user name. When a user is authenticated against a specific machine in a domain, the name of that machine is used to qualify the user record.

## chapter

# 8 The Tserver

This chapter describes the Telephony Services server software. The following topics are discussed:

**Telephony Server Software** – covers telephony server software modules and options (pop-up alarms and name server advertising), as well as version and system status information

**Loading and Unloading PBX Drivers** – describes how you can load or unload the dynamic link libraries (DLLs) for the Tserver. You can also request that a DLL be loaded automatically or manually, and add or remove a DLL if necessary.

**Telephony Server Status** – covers the Telephony Server Driver Interface (TSDI) resource information and Tserver status information.

**Tlink Status** – describes the status information reported for each Tlink. This information is available through the TSA or the TSM32 application.

**User Status** – describes the status information reported for each user who has an active connection to the Tserver.

# **Telephony Server Software**

Figure 8-1 illustrates the software modules that reside on a telephony server.



Each module belongs to one of four groups:

- A Tserver group: the Telephony Services software
- **B** PBX driver group: the software supplied by your PBX vendor to provide an interface to the PBX.
- **C** Server application group: the software required to run server applications.

**D** Transport group: the Windows NT software provided to establish TCP/IP connections with client workstations or other servers.

The PBX driver software is provided by the vendor that manufactured your PBX. The Transport Layer is part of the operating system. The remaining software modules, except for server applications, are provided by Telephony Services.

## **Telephony Server Modules**

The major server software modules and interfaces are:

- **Tserver**. The Tserver's primary function is routing messages between applications running on client workstations (or other servers) and PBX drivers. When a client application issues a Telephony Services request, the Tserver determines whether to grant the request based on the user permissions in the Security Database. If the client's request is permissible, the Tserver forwards the request to the PBX driver for processing. The Tserver also receives messages from the PBX driver and routes them to the appropriate client. When configured to do so, the Tserver creates and maintains error logs, message trace files, and traffic logs.
- The Telephony Services Driver Interface (TSDI). The TSDI is the interface between the Tserver and the PBX driver(s) on the server The TSDI allows a PBX driver to "register" services with the Tserver. These services are called Tlinks. After a service has been registered, the Tserver and the PBX driver exchange messages. Resources used by this message exchange are allocated on a per Tlink basis. Telephony Services provides a way to monitor the number of messages waiting to be processed by the Tserver and the PBX driver (by using either the TSA or TSA32).

- ◆ The Cserver. The Cserver module provides a second PBX driver interface where messages are encoded using the ECMA-180 protocol definition. It receives messages from the Tserver across the TSDI interface and maps them into ECMA-180 messages exchanged across the CSDI interface. It also provides client session management. This module is required by certain PBX driver implementations.
- The PBX driver. The PBX driver handles the messages that pass between the PBX and the PBX driver over CTI links. Each PBX vendor provides a PBX driver module to be run in conjunction with Telephony Services.

## **Telephony Server Options**

The Telephony Server options include the following:

- Enable Pop-Up Alarm Notification: Enabling this feature causes a pop-up window to be displayed whenever an alarm occurs. You may want to enable this feature if you are running a mission critical application.
- ♦ Advertise Telephony Services Name Server: This field is provided for compatibility with future releases. It should always be enabled.
- Extended Worktop Access: If you check this box, users who log in from a worktop other than their assigned worktop will be able to monitor and control the devices associated with that worktop, as well as monitor and control the devices on their assigned worktop and in their classes of service. See Chapter 3 for more details on this feature.
- Enable Automatic Administration of LAN Addresses: If the LAN address is not already assigned for the user's worktop and you enable this feature, the Tserver automatically fills in the LAN address information the next time a user logs on. (LAN addresses are only necessary if you are using the "Extended Worktop Access" feature.) See Chapter 7 for more details on this feature.
- **Transport Layer Options:** These fields are used to specify the transport method between client and server. The supported method is TCP/IP. See Chapter 7 for a complete discussion of these fields.

## **Pop-Up Alarms**

If you enable the Pop-Up Alarm Notification feature, the system displays a system modal dialog box (on the client workstation where the TSA or TSM32 is in use) whenever an alarm occurs on the attached Tserver. The system displays the dialog box even if you have minimized the administration application on your client dialog box. This dialog box must be dismissed before you can do anything. If you do not check the Enable Pop-Up Alarm Notification box, the system logs alarms, but does not display a dialog box. You may want to check this option if you are running critical applications so you can be notified of any problems as they occur.

Telephony Services generates alarms whenever an ERROR or FATAL event occurs on the telephony server. You can select which events cause an alarm to be generated. (See the section in Chapter 11 titled "Turning on Error Logging.") You will not see any alarms unless you check the pop-up notification box, as indicated above.

## Using the TSA to Enable Pop-Up Alarms



- 1. From the "Maint" menu, select "Tserver Options." The "Tserver Options" dialog box is displayed.
- 2. Make sure that the "Enable Pop-Up Alarm Notification" box is checked.

#### Figure 8-2 Enable Pop-Up Alarms (TSA)

Tserver Options		
Enable Pop-Up Alarm Notification		
Advertise Telephony Services <u>N</u> ame Server		
Extended Worktop Access		
Enable Automatic Administration of LAN Addresses		
Transport Layer Options       IPX/SPX       ICP/IP       TCP Port: 450		
IP <u>A</u> ddress: 135.20.70.5		
○ <u>H</u> ost Name		
<u>O</u> K <u>C</u> ancel		

## Using the TSM32 to Enable Pop-Up Alarms



- 1. From the "Options" menu, select "Tserver Properties." The "Tserver Properties" dialog box is displayed.
- 2. On the "General" tab, make sure that the "Enable Pop-Up Alarm Notification" box is checked.

Figure 8-3	
Enable Pop-Up Alarms (	TSM32)

Tserver Properties - ACME_NY
General Transport Components
Enable Pop-Up Alarm Notification
Advertise Telephony Services Name Server
OK Cancel Apply Help

## Name Server Advertising

This feature enables or disables the advertisement of the Tserver Tlinks. This feature is enabled by default, and it should always be left enabled. It is intended for compatibility with future releases.

## Using the TSA to Enable Name Server Advertising

1.



- From the "Maint" menu, select "Tserver Options." The "Tserver Options" dialog box is displayed.
- 2. Make sure that the "Advertise Telephony Services Name Server" box is checked.

Figure 8-4 TSA Name Server Advertising

- Tserver Options
<u>E</u> nable Pop-Up Alarm Notification
Advertise Telephony Services <u>N</u> ame Server
Extended Worktop Access
Enable Automatic Administration of LAN Addresses
Transport Layer Options         IPX/ <u>S</u> PX         ICP/IP       TCP Port: 450
IP <u>A</u> ddress: 135.20.70.5 TCP Preferred Naming Format
○ <u>H</u> ost Name
<u>O</u> K <u>C</u> ancel

288 Network Manager's Guide

## Using the TSM32 to Enable Name Server Advertising



- 1. From the "Options" menu, select "Tserver Properties." The "Tserver Properties" dialog box is displayed.
- 2. On the "General" tab, make sure that the "Advertise Telephony Services Name Server" box is checked.

Figure 8-5 TSM32 Name Server Advertising

Tserver Properties - ACME_NY
General Transport Components
Enable Pop-Up Alarm Notification
_
Advertise Telephony Services Name Server
OK Cancel Apply Help

## **Version and System Status Information**

Version and system-level status information can be displayed using the 16bit Telephony Services Administrator (TSA), 32-bit Telephony Services Maintenance (TSM32), or 32-bit Telephony Services Administration (TSA32) applications. The following table lists the type of status information that will be displayed, and indicates which of the Telephony Services Administration and/or Maintenance applications will display that information.

## Table 8-1 Tserver Version and System Status Information

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED	
1		1	Btrieve Version: The version of the Btrieve database engine.	
1	~		Cserver: the version number of the Cserver module	
Ý		~	<b>Data Dictionary Version:</b> The current version of the data dictionary. This is a file located in the \Program Files\Telephony Services\tsrv directory on the server. This file contains information describing the SDB and is used by the TSRVBTRV module. This version must match that of the SDB files. If they do not match, the TSRVSDB modules can interpret the data correctly.	
1	1		<b>Driver TSDI OAM Protocols:</b> This set of protocols is similar in function to the Tserver OAM protocols. However, the driver TSDI OAM protocols are used by PBX driver administration applications on the client and the PBX driver.	
1		~	<b>Old Dictionary Version:</b> The version of the dictnry.old file in the \tsrv directory. This file is used to determine if the SDB needs to be upgraded This is done automatically by Telephony Services. Most of the time this version matches the Data Dictionary Version.	
~		~	<b>SDB Administration Protocols</b> Protocol versions used by TSA for SDB administration	

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED		
1		1	<b>SDB Driver State:</b> the state of the following. (If the state is other the properly.)	e SDB driver, which can be one of the an normal, the system does not work	
			• Normal – The driver is in nor	mal mode.	
			• Uninitialized – The most like dictnry.sdb file, which should server. If the file has become a non-corrupted version.	ly cause is a problem with the be in the \TSRV directory on the corrupted, you must reinstall it using	
			• Initialized – The TSRVBTR unable to read the versions of cause is insufficient memory	• Initialized – The TSRVBTRV module initialized correctly but was unable to read the versions of each SDB file. The most likely cause is insufficient memory on the server.	
			• Inconsistent – The most likely cause is that the version of one or more of the SDB files on this server do not match the version number of the data dictionary. To remedy this, you need to restore a complete set of backup .dta files (that have a matching version number). Make sure you stop Telephony Services prior to manipulating any .dta files.		
			• Old Database – The versions of all the .dta files do not match the version of the dictnry.sdb file. This occurs when the automatic upgrade performed at load time does not complete successfully. Check the error log for an indication of the problem.		
<ul> <li>✓</li> </ul>		Ý	<b>SDB File Versions:</b> Each SDB file based on the version of the data di was created. These versions must dictionary for security checking to lists the version types and their co	e is stamped with a version number ctionary that was used when the file match each other and the data o work correctly. The following table rresponding file names.	
			Version Type	File Name	
			SDB User File Version SDB Worktop File Version SDB Device File Version SDB Device Group File Version SDB Tlink File Version	user.dta wktp.dta device.dta dlist.dta tlink.dta	

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED		
			SDB Tlink Group File Versi SDB Oamlink Group File V	on tlist.dta ersion oamlisy.dta	
1	1		<b>TDI:</b> the version number module, TDI.	er of the Telephony Services Driver Interface	
1	1		<b>TRAFFIC:</b> the version Reporting module, TRA	number of the Telephony Services Traffic FFIC.	
1	V		<b>TSADV:</b> the version nu module, TSADV.	mber of the Telephony Services Advertising	
1	V		<b>TSAUTH:</b> the version r Authentication module,	number of the Telephony Services TSAUTH.	
1	1		<b>Tserver CSTA Protocols:</b> the versions of TSAPI that the Tserver supports for CSTA streams.		
1	1		Tserver License Size: size of your Telephony Services license.		
*	~		<b>Tserver OAM Protocols:</b> The protocol versions that administration applications residing on a client workstation can use to talk to the Tserver. The table below shows the protocols supported by each module. A Release 2 TSA can "talk" to the Release 1 Tserver but a Release 1 TSA cannot "talk" to a Release 2 Tserver.		
			Software Module Supported Releases		
			Release 1 Server Release 2 Server Release 1 TSA Release 2 TSA Release 2.22 TSA Release 2.22 TSA32 Release 2.22 TSM32 Tserver 2.22	TS1 (NetWare only) TS2-3 (NetWare only) TS1 (NetWare only) TS1-3 (NetWare only) TS5 TS5 TS5 TS5 TS4-5	
1		~	Tserver SDB Driver V software.	ersion: the version number of the driver	

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED	
1		1	Tserver SDB Driver: the type of database driver in use (TSRVBTRV).	
1	1		<b>Tserver SDB Windows NT Version:</b> the version of Windows NT that the Tserver is running.	
<b>v</b>	~		<ul> <li>Tserver State: the state of the Tserver, which can be one of the following:</li> <li>Normal – The Tserver is in normal operation mode.</li> </ul>	
			• Bad License File – A valid license file is not installed on the server.	
			• System Error – The Tserver encountered an internal system error while loading. This could occur if you have enabled TCP/IP as a transport method, but TCP/IP is not available or did not initialize properly.	
1	1		Tserver: version number of TSRV.EXE module.	
1		1	TSLOG: the version number of the TSLOG module	
1	1		<b>TSMI:</b> the version number of the Telephony Services Maintenance Interface module, TSMI.	
1		1	<b>TSSDB:</b> the version number of the Telephony Services Security Database module, TSSDB.	
~	1		<b>TSUSR:</b> the version number of the TSUSR module.	
1		1	<b>TSVAL:</b> the version number of the TSVAL module	

## Using the TSA to View Version Information

1.



From the "Help" menu, select "About." The "About Telephony Services Administrator" dialog box is displayed, showing the version and component information.

Figure 8-6 TSA Version Information Page

A	oout Telephony Services Administrato	r
Telephony Serv	ices Administrator	
<u>V</u> ersion / Info	Component	
2.22.29.0	Telephony Services Administrator	+
2.22.29.0	TServer	
50	TServer License Size	
NORMAL	TServer State	
TS1-2	TServer CSTA Protocols	
TS4	TServer OAM Protocols	
TS1	Driver TSDI OAM Protocols	-
2.5.1	Windows MT Version	
Copyright © 199	6 Lucent Technologies Inc.	
All Rights Reser	ved.	<u>0</u> K
_		

## Using the TSA32 to View Version Information



- 1. Select the SDB icon in the tree view.
- 2. From the "Admin" menu, select "Properties." The "Tserver Properties" dialog box is displayed.
- 3. Select the "Components" tab. This tab displays a dialog box showing component and version information.

Figure	8-7	
TSA32	Version Information Page	

Tserver Prop	erties - ACME_NY	·
Options SDB Log Settings Components	]	
<u>C</u> omponents:		
Component	Version / Info	+
Btrieve Version	6.15N	
Data Dictionary Version	2.0.0.3	
Old Dictionary Version	2.0.0.3	
SDB Administration Protocols	TS4-5	
SDB Device File Version	2.0.0.3	
SDB Device Group File Version	2.0.0.3	
SDB Driver State	Normal	
SDB Oamlink Group File Version	2.0.0.3	<u> </u>
SDB Connections: 3		
OK	Cancel 🖉	Apply Help

## Using the TSM32 to View Version Information



- 1. From the "Options" menu, select "Tserver Properties." The "Tserver Properties" dialog box is displayed.
- 2. Select the "Components" tab. This tab displays a dialog box showing component and version information.

#### Figure 8-8 TSM32 Version Information Page

Tserver Properties	- ACME_NY	-
General Transport Components		
Concentration		
Component	Version / Info	1 <b>±</b>
TServer	2.22.29.0	
TServer License Size	50	
TServer State	NORMAL	
TServer CSTA Protocols	TS1-2	
TServer OAM Protocols	TS4	
Driver TSDI OAM Protocols	TS1	
WindowsNT Version	3.5.1	
TSUSR	2.22.29.0	
TSADV	2.22.29.0	
TSAUTH	2.22.29.0	+
OK Cancel	Apply	Help

# Loading and Unloading PBX Drivers

The Tserver runs as a Windows NT service. PBX drivers are implemented as dynamic link libraries (DLLs) that are loaded by the Tserver. A driver may load in one of two ways: it may be configured to load automatically each time the Tserver is started, or it may require manual startup. Similarly, a driver can be unloaded either by the Tserver (when it is stopped) or manually (at any given time).

Telephony Services provides an interface for you to load or unload a driver manually as well as the ability to set a driver for automatic or manual startup. During installation, a driver may or may not tell the Tserver about itself, so you may have to add the driver DLL name to the list maintained by the Tserver.

## **Driver DLL Information**

The status of a DLL is loading, loaded, unloading, or unloaded. A status of loaded indicates that this DLL has been successfully loaded by the Telephony Server and may register and unregister Tlinks. A status of unloaded indicates that this DLL is not currently loaded by the Telephony Server.

## Using the TSA to Display Driver DLL Information

1.



From the "Maint" menu, select "Driver DLL Information." The "Driver DLL Information" dialog box is displayed, showing a list of DLLs that are in the Telephony Server and the status of each DLL.

Figure 8-9 TSA Driver DLL Information

	Driver D	LL Informatic	IN
DLLs	Auto Load	Status	
cserver.dll g3pd.dll	No No	unioaded unioaded	
			Unload
			Disa <u>b</u> le Auto Load
			Remove
<u> </u>			
			Add
Refre	sh		<u>C</u> lose

2. Select "Refresh" to update the list of DLLs and their status with current information. (You can also accomplish this by dismissing and redisplaying the dialog box.)

298 Network Manager's Guide

## Using the TSM32 to Display Driver DLL Information

1.



From the "Options" menu, select "Driver DLL Information." The "Driver DLL Information" dialog box is displayed, showing a list of DLLs that are in the Telephony Server and the status of each DLL.

Figure 8-10 TSM32 Driver DLL Information

😑 Driv	er DLL Info	ormation -	ACN	AE_NY
<u>D</u> LLs:				
Name	Auto Load	Status		
g3pd.dll	No	Unloaded		
				Load
				Ena <u>b</u> le Auto Load
				<u>R</u> emove
 <u>ΓN</u> ame of DLL to Add <sup>−</sup>				
				Add
F	?e <u>f</u> resh		<u>C</u> I	ose

2. Select "Refresh" to update the list of DLLs and their status with current information. (You can also accomplish this by dismissing and redisplaying the dialog box.)

## Adding DLLs



- 1. In the "Driver DLL Information" dialog box, enter the name of the DLL in the "Name of DLL to Add" field. Be sure to include the extension (for example, *drivername.dll*).
- 2. Select "Add." The DLL is added to the DLL list box; the status is unloaded.



Do not use paths when entering DLL names, but do include the file extension (such as .dll). The DLL must be in the System Environment Path of the Windows NT machine that the Telephony Server is executing on, or else the Telephony Server will not be able to find the DLL when asked to load it.

## **Removing DLLs**



- 1. To remove a loaded or unloaded DLL from the Telephony Server list, select the DLL you want to remove.
- 2. Select "Remove."

300 Network Manager's Guide

## Loading and Unloading DLLs

You can load any DLLs that are unloaded, or you can unload DLLs that are currently loaded.



- 1. If a DLL is listed as "Unloaded," select "Load."
- 2. If a DLL is listed as "Loaded," select "Unload."
- 3. To toggle the status of a DLL in the list box, double-click the left mouse button.

The loading and unloading status may happen so quickly that you do not see the change. If a driver remains in either of these states, this indicates that the driver is having trouble performing the requested action and has not informed the Tserver that it has finished successfully. Check the error log, and refer to your PBX driver documentation for any corrective action.

## Configuring a DLL for Auto Load

Any of the DLLs may be automatically loaded when the Tserver is started.



- 1. Select the DLL you want to load automatically when the Tserver starts.
- 2. Select "Enable Auto Load."
- 3. To disable Auto Load, select the DLL you want, then select "Disable Auto Load."

## **Tserver Status**

The Telephony Server Driver Interface (TSDI) is the interface between the Tserver and the PBX driver. When the PBX driver is loaded, it registers services that it offers with the Tserver in the form of Tlinks.

A Tlink name is made up of four components separated by pound signs, and has the following format:

#### VENDOR#DRIVER#SERVICE#SERVERNAME

A single PBX driver can advertise more than one type of service. When users log in to Telephony Services, they select the service they need and establish a connection to it. (This may be done by the application without user intervention.) Many clients can use the same service; as a result, there may be multiple connections to a single Tlink.

The Tserver keeps client usage statistics. When a client opens a connection to a particular Tlink, the Tserver creates a record of the login that opened the connection, when it was opened, the application that opened it and the service provided by the Tlink. A summary of this information is available using the TSA, TSM32, or TSA32 application.

The Tserver status dialog boxes provide the following summary information: who has had a connection opened the longest, who has the most open connections and most application instances. Each category has an individual display box on the dialog box. These are not scrollable.

The "Tserver Status Information" dialog box is updated automatically every 5 seconds. You can refresh this screen manually by pressing the "Refresh" button. You can reset the maximum values to zero by pressing the "Reset" button.

302 Network Manager's Guide

The following table lists the type of Tserver status information that will be displayed, and indicates which of the Telephony Services Administration and/or Maintenance applications will display that information.

#### Table 8-2 Tserver Status Information

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED		
1	1		License Size indicates the size of your Telephony Services license.		
1	~		Licenses In Use indicates the number of licenses currently in use.		
<b>v</b>			<b>Longest Open Streams</b> lists the login IDs of clients who have had connections with this Tserver for the longest period of time. It also gives the time each connection was opened. The list box displays the oldest connection first.		
1	~		Max Memory Used		
1	1		Maximum Licenses Used		
1	~		Maximum SPX Logins		
1	~		Maximum TCP Logins		
×			<b>Most Open Streams</b> lists the login IDs with the most open connections to the Tserver and gives the number of open connections for each one. The dialog box lists the login with the most open connections first.		
<b>√</b>	4		<b>Reset</b> starts the system history record keeping from zero. The new history starts as soon as you press Reset. This means the values can change immediately and you might not actually see an initial value of zero.		
1		1	SDB connections		
×	4		<b>SPX logins</b> indicates the number of users connected to the server via IPX/SPX.		

The Tserver 303

TSA	TSM32	TSA32	STATUS INFORMATION DISPLAYED
1	√		<b>TCP logins</b> indicates the number of users connected to the server via TCP/IP.
~	1		Tlink Registrations
1	1		<b>Total Memory In Use</b> indicates how much memory is being used by the Tserver.
1	1		Used SPX Connections

## Using the TSA to View Tserver Status Information

1.



To obtain status information on the Tserver that is currently being administered, select the "Tserver" option from the "Status" menu. The Tserver Status Information dialog box is displayed.

Figure 8-11 TSA Tserver Status Information

<mark>_</mark>	Tserver Stat	us Information	
License Size:	50	Used SPX Connections:	0
Licenses In Use:	0	SPX Logins:	0
Tlink Registrations:	6	TCP Logins:	4
Total Memory In Use (bytes):	65742	SDB Connections:	6
Max Memory Used (bytes):	121490		
Maximum Licenses Used:	1		
Maximum SPX Logins:	0	He <u>s</u> et	
Maximum TCP Logins:	25		
Longest Open Stream	ms:	Most Open St	reams:
Time Open User		#Open Üser	
10/03 14:22 LSM		4 LSM	
10/03 14:23 LSM			
10/03 14:25 LSM			
10/03 14:25 LSM			
<u> </u>	efresh	<u>C</u> lose	

2. To reset system history, press the "Reset" button. This starts the system history record keeping from zero.

The fields that are reset are:

- Max Memory Used
- Max Licenses Used
- Maximum SPX Logins
- Maximum TCP Logins

The Tserver 305

## Using the TSA32 to View Tserver Status Information

1.

Procedure

Select the SDB icon from the tree view.

- 2. From the "Admin" menu, select "Tserver Properties." The "Tserver Properties" dialog box is displayed, showing tabs for "Options," "SDB Log Settings," and "Components."
- 3. Select the "Components" tab. The SDB connections information appears at the bottom of the dialog box, below the Component/Version information box.

Figure 8-12 TSA32 Tserver Status Information

Tserver Proper	rties - ACME_NY
Options SDB Log Settings Components	
<u>C</u> omponents:	
Component	Version / Info 🔹
Btrieve Version	6.15N
Data Dictionary Version	2.0.0.3
Old Dictionary Version	2.0.0.3
SDB Administration Protocols	TS4-5
SDB Device File Version	2.0.0.3
SDB Device Group File Version	2.0.0.3
SDB Driver State	Normal
SDB Oamlink Group File Version	2.0.0.3
SDB Connections: 3	
ОК	Cancel Apply Help

**306** Network Manager's Guide

## Using the TSM32 to View Tserver Status Information



1. Open a TSM32 session to the Tserver. Status information for the Tserver appears on the screen in front of you.

Figure 8-13 TSM32 Tserver Status Information

🗖 Telephony Serv	ices Ma	intenance - [ACME_NY]	-	•
- <u>F</u> ile <u>O</u> ptions ⊻iew	<u>W</u> indo	w <u>H</u> elp		ŧ
<u>L</u> 12221/%	? №	<u>'</u>		
License Size:	50	Used SPX Connections:	0	
Licenses In Use:	1	SPX Logins:	0	
Tlink Registrations:	6	TCP Logins:	23	
Total Memory In Use (bytes):	72529			
Max Memory Used (bytes):	121490			
Maximum Licenses Used:	1			
Maximum SPX Logins:	0	Heset		
Maximum TCP Logins:	25			
<u>R</u> efresh	<u>_</u> lo	use Help		
For Help, press F1				//.

The Tserver 307

2. To reset system history, press the "Reset" button. This starts the system history record keeping from zero.

The fields that are reset are:

- Max Memory Used
- Maximum Licenses Used
- Maximum SPX Logins
- Maximum TCP Logins

The new history starts immediately.

#### **Resetting the Refresh Rate**

You can change the rate at which Tserver status information is refreshed. The rate affects only the information on the TSM32 status information screen. If you have multiple connections (to other Tservers), any change you make to the refresh rate affects all the Tservers to which you are connected.



1.

To reset the refresh rate, select "Refresh Timer" from the "View" menu. The "Refresh Timer" dialog box is displayed.

Figure 8-14 TSM32 Refresh Timer

Refresh Timer	•
<u>R</u> efresh rate for Tserver information (seconds):	50 -
OK Cancel H	Help

2. Enter a new time interval, or use the arrows to select a new time interval. Press "OK" when you are done.
# **Tlink Status**

The Tserver manages the TSDI resources needed by each Tlink.

When the Tserver gets a request from a client application, it creates a TSDI message and puts it in a message queue for the appropriate Tlink. If the PBX driver is idle, it can read this message, process the information and return the memory used by the message to the memory pool for that Tlink. If the PBX driver is busy, the message remains in the incoming message queue until it can be processed.

The system provides a default value for the maximum amount of memory that Telephony Services allocated for the Tlink. Generally, these defaults should be sufficient, but you may want to monitor your resource usage and tune these parameters. If the amount of memory allocated for this Tlink reaches the administered limit, further requests to and from this Tlink are not processed until some of this memory has been released. The Tserver rejects incoming requests from client applications, indicating that it has run out of memory.

The following table lists the type of status information that will be displayed for each Tlink, and indicates which of the Telephony Services Administration and/or Maintenance applications will display that information.

#### Table 8-3 Tlink Status Information

TSA Tlink Information	TSA Tlink Status	TSM32	STATUS INFORMATION DISPLAYED
		×	<b>Applications</b> is a list box that shows all the different types of applications currently using the Tserver. When an application establishes a connection with the Tserver, it gives the name of the application.
1			<b>Connections</b> indicates the number of connections to this Tlink. Each client or server that has established a connection is included in this count.
	4	*	Current Buffer Space Allocation is the amount of TSDI memory in use by this Tlink. The difference between this number and the TSDI Size is the amount of TSDI memory left available to this Tlink. The amount of memory in use is the sum of the following four fields: Number of Bytes: Queued to Driver Number of Bytes: Queued to Tserver Number of Bytes: Allocated By Driver Number of Bytes: Allocated by Tserver These four values appear on the "Tlink Information Details" dialog box, while their sum appears on the "Tlink Status Details" dialog box.
<b>~</b>		×	Flow Controlis a mechanism for preventing problems caused by memory exhaustion. When the amount of memory allocated for this Tlink reaches the maximum size of the TSDI buffer, further requests from this Tlink cannot be processed until some of this memory has been released. If the driver has indicated to the Tserver that it can use flow control, you can change the default flow control level to a higher value. Use the "Tlink Information Details" dialog box in the TSA or the "Tlink Status Information"

TSA	TSA	TSM32	STATUS INFORMATION DISPLAYED
Tlink	Tlink		
Information	Status		
			dialog box in the TSM32 to change the value. If the driver cannot use flow control, the flow control field will be "Disabled," and you will not be able to change the value.
×			<b>High Water Mark</b> is threshold at which the TSDI begins to warn the driver and the Tserver that the maximum TSDI Size may soon be reached.
<b>√</b>		Ý	<b>Invoke IDs</b> provide detailed information about resources used by the Tserver. They are provided in case you have a problem and your service representative needs this detailed information to resolve it.
			<b>Invoke IDs</b> - In Use indicates the number of unique invoke IDs currently in use by this Tlink. The Tserver guarantees a Tlink that the invoke IDs on all requests within a connection are unique, so the Tserver saves the invoke ID generated by the application and passes the Tlink a unique Invoke ID. When a Tlink responds to an application request with a confirmation message, the application invoke ID is returned to the application. This field indicates how many outstanding client requests a Tlink is currently processing.
			If your application uses routing selection requests, the number of invoke IDs can get large. This request comes from a client application but has no response from the PBX driver. The Tserver has no way of knowing when to free up the invoke ID. It cleans up IDs that have been around for more than two minutes, but you may see a high level of invoke ID usage for this reason.
			<b>Invoke IDs</b> - Max Used indicates the largest number of client request messages that have been outstanding at any one time since the Tserver was loaded or since

TSA	TSA	TSM32	STATUS INFORMATION DISPLAYED
Tlink	Tlink		
Information	Status		
			the Max Used field was reset to zero.
			<b>Reset</b> is provided so that you can reset the Invoke IDs
			- Max Used field to zero.
			Number of Bytes contains the count of bytes in each of the five possible states: queued to the Tlink, queued to the Tserver, allocated by the Tlink, 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 Tlink is close to reaching its limit. Messages (i.e., the number of bytes in the message) that are privately allocated by the Tserver are not charged against the total memory allocated for this TSDI interface. Currently, the Tserver allocates private TSDI buffers only for keeping track of each new open connection.
×			<b>Number of Messages</b> contains the count of messages in each of the five possible states: queued to the Tlink, queued to the Tserver, allocated by the Tlink, 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 that are privately allocated by the Tserver are not charged against the total memory allocated for this TSDI interface.
			Number of TSDI Bytes contains the count of bytes in each of the five possible states: queued to the Tlink, queued to the Tserver, allocated by the Tlink, 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 Tlink is close to reaching its limit. Messages (i.e., the number of bytes in the message) that are privately allocated by the Tserver are not charged against the total memory allocated for this TSDI interface. Currently, the Tserver allocates private TSDI buffers only for keeping track of each new open

# 312 Network Manager's Guide

TSA	TSA	TSM32	STATUS INFORMATION DISPLAYED
Tlink	Tlink		
Information	Status		
			connection. (This information is available from the "TSDI" tab of the "Tlink Status" dialog box.)
		*	Number of TSDI Messages contains the count of messages in each of the five possible states: queued to the Tlink, queued to the Tserver, allocated by the Tlink, 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 that are privately allocated by the Tserver are not charged against the total memory allocated for this TSDI interface. (This information is available from the "TSDI" tab of the "Tlink Status" dialog box.)
	×		<b>Open Applications</b> is a list box that shows all the different types of applications currently using the Tserver. When an application establishes a connection with the Tserver, it gives the name of the application.
	~	1	<b>Open Connections</b> indicates the number of connections to this Tlink. Each client or server that has established a connection is included in this count.
		~	<b>Outstanding Connections</b> indicates the current number of TCP/IP connections to this Tlink. (This information is available from the "TCP/IP" tab of the "Tlink Status" dialog box.)
		1	<b>Registered</b> indicates whether the Tlink is registered with the Tserver (Yes o r No).
	×		<b>Requested TSDI Buffer Space</b> is the size (in bytes) of the TSDI buffer. This is usually the same as the TSDI size on the "Tlink Information Details" dialog box.
1		1	<b>Stream Type</b> is the type of service that the Tlink (stream) provides. This can be either CSTA or OAM. When the PBX driver registers with the Tserver, it indicates the type of

TSA Tlink Information	TSA Tlink Status	TSM32	STATUS INFORMATION DISPLAYED
			service it provides.
1			<b>Supported Protocols</b> are the TSAPI versions supported by this Tlink.
	×	1	<b>Tlink Security</b> is the security level the PBX driver requested when it registered the Tlink with the Tserver. The possible levels are:
			None – No checking is done on requests to establish a connection or on any CSTA or OAM request.
			Login – Checking is done only on establishing connection requests, not on requests across open OAM and CSTA connections.
			CSTA – Checking is done on requests to establish a connection and on all applicable CSTA requests.
		1	<b>TSDI Buffer Control</b> provides the following information (described elsewhere in this table):
			Current Buffer Space Allocation TSDI Size TSDI High Water Mark
			(This information is available from the "TSDI" tab of the "Tlink Status" dialog box.)
		1	<b>TSDI High Water Mark</b> is the amount of memory allocated for this driver before the TSDI begins to warn the driver and the Tserver that the maximum TSDI Size may soon be reached.
✓		×	<b>TSDI Size</b> is the maximum size, in bytes, of the TSDI buffer. If you administer the Tlink and set this value, it becomes the maximum amount of memory the Tlink can use. If you do no administer the Tlink, the Tserver creates a Tlink object when the PBX driver registers the first time. In this case, the PBX driver says how much memory it wants. You can override

TSA Tlink Information	TSA Tlink Status	TSM32	STATUS INFORMATION DISPLAYED
			this value at any time. The minimum value is 65000 bytes and the maximum is 2,100,000,000. The Number of Bytes information shows how close the driver is to reaching this maximum. The TSDI Size must always be larger than the High Water Mark value.
1		1	<b>Version</b> is the build version of the driver providing the service.

Remember that the resource information is provided on a per Tlink basis. You must first select the Tlink you want to monitor and then display the status information.

## Using the TSA to View Resource Information

1.

The TSA gives you two views of Tlink resource status. The first view provides detailed TSDI resource information for a Tlink. The second view presents a summary of active Tlink status and is display only.

#### **Viewing Detailed Information**



- For the detailed view of Tlink resource data, select "Tlink Information" from the "Maint" menu. This displays a list of Tlinks.
- 2. Highlight the Tlink you want and select "View" to display the "Tlink Information Details" dialog box.

Figure 8-15 Tlink Information Details Dialog Box

😑 🛛 Tlink Informati	on Details	for LUCENT#CSTASERV#C	STA#ACME_NY
TSDI <u>S</u> ize (bytes): 15	72864	<u>H</u> igh Water Mark (bytes):	1258291
IPX/SPX Info		Connections:	20
27731771110		Stream Type:	CSTA
<u>T</u> CP/IP Info		Supported Protocols:	TS2
	,	Version:	2.22.29.0
Flow Control (TSDI Buffe	ers)		
		Disabled	
Number of Messages			_
Queued to Tlink:	1	Allocated by Tlink:	0
Queued to Tserver:	0	Allocated by Tserver:	1
Tserver Private:	107		
Number of Bytes			
Queued to Tlink:	172	Allocated by Tlink:	0
Queued to Tserver:	0	Allocated by Tserver:	172
Tserver Private:	3646	0	
	nvoke IDs —		1
		Max Used	
<u> </u>	Use: 2	20 <u>R</u> eset	<u>C</u> ancel

316 Network Manager's Guide

#### 3. Change fields as necessary. The fields you can change are:

- TSDI Size
- High Water Mark this field should always be less than the TSDI size.
- Max Used Reset resets the Max Used field to zero.

#### 4. If applicable, change the flow control value.

If the driver cannot use flow control, the flow control field will be "Disabled," and you will not be able to change the value.

If the driver has indicated to the Tserver that it can accept flow control information, you can change the default flow control level to a higher value. The "Tlink Information Details" dialog box will include a "Max Flow Allowed" field and a "Max Flow Reached" field. The following is a sample "Tlink Information Details" dialog box with Flow Control enabled:

😑 🛛 🗖 Tlink Informat	ion Details f	or LUCENT#WICHITA#C	STA#ERIN
TSDI <u>S</u> ize (bytes): 157286	4 <u>H</u> igh	Water Mark (bytes):	1258291
IPX/SPX Info	Conr	ections:	0
	Strea	ат Туре:	CSTA
<u>T</u> CP/IP Info	Supp	oorted Protocols:	тѕз
	Vers	ion:	Unknown
⊂ Flow Control (TSDI Buffers) — Max Flow Allowed:	10		
Max Flow Reached:	0	Rese	et
Number of Messages			
Queued to Tlink:	0	Allocated by Tlink:	0
Queued to Tserver:	0	Allocated by Tserver:	0
Tserver Private:	4		
Number of Bytes			
Queued to Tlink:	U	Allocated by Tlink:	U
Queued to Iserver:	U	Allocated by I server:	U
Tserver Private:	5460		
	e IDs ———		
		Max Used	
<u>O</u> K In Use:	0	0 <u>R</u> eset	<u>C</u> ancel

The Tserver 317

- 4a. Change the Max Flow Allowed value as necessary.
- 4b. Select "Reset" to reset the Max Flow Reached value to zero.

#### **Viewing Summary Information**



- 1. To view summary information, select the "Tlink" option from the "Status" menu. This displays a list of active Tlinks.
- 2. Highlight the Tlink you want and select "View." The "Tlink Status Details" dialog box is displayed.

Figure 8-16 Tlink Status Details Dialog Box

Tlink 9	atus Dataile
Tlink:	LUCENT#CSTASERV#CSTA#ACME_NY
Open Connections:	20
Tlink Security:	CSTA
Requested TSDI Buffer Space (bytes):	1572864
Current Buffer Space Allocation (bytes):	172
Open Applications MultiThread	<u>C</u> lose

3. Select "Close" when you are done viewing status information.

# Using the TSM32 to View Resource Information

1.

TSM32 gives you three views of Tlink resource status. The first view provides detailed Tlink resource information. The second view provides detailed TSDI resource information for a specific Tlink. The third view shows the outstanding TCP/IP connections for that Tlink.

#### **Viewing Detailed Information**



- Select "Tlink Status" from the "Options" menu. This displays the three tabs that are available for the "Tlink Status" dialog box.
- 2. Select a Tlink from the drop-down list on the "Information" tab (the first tab for this screen). The information for that Tlink is displayed.



🗖 Tlink Statu	s - ACME_NY	-
Information TSDI TCP/IP		
Ink: LUCENT#CSTASERV#CS	TA#ACME_NY	<u>+</u>
Registered?	Yes	
Open Connections:	20	
Stream Type:	CSTA	
Version:	2.22.29.0	
Supported Protocols:	TS2	
Tlink Security:	CSTA	
Flow Control (TSDI Buffers): Invoke IDs	Disabled	
In Use:	19	
Max Used:	20	<u>R</u> eset
Applications:		
Telephony App 1 Telephony App 10 Telephony App 11 Telephony App 12 Telephony App 13 Telephony App 14 Telephony App 15 Telephony App 16	•	Refresh
	Cancel	Apply Help

3. If necessary, select "Reset" to reset the "Max Used" field in the "Invoke Ids" box to zero.

#### 4. If applicable, change the flow control value.

If the driver cannot use flow control, the flow control field will be "Disabled," and you will not be able to change the value.

If the driver has indicated to the Tserver that it can accept flow control information, you can change the default flow control level to a higher value. The "Information" tab on the "Tlink Status" dialog box will include a "Max Flow Allowed" field and a "Max Flow Reached" field. The following is a sample "Tlink Status" dialog box with Flow Control enabled:

	Tlink Status	- ERIN	▼
Information TS	DI TCP/IP		
Tlink:	LUCENT#WICHITA#CSTA#ERIN		t
R O S V S	Registered? Open Connections: Stream Type: Version: Supported Protocols:	Yes 0 CSTA Unknown TS3	
T Fla M	Tink Security: ow Control (TSDI Buffers) fax Flow Allowed: fax Flow Reached:	None	Reset
-Inv In M	roke IDs 1 Use: flax Used:	0 0	<u>R</u> eset
	pplications:		Refresh
	ОК	Cancel	Apply Help

The Tserver 321

- 4a. Change the Max Flow Allowed value as necessary.
- 4b. Select "Reset" to reset the Max Flow Reached value to zero.

## Viewing TSDI Resource Information

1.



From the "Tlink Status" dialog box, select the TSDI tab. TSDI information is displayed for the Tlink you selected from the "Information" tab.

#### Figure 8-18 Tlink Status TSDI Dialog Box

💳 🛛 🚽 Tlink Status - AC	ME_NY
Information TSDI TCP/IP	
Tlink: LUCENT#CSTASERV#CSTA#AC	ME_NY
Number of TSDI Messages	
Queued to Tlink:	3
Queued to Tserver:	2
Tserver Private:	138
Allocated by Tlink:	1
Allocated by Tserver:	16
Number of TSDI Bytes	
Queued to Tlink:	516
Queued to Tserver:	2756
Tserver Private:	37431
Allocated by Tlink:	172
Allocated by Tserver:	2628
TSDI Buffer Control (bytes)	
Current TSDI Buffer Space Allocatio	on: 6072
TSDI <u>S</u> ize:	1572864
TSDI <u>H</u> igh Water Mark:	1258291
OK Ca	ancel Apply Help

- 2. Change fields as necessary. The fields you can change are:
  - TSDI Size
  - TSDI High Water Mark this field should always be less than the TSDI size.

### Viewing TCP/IP Information



1.

From the "Tlink Status" dialog box, select the TCP/IP tab. TCP/IP information is displayed for the Tlink you selected from the "Information" tab.



-	Tlink Status - ACME_NY
Information T	SDI TCP/IP
Tlink:	LUCENT#CSTASERV#CSTA#ACME_NY
	Outstanding Connections Current: 0
	Max Used: 1 <u>R</u> eset

The Tserver 323

2. If necessary, select "Reset" to reset the "Max Used" field in the "Outstanding Connections" box to zero.

# **User Status**

You can get the following information for each user who has an active connection to the Tserver:

- Login ID: the user's login ID.
- **Open Streams**: the number of open connections the user has to the Tserver.
- Closed Streams: the number of connections to the Tserver that the user has closed.
- Applications: provides details for all applications associated with a user's login ID. Indicates the name of the application, the time that the user initially opened the connection, the time that the user closed the connection, and the name of the Tlink to which the open connection request was sent.

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.

You can select an individual login and request additional information. You can also elect to drop an active connection or get detailed connection information for that login.

# Using the TSA to View Status Information

1.

Procedure

Select the "User" option from the "Status" menu. The "User Status Information" dialog box is displayed.

Figure 8-20 TSA User Status Information Dialog Box

😑 User S	tatus Informat	ion	
<u>L</u> ogin ID	Open Streams	Closed Streams	
ADMINISTRATOR	0	2	
	1 20	2 1	
⊻iew	<u><u>C</u>le</u>	ose	

This dialog box lists the current open connections to the Tserver, plus the number of most recently closed connections (up to 50).

#### 2. To display detailed information, select a user from the list and select "View." The "User Status Details" dialog box is displayed.



Invalid logins can sometimes appear in the "Open Streams" list, even though the login was not able to open any streams. Invalid logins are included in the list to assist the administrator in tracking any unsuccessful or unauthorized login attempts.

Figure 8-21 TSA User Status Details Dialog Box

-	💳 User Status Details - LSM					
Application TSA16 TSA16 TSA16 TSA16	Time Opened 10/04 13:33 10/04 13:33 10/04 14:58	Time Closed 10/04 13:34 10/04 13:34	Tlink Name LUCENT#SDB_OAM#OAM#ACME_NY TSERVER#TSRV_OAM#OAM#ACME_NY TSERVER#TSRV_OAM#OAM#ACME_NY			
	Close Open <u>S</u> tream	ns?	Close			

# Using the TSM32 to View Status Information

1.

Procedure

From the "Options" menu, select "User Status." The "User Status" dialog box is displayed.

Figure 8-22 TSM32 User Status Dialog Box

	User Status - ACME_NY						
Users:	User Status Information						
	Open Streams: 1	Closed Streams: 2					
LSM	Applications:						
PATM	Name Time Opened	Time Closed Tlink Name					
	TSA16 10/04 13:33	10/04 13:34 LUCENT#SDB_OAM#OAM#ACM					
	TSA16 10/04 13:33	10/04 13:34 ISERVER#ISEV_DAM#0AM#A					
	TSA16 10/04 14:58	ISERVER#ISRV_DAM#DAM#A					
+ +		Close All Opened Streams?					
	<u>R</u> efresh <u>C</u> lo	Dse Help					

# 2. Select a user from the list. The information in the "User Status Information" dialog box changes for each user.

Note

Invalid logins can sometimes appear in the "Open Streams" list, even though the login was not able to open any streams. Invalid logins are included in the list to assist the administrator in tracking any unsuccessful or unauthorized login attempts.

# **Dropping a User Connection**

When you issue a "drop connection" request, the system requires that you confirm your request to drop all connections for the specified user since doing so is a destructive action.



Use the "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 user and/or the user's application.
- The user's application may be degrading system performance.
- Troubleshooting procedures indicate the user's application may be the source of a problem.

#### Using the TSA to Drop a User Connection

1.



To drop connections for a particular user, select the user from the list in the "User Status Details" dialog box.

User Status Details - LSM						
<u>Application</u>	Time Opened	Time Closed	Tlink Name			
TSA16	10/04 13:33	10/04 13:34	LUCENT#SDB OAM#OAM#ACME NY			
ISA16	10/04 13:33	10/04 13:34	ISERVER#ISRV_UAM#OAM#ACME_NY			
			· · · · · · · · · · · · · · · · · · ·			
	Close Open <u>S</u> trean	ns?				

2. Select "Close Open Streams." The "Drop Connections Confirmation" dialog box is displayed.

Figure 8-23 Drop Connections Confirmation (TSA)



3. Select "Yes" to confirm.

#### Using the TSM32 to Drop a User Connection

1.



To drop connections for a particular user, select the user from the list in the "User Status" dialog box.

	User St	atus - ACME_N	Y	•
Users:	User Status Information			
All Osels ADMINISTRATOR	Upen Streams: Applications:	1	Closed Streams:	2
PATM	Name Time Oper	ed Time Closed	Tlink Name	
	TSA16 10/04 13:3	3 10/04 13:34	LUCENT#SDB_OAM#OA	M#ACM
	TSA16 10/04 13:3	3 10/04 13:34	TSERVER#TSRV_OAM#	OAM#A
	TSA16 10/04 14:5	18	ISERVER#ISRV_UAM#	UAM#A
		Close All Oper	ed Streams?	
+ +		ciose All Oper		
	<u>H</u> efresh		Help	

2. Select "Close All Opened Streams." The "Telephony Services Maintenance" dialog box is displayed.

#### Figure 8-24 Drop Connections Confirmation (TSM32)



- 3. Select "Yes" to confirm.
- 330 Network Manager's Guide

chapter

# **9** Telephony Services Traffic Measurement

This chapter discusses the Telephony Services Traffic Measurements feature, which provides a traffic viewer for the traffic reports, the traffic log, and measurement alarms.

The traffic measurements feature allows you to monitor your CTI configuration. The purpose of this feature is to measure the flow of application traffic (CSTA and ACS messages) from clients to the PBX driver and from the PBX driver back to clients. This feature does *not* include all traffic over the LAN; it includes only the ACS and CSTA messages defined in the TSAPI protocol.

# **Measuring Traffic**

Traffic measurements are calculated throughout the system at three interfaces:

- Between the PBX Driver and the PBX. The PBX driver measurements are taken at the interface to the PBX. The measurements consist of the messages the driver sends to the PBX and the messages the driver receives from the PBX. In order for these measurements to be taken, the PBX driver must be written to support the traffic measurements feature.
- Between the PBX Driver and the Tserver. The TSDI measurements are taken between the interface to the PBX driver and the interface to the Tserver. The measurements consist of the ACS and CSTA messages passed between the PBX driver and the Tserver on behalf of the client. These measurements are reported on a per-Tlink basis.
- Between the Tserver and the Clients. The Tserver measurements are taken at the interface to the client. The measurements consist of the ACS and CSTA requests the Tserver receives from the client and the responses the Tserver sends to the clients.



The following diagram illustrates the interaction of these three interfaces and also lists the measurements taken at each interface:

Uplink and downlink refer to the direction of the message in relation to the PBX. Downlink means that the message is being sent in the direction of the PBX. Uplink means that the message is being sent away from the PBX.

One measurement not shown is the rejection rate. Both the PBX driver and the Tserver report a rejection if they cannot allocate the necessary system resources to process a message. The Tserver only rejects messages in the downlink direction and the PBX driver rejects messages in the uplink direction.

By combining the measurements from all of these interfaces you are able to identify any bottlenecks in the configuration and make changes as necessary.

Telephony Services Traffic Measurement 333

# **Telephony Services Traffic Viewer**

Telephony Services for Windows NT provides an Telephony Services Traffic Viewer application for the Traffic Measurements feature. This application administers traffic settings and allows you to view current traffic data and history reports. The application is installed as part of Telephony Services.

To start this application, double-click on the "Telephony Services Traffic Viewer" icon in the "Telephony Services for Windows NT" program group. The "Telephony Services Traffic Viewer" dialog box looks like this:

#### Figure 9-1 Telephony Service Traffic Viewer

Telephony Services Traffic Viewer
System Settings
Enable Traffic Measurements
Log File Size (bytes):
Peak Measurement Interval
Settings and Reports
<u>I</u> server <u>T</u> link <u>R</u> eset

334 Network Manager's Guide

The Traffic Viewer dialog box provides access to three sets of information:

- System Level Settings
- Tserver Settings and Reports
- Tlink Settings and Reports

The values for these settings remain as administered throughout a reboot of the server.

## System Level Settings

The System Settings area of the main dialog displays the global settings for the traffic feature. The "Enable Traffic Measurements" check box can be toggled to enable or disable the traffic measurements feature. To enable traffic, you must check this box as well as the individual settings for the Tserver and Tlinks (see "Tserver" settings and "Tlink" settings). The advantage of having this global setting is that it allows you to turn off traffic measurements temporarily without having to change all of the other settings. This allows for easy enabling and disabling of measurements.

The minimum size of the traffic log is 10000 bytes; the maximum is 2,100,000,000 bytes. The default size is 1 megabyte (1,000,000). You can set the peak measurements interval to between 5 and 15 seconds.



If you reduce the size of an existing traffic log, at the next hour the file will be truncated. If you want to save the traffic data in the file, you must copy it to another name or interface before you change the size of the file.

You must select "Apply" for any changes to take effect.

Telephony Services Traffic Measurement 335

## **Tserver Traffic Settings and Reports**

The Tserver Traffic Settings and Reports provide traffic information for the Tserver and Tlink, and also provide a "Reset" button so that you can reset the traffic measurements for the entire system.

#### **Tserver Settings/Current Report**

Select the "Tserver" button from the "Telephony Services Traffic Viewer" main dialog box to display the "Tserver Traffic Settings and Reports" dialog box.

#### Figure 9-2 Tserver Traffic Settings and Reports

Tserver Traffic	Settings and Re	eports	
Settings/Current Report Tserver History			
Tserver Setting and Alarm Threshold			
Enable Tserver Traffic Reporting			Downlink
	<u>P</u> eak Arrival Rate:		500
Tserver Current Traffic Data			
Time: 10/04/96 17:40:02		Uplink	Downlink
Peak Meas. Interval (seconds): 15	Count:	73237	24416
	Peak:		160
	Time:		09:39
	Rejected:		0
	Cancel		Apply

336 Network Manager's Guide

From the "Settings/Current" tab you can enable or disable the Tserver's traffic reporting interface to and from clients, and reset the downlink peak arrival rate threshold.

You must select "OK" or "Apply" for any changes to take effect.

The "Settings/Current" tab also displays the current traffic being reported by the Tserver. This screen updates every 5 seconds while the screen is active. It will only update if the "Tserver Traffic Reporting" is enabled.

For the downlink direction, the current traffic report shows the arrival count, peak arrival rate, time that the peak was reached, and number of messages rejected. (See Figure 9-2.) This tab also shows the uplink arrival count.

The measurements shown are moved to the traffic history report and to the traffic log on the hour. The values displayed in this report are then reset to zero for the next current hour.

#### **Tserver History Report**

To see the last 72 hours of Tserver data, select the "Tserver History" tab. This report has an entry for each of the last 72 hours (during which the "Tserver Traffic Reporting" feature was enabled). The report contains a line of data for each hour and provides the same information as the Telephony Service Current report. The report does not tell you whether the "Tserver Traffic Reporting" feature was disabled for portions of an hour; it only reports data for the time the feature was enabled.

### Figure 9-3 Tserver History

-	Tserver Traffic Settings and Reports							
5	Settings/Current F	eport Tserver	History					
	<u>D</u> ownlink					<u>U</u> plink:		
	Date/Time	Rate	Peak	Time	Interval	Date/Time	Rate	
	10/04 16:00	37064 36057	160 160	19:23 42:22	15	10/04 16:00	111192	
	10/04 14:00	35558	160	11:53	15	10/04 13:00	106646	
	10/04 13:00	10941	160	57:54	15	10/04 13:00	32768	
	L							
	+				+	+	<b>+</b>	
					Cancel	Apply		

# **Tlink Traffic Settings and Reports**

Select the "Tlink" button from the "Telephony Services Traffic Viewer" main dialog box to display the "Tlink Traffic Settings and Reports" dialog box.

Figure 9-4
Tlink Traffic Settings and Reports

😑 Tlink Traffi	c Settings and Re	ports	
Settings Current Report Tlink History TSDI	History		
LUCENT#CSTASER	V#CSTA#ACME_NY		<b>±</b>
Tlink Traffic Registration R	egistered		
<sub>E</sub> TSDI Setting and Alarm Thresholds			
Enable TSDI Traffic Reporting		Uplink	Downlink
	Peak <u>A</u> rrival Rate:	372	372
	<u>Q</u> ueue Length:	2	2
	Q <u>u</u> eued Time	100	100
Tlink Setting and Alarm Threshold			
🔀 Enable Tlink Traffic Reporting		Uplink	
	Peak Arrival Rate:	372	
Cserver Setting and Alarm Thresho	ld		
Enable <u>C</u> server Traffic Report	in <u>c</u>	Uplink	
	Peak Arrival <u>R</u> ate:	372	
	OK Cance	:I	Apply

#### Tlink Settings

The Tlinks field on the "Settings" tab displays a list of T links from which to choose. This list includes only those Tlinks that have registered with the Tserver as CSTA services. If no CSTA Tlinks are registered, the list will be empty. Tlinks in the list have not necessarily registered with the Tserver for traffic reporting.

When you select a Tlink, the current traffic settings for that Tlink are displayed.

The "Tlink Traffic Registration" field indicates whether the driver has registered for traffic reporting. (If you check the "Enable Tlink Traffic Reporting" field, no measurements will be taken until the driver is loaded again.) If the driver has not registered, no measurements can be taken. You can still check the Enable TSDI Traffic Reporting field and administer any of its alarm thresholds, since TSDI measurements can always be taken regardless whether the Tlink has registered for traffic reporting.

If the Tlink does not register for traffic reporting, consult with the vendor of your PBX driver to see if they support traffic reporting.

If you are using a PBX driver that uses the Cserver module, the "Cserver Setting and Alarm Threshold" will be enabled. This allows you to modify the settings for the Cserver.

You must select "OK" or "Apply" for any changes to take effect.

#### **Tlink Traffic Reports**

For each Tlink, you can display current traffic information or history reports. If you are using a PBX driver that depends on the Cserver module, another page appears on this dialog. This option allows you to display Cserver Traffic History. The history reports do not update automatically, but they do update each time the page is selected.

340 Network Manager's Guide

#### Tlink Current Report

For your convenience the Tserver traffic measurements are shown here as well as the Tlink related measurements. If you have multiple CSTA Tlinks running on this Tserver, the Tserver measurements include all of this traffic.

All of the measurements are shown here as in the history report except for the TSDI average queue length and queued time. These averages are not calculated until the hour is up. The queued time shown is in milliseconds.

This dialog box automatically updates every 5 seconds while the screen is active. The measurements shown are moved to the Tlink, TSDI, and Cserver history reports and to the traffic log on the hour. The values are then reset to zero for the next hour.

If you are using a PBX driver that depends on the Cserver module, another set of measurements appears under the "Cserver Current Traffic Data" area of this tab. For these measurements to be taken, the "Enable Cserver Traffic Reporting" check box on the "Settings" tab must be enabled.

#### Figure 9-5 Tlink Current Report

	Tli	nk Traffic S	ettings and Repo	rts			
Settings Current Report Tlink History TSDI History							
Tlink: LUCENT#CSTASERV#CSTA#ACME_NY							
Time: 10/04/961	7:42:07		Peak Meas. Interval	(seconds): 15			
Tserver Current Traffic	Data		Tlink Current Traffic	: Data			
	Uplink	Downlink		Uplink	Downlink		
Count:	76511	25506	Count:	76500	25500		
Peak:		160	Peak:	480			
Time:		09:39	Time:	16:24			
Rejected:		0	Rejected:	0			
				//			
-ISDI Current Traffic D	ata Uplink	Downlink	Lserver Lurrent Tra	irric Data Uplink	Downlink		
Count:	76500	25500	Count:	0	0		
Peak:	480	160	Peak:	0			
Time:	16:24	16:24	Time:	00:00			
Max Queue	50	10	Rejected:	0			
Max Queued Time (msec):	1973	1292					
			K Cancel	Apply	]		

#### **Tlink History Report**

To see the last 72 hours of Tlink data, select the "Tlink History" tab. This report has an entry for each of the last 72 hours (during which the "Tlink Traffic Reporting" feature was enabled). The report contains a line of data for each hour and provides the same information as the current Tlink traffic report. The report does not tell you whether the "Tlink Traffic Reporting" feature was disabled for portions of an hour; it only reports data for the time the feature was enabled.

342 Network Manager's Guide

Figure 9-6 Tlink History

Tlink Traffic Settings and Reports						
Settings Current Report Tlink History TSDI History						
Tlink: LUCENT#CSTASERV#CSTA#ACME_NY						
Uplink:					<u>D</u> ownlink	
Date/Time	Rate	Peak	Time	Interval	Date/Time	Rate
10/04 16:00 10/04 15:00 10/04 14:00 10/04 13:00	111192 108030 106626 32328	480 480 480 480	08:24 43:23 11:53 57:54	15 15 15 15	10/04 16:00 10/04 15:00 10/04 14:00 10/04 13:00	37064 36010 35542 10775
OK Cancel Apply						

Telephony Services Traffic Measurement 343

#### **TSDI History Report**

To see the last 72 hours of TSDI data, select the "TSDI History" tab. This report will have an entry for each of the last 72 hours (during which the "Tlink Traffic Reporting" feature was enabled). This report provides the same information as the TSDI current traffic report. The report does not tell you whether the "Tlink Traffic Reporting" feature was disabled for portions of an hour; it only reports data for the time the feature was enabled.

The report also contains the average queue lengths and average queued times. The queued times are shown in milliseconds.
Figure 9-7 TSDI History

Tlink Traffic Settings and Reports							
Settings Current Report Tlink History TSDI History							
Tlink: LUCENT#CSTASERV#CSTA#ACME_NY							
<u>U</u> plink:							
Date/Time	Rate	Peak	Time	Interval	QL Avg	QL Max	
10/04 16:00	111192	480	08:24	15	1	24	
10/04 15:00	108030	480	43:23	15	1	45	- 1
10/04 14:00	106626	480	11:53	15	1	55	
10/04 13:00	32320	400	07:04	10	2	00	
•							
Downlink							
_							
Date/Time	Rate	Peak	Time	Interval	QLAvg	QL Max	
10/04 16:00	37064	160	19:23	15	0	5	- 1
10/04 15:00	36010	160	43:23	15	U	11	- 1
10/04 14:00	3004Z 10775	160	11:53	15	1	10	
10/04 13:00	10775	160	07:04	10	I	10	1
4							
		Γ	ОК	Cancel	Applu		

Telephony Services Traffic Measurement 345

#### **Reset Current Measurements**

Select the "Reset..." button from the "Telephony Services Traffic Viewer" main dialog box to reset the current measurements to zero. The confirmation dialog box is displayed, asking you to confirm that you wish to reset these measurements. If you select "Yes," the Traffic Viewer application resets the measurements for the entire system: the Tserver, each Tlink, TSDI, and Cserver.

#### Figure 9-8 Reset Confirmation



## Traffic Reports

Traffic data such as arrival rates, departure rates, and queue measurements are reported on an hourly basis. At the top of each hour the measurements are gathered for the past hour and are made available on the history report dialog boxes (see the section "Telephony Services Traffic Viewer" earlier in this chapter) and in the traffic log. The history reports display up to 72 hours of data. To view data prior to this time interval, refer to the traffic log. The history reports are lost when the corresponding module is unloaded. For example, unloading a PBX driver causes the history reports for this Tlink (including the TSDI history report) to be cleared. The traffic log, however, retains this information.

The history reports for the Tlink and TSDI measurements contain an entry if either of these interfaces is enabled. If one is disabled, the history report still contains an entry because the other is enabled. The data for the disabled interface is zero, since no traffic measurements are really being recorded for this interface. The traffic log does not contain information for this entry.

The Traffic Viewer also provides a "current" traffic report which automatically updates and shows the measurements as they are being taken for the current hour. At the top of the hour, the measurements on this dialog box are reset to zero since these measurements have been moved to the history report and traffic log.

The peak arrival rates are calculated at a regular interval (known as the Peak Measurement Interval). This interval is administered from the "System Settings" dialog box of the Tele phony Services Traffic Viewer. The default value is 15 seconds. The history report and traffic log show the maximum peak arrival rate for each hour.

Telephony Services Traffic Measurement 347

# **Traffic Log**

In addition to placing the measurements into the history reports on the hour, the Tserver also writes this information to a traffic log file. This file is maintained in a directory specified during installation (the default path for the file is \Program Files\Telephony Services\tsrv\logfiles\traffic.txt). You can read this file at any time, but do not write to it. If you need to modify the data in the file, copy it to another name and modify that copied version, not the original version.



Do not use MS Word for Windows to view the file. This editor can prevent the Tserver from accessing the file. This is the only editor known to affect the Tserver. If you open the log with Word, the Tserver can no longer write to the file and traffic data can be lost.

The traffic log is a circular file whose maximum size is set through the "System Settings" dialog box. When the file reaches its maximum size, the Tserver begins overwriting the information from the top of the file, adding a "Last Log Record" message to indicate where it began overwriting information. The Tserver writes to the log at the following times:

- Each hour (for each measurement type [Tserver, Tlink, TSDI] that was enabled during that hour)
- When a PBX driver module (that was reporting traffic measurements) is unloaded
- When the Tserver module is unloaded

The log only contains data for an interface if that interface was enabled for at least part of the hour.

The traffic log contains more information than the history reports since it does not get cleared when the Tserver or PBX driver modules are unloaded. The log contains entries when either of these modules is unloaded, and it can contain more than 72 hours of data depending on the administered size of the log.

#### Sample Traffic Log

The following is an example of the text that is written to the traffic log at the top of the hour. In this example, a PBX driver has registered with the Tserver to provide CSTA services and to provide traffic measurements. The traffic setting for this Tlink, the TSDI associated with this Tlink, and the Tserver traffic setting have all been enabled. All entries in the traffic log are prefaced with a date and time and an identifier indicating which interface generated these measurements.

4-15-96 11:00:00am DRIVER:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME Uplink: 23 Peak: 3 PeakTime: 50:45 Thresh: 372 Interval: 15 Rejected: 0 Downlink: 21

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME Uplink: 34 Peak: 5 PeakTime: 50:45 Thresh: 372 Interval: 15

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME Downlink: 43 Peak: 5 PeakTime: 37:31 Thresh: 372 Interval: 15

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME QLen Uplink Max: 1 Avg: 1 Thresh: 2

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME QLen Downlink Max: 2 Avg: 1 Thresh: 2

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME QTime Uplink Max: 0 Avg: 0 Thresh: 1

4-15-96 11:00:00am TSDI:PBX\_VNDR#CSTASERV#CSTA#SERVERNAME QTime Downlink Max: 0 Avg: 0 Thresh: 1

4-15-96 11:00:00am TSERVER Uplink: 36 Downlink: 37 Peak: 4 PeakTime: 37:31 Thresh: 372 Interval: 15 Rejected: 0

The first entry for the Tlink measurements includes the uplink arrival rate, the maximum peak arrival rate and when this occurred during the hour (minutes:seconds), the administered alarm threshold for this arrival rate, the Peak Measurement Interval, the number of messages rejected, and the downlink departure rate.

Telephony Services Traffic Measurement 349

The next six entries show the TSDI measurements, with a separate line for the different uplink and downlink measurements. The measurements include the following fields:

- **Thresh:** contains the administered alarm threshold for the associated measurement
- Max: contains the maximum queue length and queued time
- Avg: contains the average queue length and queued time

The last entry shows a set of Tserver measurements plus the alarm threshold for the downlink peak arrival rate, the Peak Measurement Interval, and the number of downlink messages rejected.

If the TSDI interface had been disabled for the entire hour (see the Tlink Traffic Settings dialog box), the log would contain only a line for the Tlink and for the Tserver. Note that the TSDI traffic history report would contain an entry for this hour as mentioned in the Traffic Report section.

# **Measurement Alarms**

The traffic measurements feature allows you to set alarm thresholds for certain measurements. This ties in with the Tserver's alarm notification feature which causes a dialog box to be displayed at the TSA or TSM32 when an alarm occurs on the Tserver. When an alarm threshold is reached, the Tserver places an error message in the error log with the severity level of WARNING and sends this error message to the TSA or TSM32.

The message indicates which measurement reached its threshold.



Be aware that generating an alarm to the TSA or TSM32 ties into the error log settings. To generate an alarm message, you must ensure that the ALARM destination is set for the WARNING level. Otherwise, an alarm is not generated or sent to the TSA or TSM32.

#### chapter

10

# The Cserver

The Cserver (CSTA server) performs certain management and mapping functions on behalf of PBX driver(s) that use the CSDI interface. It receives messages from the Tserver across the TSDI interface and maps them into ECMA-180 messages exchanged across the CSDI interface. It also provides client session management.

PBX vendors may choose to implement either the TSDI or CSDI interface. If the Cserver is not required by your PBX driver, you do not need the information presented in this chapter.

The following figure illustrates how the Cserver fits into Telephony Services:

Figure 10-1 Cserver Implementation



The CSDI interface is similar to the TSDI Interface in that messages are exchanged between the Cserver and the PBX driver across the interface. At startup, the PBX driver registers services with the Cserver which, in turn, registers them with the Tserver. Each service represents a Tlink. Each Tlink has a set amount of memory available for CSDI communications on that Tlink. The amount of memory is administrable.

## **Flow Control**

Flow control provides a mechanism for regulating the amount of data exchanged across an interface. Like the Tserver, you can modify the amount of memory to be used for messages by the CSDI in passing information back and forth between the Cserver and the PBX driver on a per-Tlink basis. You can also set the high water mark, the point at which flow control is invoked in the Cserver, and the low water mark, the point at which the Cserver returns to normal processing.

The Cserver has four message queues per Tlink:

- Messages waiting to be processed by the PBX driver
- Messages allocated by the Cserver
- Messages waiting to be processed by the Cserver
- Messages allocated by the PBX driver

plus an internal queue that the Cserver uses. As a message is put in any of these queues, the number of bytes needed for the message is added to a total count of allocated bytes for that Tlink. When a message is removed from a queue, the number of bytes is subtracted from the total. If the telephony server is busy, messages may build up in the queues because the various processes do not have enough time to process all the messages. If the count of allocated bytes reaches the high water mark set for that Tlink, the Cserver invokes flow control. When flow control is invoked, the Cserver does not accept any incoming messages from the Tserver. Since these are client application requests, users see the performance of their application degrade. At the same time, the Cserver lets the PBX driver know that an overload condition exists. The PBX driver may choose to notify the PBX that it cannot handle incoming requests. (This is up to the PBX vendor.) The overload condition is turned off when the count of allocated bytes goes below the low water mark set for that Tlink.

You can affect the performance of the Cserver by modifying the amount of memory available for the message queues and by setting the high and low water marks to reasonable numbers.

# **Cserver Status Information**

The Cserver provides detailed status information to let you know how the Cserver resources are being used. The information discussed in this section is available using the TSA and TSM32 applications. These interfaces are described in the next section.

## **Client Statistics**

The following parameters are tracked by the Cserver for each Tlink that has registered with the Cserver.

- **Driver ID**: This is the handle assigned by the Cserver to the Tlink instance. The driver ID is an integer and has the same value as the driver ID returned by the Tserver for any given Tlink.
- Client Sessions: The number of active client connections (sessions) associated with this Tlink.
- Active Requests: The number of active requests associated with this Tlink. An active request is one that has been issued to the PBX driver by the Cserver but has not been responded to by the PBX driver.

- Monitors: When a client starts an application, it may send monitor requests to the PBX asking it to notify the client application when certain events occur. Clients can issue many such requests on a single open connection. The Cserver must keep track of these monitor requests and make sure the event reports from the PBX driver are sent to the correct client application(s). This number represents the total number of active monitor registrations for this Tlink.
- Route Registrations: When a client starts a routing application, it sends routing registration requests to the PBX telling the PBX that the application wants to route all calls to a device on the PBX. Clients can issue many such registration requests on a single open connection. The Cserver must keep track of these registrations and make sure routing messages from the PBX driver are sent to the correct client application. This number represents the total number of active CSTA route registrations for this Tlink.
- **Routing Dialogs**: When the PBX receives an incoming call that requires routing by a client application, it sends a routing request to the telephony server. This request initiates a dialog that remains active as long as the call is in the process of being routed. The dialog ends when either the client or the PBX sends a Route End message.
- System Status Registrations : TSAPI has a provision that allows client applications to request notification of changes in the status of the PBX. If a client makes such a request, the Cserver keeps track of the request and sends an event when a change occurs. A client can make only one request for each open connection. This field is a count of the number of active requests for this Tlink. A maximum of 50 clients can be simultaneously registered for system status.

• **System Status**: The PBX driver reports the status of each Tlink. The Tlink must be in one of the following states:

STATE	DESCRIPTION
Initializing	The Tlink is initializing. It is temporarily unable to respond to requests.
Disabled	Monitor requests have been disabled. Other requests may also be disabled, but the Tlink provides a reject response in each case.
Enabled	Requests and responses are enabled usually after a disruption. The Tlink enters this state when it is done initializing. This state indicates that there are no outstanding monitor requests.
Messages lost	Requests, responses and event reports may have been lost.
Normal	Service is normal.
Overload imminent	Tlink may reject new requests.
Overload reached	The Tlink may shed load and issue Stop Monitor requests to the client. It may also reject additional Service Requests.
Overload relieved	The Tlink is no longer in overload.

## **CSDI Memory Allocation**

This group of numbers gives details on the currently administered CSDI buffer allocation and usage statistics for this Tlink. Buffer usage is expressed in bytes.

- CSDI Size the maximum amount of CSDI buffer space available to this Tlink. The default value is 1.5 megabytes but you may modify it. A flow control mechanism is in place to prevent problems caused by memory exhaustion. When the amount of memory allocated for this Tlink reaches this maximum, further requests from this Tlink cannot be processed until some of this memory has been released. The CSDI Usage and Number of Bytes information shows how close the Tlink is to reaching this maximum.
- CSDI High Water Mark When the amount of memory used by the CSDI for this Tlink reaches or exceeds this value, the Cserver enables flow control and stops processing incoming messages from the Tserver.
- CSDI Low Water Mark the amount of memory allocated for this Tlink that must be reached (i.e., go <u>below</u> this amount) before the Cserver starts processing incoming messages from the Tserver again.
- **CSDI Usage** the amount of memory that is currently being used by this Tlink in its four message queues. If this amount goes above the CSDI High Water Mark, the Cserver stops accepting messages from the Tserver and informs the PBX driver that it has turned on flow control. Flow control is not turned off until this number goes below the CSDI Low Water Mark.

## **Buffer Usage**

This section gives the number of messages on each of the four queues used by the Tlink and the one queue private to the Cserver. The four queues that are tracked are shown in the following figure:

Figure 10-2 Tracking Message Queues





- Queue A (Queued to Tlink, Queued to Driver): This queue contains messages sent to the PBX driver by the Cserver. Messages remain in this queue until the PBX driver processes them and releases the memory.
- Queue B (Allocated by Cserver, Allocated by CSTA): This contains messages allocated by the Cserver but not yet sent to any Tlink. These messages can either be put in a queue or the Cserver can release the memory.
- Queue C (Allocated by Tlink, Allocated by Driver): This contains messages allocated by the PBX driver but not yet sent to any Tlink. These messages can either be put in a queue or the PBX driver can release the memory.

The Cserver 359

Queue D (Queued to Cserver, Queued to CSTA): This contains messages sent to the Cserver by the PBX driver. These messages remain in the queue until the Cserver processes them and releases the memory.

The statistics for each queue are presented in terms of number of messages in each queue and the number of bytes taken up by these messages. The sum of the bytes in each queue is the value displayed in the Current Usage field. This total is also used to enable and disable flow control.

There is a fifth queue, private to the Cserver. These messages and the bytes used are not charged against the total memory allocated for this CSDI interface. The Cserver uses these buffers to keep track of monitor requests, route registrations, and other items.

360 Network Manager's Guide

## **Message Traffic**

These fields contain the count of messages exchanged over the CSDI and TSDI interfaces for this Tlink since the Tlink registered. The counts are shown as viewed from the Cserver and are displayed according to the four possible types of message exchanges.

- AA Sent to Tlink
- BB Received from Tlink
- CC Received from Tserver
- DD Sent to Tserver

Figure 10-3 Message Exchange



## Semaphores

These fields contain the values of the register, receive, send, and outbuf semaphores that the Cserver uses for this Tlink. This information is provided for troubleshooting problems.

- The **register semaphore** (**Register**) is used for internal thread synchronization purposes during Tlink registration. When Tlink registration is successful, this semaphore should always have a value of 2, corresponding to the two threads created within the Cserver for this Tlink registration.
- ◆ The receive semaphore (Cserver receive) is used to manage thread synchronization associated with receiving CSDI buffers from the Tlink. This semaphore is incremented when the Tlink sends a message to the Cserver and is waited on by the Cserver when it wishes to receive a message from the Tlink. The value of this semaphore is typically -1, indicating that the Cserver is waiting for a message from the Tlink but the Tlink has not sent any messages. The value will be 0 or greater when the Cserver receive queue begins to fill with messages that have not yet been received.

- ♦ The send semaphore (Tlink receive) is used to manage thread synchronization associated with sending CSDI buffers to the Tlink. This semaphore is incremented when the Cserver sends a message to the Tlink and is waited on by the Tlink when it wishes to receive a message from the Cserver. The value of this semaphore is typically -1, indicating that the Tlink is waiting for a message from the Cserver but the Cserver has not sent any messages. The value is 0 or greater when the Tlink receive queue begins to fill with messages that have not yet been received.
- ♦ The outbuf semaphore (Out Buf) is used to manage the use of Cserver internal buffers for message encoding purposes. The value of this semaphore is typically 1, indicating that the buffers are available. The value of the semaphore may temporarily change to 0 or -1 when message traffic is passing through the Cserver.

## Internal Buffer Sizes

These fields display the sizes in bytes of Cserver internal buffers used for message encoding and decoding purposes. The buffers may grow as needed up to 65,344 bytes. The buffers grow in size as needed according to the sizes of the messages being passed between the Cserver and Tlink. This information is displayed for troubleshooting purposes only.

# **Displaying Cserver Status Information**

The status information described in the previous section is available through the TSA and TSM32 applications. (The only fields you can change for the Cserver are CSDI size, High Water Mark, or Low Water Mark.)

## Using the TSA to View Cserver Status Information

1.



From the "Maint" menu, select "Cserver Tlink Information." The "Cserver Tlink Information" dialog box is displayed.

#### Figure 10-4 Cserver Tlink Information Dialog Box

Cserver Tlink Information			
<u>T</u> links		Registered?	
ROLM#CSTAS	ERV#CSTA#ACME_NY	No	
<u>⊻</u> iew…		<u>C</u> lose	
<u>V</u> iew		<u>C</u> lose	ļ

2. Select the driver whose resources you wish to view, then select "View." The "Tlink Information Details" dialog box for that driver is displayed.

364 Network Manager's Guide

#### Figure 10-5 Tlink Information Details Dialog Box

🗖 📃 Tlink I	nformation Details for	ROLM#CSTASERV#CS	TA#ACME_NY	
CSDI <u>S</u> ize (bytes):	1572864 CSDI Usag	je (bytes): O O	Sys Stat Reg: Boute Reg:	0
<u>H</u> igh Water Mark (bytes):	1258291 Bequests:	0	Routing Dialogs:	n
Low Water Mark (bytes):	629145 Monitors:	Ő	Houting Dialogs.	0
,	System Sta	atus: unregistero	ed	
┌ Semaphores				
Register: 0	Cserver Rcv: 0	Tlink Rov: 0	Out Buf:	0
☐ Internal Buffer Sizes	(bytes)			
Cserver In: 0	Cserver Event:	O ROPM	Buf: O	
Cserver Out: 0	BER Buf:	0		
☐ Number of Messages				
Queued to Tlink:	0	Allocated by Tlink:	0	
Queued to Cserver:	0	Allocated by Cserver:	0	
Cserver Private:	0			
Number of Bytes ──				
Queued to Tlink:	0	Allocated by Tlink:	0	
Queued to Cserver:	0	Allocated by Cserver:	0	
Cserver Private:	0			
☐ Message Traffic				
Received from Tlink:	0	Sent to Tlink:	0	
Received from Tserve	er: O	Sent to Tserver:	0	
	<u>0</u> K	<u> </u>	cel	1

3. Select "Cancel" to return to the "Cserver Tlink Information" dialog box. (If you made any changes to the CSDI size, High Water Mark, or Low Water Mark fields, select "OK" to accept the changes.)

## Using TSM32 to View Cserver Status Information

1.



From the "Options" menu, select "Tlink Status." The "Tlink Status" dialog box is displayed, showing tabs for "Information," "TSDI," "TCP/IP," and "CSDI."

Figure 10-6 Tlink Status Dialog Box

	Tlink Status - AC	ME_NY		-		
Information TSDI TCP/IP CSDI						
<u>I</u> link: ROLM#CST	ROLM#CSTASERV#CSTA#ACME_NY					
Registered?	N	۹o				
Open Connection	ns: O	)				
Stream Type:	C	CSTA				
Version:	L	Jnknown				
Supported Protoc	cols:					
Tlink Security:	C	CSTA				
Flow Control (TSI Invoke IDs	DI Buffers): D	Disabled				
In Use:	0	)				
Max Used:	0	) []	<u>R</u> eset			
Applications:						
			Re <u>f</u> res	h		
			<u>D</u> elete	-		
L	OK Ca	ancel <u>Ap</u>	ply	Help		

366 Network Manager's Guide

2. Select the "CSDI" tab to view Cserver information for this Tlink.

Figure 10-7 Tlink Status - CSDI Tab

-	Tlink St	tatus - ACME_NY	-
Information TSDI	TCP/IP CSDI		
Tlink: R0	) DLM#CSTASERV#(	CSTA#ACME_NY	
CSDI Usage (bytes): Sessions: Requests: Monitors:	0 0 0 0	System Status: Sys Stat Reg: Route Reg: Routing Dialogs:	Unregistered 0 0 0
Register: Cserver Receive: Tlink Receive: Out Buf:	0 0 0 0	Queued to Tlink: Queued to Cserver: Cserver Private: Allocated by Tlink: Allocated by Cserver:	0 0 0 0 0
Internal Buffer Sizes Cserver In: Cserver Out: Cserver Event: BER Buf: ROPM Buf:	(bytes) 0 0 0 0 0	Number of Bytes Queued to Tlink: Queued to Cserver: Cserver Private: Allocated by Tlink: Allocated by Cserver:	
-CSDI Buffer Control CSDI <u>S</u> ize: CSDI <u>H</u> WM: CSDI <u>L</u> WM:	(bytes) 1572864 1258291 629145	Message Traffic Received from Tlink: Received from Tserver Sent to Tlink: Sent to Tserver:	
		Cancel	Apply Help

3. Select "Cancel" to return to the "Telephony Services Maintenance" main dialog box. (If you made any changes to the CSDI size, High Water Mark (HWM), or Low Water Mark (LWM) fields, select "OK" to accept the changes.)

# **Error Logging**

The Cserver uses the same error log as the Tserver and the SDB drivers, presenting a chronologically accurate trace of events. Errors are categorized by severity: TRACE, CAUTION, AUDIT\_TRAIL, WARNING, ERROR, and FATAL. Each error logged includes the date, time, location of the error, a specific error code, and supporting text for each error. You can choose the destination for errors by their severity. See Chapter 11 for more details.

# **Cserver Message Tracing**

Cserver message tracing assists in troubleshooting by allowing you to see the flow of messages into and out of the Cserver for a set of users or a set of Tlinks. The Cserver message tracing facility logs to the same message trace file as the Tserver. This way, if Tserver message tracing is also enabled, the trace output generated by both the Tserver and Cserver can be viewed together in the same file.

For more details on Message Tracing in the Cserver, refer to Chapter 11, "Troubleshooting." chapter

# **11** *Troubleshooting*

This chapter provides a step-by-step approach to resolving system problems or identifying trouble areas so that the correct support organization can be contacted. A flowchart provides the steps you should take in investigating any problem. By following these steps in the order presented, you can usually isolate the problem to the individual workstation, server, or PBX network. Each potential trouble area is discussed in more detail: common Tserver problems, application problems, Telephony Services availability, Tlink availability, permissions, version information, automatic administration of LAN addresses, the SDB database engine, and performance.

This chapter also contains a detailed discussion of the troubleshooting mechanisms and tools provided by Telephony Services – how they work and what they are used for. Output from some of the tools is often needed if you cannot resolve the problem on your own and you need to escalate your problem.

In addition, this chapter provides tables of error codes for errors that Telephony Services returns to a particular application. Error codes are provided for CSTA universal failure events, ACS universal failure events, and security database errors.

# **Problem Areas for Troubleshooting**

Figure 11-1 illustrates the normal flow of troubleshooting activity. If you follow the steps in the order indicated by the flowchart, you should be able to isolate the cause of the trouble, whether it is in the application, the library, the Tserver, the PBX driver or the PBX.

Troubleshooting 369

Figure 11-1 Troubleshooting Flowchart



## **Common Tserver Problems**

The Windows NT machine where Telephony Services is installed must be available and must be running Telephony Services. If you cannot access the telephony server you want, verify that the Windows NT machine on which the telephony server is loaded is up and is functioning properly.

You can verify the state of the Tserver by opening the "TSAPI Telephony Services" application. (You can open this application by selecting "TSAPI Telephony Services" from the "Services" icon in the Control Panel, or by selecting the "TSAPI Telephony Services Controller" icon in the "Telephony Services for Windows NT" program group.) This application shows the last known state of Telephony Services. Click on the "Refresh" button to ensure that the information being displayed is up to date.

The following sections present common Tserver problems you may encounter, as well as recommendations for solving them.

#### **Tserver Authentication Problems**

If you are unable to log on to the Tserver, it may be one of two problems:

- If you receive the message "No logon permission" (ACS Universal Failure 111), then you need to be granted the following advanced NT user right: Log on as a service. See the section titled "Assigning User Rights" in Chapter 7.
- If you receive the message "Bad login or password" (ACS Universal Failure 25), try the following:
  - Use the Windows NT User Manager to verify that the login is a valid Windows NT Username.
  - From the Windows NT User Manager, check the setting of the option "User Must Change Password at Next Logon." If this checkbox is set, either clear the checkbox, or log into the Windows NT machine and change your password.
  - If you are not certain you are using the correct password, use the Windows NT User Manager to reset the password to a known value.



This error may also be returned if the login being validated against exists in a Trusted Domain of the Domain in which the Tserver is running, and this login is disabled in the Trusted Domain.

#### **Tserver Initialization Problems**

When the Tserver does not initialize properly, the following behavior may be observed:

The Tserver will not start when using the TSAPI Telephony Services Controller or the Services control panel. The first time Telephony Services is started, it performs several additional tasks, including creating the Security Database and adding entries to the Windows NT registry. On a 486-class machine, Telephony Services may not be able to complete these tasks in the time allotted. If the following message is displayed, attempt to start Telephony Services again:

Couldn't start TSAPI Telephony Services: The service did not respond to the start request in a timely fashion.

 You are unable to establish a connection to the Tserver. An ACS Universal Failure 19 (No SDB) is returned for the acsOpenStream() request.

For new installations, verify the following:

• The system was restarted after the installation.

This is a requirement, although no message is displayed about this during the installation procedures.

• Installation procedures completed successfully.

No errors were received during the installation of each component selected, and there was a message indicating a complete install for each component.

• Btrieve software was installed.

The Tserver requires the Btrieve software to be installed on the machine. Make sure that this component was selected during the Tserver installation.

Troubleshooting 373

• Tserver's IP address is correct.

Execute the TSAPI Telephony Services Controller and select the "Advanced" button. Verify that the IP address is the IP address configured for one of the NICs on the Windows NT machine. If it is not correct, select "Change IP Address" and enter the correct address.

For existing installations, verify the following:

- The Tserver unloaded properly. If the Tserver was running previously and it stopped unexpectedly (i.e., crashed), it might have unloaded improperly. At this point, the Windows NT machine needs to be restarted.
- The Microsoft® service pack 4 is installed. From the Windows NT Program Manager, choose "Help" and then "About."
- ◆ All of the Telephony Services software components are installed. If you install any service packs or if you upgrade Windows NT software on a machine that already had Telephony Services installed, make sure you reinstall all of the Telephony Services software components, including Btrieve. Then, try to restart the Tserver.

#### **Tserver Not Listed as a Service**

If there is a power loss, or if there is any type of reboot without first performing a normal Windows NT shutdown, the Tserver does not appear as an installed service in the "Services" control panel, even though the product is installed.

If this occurs, try the following:

- 1. From the "Telephony Services for Windows NT" program group, double-click on the "TSAPI Telephony Services Controller" icon.
- 2. Select the "Advanced" button, then select "Install Service" from the "TSAPI Telephony Services Advanced Functions" dialog box.

#### **Tserver Uninstalled While Still Running**

The TSAPI Telephony Services Controller "Advanced" feature allows you to uninstall the Tserver while it is still running. If you then attempt to stop the Tserver from the control panel (by selecting the service in the "Services" dialog box and selecting the "Stop" button), you will see the following error:

Server name invalid

To prevent this error, do the following:

- Stop Telephony Services using the "TSAPI Telephony Services Controller." (From the "Telephony Services for Windows NT" program group, double-click on the "TSAPI Telephony Services Controller" icon. Select "Stop" from the main window of the "TSAPI Telephony Services Controller.")
- Unregister this service with the Windows NT Service Manager by selecting the "Advanced" button from the main window of the "TSAPI Telephony Services Controller." Select "Uninstall Service" from the "TSAPI Telephony Services Advanced Functions" dialog box.
- 3. From the "Telephony Services for Windows NT" program group, double-click on the "unInstall Telephony Services" icon. When the uninstall program completes, a dialog box appears, indicating the components that have been removed from your system. Select "OK" to complete the uninstall process.



Should you need to reinstall the Telephony Services software, it is recommended that you do not uninstall the currently installed Telephony Services software before performing the reinstall. This is because many of the parameters used by Telephony Services are stored in the Windows NT registry. When the software is uninstalled, these parameters are also removed. Use the uninstall procedure only if it becomes necessary.

#### **Tserver Hangs While Trying to Access Novell NT Requester**

If you are trying to access Novell's NT Requester Version 3.5b (Novell's NetWare Client for NT V3.5b) and your login and password combination do not exist on the NetWare machine on which the Requester is administered, the Tserver will hang. No one will be able to open a stream to the Tserver. This is because Telephony Services for Windows NT is not compatible with Version 3.5b of Novell's NetWare Client for NT.

If you want to access the "Client Service for NetWare" (by selecting the "CSNW" program group from the Control Panel), you must install or upgrade to Version 4.0 of the NetWare Client for NT.

#### **Problems Opening a Stream**

If no Tlinks are listed when the user begins the application, or if the application displays a message indicating that a -5 error (No servers found) has occurred, check the following:

- Is the Tserver running? Verify the current state of the Tserver from the TSAPI Telephony Services Controller. Select "Refresh" to ensure that the information being displayed is up to date.
- Is the driver loaded? Use the "Driver DLL Information" dialog box from the TSA or the TSM32 application to verify that the driver is loaded.
- Is TCP/IP installed on the client? For Win16 and Win32 clients, double-click on the "Network" icon in the Control Panel to check the client configuration.

◆ Is there TCP/IP connectivity between the server and the client? From the Telephony Server, go to the "Main" program group and double-click on the MS-DOS® icon. Enter the following:

ping <client IP address>

If TCP/IP connectivity exists, the ping utility will display four messages indicating that a reply was received from the client.

If TCP/IP connectivity does not exist:

- Verify the physical wiring for the client and the server.
- Verify that the LAN cards in the client and server are configured properly.
- Check the link integrity settings for the LAN cards and for any Ethernet hubs to which the client and server are connected.
- Does the Telephony Services Library configuration file on the client (TSLIB.INI or tslibrc) contain the correct IP address and/or host name of the installed Tservers?
- If the Telephony Services Library configuration file on the client contains host names instead of IP addresses, is host name resolution (Domain Name Services [DNS] or Windows Internet Name Services [WINS]) configured and working?
- Does the client have the current Telephony Services Library installed?

If the available Tlinks are listed but the open stream request fails, the following ACS Universal Failure Errors may indicate the problem:

TSERVER\_NO\_USER\_RECORD (26)

The user is not administered in the SDB.

◆ TSERVER\_OLD\_TSLIB (90)

The Telephony Services software on the client needs to be updated.

Troubleshooting 377

◆ TSERVER\_DRIVER\_LINK\_UNAVAILABLE (1007)

The PBX driver is loaded, but the CTI link is currently unavailable.

TSERVER\_NO\_LOGON\_PERMISSION (111)

You do not have the Windows NT "Log on as a service" right. See "Tserver Authentication Problems" earlier in this chapter.

TSERVER\_BAD\_PASSWORD\_OR\_LOGIN (25)

Has the user been administered in Windows NT? Are the login ID and password correct? See "Tserver Authentication Problems" earlier in this chapter.

#### **Problems Accessing a Device**

Frequently, application errors will result because you do not have the correct permissions assigned in the Security Database. To determine whether users have permissions to access a device, the Tserver checks:

- the devices associated with the user's assigned worktop. Users always have permission to monitor and control the devices associated with their assigned worktop.
- the user's class of service options. Depending on the type of request, the Tserver will check the device group assigned to the user's Call Control, Device/Device Monitor, Call/Device Monitor, or Routing class of service to see if that device group contains the device.



The class of service options are the only way to grant users Call/Device Monitor and Routing permissions.

the devices associated with the worktop to which the user is logged in, provided that the Extended Worktop Access feature is enabled. When the Extended Worktop Access feature is enabled, the Tserver searches the Security Database for a worktop with the same LAN address as the client workstation to which the client is logged in. If a match is found, the user is permitted to monitor and control the devices associated with that worktop.

If the user does not have permission to access a device, the Tserver will return one of the following ACS Universal Failure Errors:

◆ TSERVER\_NO\_DEVICE\_RECORD (27)

The device is not administered in the SDB. Use the TSA or the TSA32 application to create the device in the SDB and to associate it with the user's worktop or class of service options.

◆ TSERVER\_DEVICE\_NOT\_SUPPORTED (35)

The device is assigned to a specifi c Tlink Group, but the user is trying to access the device on a stream for a Tlink that is not a member of that Tlink Group. Ensure that the user opened the stream to the correct Tlink. If so, you can either:

- add that Tlink to the Tlink Group specified for the device, or
- specify a different Tlink Group for the device that includes that Tlink.

#### ◆ TSERVER\_DEVICE\_NOT\_ON\_HOME\_LIST (49)

The user has an assigned worktop, but this device is not associated with that worktop. You can either:

- associate the device with the user's worktop, or
- assign the device to the user's Call Control and/or Device/Device Monitoring class of service options.

Troubleshooting 379

#### TSERVER\_DEVICE\_NOT\_ON\_AWAY\_LIST (51)

The user does not have an assigned worktop. The worktop from which the user is logged in is administered in the SDB, but this device is not associated with that worktop. You can either:

- assign a worktop to the user that includes the device, or
- associate the device with the worktop from which the user is logged in, or
- assign the device to the user's Call Control and/or Device/Device Monitoring class of service options.

#### TSERVER\_DEVICE\_NOT\_ON\_CALL\_CONTROL\_LIST (50)

The user does not have an assigned worktop. The user is assigned Call Control class of service permissions, but the device is not a member of their Call Control Access Group. You can either:

- assign a worktop to the user that includes the device, or
- assign the device to the user's Call Control Access Group.
- TSERVER\_DEVICE\_NOT\_ON\_ MONITOR\_DEVICE\_LIST (53)

The user does not have an assigned worktop. The user is assigned Device/Device Monitoring class of service permissions, but the device is not a member of their Device/Device Monitoring Access Group. You can either:

- assign a worktop to the user that includes the device, or
- assign the device to the user's Device/Device Monitoring Access Group.
#### TSERVER\_DEVICE\_NOT\_ON\_ MONITOR\_CALL\_DEVICE\_LIST (54)

The user is assigned Call/Device Monitoring class of service permissions, but the device is not a member of their Call/Device Monitoring Access Group. Assign the device to the user's Call/Device Monitoring Access Group.

#### ◆ TSERVER\_DEVICE\_LIST\_EMPTY (63)

The user is not allowed to perform this type of request on any device. Depending on the type of request, you can either:

- assign a worktop to the user that includes the device, or
- assign the device to the appropriate class of service options.

#### ◆ TSERVER\_EXCEPTION\_LIST (39)

The device is a member of an Exception Group that is associated with either the user's assigned worktop, the user's class of service options, or, if the Extended Worktop Access feature is enabled, the worktop from which the user is logged in. Determine which of these groups is the Exception Group that contains the device, and remove or change the group assignment.

#### ◆ TSERVER\_USERS\_RESTRICTED\_HOME (30)

The user is logged in from a worktop other than their assigned worktop, but the Extended Worktop Access feature is not enabled. You can either:

- change the user's assigned worktop to the worktop from which they are logged in, or
- associate the device with the user's assigned worktop, or
- assign the device to the user's Call Control and/or Device/Device Monitoring class of service options, or
- enable the Extended Worktop Access feature.

#### **Problems Loading a Driver**

You can load and unload drivers using the "Driver DLL Information" option in the administration software (the TSA or the TSM32 application - see Chapter 8). When you enter a DLL name in the "Name of DLL to Add" field, the application does not check if this name is valid or not. The only time this is determined is when the Tserver actually tries to load the DLL you named. If the name is invalid, the following error message is displayed:

Load of driver library failed

This message can mean either a bad DLL name was provided, or that a valid DLL failed to load for other reasons.

To ensure that the DLL is properly loaded, verify the following:

• The DLL name you want to add is valid.

Use the TSA or the TSM32 application to remove the bad DLL name, then add the correct DLL name.

• The driver and its supporting DLLs are located in the system environment path.

If the Telephony Services soft ware was just installed, try rebooting the server.

## **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 the installation manual for detailed information on installing client and server Telephony Services; versions required for the various files; and minimum requirements for both the client and server (processor, RAM, software versions).

If an application is not working, but has worked in the past, a recent change or upgrade could be the cause. If this is the case, back out the change or upgrade and see if the problem still exists.

If an application is not working on 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, especially permissions, administered correctly for the application?
- In order for TSLIB for Windows NT to work properly, Windows must be running in the enhanced mode (meaning that you must have typed "win" to enter Windows). The Windows Program Manager Help window displays the operating mode of the client workstation.
- If you receive the message "No logon permission" (ACS Universal Failure 111), then you need to be granted the Windows NT user right:
   Log on as a service. See the section titled "Assigning User Rights" in Chapter 7.
- If you see an error indicating that the login or the password is incorrect (such as ACS Universal Failure Event 25, "Bad login or password"), verify that the login and password are correctly administered in the server operating system.

If you receive this message when trying to open a connection to the Tserver and you know your password is correct, you may have to change your password. From the Windows NT User Manager application, check the option "Users Must Change Password at Next Logon." If this is option is enabled, have the user change their password and log on again.

• If you see an error indicating that no user record is present (ACS Universal Failure Event 26), the user attempting to login has a login but does not have a User object in the SDB. You must add this user to the SDB.

## **Changing User Permissions**

Telephony Services requires that users be administered in Windows NT and in the security database with the appropriate permissions to access the devices that will be used by their application. If this has not been done correctly, then any requests made by the application on behalf of that user will fail. The most common problems are summarized in the section, "Common Tserver Problems."

If the application is working for some users but not for a particular user, there might be a problem with the permissions for that user. First, see if the user can log in from another workstation that is functioning properly. If they can log in from the other workstation, the problem probably is the workstation. If they cannot log in from another workstation, the problem is likely to involve permissions.

To determine this, run the TSTest application, then check for a specific error code that reflects a permission problem. If you see an error code, follow the corrective action provided in the section "ACS Universal Failure Events" later in this chapter.



Remember to change the permissions appropriately to conform with the necessary security procedures.



Changes made to a user's permissions level are not effective until the client ends any applications currently running and restarts them. As a last resort, use the following procedures to assign full user permissions. (If the user performs administrative functions, verify that the user is a member of the appropriate admin access group. See Chapters 4 and 5 for details on providing administration privileges.)

#### Using the TSA to Assign Full User Permissions



- 1. Select the "Users" option from the "Admin" menu. The "User Information" dialog box is displayed.
- 2. Select the desired user and select "Edit" to modify this user object. The "Edit User" dialog box s displayed.
- 3. Select "Options" to display the "Edit User Options" dialog box.
- 4. To give this user full telephony permissions to control, monitor, and route any device:
  - **a.** Select "Any Device" under Call Control Services.
  - **b.** Select "Any Device" under Monitoring-Only Services, "Device/Device" option.
  - **c.** Select "Any Device" under Monitoring-Only Services, "Call/Device" option.
  - **d.** Enable the "Allow" field of the Monitoring-Only Services, "Call/Call" option.
  - **e.** Select "Any Device" under Routing Services (if the application needs to route incoming telephone calls).

Select "Close" when you have completed your selections.

- 6. Select "OK" from the "Edit User" dialog box, then select "Close" from the "User Information" dialog box.
- 7. Select "Devices" from the "Admin" menu. The "Device Information" dialog box is displayed.

- 8. Select the device associated with the user's worktop and then select "Edit." The "Edit Device" dialog box is displayed. Set the "Tlink Group" attribute to "Any Tlink." Select "OK."
- 9. Select "Close" from the "Device Information" dialog box.
- 10. Instruct the user to restart the application.

#### Using the TSA32 to Assign Full User Permissions

Procedure

- 1. Select the "Users" icon from the SDB tree view.
- 2. Double-click on the login ID for the user. The "User Properties" dialog box is displayed.
- 3. Select the "Class of Service" tab.
- 4. To give this user full telephony permissions to control, monitor, and route any device:
  - **a.** Select "Any Device" under Call Control Services.
  - **b.** Select "Any Device" under Monitoring-Only Services, "Device/Device" option.
  - **c.** Select "Any Device" under Monitoring-Only Services, "Call/Device" option.
  - **d.** Enable the "Allow" field of the Monitoring-Only Services, "Call/Call" option.
  - **e.** Select "Any Device" under Routing Services (if the application needs to route incoming telephone calls).

Select "OK" when you have completed your selections.

5. Select the "Devices" icon from the SDB tree view.

- 6. Double-click on the Device ID of the device associated with the user's worktop. The "Device Properties" dialog box is displayed. Set the "Tlink Group" attribute to "Any Tlink." Select "OK."
- 7. Instruct the user to restart the application.

## **Checking Version Information**

It is important that the telephony server and its software modules have the same software versions. The version numbers for the following software components should all be the same: Tserver, TSUSR, TSADV, TSAUTH, TRAFFIC, TSMI, TDI, TSVAL, TSSDB, and Tserver SDB Driver. If the versions are mismatched, you must reinstall Telephony Services on the server.

Telephony Services requires specific versions of Windows NT Workstation or Windows NT Server. These requirements are outlined in the installation guide.

To verify that the telephony server and software module version numbers all match, use the TSA (which includes all the modules in one list) or use the TSA32 and the TSM32 (the TSA32 lists SDB modules; the TSM32 lists server modules).

#### Using the TSA to View Version Information

In TSA, select the "About" option from the "Help" menu. This displays a dialog box containing the version and component information for the Tserver software and all the modules.

#### Using the TSA32 to View Version Information

In the TSA32, select the SDB icon from the tree view, then select "Properties" from the "Admin" menu. Then select the "Components" tab from the "Tserver Properties" dialog box. This displays a dialog box containing component and version information for the Tserver SDB Driver Versions, TSSDB, and TSVAL modules.

#### Using the TSM32 to View Version Information

In the TSM32, select "Tserver Properties" from the "Options" menu. Then select the "Components" tab from the "Tserver Properties" dialog box. This displays a dialog box containing the component and version information for the Tserver software and the TSUSR, TSADV, TSAUTH, TRAFFIC, TSMI, and TDI modules.

## Automatic Administration of LAN Addresses

#### Symptom:

You have enabled the "Automatic Administration of LAN Addresses" feature and you are using TCP/IP, but the TCP/IP address is not being stored in the LAN address field of the Worktop object.

#### Check:

Check the "Naming Format" you have chosen for TCP/IP. If you have chosen "Host Name," the problem may be that host name resolution n (Domain Name Services [DNS] or Windows Internet Name Services [WINS]) is not working properly. Verify that host name resolution is properly configured (using the "Network" icon on the Windows NT Control Panel) and that each client is registered. To check host name resolution, attempt to ping the client from the Tserver using the client's host name.

## SDB Database Engine is not Working Properly

#### Symptom:

You have just started up Telephony Services. When users attempt to establish a connection to the Tserver, the acsOpenStream() request fails with ACS Universal Failure 19 (No SDB). The errlog.txt file contains the errors "Btrieve not loaded!" and "the SDB database engine is not functioning properly."

#### Check:

1. If you are starting up Telephony Services for the first time, check that Telephony Services can find all the pieces of software that it needs to function correctly. The underlying database engine requires the three pieces of software in the table below. Make sure that these three pieces exist in a directory that is in the PATH variable on your server. If any pieces are missing, or have an incorrect size or date, reinstall Btrieve on your server.

Btrieve Component	Size of Component	Date of Component File	
WBTRV32.DLL	62464	10/25/95	
W32MKDE.EXE	298496	10/12/95	
W32MKRC.DLL	110080	10/12/95	

- 2. If your system has been running fine but has started experiencing this problem, reboot the server and start up Telephony Services again. If you did not reboot the system after installing the server software, reboot it now.
- 3. If this still doesn't solve the problem, look for TSRVBTRV errors in the errlog.txt file and refer to the documentation for that error at the end of this chapter.

## SDB is Unavailable

#### Symptom:

The SDB is unavailable. The administration applications will not allow access to the administration functions.

If you are using the TSA, you will see the error "SDB not ready. Administration functions will not be available. Failure code 6."

If you are using the TSA32, you will see the error "STOP Only Tserver properties will be available for Tserver %. SDB is unavailable [16002]. "

#### Check:

Reboot the server or workstation on which Telephony Services is running. Use the following procedure:

- 1. End all jobs that are running and return to the Program Manager.
- 2. From the "File" menu, select the "Shutdown" option. Select "Shutdown and Restart." Select "OK."
- 3. (This step is optional.) When the server has restarted, make a copy of the error log. Copy the file in \...\tsrv\logfiles\errlog.txt to another name before you start Telephony Services. If the problem persists, the information in this file may be useful.
- 4. Restart Telephony Services. You can do this by double-clicking on the "TSAPI Telephony Services Controller" icon in the "Telephony Services for Windows NT" program group. Press the "Start" button to start Telephony Services.

## Slow Performance

If the performance of Telephony Services is slow, check the following:

- 1. Make sure that the tracing features in Telephony Services are turned off. (This includes the error log TRACE level, Tserver message tracing, and Cserver message tracing.) These features are meant to gather information only when your telephony applications are not working as expected. They gather detailed information and write it to disk, doubling or tripling the amount of CPU resources required by Telephony Services. They should be turned off in normal situations.
- 2. Be aware of other applications that are running on the same server. Most applications are well behaved and do not consume CPU resources. However, some older editors, such as "EDIT," "NOTEPAD" and "VI" do not take advantage of the multi-threaded environment of NT and do not behave well. If you use these editors, the performance of Telephony Services will suffer.
- 3. Check the "TCP Preferred Naming Format" setting (available on the "Tserver Options" dialog box in the TSA or the "Tserver Properties" dialog box in the TSA32). The "TCP Preferred Naming Format" feature is only used if you have enabled "Extended Worktop Access" or "Automatic Administration of LAN Addresses." If both of these features are disabled, this field should be set to "IP Address" (this is the default).

If the "Extended Worktop Access" or "Automatic Administration of LAN Addresses" features are enabled and you use the "Host Name" setting for the preferred format, the Tserver must be able to resolve the host name using some form of host-name resolution, such as Domain Name Services (DNS) or Windows Internet Name Services (WINS). Enter the IP addresses you want to use for host-name resolution in a local HOSTS file, a DNS HOSTS file, or a WINS HOSTS file. Do not use a LAN Manager Hosts (LMHOSTS) file. This is because the Tserver only searches for addresses in files with the specific name of HOSTS (no extension). If no HOSTS files are found, slow performance or a time out failure will result.

- 4. Check the tasking options for your server (double-click on the "System" icon on the Control Panel). This causes the "System" dialog box to be displayed. Select the "Tasking" button. The dialog box that is displayed allows you to modify the Foreground/Background responsiveness of your server. You should select the third option, "Foreground and Background Applications Equally Responsive." See your Windows NT documentation for more information.
- 5. Use the Windows NT "Performance Monitor" in the "Administrative Tools" program group to see how system resources are being used.

## **Troubleshooting Mechanisms**

A number of mechanisms are provided in the Telephony Services platform to help you troubleshoot problems on your system. These mechanisms should be used in concert to help diagnose problems. The following list enumerates the troubleshooting facilities that are described in this document.

NAME	DESCRIPTION
Error Logging	The error logging facility allows you to capture information about any possible errors that occurred on the Tserver. It also provides tracing capabilities that produce information about the progress of a message once it has been received by the Tserver from either the client or the PBX driver.
Event Logging	The event log captures selected errors or events to provide tracing capabilities.
SDB Logging	The SDB log captures errors or events that occurred in the SDB and writes them to the SDB log file.
Tserver Message Tracing	The Tserver message tracing facility allows you to log ECMA- 179 messages that are received by the Tserver and sent to the PBX driver and received from the PBX driver and sent out to either the client or server library. These messages can be paired up with messages logged at the library (client) level to see if the application and telephony server are communicating properly.
Cserver Message Tracing	Cserver message tracing allows you to see the flow of messages into and out of the Cserver for a set of users or a set of Tlinks. Tracing is provided at the CSTA protocol and/or ROSE protocol level.
TS Spy	This message tracing facility for the Win16 and Win32 Telephony Services libraries allows you to view and/or log messages that are sent back and forth between a client application and the telephony server. There are separate versions of the TS Spy utility for the 16-bit and 32-bit libraries.

NAME	DESCRIPTION
TSTest	TSTest is a simple test application provided on each client platform. This application makes a call between two stations, primarily to verify that the client is set up correctly and the necessary administration has been done on the Telephony Server.
Error Codes	Errors that Telephony Services returns to application are explained in the error table provided in this chapter.

## **General Logging Information**

Telephony Services creates several logs to aid in the tracing of system problems. Although the logs are always created, the appropriate log settings must be enabled by the administrator. The files maintained by Telephony Services are:

- the Error Log
- the Message Trace Log
- the SDB Transaction Log

Each log is a single ASCII file, and resides in the \Program Files\Telephony Services\tsrv\logfiles directory. Each file has two parameters associated with it: the maximum size of the file, and the current offset within the file.

#### Maximum Log Size

The maximum size parameter allows you to limit the size of the file. The default value is one megabyte; you can modify this value to be smaller or larger depending on your disk availability and the nature of the problem you are tracing. This parameter is important because once the files reaches this size, it begins again at the beginning of the file, overwriting previous data. Obviously, the smaller the size, the less information in the file.

#### Last Log Record

To help you find the most current log entry in the log, the text "Last Log Record" is written to the file after the last record is logged. Data immediately following this line is the oldest data in the log; the data before it is the newest. You can verify this by examining the timestamps of each log entry.

The following is a sample log file:

06/19/96 15:13:52 TDI 18 10 AUDIT\_TRAIL: :TDI: Driver 3 TSERVER#CSRV\_OAM#OAM#TWIGA Registered successfully 06/19/96 15:13:52 TDI 18 10 AUDIT\_TRAIL: :TDI: Driver 4 LUCENT#SIMSERV#SIM#TWIGA Registered successfully 06/19/96 15:13:52 TDI 18 10 AUDIT\_TRAIL: :TDI: Driver 5 LUCENT#CSTASERV#CSTA#TWIGA Registered successfully

Last Log Record

#### Current Log Offset and Decreasing the Size of a Log File

The current offset is a parameter that the logging feature uses to keep track of its current location in the log file. This becomes important when the file wraps around and it isn't immediately obvious where the dividing line between new and old data is.

You can decrease the size of each log file using the TSA16 and/or the TSM32. If you choose to do so, you will lose some information when the file is truncated. How much you lose depends on the location of the current offset parameter in relation to the new file size. If it is less than the new file size, the log is simply truncated. If, however, the current offset points to the part of the file that was truncated, the current offset is reset to the beginning of the file. This means that any new data overwrites the data at the beginning of the file.

When the file is created, a header giving the time of creation is written to the file. Should the file wrap around, a new wraparound header is written to the beginning of the file, giving the time that the wraparound occurred.

#### **Error Log Entry Format**

Each error log entry consists of the following fields:

- **Date**: the date that the message was logged
- **Time**: the time of day that the Tserver received the error message.
- Module: the name of the module that is logging this error. This can include both Tserver and PBX driver modules.
- Location Code: a number identifying the location in the software where the error occurred. This number is used by customer support services to identify the problem.
- Error Code: a number indicating the particular error that occurred. This number is used by customer support services to identify the problem.
- Severity Level: one of the six different severity levels: TRACE, CAUTION, AUDIT\_TRAIL, WARNING, ERROR, FATAL.
- Error Message Text: text describing the reason for the error.

The following sample error log entry would appear for a Tserver AUDIT\_TRAIL message logged at 6 p.m. (18:00:13) on May 22, 1996, indicating that the driver with the specified Tlink name has successfully registered with the Tserver. The location code field is set to 2018 and the error code field is set to 10.

05/22/96 18:00:13 TSERVER 2018 10 AUDIT\_TRAIL: TDI: Driver 0 VENDOR#DRIVER#CSTA#SERVER\_NAME Registered successfully

#### Increasing the Size of the Message Trace File

If you find that the message log is not capturing enough information to be useful to you, you can enlarge it from its default size of 1 megabyte so that it will hold more data.

#### Message Trace Format

Each entry in the message trace output file consists of a header followed by the contents of the TSAPI message. The header consists of the following fields:

- **Date**: the date the message was logged
- **Time**: the time that the Tserver logs the message (before sending the message on)
- Login: the login specified in the acsOpenStream() request. This login appears for all messages associated with this connection. (This field is blank for the acsOpenStream() request because this information is not available at the point of tracing the message. However, the login is still available because it is one of the fields in the acsOpenStream() request. See the example below.)
- ◆ App Name: the name of the application that was specified in the acsOpenStream() request. This name appears for all messages associated with this connection. This field is blank for the acsOpenStream() request because this information is not available at the point of tracing the message. However, the application name is still present because it is one of the fields in the acsOpenStream() request. See the example below.
- SessionID: a unique number that the Tserver uses to identify this connection.
- **TransportID**: the port and IP address of the connection.
- **InvokeID**: if applicable, the invoke ID of the request as defined by TSAPI.
- MonitorCrossRefID: if applicable, the monitor cross reference ID. Not all messages use this identifier.
- **Tlink Driver**: the advertised service for the driver to which this connection is open.

Message: the name of the TSAPI message, (for example, ACSOpenStream or CSTAMakeCall). Following this field is information relevant to this type of message. All the fields in the message are listed with their contents.

The following is an example of an ACSOpenStream request message logged to the trace file.

```
02/21/96 12:27:38 Login: jen App Name: Example Application
SessionID: 6d2 TransportID: 5057:00000099:0000c045635b
InvokeID: 2 MonitorCrossRefID: 9976455f
Driver:PBX_VNDR#LINK1#CSTA#SERVER_NAME Message: value
ACSOpenStream ::= {
    streamType 1,
    serverID "PBX_VNDR#LINK1#CSTA#TSERVER1",
    loginID "jen",
    cryptPass '0000000000000'H,
    applicationName "Example Application",
    level 1,
    apiVer "TS2",
    libVer "2.20g",
    tsrvVer "2.20g"
}
```

The next example shows the cstaMakeCall() request from a client to the PBX driver and the CSTAMakeCallConfEvent from the PBX driver back to the client. The message contents show that a call is being made from extension 4441 to 4442.

```
02/21/96 12:27:48 Login: jen App Name: Example Application
SessionID: 6d2 TransportID: 5057:00000099:0000c045635b
InvokeID: 4
MonitorCrossRefID: 9792455f
       Driver: PBX_VNDR#LINK1#CSTA#TSERVER1
       Message: value CSTAMakeCall ::=
{
  callingDevice "4441",
calledDevice "4442"
}
02/21/96 12:27:48 Login: jen App Name: Example Application
SessionID: 6d2 TransportID:
5057:00000099:0000c045635bInvokeID: 4 MonitorCrossRefID: 0
        Driver: PBX_VNDR#LINK1#CSTA#TSERVER1
       Message: value CSTAMakeCallConfEvent ::=
{
  newCall
  {
    callID 1,
deviceID "4441",
    devIDType 0
  }
}
```

#### Viewing the Log Files

All logs can be viewed with standard editors. Some editors will force you to view a read-only copy of the file; others will allow you to write to the file. Any changes you make may be overwritten by the Tserver. If you want to view or edit the file, it is recommended that you first copy it to another name before viewing or editing it.



Do not use MS Word for Windows to view the file. This editor can prevent the Tserver from accessing the file. This is the only editor known to affect the Tserver.

The default path for the log files is \Program Files\Telephony Services\tsrv\logfile. The default name for the error log file is **errlog.txt**. The default name for the message trace file is **msgtr.txt**. The default name for the SDB log file is **sdblog.txt**.

You can view the error log file using the "Tserver Error Log" icon in the "Telephony Services for Windows NT" program group. However, you cannot remove the log file while Telephony Services is running.

The Tserver message tracing facility logs to the same message trace file as the Cserver. This way, if Tserver message tracing is also enabled, the trace output generated by both the Tserver and Cserver can be viewed together in the same file. Except for the use of the same file, the Tserver and Cserver message tracing facilities operate independently of each other.

## Tserver Error Log

The error logging feature provides a common error log for viewing the errors generated by the Tserver or the PBX drivers that choose to log to this file. Some drivers may choose to use their own error logging mechanism in addition to or instead of the Tserver common error log.

This section discusses the format of the error log entries which applies to all modules that use this feature.

Errors are logged in the error log when the module

- Detects a system error that may affect its performance
- Rejects a client request resulting from a security violation
- Receives a failure from another module
- Detects an internal error

The error logging feature provides six different severity levels with the following definition guidelines.

SEVERITY LEVEL	TYPES OF PROBLEMS LOGGED
TRACE	Trace message (for troubleshooting transient problems).
CAUTION	Non-service-affecting software condition that is not fatal.
AUDIT_TRAIL	Important (normal) events: driver loaded, link reset, etc.
WARNING	Indicates a problem that of itself is not service-affecting, but indicates a condition that may become a problem (e.g., low
	resources).
ERROR	Service-affecting condition that is not fatal.
FATAL	Fatal problem with the logging module.

#### Selecting the Correct Severity Level

You can pick the types of errors that are logged to the error log. By default, all errors but TRACE level errors are logged. FATAL and ERROR level errors are always logged (you cannot turn off logging on these levels) because errors at these levels can have a serious impact on the operation of Telephony Services.



You should turn on TRACE level messages only under instruction from an authorized service assistant because many events will be logged and system performance will be degraded.

#### **Reporting Errors**

You can direct the Tserver to report errors using one of the following methods:

◆ Log the errors to a file (errlog.txt). This file resides in the \Program Files\Telephony Services\tsrv\logfiles directory (the logfiles subdirectory of the Tserver directory; the Tserver directory is the directory where Telephony Services was installed.) The default for this path is \Program Files\Telephony Services\tsrv.

This is a circular file with an administrable maximum size. The text "Last Log Record" is written to the file after the last record is logged. Data immediately following this line is the oldest data in the log; the data before it is the newest.

Because messages in the error log file are overwritten after a period of time, you should examine the log in a timely manner so you do not lose the information you need.

By default, all errors are logged except TRACE level errors.

• Log errors to the Windows NT Event Log. By default, logging to the Event Log is enabled for the FATAL and ERROR levels. Only FATAL and ERROR levels can be administered for the Event Log.



To view Telephony Services error messages with the Windows NT Event Viewer, choose "Application" from the "Log" menu of the Event Viewer.

Report an alarm message to the TSA or the TSM32 application. This causes a pop-up alarm to appear on the workstation of the administrator notifying them that a problem has occurred. This dialog box must be dismissed before you can do anything else at the workstation. By default, only ERROR and FATAL errors are reported this way.

### **Turning on Error Logging**

You can use the TSA or the TSM32 to turn on error logging. The Error Log File and Alarm Generation destinations cannot be disabled for the ERROR and FATAL severity levels. The TRACE level can never be enabled for Alarm Generation.

You can set the maximum size of the error log file. The default log size is approximately 1 megabyte. If you are investigating a problem, you may want to make this larger so you can retain more log file messages over a longer span of time.

## Using the TSA to Select Error Logging Destinations

1.



Error Logging Dialog Box (TSA)

Figure 11-2

From the "Maint" menu, select "Error Logging." The "Error Logging" dialog box is displayed.

- Error Lo	aging [			
Select destinations for each level	of error reporting desired.			
FATAL - Fatal errors in the Tserver or a registered Event Log	I Tlink ⊠ Error Log File ⊠ Alarm Generation			
► ERROR - Service-affecting, non-fatal errors         ⊠ Event Log         ⊠ Alarm Generation				
WARNING - Not service-affecting, but may become a problem           Event Log         Error Log File           Alarm Generation         Image: Content Log File				
AUDIT TRAIL - Important events (e.g., tlink loade	ed, link reset, etc) ⊠ E <u>r</u> ror Log File □ Alar <u>m</u> Generation			
CAUTION - Unexpected software condition that is not fatal Use Firer Log Event Log Alarm Generation				
TRACE - Trace messages for informational purposes     □ Event Log     □ Event Log				
Log File: \\acme_ny\progra~1\tel	eph~1\tsrv\logfiles\errlog.txt			
Log File Size (bytes): 1000000	0 <u>K</u> C <u>a</u> ncel			

- 2. Select the destination(s) you want to use.
- 3. If you want to change the size of the error log, enter the number of bytes in the "Log File Size" field.
- 4. Select "OK" to submit your changes. Select "Cancel" if you do not want to make any changes.

#### Using the TSM32 to Select Error Levels

Procedure 123

1. From the "Options" menu, select "Error Logging." The "Error Logging" dialog box is displayed, showing tabs for "Error Log," "Alarms," and "Event Log."

Figure 11-3 Error Logging Dialog Box (TSM32)

Error Logging - ACME_NY				
Error Log Alarms Event Log				
Select Error Levels to be recorded in the Tserver Error Log File:				
FATAL - Fatal errors in the Tserver or a registered Tlink				
ERROR - Service-affecting, non-fatal errors				
🔀 WARNING - Not service-affecting, but may become a problem				
▼ AUDIT TRAIL - Important events (e.g., tlink loaded, link reset, etc)				
K _AUTION - Unexpected software condition that is not fatal				
IRACE - Trace messages for informational purposes				
Log File: \\acme_ny\progra~1\teleph~1\tsrv\logfiles\errlog.txt				
Log File Size (bytes): 1000000				
OK Cancel Apply Help				

2. From each of the "Error Log," "Alarms," and "Event Log" tabs, select the error levels you want to use.

- 3. If you want to change the size of the error log, enter the number of bytes in the "Log File Size" field.
- 4. Select "OK" to submit your changes. Select "Cancel" if you do not want to make any changes.

## **Tserver Message Tracing**

The message trace feature provides a means for viewing a history of TSAPI messages sent to and from the Tserver. This includes messages from client workstations to a PBX driver and from that driver to client workstations. Using the TSA or the TSM32, you can enable this feature for:

- All messages
- All users of selected Tlinks
- Selected users of all Tlinks
- Selected users of selected Tlinks

Message tracing may be useful in determining the cause of a problem. Used in conjunction with TS Spy, which traces messages through the TSLIB interface, you can determine

- Whether the Tserver received the message from the client (use TS Spy to verify that the message was sent)
- If an application is setting message parameters correctly
- Whether the Tserver received the expected response from the driver. Perhaps the application is waiting for a particular event before it makes another request, but it received a different event instead. Use TS Spy to verify that the client receives the driver response from the Tserver.
- Whether the Tserver was expecting a message, but nothing was received (or, the Tserver was not expecting a message, but one was received)

If you find that the message log is not capturing enough information to be useful to you, you can increase the size from the default value of 1 megabyte so that it can hold more data.

#### **Turning On Tserver Message Tracing**

With the TSA or the TSM32 you can trace all messages to and from the Tserver or set custom tracing options. You can use the following options:

- To trace all TSAPI messages, choose "Enable All Tracing" from the "Tserver Trace Options" box and select "OK."
- To trace selected TSAPI messages, choose "Enable Tracing for Selected Items" from the "Tserver Trace Options." The Trace all Users for selected Tlinks list box displays all of the registered Tlinks. To enable tracing for a specific Tlink, either double-click on the Tlink name, or highlight the Tlink name and select "Tlink Trace."

The "Users" list box in the **Trace selected Users to all or selected Tlinks** display area displays all users who have active connections to the Tserver. To enable tracing for a specific user, either double-click on the user's login ID, or highlight the login ID and select "User Trace."

When you enable tracing for a user, all Tlinks to which that user has open connections are listed in the **Tlinks in Use by the selected User** list box. By default, tracing is enabled for all of these Tlinks. To disable tracing for a specific Tlink for this user, either double-click on the Tlink name in this list box, or highlight the Tlink name and select "User/Tlink" trace.

When you have finished making your selections, select "OK."

• To disable tracing for the individual users and Tlinks listed, you can select them individually or check the "Disable All Tracing" button and then select "OK."



Because message tracing causes the system to operate more slowly, it is recommended that you set the message trace parameters only when troubleshooting.

If you find that the message log is not capturing enough information to be useful to you, you can increase the size from the default value of 1 megabyte so that it can hold more data.

#### Using the TSA to Enable Message Tracing

1.



From the "Maint" menu, select "Tserver Message Tracing." The "Tserver Message Tracing" dialog box is displayed:

#### Figure 11-4 Tserver Message Tracing (TSA)

Tserver Message Tracing			
Tserver Trace Options Enable All Tracing Enable Tracing for <u>S</u> elected Items Disable All Tracing	Trace all Users for selected Tlinks LUCENT#CSTASERV#CSTA#ACME_NY LUCENT#SDB_DAM#DAM#ACME_NY LUCENT#SIMSERV#SIM#ACME_NY TSERVER#CSRV_DAM#DAM#ACME_NY TSERVER#NSRV#NSRV#ACME_NY		
Items being traced are indicated with an " * ". Trace selected Users to all or selected Tlin			
Users: LSM PATM	I links in use by the selected User:		
User <u>T</u> race	User / Tlink T <u>r</u> ace		
Trace <u>F</u> ile: \\acme_ny\progra~1\teleph~1\tsry\logfiles\msgtr.txt			
Trace File Size (bytes): 1000002	<u>O</u> K <u>C</u> ancel		

- 2. Select an option from the "Tserver Trace Options" box.
- 3. If you selected "Enable Tracing for Selected Items," select the Tlinks and/or users for which you wish to enable tracing.

- 4. To change the size of the message log, enter the number of bytes in the "Trace File Size" field.
- 5. After you have selected your tracing options, select "OK" to begin tracing.

#### Using the TSM32 to Enable Message Tracing

1.



From the "Options" menu, select "Message Tracing." The "Message Tracing" dialog box is displayed, showing tabs for "Tserver Message Trace" and "Cserver Message Trace."

Figure 11-5 Tserver Message Tracing (the TSM32)

🛥 Message Tracing - ACME_NY 💌				
Tserver Message Trace Cserver Message Trace				
Terver Trace Options Enable All Tracing Enable Tracing for Selected Items Disable All Tracing	LUCENT#CSTASERV#CSTA#ACME_NY LUCENT#SDB_OAM#OAM#ACME_LA LUCENT#SDB_OAM#OAM#ACME_NY LUCENT#SDB_OAM#OAM#MAMBA LUCENT#SDB_OAM#OAM#SIMBA LUCENT#SDB_OAM#OAM#TWIGA LUCENT#SIMSERV#SIM#ACME_NY 	No No No No No No No No No No ♥		
Hace selected osers to all of selected fi	Tinks in use by the selected Lleer			
Name Trace No	Name	Trace		
User Tra <u>c</u> e	User/Tlink T <u>r</u> ace			
Trace File: V Trace <u>F</u> ile Size (bytes):	\\acme_ny\progra~1\teleph~1\tsrv\logfiles\msgtr.txt 1000002			
	OK Cancel Apply	Help		

- 2. From the "Tserver Message Trace" tab, select an option from the "Tserver Trace Options" box.
- 3. If you selected "Enable Tracing for Selected Items," select the Tlinks and/or users for which you wish to enable tracing.
- 4. To change the size of the message log, enter the number of bytes in the "Trace File Size" field.
- 5. After you have selected your tracing options, select "OK" to begin tracing.

## **Cserver Message Tracing**

Cserver tracing assists in troubleshooting by allowing you to see the flow of messages into and out of the Cserver for a set of users or a set of Tlinks. (See Figure 11-6.) Tracing is provided at the CSTA protocol and/or ROSE protocol level. That is, messages exchanged across the CSDI interface are composed using two separate protocol layers: the CSTA (that is, ECMA-180 standard) protocol and the ROSE (X.229 standard) protocol. By selecting the appropriate options, the message tracing facility displays the message content according to the selected protocol layer(s). A separate line of output is generated in the message trace file for each type of tracing that is selected.

Figure 11-6 Cserver Message Flow



The format for Cserver message trace file is the same as for the Tserver message trace file. Refer to the section "Message Trace Format" earlier in this chapter for header information and a sample trace message.

#### **Turning On Cserver Message Tracing**

You can use the TSA or the TSM32 to trace all messages through the Cserver or to set up custom tracing options. To set tracing options, you can use

- Enable All Tracing traces all Cserver messages for current and future registered Tlinks. You may choose to trace either or both CSTA messages and ROSE messages.
- Enable Tracing for Selected Tlinks traces only the selected Tlinks for all users (including users connecting after tracing is enabled). To select a Tlink for tracing, either double-click the Tlink name or highlight the Tlink name and select "Trace Select." Each double-click or depression of the "Trace Select" button changes the tracing type. It takes four double-clicks or button depressions to cycle through all the possible tracing combinations.
- **Disable All Tracing** discontinues tracing (after the OK button is pressed). Selecting this option disables all other options in the dialog box. Once tracing is stopped, all trace settings are cleared and must be reentered to turn on tracing again.

#### Using the TSA to Enable Cserver Message Tracing

1.



From the "Maint" menu, select "Cserver Message Tracing" to display the "Cserver Message Tracing" dialog box.

Figure 11-7 Cserver Message Tracing (TSA)

- Cserv	ver Message Tracing	
CSTA Trace Options <u>E</u> nable All Tracing <u>CSTA Messages             <u>R</u>OSE Messages   </u>	Trace <u>a</u> ll Users for selected Tlinks	
<ul> <li>Enable Tracing for <u>Selected Tlinks</u></li> <li><u>D</u>isable All Tracing</li> </ul>		
Tlinks being traced are indicated by: "C" - CSTA message trace "R" - ROSE message trace	<u>T</u> race Select	
Trace File: //acme_ny/progra~1/teleph~1/tsrv/logfiles/msgtr.txt		
	<u>O</u> K <u>C</u> ancel	

- 2. To trace all Cserver messages, choose "Enable All Tracing" and then select "CSTA Messages" and/or "ROSE Messages."
- 3. To enable tracing for selected Tlinks, choose "Enable Tracing for Selected Tlinks."

In the **Trace all Users for selected Tlinks** display area, either doubleclick on a listed Tlink, or select the Tlink and choose "Trace Select" until the appropriate levels for the trace link are displayed.

4. After you have selected your tracing options, select "OK" to begin tracing.

#### Using the TSM32 to Enable Cserver Message Tracing

1.



From the "Options" menu, select "Message Tracing." The "Message Tracing" dialog box is displayed, showing tabs for "Tserver Message Trace" and "Cserver Message Trace." Select the "Cserver Message Trace" tab.

Figure 11-8 Cserver Message Tracing (TSM32)

Tserver Message Trace       Cserver Message Trace         CSTA Trace Options       Enable All Tracing         CSTA Messages       BOSE Messages         Brable Tracing for Selected Tlinks       Disable All Tracing         Trace all Users for selected Tlinks       Name         ROSE CSTA       Irace Select		Message Tracing - AC	ME_NY		•
CSTA Trace Options Enable All Tracing CSTA Messages BoSE Messages Enable Tracing for Selected Tlinks Disable All Tracing Trace all Users for selected Tlinks Name ROSE CSTA Irace Select	Tserver Message Trace	Cserver Message Trace			
		TA Trace Options         Enable All Tracing         CSTA Messages         BOSE Messages         Enable Tracing for Selected Tlinks         Disable All Tracing         Ice all Users for selected Tlinks         lame         Irace Select	ROSE CSTA	A	

2. To trace all Cserver messages, choose "Enable All Tracing" and then select "CSTA Messages" and/or "ROSE Messages."

# 3. To enable tracing for selected Tlinks, choose "Enable Tracing for Selected Tlinks."

In the **Trace all Users for selected Tlinks** display area, either doubleclick on a listed Tlink, or select the Tlink and choose "Trace Select" until the appropriate levels for the trace link are displayed.

4. After you have selected your tracing options, select "OK" to begin tracing.

## Log File Sizes

You can adjust the maximum size of the error log, the Tserver Message Trace File, and the SDB log. The default setting for each of these files is 1 megabyte. You can increase this so that the file will hold more data. To do so, enter the number of bytes in the appropriate field.

#### Using the TSA to Administer Log and Trace File Sizes

1.



From the "Maint" menu, select the appropriate option: "Error Logging," "Tserver Message Tracing," or "SDB logging."

- 2. Set the "Log File Size" or the "Trace File Size" as desired.
- 3. Select "OK" to submit the change.

#### Using the TSA32 to Administer the SDB Log File Size



- 1. Select the SDB icon from the tree view.
- 2. From the "Admin" menu, select "Properties." The "Tserver Properties" dialog box is displayed, showing tabs for "Options," "SDB Log Settings," and "Components." Select the "SDB Log Settings" tab.
- 3. Set the "SDB Log File Size" as desired.
- 4. Select "OK" to submit the changes.

#### Using the TSM32 to Administer the Error Log File Size



- 1. From the "Options" menu, select "Error Logging." The "Error Logging" dialog box is displayed, showing tabs for "Error Log," "Alarms," and "Event Log."
- 2. On the "Error Log" tab, set the "Log File Size" as desired.
- 3. Select "OK" to submit the change.

Using the TSM32 to Administer the Tserver Trace File Size

Procedure

- 1. From the "Options" menu, select "Message Tracing." The "Message Tracing" dialog box is displayed, showing tabs for "Tserver Message Trace" and "Cserver Message Trace."
- 2. On the "Tserver Message Trace" tab, set the "Trace File Size" as desired.
- 3. Select "OK" to submit the change.

## Client Message Tracing (TS Spy)

The Telephony Services Spy (TS Spy) client message tracing applications allow you to see the flow of messages through the client Telephony Services Library (TSLIB). Messages are traced as they enter and leave the library in both directions: from application(s) to the Tserver and from the Tserver to application(s). Internal library/Tserver communication may also be traced. Trace messages are immediately displayed to the screen and may also be sent to a file specified by the user.

The following table gives the name of this utility on each client platform.

CLIENT	APPLICATION NAME	INI FILE NAME	NOTES
Windows	TSSPY.EXE	TSSPY.INI	Requires CSTA.DLL
Windows NT	TSSPY32.EXE	TSSPY32.INI	Requires CSTA32.DLL
Windows 95	TSSPY32.EXE	TSSPY32.INI	Requires CSTA32.DLL

## Starting TS Spy

To start the TS Spy application for 16-bit applications, double-click on the "TS Spy" icon in the "TS Win16 Client" program group.

To start the TS Spy application for 32-bit applications, double-click on the "TS Spy" icon in the "TS Win32 Client" program group.

The "Telephony Services Spy for Windows" or the "Telephony Services Spy for Win32" dialog box is displayed.



Because it is possible to run both 16-bit applications and 32-bit applications on Windows 95 and Windows NT, be sure that you start the correct version of TS Spy to see the messages being traced for a particular application.
# Figure 11-9 Telephony Services Spy for Windows (16-bit)

— Tel	ephony Services S	py for Windov	٧S	▼ ▲
<u>F</u> ile <u>E</u> dit	<u>O</u> ptions			
Tracing <u>Enabled</u> Open Closed	<u>D</u> isabled Streams (+): 0 Streams (-): 0		5	
<u>H</u> andle:	Server ID	Appl	Login	
Output				
				*
•				•
No trace file				

Figure 11-10 Telephony Services Spy for Win32 (32-bit)

-	Tele	phor	ıy Ser∖	vices S <sub>l</sub>	py fo	r Wir	132	-	·
<u>F</u> ile	<u>E</u> dit	<u>O</u> p	tions						
Tracir • En	abled		⊖ <u>D</u> isa	bled			Æ	7	
_	Open :	Strea	ims (+):	0			Ģ	<b>y</b> .	
L	losed	Strea	ams (-):	0					
Handle:			Serv	er ID		A	ppi	Log	In
		_			_				
Uutput									
									1
		_			_				+
	6lo							•	
Notrace	nie								

The first time the application is used on a client, it appears as shown in the top left corner of the display. Like most Windows applications, the TS Spy window may be moved and resized. When the application is closed, the screen location as well as other parameters (discussed later) are preserved in the utility's .INI file, located in the WINDOWS directory.

The following items are displayed in the screen:

- ◆ **Tracing...**: The **Disabled/Enabled** radio button pair is used to disable and enable message tracing. Tracing is initially enabled. Tracing may be enabled and disabled at any time while TS Spy is running. On exit, the current setting of this flag is saved in the .INI file.
- **Open Streams (+)**: Indicates the number of streams currently open from the TSLIB to all telephony servers. This number is updated in real time as applications open and close connections.
- Closed Streams (-): Indicates the number of streams previously open from the TSLIB to all telephony servers, but which are now closed. This number is updated in real time as applications close streams.
- Streams List: Displays information about currently and previously open connections from the TSLIB to all telephony servers. Currently open connections are indicated with a "+" prefix on the Handle. Streams that were previously open but are now closed are indicated with a "-" prefix on the Handle.

The top list box displays the following information for each stream:

- Handle: The internal ID for this stream. All the message lines in the trace file are prefixed with the handle of the connection to which the message belongs. The handle is generated by the TSLIB.
- Server ID: The Tlink to which this connection has been opened. This information is provided to the TSLIB by the application when a request is made to open a connection.
- Appl: The name of the application that has opened this connection. This information is provided to the TSLIB by the application when a request is made to open a connection.

- Login: The login ID under which the application has opened this connection. Multiple applications may be opened under the same or different login IDs at a single client. This information is provided to the TSLIB by the application when a request is made to open a connection.
- **Output**: Displays the trace output in real time as messages are passed through TSLIB. This output window can display approximately 30,000 characters of trace history. Once the output limit has been reached, the oldest trace information is deleted in favor of the newer trace information. For long trace outputs, it is recommended that the trace be logged to a file (discussed below).
- **Trace file Status Line**: This line, below the Output window, is a status line indicating whether logging to a file is active or not. The default is "No trace file." When file logging is active, this line indicates the file name (with full path) and file size.

# **TS Spy Menu Options**

- File: This menu contains one menu item: Exit. This menu item is used to exit TS Spy. The system menu may also be used to exit the application
- ♦ Edit: This menu contains the following menu items: Copy, Clear Buffer, Select All, and Purge Closed Streams. Copy, Clear Buffer and Select All operate on the Output window; Purge Closed Streams operates on the Streams List.
  - Copy copies the selected text (if any) from the Output window onto the Clipboard. The text is then available to be pasted into any application of your choosing. If no text is selected in the Output window, this menu item is grayed and disabled.
  - Clear Buffer clears out the contents of the Output window. Once this is done, the original contents are lost (the data is NOT copied to the Clipboard).

- Select All selects all of the text in the Output window.
   The Copy menu item can then be used.
- Purge Closed Streams deletes all closed connections (indicated with a "-" prefix) from the Streams List and resets the Closed Streams count to 0, leaving only currently open connections in the Streams List.
- ♦ Options: This menu contains the following menu items: Always On Top, Auto-Trace New Streams, Show Internal Events, and Log To File. These options are all saved in the .INI file and, unless otherwise indicated, are initially off. A check mark next to the menu item indicates that the option is currently enabled. Selecting any menu item toggles its state. Select the menu item once to enable the option; select the menu item again to disable the option.
  - Always On Top causes TS Spy to always be visible topmost on the display.
  - Auto-Trace New Streams causes newly opened connections (which open after TS Spy is started) to be traced automatically. This option is described in more detail in Individual Connection Tracing. This option is initially ON.
  - Show Internal Events causes non-application messages to be traced. The majority of messages normally traced through the CSTA.DLL or the CSTA32.DLL are application-to-telephony server and telephony server-toapplication messages. However, there are a small number of messages that the TSLIB generates to facilitate application/telephony server communications. Turning this option on will cause these internal messages to be traced.
  - Log To File causes all trace messages to be logged to a file specified by the user. This option is described in more detail in File Logging.

# **TS Spy File Logging**

Since the **Output** window holds approximately 30,000 characters and is easy to overflow, it is desirable to have a larger, more permanent method of storing the trace output. This method is logging the trace messages directly to a file. This file may be located anywhere that can be accessed by your PC. It could be your own hard disk (or floppy disk) or a network drive on a file server.



The log file grows without bound as trace output is recorded. Use this option with care to avoid using excessive disk space.

When file logging is enabled, the trace output is still sent to the TS Spy **Output** window so the user can still see the trace activity. The application can be reduced in size so that only a couple of lines of output are visible at a time or it can be minimized to an icon. This speeds up the tracing, as there is less screen updating to do for each message.

# **Activating File Logging**

To turn on File Logging, select the **Log To File** menu item under the **Options** menu. A "Create Trace File" dialog box appears and allows you to enter the drive, directory and file name for the trace file. The default extension given to TS Spy trace files is **.trc**, but you may enter any filename and extension.



-	Create Trace File	
File <u>N</u> ame: msg1.trc MSG1.TRC #	<u>D</u> irectories: c:\trcfiles ☐ c:\ ♪ trcFiles	Cancel
Save File as <u>Type:</u> Trace Files (*.trc)	Dri <u>v</u> es:	• Net <u>w</u> ork

Enter a valid filename (the directory must already exist) and select "OK." If the entered filename does not already exist, the file is created and is open for trace output. If the entered filename already exists, you are prompted for replacement confirmation:

#### Figure 11-12 Create Trace File Replacement Confirmation



If you select **No**, the Create Trace File dialog is redisplayed for further input. If you select **Yes**, *the original file is deleted and replaced with a new, empty file that is open and ready for trace output*.

Once a trace file is open, the file name and size are reported on the status line at the bottom of the TS Spy window.

Figure 11-13 Telephony Services Spy for Win32 (Trace File)

🗕 Teleph	ony Services Spy	for Win32	<b>•</b>
<u>F</u> ile <u>E</u> dit <u>C</u>	<u>)</u> ptions		
Tracing • Enabled	O <u>D</u> isabled	e	
Open Sti	eams (+): 0	- m	,
Closed St	reams (-): 0		
<u>H</u> andle:	Server ID	Appl	Login
<u>O</u> utput			
			<b>1</b>
+			+
C:\trcFiles\ msg1.tr	c : O bytes		

The number of bytes indicates the size of the trace file and will increase as messages are placed in the file.

# **Deactivating File Logging**

If file logging is left on when TS Spy is closed, the log file is automatically closed. File logging may also be deactivated by selecting the **Log To File** menu item. A dialog box is displayed, asking if you want to close the trace file.

Figure 11-14 Trace File Close Request



Figure 11-15 Create Trace File Close Confirmation

Telephony Services Spy for Win32
Trace file C:\trcFiles\ msg1.trc will be closed.
 OK

If you select **Cancel**, file logging continues. If you select **OK**, the log file is closed and TS Spy reports **No trace file** on its status line.

#### TS Spy Individual Connection Tracing

If a stream (connection) has tracing enabled, that connection is selected in the **Streams List**. When TS Spy is first started, tracing is enabled for all connections that are currently open, so all of the connections in the streams list are initially selected. To deselect a stream, click on the connection once with the mouse. (The **Streams List** is a multiselection list box).

If you enable **Auto-Trace New Streams**, new connections are traced as they are opened. If this option is not selected, new connections are NOT traced as they are opened. This option is saved in the .INI file. The default setting is ON, so that the default setting for TS Spy is to trace all current and future open connections.

#### TS Spy Client Library Model

In understanding the trace output, it is useful to think of the client library as a two-way pipeline, with messages entering and leaving both ends. Messages may originate or terminate in one of three places:

- The application
- The Tserver
- The client library (for internal events)

The trace records track the progress of a message through the pipeline, enabling you to determine which messages have been sent and whether or not they have reached their destination.

Normally, two trace records are generated for each message: one as it enters the pipeline, and one as it exits. Messages entering and leaving the application side (or the library itself) are presented in detail, with the value of each data element displayed in an appropriate format. The corresponding trace records to/from the Tserver only indicate successful transport of the message across the network.

#### TS Spy Trace Records

Trace records displayed in the **Output** window (or trace file) are separated by blank lines. Each begins with a date/time stamp and one of the following phrases which describes the record:

- **RECEIVED FROM APPLICATION-** the application has generated a message to be delivered to the Tserver. The message is displayed in detail.
- **DELIVERED TO TSERVER** the Tserver has acknowledged receipt of the message. Notification only.
- RECEIVED FROM TSERVER- a message from the Tserver has arrived in the client library receive queue. Notification only.
- DELIVERED TO APPLICATION- the application has accepted the message from the client library. The message is displayed in detail.
- FROM LIBRARY the client library has generated an internal message to be delivered to the Tserver. The message is displayed in detail.
- FOR LIBRARY the client library has accepted an internal message from the Tserver. The message is displayed in detail.

A typical request from an application generates four trace records, in the following sequence: **DELIVERED TO TSERVER RECEIVED FROM APPLICATION, RECEIVED FROM TSERVER DELIVERED TO APPLICATION.** An event report from the Tserver generates only the latter two records. Trace records from multiple messages may be interleaved.

The following samples show a portion of the trace output resulting from a cstaMakeCall request:

Figure 11-16 Telephony Services Spy for Windows Trace Output

<ul> <li>Telephony Services Spy for Windows</li> </ul>	-
<u>F</u> ile <u>E</u> dit <u>O</u> ptions	
Tracing • Enabled Disabled	
Closed Streams (-): 1	
Handle: Server ID Appl Login	
+0080: LUCENT#CSTASERV#CSTA#ACME_N_TSTestpatm -0080: LUCENT#CSTASERV#CSTA#ACME_N	
Output	
0080: [10/03/96 18:36:39] 0080: DELIVERED TO TSERVER: 0080: CSTAMakeCall	<u>+</u>
0080: [10/03/96 18:36:39] 0080: RECEIVED FROM APPLICATION: 0080: InvokeID 0 0080: CSTAMakeCall ::= 0080: { 0080: callingDevice "401", 0080: calledDevice "426" 0080: }	
0080: [08/15/96 01:33:52] 0080: RECEIVED FROM TSERVER: 0080: CSTAMakeCallConfEvent 0080: Application not notified (notifyAll == FALSE)	
0080: [10/03/96 18:36:39] 0080: DELIVERED TO APPLICATION: 0080: InvokeID 0 0080: CSTAMakeCallConfEvent ::=	*
C:\TRCFILES\MSG1.TRC: 2829 bytes	•

Figure 11-17 Telephony Services Spy for Win32 Trace Output

Telephony Services Spy for Win32	•	
<u>F</u> ile <u>E</u> dit <u>O</u> ptions		
Tracing       Disabled         Open Streams (+): 1       Image: Closed Streams (-): 0         Handle:       Server ID       Appl         +3039260:       LUCENT#CSTASERV#CSTA#ACM       TSTest	Login PATM	
3039260: [10/03/96 15:41:15] 3039260: RECEIVED FROM APPLICATION: 3039260: InvokeID 0 3039260: CSTAMakeCall ::= 3039260: { 3039260: callingDevice ''401'', 3039260: calledDevice ''426'' 3039260: }		+
3039260: [10/03/96 15:41:15] 3039260: RECEIVED FROM TSERVER: 3039260: CSTAMakeCallConfEvent 3039260: Application not notified (notifyAll == FALSE)		
3039260: [10/03/96 15:41:15] 3039260: DELIVERED TO APPLICATION: 3039260: InvokeID 0 3039260: CSTAMakeCallConfEvent ::=		+
No trace file	•	

## **TS Spy Error Records**

Certain network errors are also reported by TS Spy. These reports are displayed in the following form:

#### CONNECTION TERMINATED BY TSERVER (condition code = xxxx)

where **xxxx** is a numerical error code in hexadecimal notation. The most common error codes reported are:

2745 (this means the connection is aborted)2746 (the connection has been reset)2742 (the network is down)

Other codes are possible under unusual conditions. Report the code to technical support when you request assistance.

# **Telephony Services Test Application (TSTest)**

The Telephony Services Test application (TSTEST.EXE for 16-bit clients or TSTEST32.EXE for 32-bit clients) is a simple test application for TSLIB for Windows NT that runs on a Windows 3.1x client or on a Windows NT/Windows 95 client. The application makes a call between two stations. The application is documented in this guide to provide two capabilities:

- To determine if a trouble lies within the system versus an application. That is, if the test application works, the user knows that Telephony Services software and an application are successfully communicating. This would indicate that the trouble reported is most likely in the application the user was trying to activate.
- To display the error code, if an application does not return an error code and display it. This could be useful in certain trouble scenarios, such as inadequate buffers or incompatible file versions. However, just because a certain application is causing errors to occur does not guarantee that the test application will be able to cause the same errors.

The test application is designed only to perform a simple call. It performs the following calls:

ACSOpenStream

CSTAMakeCall (from the calling party to the called party)

CSTAClearCall

**ACSCloseStream** 

# Starting the Test Application

To start the test application, double-click on the "TSTest" icon in the "TS Win16 Client" or "TS Win32 Client" program group.

The "TSTest Telephony Services Test Application" dialog box is displayed.

### Figure 11-18 TSTest Telephony Services Test Application

	TSTest Telephony Services Test Application
<u>S</u> erver:	LUCENT#CSTASERV#CSTA#ACME_NY 🛃
<u>U</u> ser:	
<u>P</u> assword:	
	Make Telephone Call
	Erom:
	<u>I</u> o:
	Dial

If the call was successfully completed the following dialog box is displayed:

Figure 11-19

TSTest Telephony Services Test Application Success

	TSTest Telephony Services Test Application
0	Call successfully originated. Dismiss this message box to terminate call.
	OK

If the call was not successful, the following dialog box is displayed:

#### Figure 11-20

**TSTest Telephony Services Test Application Failure** 



A description of the failure code can be found in the "ACS Universal Failure Events" section of this chapter.

# **Error Codes**

# **CSTA Universal Failure Events**

The errors listed below are errors that occurred when an application requested a driver or server function and there was a failure. The first column gives the number identifying the error. The second column indicates the type of error (such as "State Incompatibility Errors" or "System Resource Availability Errors") and provides a description of the error.

Corrective action for some errors can be self-evident. For example, if a wrong number was called, or if a call was dropped before the requested action could take place, check the number and repeat the request. In other cases, you may need to consult the documentation for your PBX driver.

ERROR CODE	DESCRIPTION		
	Operations Class		
0	Server has detected an error that is not one of the defined errors. The server cannot be more specific.		
1	Server has detected an error in the operations class that is not one of the defined errors. The server cannot be more specific.		
2	The request is not compatible with the object.		
3	The parameter has a value that is not in the range defined for the requested service.		
4	The parameter has a value that is not known to the server.		
5	The calling device is not valid.		
6	The called device is not valid.		
7	The request cannot be provided because the specified device is not authorized for the service.		
8	The request cannot be provided because the specified device is not authorized for the service.		
9	The request cannot be provided because the called device is not authorized for the service.		
10	The request cannot be provided because the calling device is not authorized for the service.		

ERROR CODE	DESCRIPTION
11	The CSTA call identifier is not valid.
12	The CSTA device identifier is not valid.
13	The CSTA connection identifier is not valid.
14	The service request specified a destination that is invalid.
15	The service request specified a feature that is invalid.
16	The service request indicated an allocation condition that is not valid.
17	The service request specified a cross reference ID that is not valid.
18	The service request specified an object type that is outside the range of valid object types for the service.
19	The request violates a security requirement.
	State Incompatibility Errors
21	Server has detected a state incompatibility error that is not one of the defined errors.
22	The object is in an incorrect state for the service.
23	The connection Identifier specified in the active call parameter of the request is not valid.
24	The requested service operates on an active call, but the call is not in the active state.
25	The requested service operates on a held call, but the call is not in the held state.
26	There is no call associated with the CSTA connection identifier of the Clear call request.
27	The specified CSTA connection identifier of the Clear Connection request does not exist.
28	There is no call for the CSTA connection identifier specified as the call to be answered.
29	There is no call for the CSTA connection identifier specified as the call to be completed.
	System Resource Availability Errors
31	Server has detected a system resource error that is not one of the defined errors.
32	The service is supported by the server, but is temporarily busy.
33	An internal resource is busy. There is a high probability that the service will succeed if retried.
34	The service requires a resource that is out of service.
35	The server sub-domain is busy.
36	The server sub-domain is out of service.
37	The request will exceed the server's overall limit on the number of monitors.
38	The request will exceed the server's limit on the number of members of a conference.

ERROR CODE	DESCRIPTION
	Subscribed Resource Availability Errors
41	Server has detected a subscribed resource availability error that is not one of the defined errors.
42	The request would exceed the server's limit on the number of monitors for the specified object.
43	The limit on the number of external trunks would be exceeded by this request.
44	The limit on the number of outstanding requests would be exceeded by this request.
	Performance Management Errors
51	Server has detected a performance management error that is not one of the defined errors.
52	A performance limit has been exceeded.
	Security Errors
60	Server has detected a security error that is not one of the defined errors.
61	The server has detected an error in the sequence number of the operation.
62	The server has detected an error in the time stamp of the operation.
63	The server has detected an error in the PAC of the operation.
64	The server has detected an error in the seal of the operation.
70	This is a PBX Driver internal error, but it cannot be any more specific. A system administrator may find more detailed information about this error in the error logs Report this error to the PBX driver vendor.
71	This is a PBX Driver internal error, but not a defined error. A system administrator should check the error logs for more detailed information about this error. Report this error to the PBX Vendor.
72	The invoke Id in the service request is being used by another outstanding service request. This service request is rejected. The outstanding service request with the same invoke Id is still valid.
73	The service request from a client application is not defined in the API. A CSTA request with a 0 or negative Invoke ID will receive this error.

ERROR CODE	DESCRIPTION
75	The system lacks internal resources such as the memory or data records to process a service request. This failure may reflect a temporary situation. The application should retry the request.
76	An acsOpenStream session is terminating. This error is sent for every outstanding CSTA request of this ACS Handle. If the session is not closed in an orderly fashion, the application may not receive this error. For example, a user may power off the PC before the application issues an acsCloseStream request and waits for the confirmation event. In this case, the acsCloseStream is issued by the Tserver on behalf of the application and there is no application to receive this error. If an application will receive this error for every outstanding request.
77	The system detects that it cannot provide the service due to the failure or shutting down of the communication link between the Telephony Server and the PBX. This error is sent for every outstanding CSTA request for every ACS Handle affected. Although the link is down or the switch is out of service, the PBX driver remains loaded and advertised. When the PBX is in this state, all CSTA Service requests from a client will receive a negative acknowledgment with this unique error code.
78	The PBX Driver did not receive the response of a service request sent to the PBX in the allotted time. The timer of the request has expired. The request is canceled and negatively acknowledged with this unique error code. When this occurs, the communication link between the Telephony Server and the PBX switch may be congested. This can happen when the PBX and/or the Tserver exceeds their capacity.
79	For a device, the PBX processes one service request at a time. The PBX driver queues CSTA requests for a device. Only a limited number of CSTA requests can be queued on a device. If this number is exceeded, the incoming client request is negatively acknowledged with this unique error code.
	ROSE Errors Code from CSTA Module
80	The type of the APDU, as evidenced by its Type Identifier, is not one of the four defined by Recommendation X.229.
81	The structure of the APDU does not conform to Recommendation X.229.
82	The structure of the APDU does not conform to the standard notation and encoding defined in Recommendation X.208 and X.209.
83	The association-initiator is not willing to perform the invoked operation because it is about to attempt to release the application -association.
84	There is no operation in progress with an Invoke-ID equal to the specified Linked-ID.
85	The invoked operation, referred to by the Linked-ID, is not a parent-operation.
86	The invoked child operation, referred to by the Linked-ID, is not allowed by the invoked parent-operation.

ERROR CODE	DESCRIPTION
87	The type of the Result parameter supplied is not that agreed between the ROSE-users.
88	The reported error is not one of those agreed between the ROSE-users.
89	The reported error is not one that the invoked operation may report.
90	The type of error parameter supplied is not that agreed between the ROSE-users.

# **ACS Universal Failure Events**

The following are TSLIB error codes. The first column gives the number identifying the error. The second column provides a description of the error. The third column provides possible corrective action for the error or indicates a contact to help you determine the problem.

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 connection.	Is the correct version of IPX being used? If yes, contact the application developer since the application is trying to open too many connections 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.
-8	Following initial connection, the server has failed to respond within a specified amount of time (typically 10 seconds)	Call your support number and report error.
-9	The connection 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 connection 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 or TSM32 to check Tlink resources. If traffic reports show no overload, call application developer.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
-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.

The following are ACS Universal Failure event error codes. The first column gives the number identifying the error. The second column provides a description of the error. The third column provides possible corrective action for the error or indicates a contact to help you determine the problem.

ERROR	DESCRIPTION	
	The client library detected that the connection	1 Other errors may have been sent by the
0	failed	The rest of the connection was taken down
	lalied.	If so, follow the procedures for this error
		2 If no other errors were received from the
		Z. If no other errors were received from the
		still running and look for LAN problems
1	The Tserver could not begin execution of a	There is a serious system problem. These errors
	thread group which is necessary for it to run	will appear in the Tserver error logs. Consult the
	nronerly	logs for the return code
2	The Tserver has an internal system error	This error should never be returned to an
2		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.
3	The specified driver has not sent any heart beat	Look for driver error messages and/or contact
-	messages to the Tserver for the last three	the driver vendor to determine why it is no longer
	minutes. The driver may be in an inoperable	sending the heartbeat messages.
	state.	
4	This error is no longer used.	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.
5	The Tserver was unable to release Tserver	Consult the error log files for a corresponding
	driver interface (TSDI) memory back to the	error message. The error code associated with
	operating system.	this error message should be one of the
		following:
		<ul> <li>-1 - a corresponding FATAL error will be</li> </ul>
		generated indicating the call failed. Follow the
		description for this error message.
		• -2, -9, or -10 - internal iserver software error.
		Collect the error log files and message trace files
		and escalate the problem

ERROR	DESCRIPTION	
6	The Tserver was unable to send a message to the specified driver.	Consult the error log files for a corresponding error message.
		1. This error can indicate that the driver unregistered while the Tserver was processing messages for it or that there is a software problem with the Tserver. Verify that the driver was loaded at the time of the error.
		2. The error code ( <b>rc</b> ) should be one of the following: -2, -6, -9, -10. All these errors indicate an internal Tserver software error. Collect the error log files and message trace files and escalate the problem.
7	The Tserver was unable to receive a message from the specified driver.	Consult the error log files for a corresponding error message. The error code (c) should be one of the following:
		• -1 - a corresponding FATAL error will be generated indicating the call failed. Follow the description for this error message.
		<ul> <li>-2 - internal Tserver software error. Collect the error log files and message trace files and escalate the problem.</li> </ul>
8	A driver, internal to the Tserver, failed to register properly. The Tserver will not run properly without this driver.	There is a serious system problem. These errors will appear in the Tserver error logs. Consult the logs for the return code.
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 return code.
10	This error code has multiple meanings and should not be returned to the application.	Consult the error log files for a corresponding error message.
11	The Tserver was unable to allocate a piece of memory.	<ol> <li>Verify that the server has enough memory to run the driver and Tserver.</li> <li>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.</li> </ol>
12	The Tserver was unable to encode a message from a driver.	This error should never be returned to an application. Consult the error log files for a corresponding error message. If the error appears in the error logs, it indicates that the Tserver does not recognize the message from the driver. Call your support number.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
13	The Tserver was unable to decode a message from a client workstation.	The application is most likely using an old version of the client library. 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.	<ol> <li>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.</li> <li>Determine if either of these two cases is true.</li> <li>If this error occurs repeatedly and these conditions are not true, call your support number.</li> </ol>
15	The Tserver received a message from the client to be sent to a driver that is not a valid TSAPI request.	Verify that the message the client is sending is a valid TSAPI request. If it is then there is a problem with the Tserver. Call your support number.
16	The Tserver received an ACSOpenStreamConfEvent from a driver which does not have one of the version fields set correctly. The confirmation event will still be sent to the client with the version field set to "UNKNOWN."	This error will appear in the error log files and will indicate which field is invalid. Call your support number.
17	The Tserver received a message from the specified driver that is too large for it to process.	Use the Telephony Services administrator to increase the number of Send ECBs for this driver.
18	The Tserver does not have the internal resources to process this request.	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.
19	The Tserver was unable to initialize the Security Database when loading.	Look for other errors that might indicate a data base initialization problem.
20	The Tserver determined that a particular TSAPI message did not require Security Database validation. This code is an internal one and should never be returned to an application.	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.
21	The Tserver determined that a particular TSAPI message did require a Security Database validation. This code is an internal one and should never be returned to an application.	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.
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.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
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 application or the client library. Use TS Spy to verify that the application is attempting to open a stream to the correct Tlink
24	The stream type of an ACSOpenStream request was invalid.	A software problem has occurred with the client library. Call your support number
25	The password, login, or both from an ACSOpenStream request did not pass the Tserver authentication checks. A Tserver running on a Windows NT server uses NT authentication mechanisms. The user must have a valid entry in the NT user database. This error may also be returned if the login being validated against exists in a Trusted Domain of the Domain in which the Tserver is running, and this login is disabled in the Trusted Domain.	<ol> <li>Validate that the user login and password were entered correctly into the application.</li> <li>Use the Windows NT User Manager tool verify that the user's login and password are correct.</li> <li>If the user must change their password at next login, log in to Windows NT and change the password before starting the application.</li> </ol>
26	No user object was found in the security database for the login specified in the ACSOpenStream request.	<ul> <li>Verify the user has a user object in the security database by using the TSA or the TSA32.</li> <li>Validate that the user's login in the security database exactly matches the Windows NT username. Create a user object for this user if none exists.</li> </ul>
27	No device object was found in the security database for the device specified in the API call.	Create a device object for the device the user is trying to control in the Tserver security database by using the TSA or the TSA32. • Create a device for this device. Note: Make sure the assigned Tlink group for this device includes the correct Tlink.
28	The specified device did not appear on any of the searched lists, and more than one of the lists was not blank.	Change the user's administration so that the user has permission to control the device through either the user's worktop object (worktop administration) or through one of the Classes of Service (user administration).
30	The user tried to access a worktop other than his/her own worktop while the "Extended Worktop Access" feature was disabled; however, permission to access this device on this worktop was granted.	Either enable the "Extended Worktop Access" feature or change the user's worktop or Class of Service options to include permissions for the device at the worktop where the user is logged in
31	This error is no longer used.	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.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
32	This error is no longer used.	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
33	This error is no longer used.	This error should never be returned to an application or appear in the Tserver error logs.
34	The Tserver read a device object from the security database that contained corrupted information. The device object 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 Tlink group administered for this device does not contain the CTI link to which the user opened an connection.	<ol> <li>Validate that the user opened the connection to the correct CTI link.</li> <li>If the CTI link to which the stream was opened can support this device, use the TSA or the TSA32 to ensure that the correct Tlink group is assigned to the device or change the Tlink group for the device to "Any Tlink."</li> </ol>
36	This error is no longer used.	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.
37	A memory allocation 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 return code.
38	The Tserver has received a message from the application or the driver that it does not recognize.	Verify that the offending message is valid according to TSAPI. If it is a valid message then there may be a software problem with the Tserver. Call your support number.
39	The device in the API call is a member of an exception group which is administered as part of the user's worktop, Class of Service, or "Extended Worktop Access" is enabled and the user is logged in.	Determine which of the device groups is an exception group and either remove this device from the group or create a new group that reflects the correct access permissions.
40	The user login which is attempting to open an OAM stream to a PBX driver is a member of an Admin Access group, but this Admin Access group does not contain the OAM Tlink specified by the application (TSA, TSA32, TSM32, or the driver OAM).	Use the TSA or the TSA32 to verify that this OAM Tlink is assigned to the user's Admin Access Group.
41	An attempt to open a stream to an OAM application was made but the specified Tlink is not in the security database.	<ol> <li>Verify that the user has entered the correct Tlink name.</li> <li>Use the TSA or the TSM32 to verify that the specified Tlink is registered.</li> </ol>

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
42	The user licenses maximum has been exceeded on this telephony server. No new User Licenses may be granted (that is, no new connections may be opened; however, if a user/application has an existing connection open to a Tlink, they may open another connection to the same Tlink from the same workstation using the same login).	Obtain a larger Telephony Services license.
43	The TSA or the TSM32 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 connection, 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	This error is no longer used.	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.
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 Worktop does not match the device and the device is not a member of the Secondary Device Group of the user's 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 "Extended Worktop Access" feature is enabled and the user is not working from his or her own worktop, and either the other worktop is not in the SDB or does not have any devices associated with it.	Use the TSA or the TSA32 to grant this user permission to control the device through either the worktop object (worktop administration) or through one of the "Classes of Service" (user administration).

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
50	<ul> <li>The telephony server rejected a user's request to control a device because all of the following are true:</li> <li>There is no worktop or the user has no devices associated with the worktop.</li> <li>The "Extended Worktop Access" feature is enabled and the user is not working from his or her own worktop, and either the other worktop is not in the SDB or does not have any devices associated with it.</li> </ul>	Change the user's administration so that the user has permission to control the device through either the worktop object (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: • There is no worktop or the user has no devices associated with the 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 "Extended Worktop Access" feature is enabled and the user is not working from his or her own worktop, and either the other worktop is not in the SDB or does not have any devices associated with it.	Change the user's administration so that the user has permission to control the device through either the user's worktop object (worktop administration) or through one of the "Class of Service" (user administration).
52	The telephony server has rejected a user's routing request for a device because the user has a routing access group in their Class of Service but the device is not a member of that group.	Change the user's administration so that the user has permission to control the device through the Routing Access Group "Class of Service" (User administration).
53	The telephony server rejected a user's monitor device request because the user has a device/device monitoring access group, but the device is not a member of that group.	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 does not appear on the user's call/device monitor list and the call/device monitor list is not blank.	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 disabled.	Enable the Allow option for Call/Call Monitoring Access Group in the "Classes of Service" administration in this user's record (user administration).
56	This error is no longer used.	
57	This error is no longer used.	
58	This error is no longer used.	

ERROR	DESCRIPTION	CORRECTIVE ACTION
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	This error is no longer used.	
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	This error is no longer used.	· · · · · · · · · · · · · · · · · · ·
63	All the device groups in a user's worktop and Class of Service are empty (in the set of lists searched for this type of message).	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).
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	The application has called CSTAGetDeviceList with an invalid device level. Call the application support number.
65	The connection 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.	<ol> <li>The Tserver will terminate this stream when this error occurs. Verify that the application waits for an ACSOpenStreamConfEvent before it makes any further requests.</li> <li>If the application is written correctly, Call your support number.</li> </ol>
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 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.
69	The Tserver has an internal resource problem.	There is a serious system problem. These errors will appear in the Tserver error logs. Consult the logs for the return code. Call your support number.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
70	The Tserver cannot perform service advertising due to a error.	There is a serious system problem. These errors will appear in the Tserver error logs. Consult the logs for the return code. Call your support number.
71	The Tserver encountered a error while trying to access its message trace files or the traffic log.	This a system problem. These errors will appear in the Tserver error logs. Consult the logs for the return code. Call your support number.
72	This error indicates that there is a software problem with the Tserver.	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.
73	The TSDI for the indicated driver is congested, which means that the amount of allocated TSDI space as reach the highwater mark. This occurs when the PBX driver is not processing messages fast enough.	<ol> <li>Increase the TSDI space using the TSA or the TSM32 application.</li> <li>If the driver has indicated to the Tserver that it can accept flow control information, you can change the default flow control level to a higher value. Use the "Tlink Information Details" dialog box in the TSA or the "Tlink Status Information" dialog box in the TSM32 to make the change.</li> <li>If the driver still cannot handle the message flow, then check with your PBX driver manufacturer for load capabilities of the driver. You may have to get a faster server, or split the load being handled by the driver among other Tservers.</li> </ol>
74	The Tserver cannot allocate any more memory for the driver to which the application is connected. The driver registers an amount of memory with the Tserver when it loads which the Tserver uses as a maximum amount that can be allocated at one time.	<ol> <li>Increase the TSDI space using the TSA or the TSM32 application.</li> <li>If the driver can still not handle the message flow, then check with your PBX driver manufacturer for load capabilities of the driver. You may have to get a faster server, or split the load being handled by the driver among other Tservers.</li> </ol>
75	The Tserver has received a message from a driver which contains an invokeID that it does not recognize. The Tserver will still send this message to the application.	The driver may be taking a very long time to respond to client requests. If this continues to happen 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 or the TSM32 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 or the TSM32 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 or the TSM32 application should have prevented the user from entering an ECB value that was too low. This error indicates a problem with the TSA or the TSM32 application itself.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
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.
79	This error indicates an application which is using the SPX/IPX protocol to converse with the Tserver has not processed messages sent by the Tserver in over 30 seconds. The Tserver is recovering resources used to send the application the message.	This could indicate a problem on the network, with the client application machine or with the client application itself.
80	This error is no longer used.	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.
81	A client application attempted to open a stream with a protocol version (apiVer field in acsOpenStream()) set to a value that the Tserver does not support.	Use the TSA or the TSM32 application to determine which protocol versions the Tserver supports and compare these to the requirements of the client application.
82	A client application attempted to open a stream with a protocol version (apiVer field in acsOpenStream()) set to a value that the PBX Driver the stream was destined for does not support.	Use the TSA or the TSM32 application to determine which protocol versions the Driver supports and compare these to the requirements of the client application.
83	This indicates that the Tserver is having a problem with the transport layer.	There is a serious system problem. These errors will appear in the Tserver error logs. Call your support number.
84	A client application attempted to use a TSAPI call that is not supported by the negotiated protocol version for the current connection.	Use the TSA or the TSM32 application to determine which protocol versions the Tserver supports and compare these to the requirements of the client application.
85	The application is sending a request which is not valid based on the TSAPI version negotiation performed when the stream was opened.	The application should verify that it is requesting the appropriate version of TSAPI and that the driver can support this version.
86	This is an internal error in the Tserver.	These errors will appear in the Tserver error logs. Call your support number.
87	This is an internal error in the Tserver.	These errors will appear in the Tserver error logs. Call your support number.
88	This is an internal error in the Tserver.	These errors will appear in the Tserver error logs. Call your support number.
89	A client application attempted to open a stream with a protocol version (apiVer field in acsOpenStream()) that was set to a format that the Tserver could not decipher.	The application being used has a software problem. Contact the application software vendor.

ERROR	DESCRIPTION	
90	A client application attempted to open a stream using an outdated version of the TSLIB software that is incompatible with the current TSLIB software	Upgrade the client to the current version of the TSLIB.
91	The Tserver has detected that an invalid license file was installed.	Re-install the Tserver. If the error still persists call your support number.
92	This error is no longer used.	
93	This indicates that the Tserver has a software problem.	Call your support number.
94	The user login which is attempting to open an OAM stream is not a member of an Admin Access Group.	1. If this user is allowed to perform administration operations, then use the TSA or the TSA32 to make the user a member of the appropriate Admin Access Group.
95	The Tserver has encountered an error with the TCP/IP transport.	These errors will appear in the Tserver error logs. Call your support number.
96	This indicates that the SPX transport is disabled for the Tserver.	This does indicate an error has occurred but is used as informational. If SPX is the desired transport use the TSA to enable it.
97	This indicates that the TCP/IP transport is disabled for the Tserver.	This does indicate an error has occurred but is used as informational. If TCP/IP is the desired transport use the TSA to enable it.
98	TCP/IP cannot be enabled for the Tserver because a required NetWare NLM has not been loaded.	Consult this manual to determine which NLMs must be loaded.
99	The user has tried to disable TCP/IP while the TSA or the TSM32 is using this transport.	Stop the TSA or the TSM32 application.
100	The user login which is attempting to open an TSA stream to a PBX driver does not have NDS access rights to the Tlink object for this OAM PBX driver.	Give the user Access rights to the TLINK.
101	This error is associated with several error log messages that indicate a problem opening the Security database log file.	Look for entries in the Tserver error log related to the SDB log file for more information.
102	This indicates that the Tserver has a software problem.	Call your support number.
103	This error is associated with several error log messages that indicate a problem writing the Security database log file.	Look for entries in the Tserver error log related to the SDB log file for more information.
105	The Tserver cannot load the specified driver.	Verify that the driver and its supporting DLLs are located in the system environment path. If the Telephony Services software was just installed, try rebooting the server.
106	The user tried to load a driver that is not a valid driver.	Verify that the driver supports the tdiStartDriver() and tdiStopDriver() functions. It should only support these functions if it registers with the Tserver through tdiDriverRegister().
107	An internal error occurred.	Call your support number.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
108	The user tried to add a driver name to the Driver DLL Information dialog of the TSA or the TSM32 that already exists.	There needs to be one entry only in the list for each driver. If it does not appear in the list then call your support number.
109	The user tried to load a driver that is not in the unloaded state.	If the driver is stuck in the loading or unloading state, try stopping and starting the Tserver. If this fails, call your support number. The load command will only try to load a driver that is in the unloaded state.
110	The user tried to unload a driver that is not in the loaded state.	If the driver is stuck in the loading or unloading state, try stopping and starting the Tserver. If this fails, call your support number. The unload command will only try to unload a driver that is in the loaded state.
111	The user login which is attempting to open an ACS Stream does not have "Log on as a service" permission on the Windows NT account.	In the Windows NT User Manager tool, use the Policies/User Rights option to assign this login the "Log on as a service" right.
112	The user login which is attempting to open an ACS Stream is a disabled account on the Windows NT machine.	In the Windows NT User Manager tool, select the account and then enable it.
113	The Net Logon service is not running.	Use the "Services" application (in the Control Panel program group) to start the Net Logon service.
114	The account for accessing the Tserver is restricted.	This may be due to too many failed login attempts. In the Windows NT User Manager tool, use the "User/Properties" option to make sure the user name and password information are correct. Use the "Policies/Account" option to make sure the account settings are correct. Then try to log in again.
115	The account for accessing the Tserver cannot be logged in to at this time.	In the Windows NT User Manager tool, use the "User/Properties" option to make sure the user name and password information are correct. Use the "Policies/Account" option to make sure the account settings are correct. Then wait and try to log in to the Tserver at a later time.
116	The account cannot be accessed from this workstation.	This is the workstation on which the Tserver is running. Try to access the account from a different workstation. You can also use the "Policies/Account" option in the Windows NT User Manager tool to make sure the account settings are correct.
117	The account has been locked out by the administrator.	Have the administrator reinstate the account, if appropriate. In the Windows NT User Manager tool, use the "Policies/Account" option to change or update lockout information for the account.

ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
118	The password has expired.	In the Windows NT User Manager tool, use the "User/Properties" option to change the password or set the checkbox for "Password Never Expires." You can also use the "Policies/Account" option to change or update expiration information for the password.
1000	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_DUPLICATE_ACSHANDLE.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1001	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_INVALID_ACS_REQUEST.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1002	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_ACS_HANDLE_REJECTION.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1003	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_INVALID_CLASS_REJECTION.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1004	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_GENERIC_REJECTION.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1005	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_RESOURCE_LIMITATION.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1006	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_ACSHANDLE_TERMINATION.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
ERROR CODE	DESCRIPTION	CORRECTIVE ACTION
---------------	--	--
1007	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_LINK_UNAVAILABLE.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.
1008	This is a generic error code that is provided so that PBX drivers can send ACSUniversalFailure events with values that do not conflict with the set of codes used by the Tserver. This code has the definition DRIVER_OAM_IN_USE.	This code may be used differently by each PBX driver written for Telephony Services. Refer to your PBX driver documentation for a description of this code.

## **Security Database Errors**

The errors listed below are the errors that occurred when an application requested a database function and there was a failure. The first column gives the number identifying the error. The second column gives a brief description of the error. This is also the error description that appears in the error file created by the update/upgrade function of the Bulk Administration feature. A complete description of the problem is given in column 3. Error codes that do not appear in this list are used for internal processing and should not be reported to users.

ERROR CODE	ERROR MESSAGE	DESCRIPTION
501	Corrupt dictionary	The DICTNRY.SDB file is unreadable. It must be
		restored before the SDB can be accessed.
503	Missing dictionary	The DICTNRY.SDB is not in the C:\Program
		Files\Telephony Services\tsrv\SDB directory on
		the telephony server.
504	Invalid state	The SDB database driver is not in a NORMAL
		state and so cannot process any application
		requests. Check the version information and
		correct the problem before proceeding.
505	Invalid attribute type	The INFORM1 line contains an attribute ID that is
		not in the file specified on that INFORM1 line.
		This is a fatal error since it would apply to all
		errors for that file.

Troubleshooting 453

ERROR CODE	ERROR MESSAGE	DESCRIPTION
507	Invalid file type	A (non-comment) line in the bulk admin file does not contain a valid file type in column 2. The valid file types are user.dta, wktp.dta, dlist.dta, device.dta, oamlist.dta, tlist.dta, and tlink.dta. This may also mean you have entered the wrong type of file when you requested a bulk admin function. For example, you entered the name of a simple file when you were prompted for a flat file name.
508	Attribute not in file	The attribute specified in the INFORM1 line is not in the file specified on that INFORM1 line. This is a fatal error because all the records for this file will have this error.
510	Record not found	The record to be modified or deleted is not in the database. The value in column 3 is used as the primary key. Remember that all primary keys, except for LOGIN and TLINK_NAME, are casesensitive in BTRV.
511	Database access returned error	The underlying database engine has attempted a database access and was unable to complete the request. More information can be found in the error log.
512	Inconsistent database files	BTRV only: The .dta files which make up the SDB do not all have the same version number. The SDB cannot be used until all the .dta files have the same version number
514	Connection table full	All available SDB resources are busy at this time; try again when the Tserver is not so busy.
517	Invalid context	The NDS context is not valid.
518	Login table full	All available SDB resources are busy at this time; try again when the Tserver is not so busy.
519	Failed login	Authentication against NDS failed. Either login or password or both are incorrect.
520	No permissions	The Tserver or other application attempting an SDB request does not have permission as per NDS to do the request.
521	Invalid data	The data for a particular attribute does not pass the validation routine for that attribute.
522	Missing primary key	The primary key that identifies the record to be updated has not been supplied. This value must be placed in column 3 of either the simple or flat file.
523	Mandatory attribute missing	A mandatory attribute has not been provided.

ERROR CODE	ERROR MESSAGE	DESCRIPTION
524	Invalid primary key	The attribute in error is a foreign key (the primary key of another file). The value given for this attribute is not a valid primary key. For example, if the value for the attribute WORKTOP in the USER file is <i>Mary's worktop</i> , there must be a corresponding WORKTOP, <i>Mary's worktop</i> , in the WKTP file.
526	Duplicate key	The primary key of a record to be inserted already exists in the database and may not be duplicated.
536	Contention for the same record	There has been contention for the same record between the bulk admin feature and another application which uses the SDB. This can occur when two applications try to modify or delete the same record at the same time. Try again.
537	No more disk space	The SDB database driver couldn't write a record to the file because there was no available space on the disk. This is a fatal error.
538	No memory	The SDB database driver couldn't allocate memory resources to execute an operation. Check system resources.
539	Number of open files exceeds maximum	The maximum number of files that may be opened simultaneously (as set in Btrieve) is not large enough.
548	Attribute value over allowed max	The value of the attribute is over the allowed maximum for that attribute type.
549	Attribute value under allowed min	The value of the attribute is under the allowed minimum for that attribute type.
550	Data too large	The attribute value has more characters than permitted for that attribute type.
551	Period in key	The value of a primary key contains a period, ("."). This is not permitted.
552	Write to file failed	The bulk admin program could not write to the flat file or error file. It is not a failure of a database write.
553	Read of file failed	The bulk admin process could not read the simple/flat file for update.
554	File not present	The file named in the update, upgrade, or backup file does not exist in the sys:\system\tsrv\bulk_add directory.
555	INFORM1 line is missing	The input file for bulk admin did not contain an INFORM1 line.

ERROR CODE	ERROR MESSAGE	DESCRIPTION
559	Object is referenced by another object	The user is trying to delete a record whose primary key is referenced by a foreign key in another file. For example, if a user record contains a value, <i>Mary's worktop</i> , for the WORKTOP attribute, the WKTP record whose primary key is <i>Mary's worktop</i> cannot be deleted from the database until the reference in the user record is deleted.
563	Couldn't open SDBLOG.TXT	The Tserver couldn't open the SDBLOG.TXT file when it loaded.
565	File open failure	The bulk admin feature could not open the simple, flat or error file named in the request.
571	Invalid input line	The line has invalid data in columns 1, 2 or 3. Column 1 must be a legal opcode; column 2 must be a legal file ID and column 3 must contain a primary key (CN).
574	Can't modify a multi-valued attribute	You have requested a MODIFY of an attribute that is multi-valued - like a device ID on a device group or a Tlink on either a Tlink Group or Admin Group (BTRV only). You must delete the attribute from the list and then re-add it.
575	Simple/Flat/Error files have the same names	You have requested Bulk Admin to use a flat file and error file with the same name. This would cause the data in the flat file to be corrupted.
576	Invalid vendor length	The vendor field in the advertised service can only be 8 characters. The vendor field is the first of four sets of characters in the advertised service.
577	Invalid service length	The service field in the advertised service can only be 14 characters. The service field is the second of four sets of characters in the advertised service.
578	Invalid service type	The service type field in the advertised service can only be 4 characters. The service type field is the third of four sets of characters in the advertised service. The legal service types are SIM, CSTA, OAM, OTHR, NSRV
579	Invalid service name length	The service name field in the advertised service can only be 19 characters. The service name field is the last of four sets of characters in the advertised service.

## Index

ACS Universal Failure Events, 438 acsCloseStream, 437 acsOpenStream, 437 Adding DLLs, 300 admin access group, 11, 66, 141 administering, 67, 143 creating, 69, 144 deleting, 73, 149 editing, 71, 147 viewing, 72, 147 Admin Group object attributes, 238 administering Tlink Groups, 84, 157 administration of object, 29 sample configurations, 45 Administrator application main menu, 59, 129 advertised service (Tlink), 13 allowed users administering, 74, 145 Authentication, 11, 271 local, 275 single, 271, 273 automatic administration of LAN address. 20 Automatic Administration of LAN Addresses, 262 Bulk administration, 187 adding new members to an existing group, 213 adding objects to the SDB, 213 applications, 187 automating SDB interface, 211 backing up security database, 225 creating flat file from SDB, 225 creating template, 223 error file, 199 examining files, 193 flat file, 193 installing/updating the SDB, 227 invoking, 222 procedures, 217 simple file, 203 upgrading the security database, 232 call control class of service, 42 Call/call monitoring, 43 call/device monitoring, 43 class of service call control, 42 call/call monitoring, 43 call/device monitoring, 43

device/device monitoring, 43 options, 41 routing, 44 client software, 255 components, 8 **Computer Supported Telecommunications** Applications (CSTA), 11 Computer Telephony Integration, 5, 11 Console dialog boxes version information, 290 conventions used in this document. 2 Cserver error logging, 368 flow control, 354 message tracing, 368 Cserver message tracing, 410 Cserver status information, 355 buffer usage, 359 client statistics, 355 CSDI memory allocation, 358 internal buffer size, 363 message traffic, 361 semaphores, 362 viewing, 364 viewing (TSA), 364 viewing (TSM32), 366 CSTA, 11 CSTA Universal Failure Events, 434 CTI. 11 CTI link. 11 device administration, 92, 162 associating with CTI link, 28 associating with PBX, 24 creating, 94, 163 deleting, 98, 166 editing, 95, 164 viewing, 97, 164 device group administering, 101, 167 creating, 103, 168 deleting, 109, 172 editing, 106, 170 viewing, 108, 170 device group object, 22 Device group object attributes, 237 device object, 21 device ID, 21 device type, 21 location, 21 Tlink Group, 21 Device object attributes, 236 Device/device monitoring, 43 DHCP, 63, 138, 255, 263

Dialog Box SDB Log Settings, 124, 185 Domains distinguishing users, 278 Driver DLL adding, 300 configuring auto load, 301 information, 297 loading, 301 removing, 300 status, 297 unloading, 301 Driver DLL information **TSA**, 298 TSM32, 299 Dynamic Host Configuration Protocol see DHCP, 63, 138 Error codes, 434 ACS Universal Failure Events, 438 CSTA Universal Failure Events, 434 Security Database Errors, 453 Error File - Correcting Fatal Errors, 202 Error File - Correcting Non-Fatal Errors, 201 Error File - Format, 200 error log, 436 date field, 396 error code field, 396 error message text field, 396 location code field, 396 module field, 396 severity level field, 396 time field, 396 error log entry format, 396 Error logging destinations (TSA), 403 Error logging destinations (TSM32), 404 Extended Worktop Access, 262 Flat File - Device Group Information, 197 Flat File - Device Group Section, 199 Flat File - Object Information, 196 Flat File - Order of Data Lines (Attempted Add), 212 Flat File - Order of Data Lines (Attempted Delete), 212 Flat File - User Section, 194 G3 switch administration, 4 Invoke ID, 436 LAN address administration enabling automatically, 63, 138, 284 LAN connectivity, 253 License size, 292, 303 licensing. See Tserver Status Information. See also Version and System Status Information

line format, 33 load balancing, 27 message trace TS Spy, 416 message trace format app name field, 397 date field. 397 driver field. 397 invokeID field, 397 login field, 397 MonitorCrossRefID field, 397 session ID field, 397 time field, 397 transport ID field, 397 message tracing, 405 Cserver, 410 enabling (TSA), 407 monitor reports, 11 name server advertising, 288 object device, 21 device group, 22 Tlink, 23 Tlink Group, 23 user, 17 worktop, 19 object administration required order, 76, 150 object attributes, 234 objects initial addition, 188 security database, 16 **PBX**. 12 PBX driver, 8, 12 PBX drivers loading and unloading, 297 permissions, 65, 140 extending user access to other worktops, 40 Pop-up alarms, 285 quick add using, 60, 135 Removing DLLs, 300 Reset system history, 305, 308 routing, 44 sample configurations, 45 Sample traffic log, 349 SDB, 8 automatic update, 191 changing in bulk, 189 manual pages, 239 object attributes, 234 printing, 190 programming reference, 239

SDB (security database), 12, 15 SDB log, 124, 185 sdbBackupNdsDataBase(), 245 sdbBackupNdsDataBaseConfEvent, 247 SDBUniversalFailureConfEvent, 249 sdbUpdateNdsDataBase(), 239 SDBUpdateNdsDataBaseConfEvent, 243 security database, 8 delete object, 214 modify an existing object, 213 objects, 16 security database (SDB), 12, 15 Security Database Errors, 453 security database log file wrap-around, 36 line format, 33 sample file, 35 server applications, 5 Session, 437 Simple File - Processing Errors, 209 Simple File - Sample Template, 207 Simple File Format, 206 Simple File Information, 204 slow performance, 391 Status Tserver client, 302 stream, 12 streams list appl. 419 handle, 419 login, 420 server ID, 419 Switch. 4 symbolic conventions, 2 System history resetting, 305, 308 TCP Preferred Naming Format, 263 **TCP/IP**, 255 HP-UX client setup, 259 OS/2 client setup, 258 server configuration, 256 status, 266 Tserver feature interaction, 261 UnixWare client setup, 259 Win16 client configuration, 257 Win32 client configuration, 257 **Telephony Server** modules, 283 options, 284 software modules, 282 **Telephony Services** components, 8 Telephony Services administrator (TSA), 12 Telephony Services Components, 7

Telephony Services driver interface, 283 Telephony Services library (TSLIB), 8 test application starting, 432 Tlink administration, 77, 152 creating, 80, 154 deleting, 83, 156 editing, 81 status information, 309 viewing, 82, 155 Tlink Group administering, 84, 157 creating, 85, 157 deleting, 89, 161 editing, 87, 158 viewing, 88, 158 Tlink Group object, 23 Tlink group object attributes, 237 Tlink group usage, 24 Tlink groups, 23 Tlink information accessing, 79 detailed, 316, 319 summary, 318 **TCP/IP**, 323 TSDI resource, 322 Tlink object, 23 Tlink object attributes, 237 Tlink status information, 310 Tlink usage, 24 trace record delivered to application, 427 delivered to Tserver, 427 for library, 427 from library, 427 received from application, 427 received from Tserver, 427 Traffic measuring, 332 traffic log, 348 traffic log (sample), 349 traffic measurements reset current, 346 system settings, 335 Tlink current report, 341 Tlink history report, 342 Tlink settings, 340 Tlink settings and reports, 339 Tlink traffic reports, 340 TSDI history, 344 Tserver history report, 337 Tserver settings and reports, 336

Tserver settings/current report, 336 traffic reports, 347 traffic viewer, 334 Traffic Viewer dialog boxes measurement alarms, 351 traffic log, 348 traffic reports, 347 troubleshooting, 369 ACS universal failure events, 438 application problems, 383 automatic administration of LAN addresses, 388 changing user permissions, 384 checking version information, 387 Cserver message tracing, 410 CSTA universal failure events, 434 current log offset, 395 decreasing log file size, 395 error codes, 434 last log record, 395 list of facilities, 393 logging information, 394 maximum log size, 394 problem areas, 369 SDB database engine not working properly, 389 SDB is unavailable, 390 Security Database Errors, 453 slow performance, 391 Tserver error log, 400 Tserver message tracing, 405 Tserver problems, 371 viewing the log files, 399 TS Spy edit clear buffer, 420 copy, 420 purge closed streams, 421 select all, 421 file logging, 422 deactivating, 425 individual stream tracing, 426 menu item options, 421 menu options, 420 options always on top, 421 auto-trace new streams, 421 log to file, 421 show internal events, 421 starting, 416 TS Spy error records, 430 TS Spy File Logging

activating, 422 TS Spy menu item edit, 420 file, 420 TS Spy trace records, 427 TS Spy window closed streams, 419 open streams, 419 output, 420 streams list, 419 trace file status line, 420 tracing, 419 TSA menu, 59 starting, 57 TSA (Telephony Services administrator), 12 **TSA32** menu. 129 overview, 56, 126 starting, 127 TSA32 features, 129 SDB window, 131 tool bar, 130 TSAPI. 13 **TSDI**, 283 resource information, 309 Tserver, 8, 13 common problems, 371 error log, 400 message tracing, 405 TCP/IP feature interaction, 261 Tserver administration pop-up alarms, 285 Tserver problems accessing a device, 378 authentication, 372 hangs while trying to access NetWare Client for NT, 376 hangs while trying to access Novell NT Requester, 376 initialization, 373 loading a driver, 382 not listed as a service, 374 opening a stream, 376 uninstalled while still running, 375 Tserver status, 302 Tserver status information, 303 Tserver system status information, 290 Tserver version information, 290 TSLIB. 8 typographic conventions, 3 user

creating, 119, 179 deleting, 123, 184 editing, 121, 182 viewing, 122, 182 user access to other worktops, 40 User authentication, 271 User information accessing, 118 user object, 17 administration privileges, 19 attributes, 235 class of service, 18 login, 17 name, 17 worktop name, 18 User permission granting, 39

user responsibilities, 1 users administering, 117, 178 version information, 290 worktop administering, 110, 173 creating, 112, 174 deleting, 116, 177 editing, 114, 176 viewing, 115, 176 worktop object, 19 LAN address, 20 primary device ID, 20 secondary device group, 20 worktop name, 20 Worktop object attributes, 236 Worktops, 13, 38



Lucent Technologies Bell Labs Innovations

## We'd like your opinion ...

Lucent Technologies welcomes your feedback on this document. Your comments can be of great value in helping us improve our documentation.

## PassageWay® Telephony Services for Windows NT® Network Manager's Guide Issue 3.0, February 1997

1. Please rate the effectiveness of this document in the following areas:

	Excellent	Good	Fair	Poor
Ease of Finding Information				
Clarity				
Completeness				
Âccuracy				
Organization				
Appearance				
Examples				
Illustrations				
Overall Satisfaction				

- 2. Please check the ways you feel we could improve this document:
  - Improve the overview/introduction
  - Improve the table of contents
  - Improve the organization
  - Add more figures
  - Add more examplesAdd more details

- Make it more concise
  Add more step-by-step procedures/tutorials
- Add more troubleshooting information
- Make it less technical
- □ Add more/better quick reference aids
- Improve the index

Please add details about your major concerns.\_\_\_\_

3. What did you like most about this document?

4. Feel free to write any comments below or on an attached sheet.

If we may contact you concerning yo	ur comments, please complete the following:
Name:	Telephone Number: ()
Company/Organization	Date:
Address:	

You may FAX your response to (908) 957-4562. Thank you.