Network Access
Software Management Guide

9032859

CABLETRON SYSTEMS

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Cabletron Systems, Inc.
35 Industrial Way
Rochester, NH 03867

Printed in the United States of America

Order Number: 9032859

FCC Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

VCCI Notice

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Industry Canada Notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Contents

Preface

Chapter 1 CNAS Management

Chapter 2 Management Tools

Chapter 3 User Interface

Chapter 4 Managing Load Hosts

Chapter 5 Managing Directed TFTP

Chapter 6 Initializing the Access Server

Chapter 7 Configuring LAT Characteristics

Chapter 8 TCP/IP Network Characteristics

Chapter 9 Managing AppleTalk

Chapter 10 Configuring Basic Device Characteristics

Chapter 11 Configuring Modem Signals

Chapter 12 Configuring and Managing Interactive Devices

Chapter 13 Configuring and Managing LAT Services

Chapter 14 Configuring and Managing Telnet Servers

Chapter 15 Configuring LPD Printers

Chapter 16 Configuring and Managing SLIP Ports

Chapter 17 Configuring for SNMP Access

Chapter 18 Managing the Access Server

Chapter 19 Configuring and Managing 3270 Terminal Emulation (TN3270)

Chapter 22 Managing Dial Services

Chapter 23 Managing Access Server Security

Chapter 24 Managing Remote Login

Chapter 25 Accounting

Appendix A Cable and Adapter Recommendations

Preface

Overview

Purpose

The *Network Access Software Management* guide is written for the person who sets up, maintains, and manages any one of the supported family of network access servers. To use this manual, you must be familiar with using a terminal on an access server.

TSM Users

If you have the optional network management product, Terminal Server Manager (TSM) software, review the documentation for the product before you read this manual and other access server documents. This product affects the way you install and manage access servers. Note that TSM software is available only for OpenVMS load hosts.

Using This Manual

This manual details the tasks you perform to manage your access server, and should be used with the Cabletron *Network Access Software Command Reference* guide

Conventions

This manual uses the following conventions:

- The Return key, which you must press to execute all commands, is not shown in command line displays.
- The Local> prompt, which appears in most examples, is the default access server prompt. You can change this prompt to something other than `Local>` with the SET/DEFINE/CHANGE SERVER PROMPT command.
- All numbers are expressed in decimal notation unless otherwise noted.
- All Ethernet addresses are shown in hexadecimal notation.

Convention	Meaning
`Monospaced`	`Monospaced` type in command examples indicates system output or user input. User input is in boldfaced text.
UPPERCASE TEXT	Uppercase text in command lines indicates keywords that must be entered. You can enter them in either uppercase or lowercase. You can abbreviate command keywords to the first three characters or to the minimum unique abbreviation.
lowercase italics	Lowercase italics in command syntax indicates variables for which either the user or the network access server supplies a value.
{ }	Braces in the command syntax indicate that you *must* choose one of the enclosed options. (Do not type the braces.)
[ ]	Brackets in the command syntax indicate that the enclosed values are optional. You can enter one or none. (Do not type the brackets.)
UPPERCASE BOLD	Uppercase boldface text in summaries of characteristics indicates default values.
lowercase bold	Terms in bold face type are defined in the glossary.
Ctrl/*n*	This syntax indicates a keying sequence for which you must hold down the Ctrl key while pressing the key specified by the variable *n*.
/	A slash indicates related alternate commands or options. For example, SET/DEFINE/CHANGE PORT refers to the SET PORT, DEFINE PORT, and CHANGE PORT commands. The slash (/) is not part of the command syntax.

Associated Documents

Refer to the following documentation for additional information:

- *Terminal Server Manager Installation and Use* — Provides the procedures to install and use TSM.
- *DECserver 700 Site Preparation and Maintenance* — Provides the procedures to prepare the site before installing the DECserver 700 hardware.
- *DECserver 90TL/DECserver 90M Owner's Manual* — Provides the procedures to install and operate the DECserver 90TL / DECserver 90M hardware.
- *DECserver 900TM Installation* — Provides the procedures to install and operate the DECserver 900TM hardware.
- Cabletron *Network Access Software Installation* — Describes how to install the network access software on Microsoft Windows 95 or Windows NT, OpenVMS, DIGITAL UNIX, or UNIX operating systems.
- *Release Notes* — Provide the latest information about the access server. The release notes are available with the software distribution kit and are stored in the load host directory with the other software distribution files.
- Cabletron *Network Access Software Command Reference* guide — Provides the commands to operate and manage the access server.
- Cabletron *Network Access Software Problem Solving* guide — Describes problem-solving tools and procedures for the various access servers.

Chapter 1

CNAS Management

Overview

Introduction

This chapter describes the tasks that the following types of users perform when managing the access server:

- System administrators who configure and manage the access server
- End users of network services and applications

In This Chapter

This chapter includes the following topics:

- Configuration Tasks for System Administrators
- Management Tasks for System Administrators
- User Tasks
- Storage of Configuration Settings and Changes in Memory
- Commands to Display and Change Configuration Settings

Configuration Tasks for System Administrators

Configuration Tasks

The following table lists the tasks that system administrators can perform when configuring an access server and the chapter of this manual that describes each task:

To Configure:	Refer to:
User interface	Chapter 3
Network access server on the network	Chapter 6
Devices on a port	Chapter 9
Interactive devices	Chapter 11
LAT services	Chapter 12
Telnet listeners	Chapter 13
SLIP ports	Chapter 15
3270 emulation	Chapter 18
PPP	Chapter 19
User authentication	Chapter 22

Default Settings

Although a new access server is configured and operational with factory-set defaults, you may need to customize the configuration for your use. For a list of defaults associated with each category of configuration settings, refer to the chapters listed in the previous table.

Management Tasks for System Administrators

System Management Tasks

The following table lists the tasks that system administrators can perform to manage the access server. This table also lists the chapter that describes each task.

To Manage:	Refer to:
LAT network communications	Chapter 12
TCP/IP network communications	Chapter 7
SLIP port reconfiguration	Chapter 15
SNMP communities	Chapter 16
Network access server maintenance	Chapter 17
Management of load hosts	Chapter 4
Configuring the user interface	Chapter 3
Configuring LPD printers	Chapter 14
Managing point-to-point protocol hosts	Chapter 19
Managing IPX	Chapter 20
Managing dial services	Chapter 21
Managing network access server security	Chapter 22

User Tasks

Introduction

The access server enables end users to perform tasks such as connecting to network resources and managing sessions. For a description of these tasks, refer to the Specifying the Telnet Client Session Profile section in Chapter 11.

Accessing Online Help

The tutorial for online help also describes user tasks. To start the tutorial, enter the following command on your access server:

```
Local> HELP TUTORIAL
```

Storage of Configuration Settings and Changes in Memory

Memory Types

The access server stores configuration settings in two types of memory:

- Permanent data is stored in nonvolatile random access memory (NVRAM).
- Operational data is stored in volatile random access memory (VRAM).

Power Loss

An initialization or power loss has no effect on NVRAM. When an initialization or power loss occurs, the access server overwrites the current settings in VRAM with those from NVRAM.

Commands to Display and Change Configuration Settings

Introduction

This section lists the type of commands that operate on the configuration settings stored in VRAM and NVRAM.

The CHANGE and SET commands listed in the following chapters have an immediate effect when you enter them. When you use the DEFINE command, however, the changes are delayed:

- If you use the DEFINE command to make changes to a given port, these changes take place the next time that a user logs in to the port.
- If you use the DEFINE command to make changes to access server settings, these changes take effect the next time you initialize or plug in the server.

Reference

The Cabletron *Network Access Software Command Reference* guide describes the syntax, range of values, and defaults for all these types of commands. Use the Command Reference as a source of supplementary information as you go through the examples and procedures in this manual.

Types of Commands That Operate on Configuration Settings

Figure 1-1 shows the types of commands stored in VRAM and NVRAM:

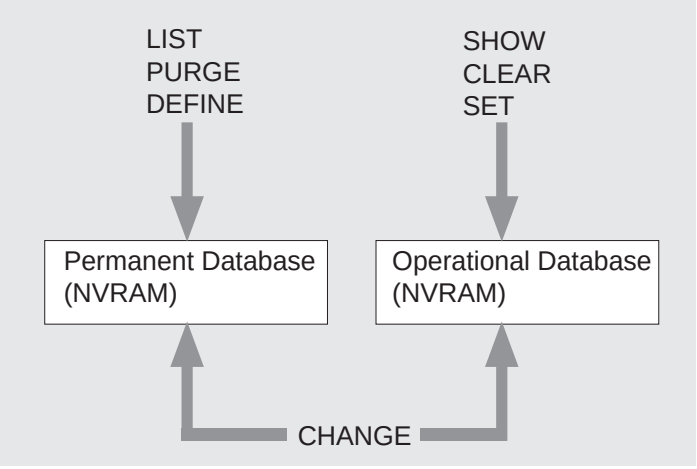


Figure 1-1. Types of Commands Stored in VRAm and NVRAM

Chapter 2

Management Tools

Overview

Introduction

This chapter describes the tools for managing the access server. These tools are:

- Access server commands
- Help
- Console port
- Remote console port
- Access Server Manager, a PC-based management tool

In This Chapter

This chapter contains the following topics:

- Access Server Commands
- Help
- Console Port
- Remote Console Port
- Access Server Manager

Access Server Commands

Introduction

The access server has a command line interface. You enter commands at a prompt on a terminal attached to an access server port. The default for the prompt is:

```
Local>
```

Reference

For a complete description of command syntax and use, refer to the Cabletron *Network Access Software Command Reference* guide.

Levels of Access Server Commands

The access server has four levels of commands as listed in the following table:

Command Level	Provides Access to	Commands to Enable and Disable
Privileged	All access server commands.	SET PRIVILEGED
Nonprivileged	A subset of privileged commands.	Default
Limited view	All nonprivileged commands except those that show or list LAT nodes, LAT services, and various Internet databases.	SET / DEFINE / CHANGE PORT n LIMITED VIEW ENABLED
Secure	A subset of nonprivileged commands that apply to the current port only.	SET / DEFINE / CHANGE PORT n SECURITY ENABLED

User Groups

For practical purposes, the access server command set syntax is divided into command groups. These groups are:

- Command descriptions
- CLEAR / PURGE commands

- SET / DEFINE / CHANGE commands
- SHOW / LIST / MONITOR commands

In the above list, the command descriptions group includes any command that does not functionally fit into the CLEAR / PURGE, SET / DEFINE / CHANGE or SHOW / LIST MONITOR groups (for example, DIAL, CONNECT, SEND, and LOOP).

Command Definitions

The following table describes the commands for the CLEAR / PURGE, SET / DEFINE / CHANGE and SHOW / LIST / MONITOR groups:

Command	Result
DEFINE	Changes NVRAM (nonvolatile random access memory). The system must be reinitialized for the changes to take effect.
SET	Changes VRAM.[1]
CHANGE	Changes both NVRAM and VRAM.
SHOW	Displays current status or information about various options from the access server operational database.
MONITOR	Displays continuously updated access server information on various options. Type any character to stop a monitor display. The MONITOR command displays have the same format as the corresponding SHOW command displays, but requires the user to be privileged.
LIST	Displays information about various options from the server's permanent database.
CLEAR	Changes VRAM.
PURGE	Changes NVRAM.

[1]VRAM is the server's volatile operational database.

Reference

For more information about this command group and its qualifiers, please refer to the Cabletron *Network Access Software Command Reference* guide.

Privileged Commands

To manage and configure the network, you use privileged commands. To enable privileged commands, use the SET PRIVILEGED command. The command line interface prompts you to enter the privileged password (which does not appear on the screen). If you forget the privileged password, you can reset the access server to its defaults by plugging the unit in while holding the reset button.

More than one port at a time can be privileged. Therefore, you should not reveal the privileged password.

Example: Enabling Privileged Commands

This example shows how to use the SET PRIVILEGED command to enable privileged commands on a port after accessing the access server.

```
Local> SET PRIVILEGED
Password> (not echoed)
Local>
```

The factory default value of the privileged password is SYSTEM.

Example: Changing the Privileged Password

To change the password, use the SET SERVER PRIVILEGED PASSWORD command. The following example shows how to use the SET SERVER PRIVILEGED PASSWORD command to change the privileged password.

```
Local> SET SERVER PRIVILEGED PASSWORD
Password> (not echoed)
Verification> (not echoed)
Local>
```

Help

Introduction

The access server provides online help about access server commands. This section describes two types of online help that are available on the access server.

HELP TUTORIAL Command

The command HELP TUTORIAL provides a brief introduction to the access server. You enter this command as follows:

```
Local> HELP TUTORIAL
```

The access server then displays a screen that explains how to use the tutorial.

HELP Command

The HELP command provides reference information for the level of commands enabled on the port that you are using.

Example: Accessing Online Help Information

The following example shows how to display the online help for the SET command and the PORT characteristic.

```
Local> HELP
[A list of topics displays here.]
Topic? SET
SET
SET changes characteristics and options stored in the
server's operational database.
Additional HELP available for:
INTERNET        PORT       NOPRIVILEGED    PRIVILEGED
SERVICE         SESSION    TELNET
SET Subtopic? PORT
```

Console Port

Displaying Port Parameters

The console port receives the access server system messages. An access server can have only one console port at a time. The default console port number is 1. To change the console port, use the SET/DEFINE/CHANGE CONSOLE PORT command.

To find out the current port number for the console port, use the SHOW SERVER command.

Reference

The console port helps with troubleshooting as described in the Cabletron *Network Access Software Problem Solving* guide.

Example: SHOW SERVER Command

The following example shows how to display the current port number for the console port. The value in for the Console Port characteristic in the display is the current port number.

```
Local> SHOW SERVER
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 0 00:16:18
Address: 08-00-2B-26-AA-99 Name: WWDOCMC Number: 0

Identification:
Circuit Timer:          80       Password Limit:   3
Console Port:            1       Prompt:      Local>
Inactivity Timer:       30       Queue Limit:    100
Keepalive Timer:        20       Retransmit Limit: 8
Multicast Timer:        30       Session Limit:   64
Node Limit:            200       Software:    WWENG2
Service Groups: 42, 46, 66
Enabled Characteristics:
Announcements, Broadcast, Dump, Lock
```

Remote Console Port

Description

The remote console port is a logical port that enables you to configure the access server from a remote terminal on the network.

Features of the Remote Console Port

The following table lists the features that distinguish the remote console port from other ports:

Feature	Description
Local switch character	~ (Tilde)
Personal computer file transfers	Unsupported
SET / DEFINE / CHANGE PORT characteristics	Available for all ports except for the remote console port
Number of sessions supported	1 at a time

Communications Utilities for Remote Console Sessions

The following table describes the four utilities you can use to connect to the remote console port on the access server:

Connection Utility	Host Type	Protocol
Network Control Program (NCP)	Network Control Program (NCP) OpenVMS Phase IV	MOP
SET HOST / MOP	OpenVMS DECnet / OSI	MOP
Telnet remote console	Internet	Telnet
Access Server Manager	32-bit Microsoft Windows, Windows 95, and Windows NT	Telnet

OpenVMS Utility — Terminal Server Manager

For OpenVMS systems, DIGITAL offers the Terminal Server manager (TSM) to facilitate managing the access server using the MOP remote console. TSM allows the user to store access information such as the maintenance password, Ethernet address, and login password for a server in a local database. The user can then establish a simple USER SERVER command and TSM will retrieve the information and establish a remote connection to the MOP console of the targeted server. Since TSM supports command scripts a highly automated interface to the MOP remote console can be created.

Network Control Program (NCP)

NCP enables you to connect to the remote console port from an OpenVMS DECnet node that is on the same Ethernet as the access server. The node must be running DECnet Phase IV software, but does not need to be a LAT service node or a load host for your access server.

Usage Considerations

Consider the following when using NCP:

- Do not confuse the SERVICE PASSWORD that you enter in an NCP command with the access server SERVICE PASSWORD. They are unrelated.
- If the access server requires that you specify the maintenance password and you omit it, NCP displays this error message:

```
Target does not respond
```

```
To disconnect from the access server, press Ctrl/D. To exit
NCP, type EXIT or press Ctrl/Z.
```

For additional information about NCP, refer to the documentation provided with your system.

Example: Using NCP to Connect to an Access Server Remote Console Port from a Load Host

The following example shows a connection from an OpenVMS DECnet Phase IV load host to an access server that has the DECnet node name SHRIMP. The maintenance password is FEDCBA. The login password is the default, ACCESS.

```
$ MCR NCP
NCP> CONNECT NODE SHRIMP SERVICE PASSWORD FEDCBA
Console connected (press CTRL/D when finished)
# ACCESS (not echoed)
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 0 00:16:38
(c) Copyright 1999, Cabletron Systems, Inc. - All Rights Reserved
Please type HELP if you need assistance
Enter username> MANAGER
Local>
```

Use of SET HOST/MOP from a DECnet/OSI OpenVMS Node

MOP enables you to connect to the remote console port from an DECnet / OSI OpenVMS node that is on the same Ethernet as the access server.

To disconnect from the access server, enter Ctrl / \ . Refer to the appropriate DECnet / OSI manual for information about how DECnet / OSI interprets passwords on the SET HOST / MOP command line.

Example: Using MOP to Connect to an Access Server from a DECnet/OSI OpenVMS Node

The following example shows a connection from a DECnet/OSI OpenVMS node to an access server remote console port. In this example:

- The access server has a DECnet node name of DGD700.
- The maintenance password is FEDCBA. On the SET HOST/MOP command line, however, the DECnet/OSI software transposes this password into the string BADCFE.
- The access server has a password of ACCESS.

```
$ SET HOST/MOP DGD700/VERIFICATION=%XBADCFE
%CCR-I-CONNEST, connection established to remote system
08-00-2B-26-AE-32 Press CTRL/ \ to disconnect, CTRL/] to send break
# ACCESS (not echoed)
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x
Uptime: 0 00:16:41
(c) Copyright 1999, Cabletron Systems, Inc. - All Rights Reserved
Please type HELP if you need assistance

Enter username> SWINSTALLER

Local>
```

Telnet Remote Console

If the access server has an Internet address, you can configure it to accept a Telnet remote console connection. Once you configure the Internet address and Telnet remote console port, the access server accepts and establishes a Telnet remote console connection to the remote console through one or more of the Telnet listeners specified by a TCP port on the access server. By default, TCP port 23 is the Telnet remote console port.

If you assign Telnet listener 23 to one or more physical ports, using the CLEAR/PURGE TELNET LISTENER 23 command only reassigns TCP port 23 as a Telnet remote console port.

Characteristics of the Telnet Remote Console Port

The following table describes the characteristics for Telnet remote console connections on the access server:

Characteristic	Description
Number of connections allowed on the remote console port at one time	1 The port is shared with the MOP remote console port so it will not be accessible to Telnet if the remote console port is active.
Default TCP port number	23 By default, the remote console is accessed via TCP port number 23. You can make the Telnet remote console port available to any of the TCP ports used by the access server Telnet listener feature.
Number of TCP ports configured to function as a remote console port	More than 1 allowed.
Maintenance password	Not required. In environments where both MOP and Telnet are used to access the remote console, setting a maintenance password for MOP does not affect Telnet.
Access server login password	Required.
IP address of the Telnet client host	Displayed in the Console User field of the SHOW SERVER STATUS display if a Telnet host is using the port. If the port is idle, this field displays the text “None Available.”
Privileged user logout	Another privileged user on a local port can log out on the remote console using the LOGOUT PORT CONSOLE command.

Access Server Manager

Description

The Access Server Manager application is a management tool for access servers. It runs on 32-bit Windows-based operating systems. The Access Server Manager has a graphical user interface that allows you to easily configure some access server features. The Access Server Loader application is integrated with the Access Server Manager.

Functions

Use the Access Server Manager to:

- Download firmware from a PC load host to the access server.
- Download IP address configuration information to the access server.
- Configure the access server network protocols.
- Configure ports for remote access and terminal server functions.
- Configure modems attached to a access server port.
- Configure access server security.
- Configure access server dialer services.
- Make a Telnet console connection to an access server and issue console commands.

Related Information

See the Cabletron *Network Access Software Installation* guide for instructions about installing this application.

Read the Access Server's online help for information about managing the access server.

Chapter 3

User Interface

Overview

Introduction

This chapter describes how to customize and manage the user interface to the access server. The access server provides two features to manage the user interface:

- A command group defines a set of commands that a specified group of users can access and execute.
- A menu provides a customized selection of commands that a specified group of users can select on the terminal screen.

Both command groups and menus can help the access server user avoid repetitive typing.

In This Chapter

This chapter contains the following topics:

- Command Groups and Menus
- Using Command Groups
- Using Menus
- Defining Menus

Command Groups and Menus

Description

In addition to convenience, command groups and menus provide the access server with a security feature. Since command groups and menus both have an associated port list, you can control which users can access them.

Command groups and menus can also enable nonprivileged users to access a subset of privileged commands. Even if command groups and menus contain privileged commands, they are available to any nonprivileged user logged in to a port in the associated port list.

Using Command Groups

Creating a Command Group

To create a command group, follow these steps:

Step	Action
1	Use the CHANGE COMMAND GROUP command to specify a command group name and port list. **Example**: The following defines the command group called SERVICE_A that is available on ports 2, 3, and 5: `Local> CHANGE COMMAND GROUP SERVICE_A PORT 2, 3, 5`
2	Enter the individual commands that define the command group.

Example: Defining a Command Group

The following example shows how to enter individual commands to define a typical command group. In this command group, the values %P1 and %P2 represent place holders for values that you specify when you execute the command group.

```
Local> CHANGE COMMAND GROUP SERVICE_A LINE 10 "CHANGE PORT %P1 LOCK ENABLE"
Local> CHANGE COMMAND GROUP SERVICE_A LINE 20 "CHANGE PORT %P1 DEFAULT PROTOCOL LAT"
Local> CHANGE COMMAND GROUP SERVICE_A LINE 30 "CONNECT LAT %P2"
```

The command group defined in this example does the following for the specified port:

1. Enables lock.
2. Sets the default protocol to LAT.
3. Connects to the LAT service specified.

Executing a Command Group

To execute a command group, use the DO command.

Example: Executing a Command Group

The following example executes the command group SERVICE_A defined in the previous example. When this command executes, it substitutes the value 3 for the port place holder %P1 and SALES for the service place holder %P2.

```
Local> DO SERVICE_A 3 SALES
```

Displaying a Command Group

Use the SHOW COMMAND GROUP command to display a command group.

Example: Displaying a Command Group

The example below shows how to display the SERVICE_A command group.

```
Local> SHOW COMMAND GROUP SERVICE_A

Command Group: SERVICE_A
Enabled on Ports
2 3 5

Line 10:
CHANGE PORT %P1 LOCK ENABLE

Line 20:
CHANGE PORT %P1 DEFAULT PROTOCOL LAT

Line 30:
CONNECT LAT %P2
```

Purging a Command Group

Use the PURGE COMMAND GROUP command to purge a command group. Use this command to delete a line from a command group, delete an entire command group, or delete all command groups.

Example: Purging Command Groups

The following example shows how to use the PURGE command to delete the command groups SERVICE_A, SERVICE_B, and all existing command groups:

```
Local> PURGE COMMAND GROUP SERVICE_A
Local> PURGE COMMAND GROUP SERVICE_B
Local> PURGE COMMAND GROUP ALL
```

Using Menus

Displaying a List of Enabled Menus

To display a list of the menus enabled on a port, use the SHOW MENU command. If you are a privileged user, the SHOW MENU command displays the names of all menus available on the access server.

To enable a menu on a port, you must use the CHANGE MENU command. See section Defining Menu Choices in this chapter.

Example: SHOW MENU Command

The following example shows how to display a list of menus:

```
Local> SHOW MENU
MAIN
HOSTS
SERVICES
```

Entering Menu Mode

To use any menu enabled on the current port, use the nonprivileged ENTER MENU command. If you are a privileged user, the ENTER MENU command enables you to use any menu available on the access server.

Example: Entering Menu Mode

The following example shows how to enter the hosts menu:

```
Local> ENTER MENU HOSTS
```

Assigning a Default Menu to a Port

To assign a default menu to a port, use the DEFINE PORT n DEFAULT MENU command. If a port has a default menu, it displays whenever you:

- Log in to the port.
- Press the Local Break key or enter the Local Switch character while in a host session.
- Log out of a host session.

Example: Assigning a Default Menu

The following example show how to assign the default menu HOSTS to port 2:

```
Local> DEFINE PORT 2 DEFAULT MENU HOSTS
```

Menu Windows

Menus are divided into two windows:

- The menu choices window appears in lines 1 through 20.
- The directions and user input window appears in lines 22 through 24.

The current selection appears in reverse video. To make a selection, use the up- and down-arrow keys to highlight a selection and press the Return key. You can also make a selection by entering the item number to the left of the selection and pressing the Return key.

Windows on Access Server Menus

Figure 3-1 shows a typical access server menu:

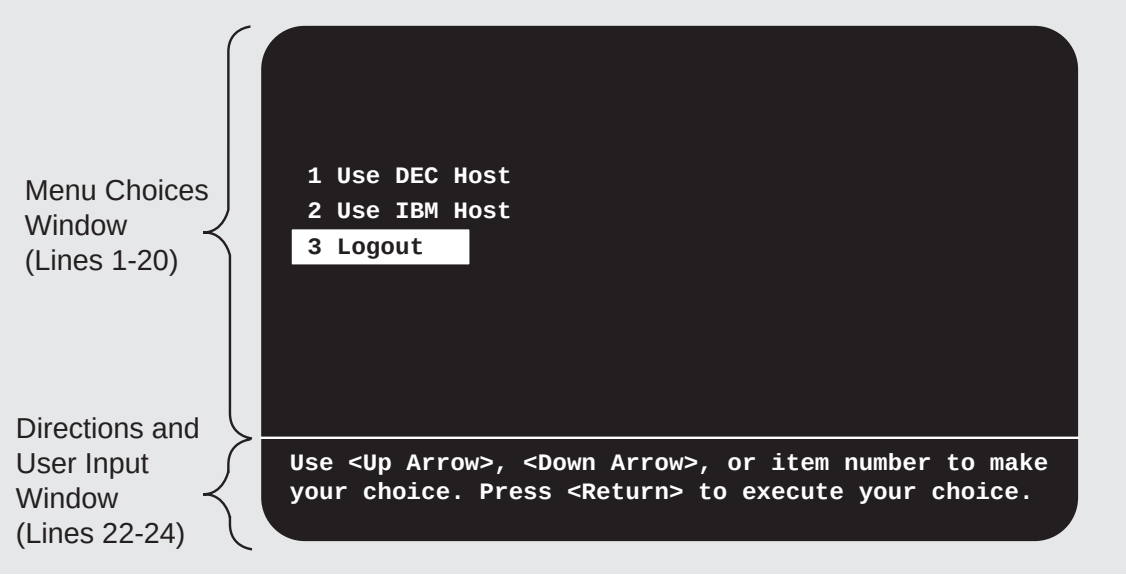


Figure 3-1. Typical Access Server Menu

Defining Menus

Introduction

This section describes how to define menus and provides examples.

Reference

For complete information about the commands mentioned in this section, refer to the Cabletron *Network Access Software Command Reference* guide.

Main Menu

Whenever the server has its factory-set default settings, it stores the main menu in NVRAM. You can display and modify the default menu using the same commands that you use for any other menu.

You may find it convenient to use the main menu as a starting point and an example for creating new menus. For example, to create a new menu entitled SERVICES based on the main menu, enter the following command:

```
Local> CHANGE MENU SERVICES FROM MAIN
```

In effect, the command above copies the main menu and gives the copy the name SERVICES. To modify the menu SERVICES, use the CHANGE MENU command as shown in the Example: Sample Definition of a Menu Selection in this chapter.

Main Menu Display

Figure 3-2 shows how the Main Menu displays on the screen:

LKG-7421-fh8

Figure 3-2. Main Menu Display

Defining Menu Choices

For each menu choice line, you can define:

- One line of display text
- A server command, which can:
  - Specify up to 8 optional input parameters
  - Be a DO command
- A prompt string for each specified input parameter
- A default string for each specified input parameter

Example: Sample Definition of a Menu Selection

The following example shows one way to define the selection Open Telnet Session that appears on line 5 of the main menu:

```
Local> CHANGE MENU MAIN LINE 5 DISPLAY "OPEN TELNET SESSION"
Local> CHANGE MENU MAIN LINE 5 P1PROMPT "ENTER HOST NAME OR IP ADDRESS"
Local> CHANGE MENU MAIN LINE 5 P1DEFAULT "16.195.1.1"
Local> CHANGE MENU MAIN LINE 5 EXECUTE "CONNECT TELNET%P1"
```

The menu selection defined in this example does the following:

1. The following text displays on line 5 of the menu choices window:

   ```
   OPEN TELNET SESSION
   ```

2. When you press the Return key, the following prompt displays in the directions and user input window:

   ```
   ENTER HOST NAME OR IP ADDRESS
   ```

3. The next step depends on whether you simply press the Return key or type a host name or address before pressing the Return key.

   - If you press the Return key without typing a host name or address, the access server executes the CONNECT TELNET command with the default string:

     ```
     CONNECT TELNET 16.195.1.1
     ```

   - If you type a host name or IP address and then press the Return key, the access server executes the CONNECT TELNET command with the specified name or address.

Displaying a Selected Menu

The ENTER MENU command enables you to display any menu that is enabled on the port. If the port is privileged, you can enter a menu whether or not it is enabled on the port.

For example, if the menu HOSTS is enabled on the current port, you enter the following command to display this menu:

```
Local> ENTER MENU HOSTS
```

The menu display has item numbers for all menu lines that have display and execute strings. The item numbers are in order (1, 2, 3, etc.) and usually do not match the line numbers used in SET MENU LINE commands or SHOW MENU displays.

If the port is type ANSI, menu items can be selected by either using the up- and down-arrow keys or by entering the item number. To use the arrow keys, press the up- or down-arrow key until the desired item is highlighted and press Return.

If the port is type SOFTCOPY or HARDCOPY, you can still enter a menu but the arrow keys are disabled. Enter the item number to select a menu item.

Exiting from a Menu

Unless the system manager wants to set up a captive menu (refer to the following section), all menus should have an executable line for LEAVE MENU. To exit from the menu, select this line (which has the display string “GOTO Command Line” on the default menu MAIN).

If the port is privileged, it is also possible to exit from the menu by entering Ctrl/C while the menu is displayed. This prevents you from being “trapped” if you accidentally create and enter a menu without a LEAVE MENU or LOGOUT command.

Using Menus to Set Up a Captive Port

A system manager can use the menus feature to set up a captive port such that users can execute commands from within the menus only. To do this, define a menu that has a LOGOUT command but no LEAVE MENU command, make this menu the default menu for the port, and define the port nonprivileged.

Displaying a Menu Definition

To display the definition for a given menu, use the SHOW MENU command.

Example: Displaying a Menu Definition

The following example shows how to display the definition for the HOSTS menu:

```
Local> SHOW MENU HOSTS

Menu:
Hosts

Enabled on ports:
2, 3, 5

Line 5 Execute:
CONNECT LAT HOST_1

Line 5 Display:
Use DEC Host

Line 7 Execute:
CONNECT TELNET 195.20.0.15

Line 7 Display:
TCP/IP Host
```

```
Line 9 Display
Logout

Line 9 Logout
LOGOUT
```

Purging Menu Lines and Entire Menus

Use the PURGE MENU command to delete a string from a menu line, an entire menu line, an entire menu, or all menus from the access server database.

Example: Commands to Purge Entire Menus and Menu Lines

The following example shows the commands to purge specific menu lines and entire menus:

```
Local> PURGE MENU MAIN LINE 5
Local> PURGE MENU HOSTS
```

Chapter 4

Managing Load Hosts

Overview

Introduction

This chapter describes the command procedures that you use to manage hosts that load the access server software image on a LAT network.

In This Chapter

This chapter contains the following topics:

- DSV$CONFIGURE
- Using a BOOTP / TFTP Server
- Upline Dumping
- Terminal Server Manager (TSM)

Load Host Procedures

Description

The specific command procedure that you use to manage the load host depends on the network version, protocol, and operating system of the load host. The following table lists the available combinations, with a reference to the related section in this chapter:

Load Host Command Procedure	Network	Protocol	Operating System	Refer to:
DSV$CONFIGURE	DECnet Phase IV DECnet/OSI	MDS	OpenVMS	DSV$CONFIGURE
/etc/add_DECserver	TCP/IP	BOOTP/TFTP	UNIX/DIGITAL UNIX	Using a BOOTP/TFTP Server
/etc/list_DECserver	TCP/IP	BOOTP/TFTP	UNIX/DIGITAL UNIX	Using a BOOTP/TFTP Server
/etc/rem_DECserver	TCP/IP	BOOTP/TFTP	UNIX/DIGITAL UNIX	Using a BOOTP/TFTP Server
/etc/upd_DECserver	TCP/IP	BOOTP/TFTP	UNIX/DIGITAL UNIX	Using a BOOTP/TFTP Server
Access Server Loader and Access Server Manager	TCP/IP	BOOTP/TFTP	WindowsNT/ Windows 95	Access Server Manager online help and the DECserver Network Access Software Installation guide

DSV$CONFIGURE

Introduction

DSV$CONFIGURE is a command procedure that runs on a DECnet Phase IV OpenVMS load host or on a DECnet/OSI OpenVMS load host. This procedure enables you to:

- Maintain configuration information about access servers.
- Modify the local MOP (Maintenance Operation Protocol) client configuration.
- Access the remote console port of the access server.

DSV$CONFIGURE is provided as part of the access server software. For information about installing DSV$CONFIGURE, refer to the installation guide provided with the access server software.

Backward Compatibility of DSV$CONFIGURE

DSV$CONFIGURE supports both DECnet Phase IV and DECnet/OSI Phase V. Upon installation, DSV$CONFIGURE automatically converts databases created by DSVCONFIG to the data format required by DSV$CONFIGURE.

Executing DSV$CONFIGURE

The procedure DSV$CONFIGURE.COM is located in the following directory:

```
SYS$COMMON:[DECSERVER]
```

Execute this procedure as follows:

```
$ @SYS$COMMON:[DECSERVER]DSV$CONFIGURE
```

Defining Symbols

You may find it useful to define a symbol for this procedure in your LOGIN.COM file. For example:

```
$ DSV == "@SYS$COMMON:[DECSERVER]DSV$CONFIGURE"
```

Example: Starting DSV$CONFIGURE and Displaying Help

The following example shows how to use the symbol DSV to start DSV$CONFIGURE. This example also shows how to use HELP to display a list of DSV$CONFIGURE commands. The remainder of this section explains each command shown.

```
$ DSV
%DSV-I-IDENT, executing DSV$CONFIGURE version x.x.x-nnn -
DSV-I-HELP, type ? any time for help

DSV> HELP

ADD     - Add a server to the system
MODIFY  - Modify an existing server's information
SET     - Synonym for MODIFY
DELETE  - Remove a comm. server from the system
LIST    - Display information about one or all servers
SHOW    - Synonym for LIST
CONNECT - Connect to a server via remote console
USE     - Synonym for connect
HELP    - Displays summary of valid commands
EXIT    - Exit this procedure
```

ADD Command

To add an access server to the system, use the following command format:

```
ADD [SERVER] [server-name]
```

The following table describes the command syntax:

Command Component	Description
SERVER	An optional keyword as in all DSV$CONFIGURE commands.
server-name	An optional way to specify the name. If you do not specify the name on the command line, DSV$CONFIGURE prompts you for it.

After you enter the ADD command, DSV$CONFIGURE displays a series of prompts. Some prompts display with defaults specified in square brackets. The values of the defaults are based on the running system.

Example: DSV$CONFIGURE ADD Command

This example shows the ADD command on a DECnet/OSI system. In this example, at the end of each line you must press return to continue.

```
DSV> ADD SERVER
_Server Name: DGD700
_Ethernet Address: 08-00-2B-26-AE-32
_Server Type: DS700
_Service Circuit [SVA-0]:
_Maintenance Password [none]: FEDCBA _Dump File
[MOP$DUMP:DS7DGD700.DMP]:
_Load Image [MOP$LOAD:WWENG2.SYS]:
```

After entering the ADD command, you can display information about the MOP client with the:

- DSV$CONFIGURE LIST command
- NCL SHOW command for DECnet/OSI
- NCP SHOW NODE command for DECnet Phase IV

If you use DECnet Phase IV, the required DECnet address prompt has a default of the first unused address in area 13. You no longer need to enter an external SHOW NODE 13.* command prior to adding an access server.

MODIFY and SET Commands

The MODIFY and SET commands operate in a manner similar to the ADD command. These commands provide defaults for each prompt. The defaults are the existing values for the server.

The syntax, prompts, and displays for the SET and MODIFY commands are similar to those for the ADD command.

DELETE Command

The DELETE command removes an access server. This command clears both the permanent configuration data stored on disk and the operational data stored in memory.

The syntax of the DELETE command is identical to that for the ADD command.

Example: DELETE Command for DSV$CONFIGURE

The following example shows the DELETE command. This example omits the optional SERVER keyword. In this example, NCL displays the message NODE 0 MOP Client DGD700 on a DECnet/OSI system. NCP displays a similar message on a DECnet Phase IV system.

```
DSV> DELETE DGD700
Server:              DGD700            Circuit:          SVA-0
Address:         08-00-2B-26-AE-32     Maint. Password: FEDCBA
Type:              DS700
Dump File:         MOP$DUMP:DS7DGD700.DMP
Image File:        MOP$LOAD:WWENG2.SYS
Are you SURE you want to delete this server??? [No]: YES
Node 0 MOP Client DGD700 at 1992-10-26-13:31:29.378-05:00I0.176
```

LIST and SHOW Commands

The LIST and SHOW commands display information about an access server. The syntax of the LIST command is identical to that for the ADD command with one exception: server-name can be a wildcard character.

Example: LIST Command for DSV$CONFIGURE

The following example shows the data that the LIST and SHOW commands display. In this example, the DECnet address would also display if this were a DECnet Phase IV node.

```
DSV> LIST SERVER
_Server Name:   DGD700
Server:         DGD700              Circuit:          SVA-0
Address:      08-00-2B-26-AE-32     Maint. Password: FEDCBA
Type:           DS700
Dump File:      MOP$DUMP:DS7DGD700.DMP
Image File:     MOP$LOAD:WWENG2.SYS
```

CONNECT and USE Commands

The CONNECT and USE commands enable you to communicate with the remote console port on the access server. DSV$CONFIGURE uses CCR to make the connection. Once DSV$CONFIGURE makes the connection, you can use most any access server command supported at any physical port.

Example: CONNECT Command for DSV$CONFIGURE on a DECnet/OSI System

The following example shows how to use CCR and DSV$CONFIGURE to connect to a remote console port from a DECnet / OSI system:

```
DSV> USE DGD700
%CCR-I-CONNEST, connection established to remote system 08-00-2B-26-AE-32
Press CTRL/ \ to disconnect, CTRL/] to send break
# ACCESS (not echoed)
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 0
00:16:47
(c) Copyright 1999, Cabletron Systems, Inc. - All Rights Reserved
Please type HELP if you need assistance
Enter username> Dave
Local> SHOW USER
Port                  Username Status              Service
3                              Connected
10                    User 10  Connected
11                    TELNET   Local Mode
Local> <Ctrl/\>
```

Example: CONNECT Command for DSV$CONFIGURE on a DECnet Phase IV System

The following example shows how to use CCR and DSV$CONFIGURE to connect to a remote console port from a DECnet Phase IV system. From a user's perspective, the only difference between DECnet / OSI and DECnet Phase IV is the disconnect character:

- DECnet / OSI Phase V uses Ctrl / \ (backslash).
- DECnet Phase IV uses Ctrl / D.

```
DSV> USE DGD700
Console connected (press CTRL/D when finished) - ACCESS Network
Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x
Uptime: 0 00:16:52
(c) Copyright 1999, Cabletron Systems, Inc.  - All Rights Reserved
Please type HELP if you need assistance
Enter username> Dave
Local> <CTRL/D>
```

Context-Sensitive Help for DSV$CONFIGURE

DSV$CONFIGURE provides context-sensitive help. At any prompt other than the Local> prompt after a CONNECT / USE command, type a question mark (?) for an explanation.

Using a BOOTP/TFTP Server

Introduction

A BOOTP / TFTP server is a UNIX host that downloads the access server software using the BOOTP and TFTP protocols. The BOOTP / TFTP server stores the information necessary to downline load the access server software in the /etc/bootptab file.

Reference

For information about installing and configuring a BOOTP / TFTP server refer to the Cabletron *Network Access Software Installation* guide.

IP Address Configuration Via BOOTP

The Cabletron Network Access Software contains enhanced BOOTP functionality. The access server stores several important Internet parameters from the BOOTP server. This ability to store data for future use may be used whether the access server operating software is loading from FLASH RAM, or via a load host using the MOP protocol. The factory default settings for this feature now send a BOOTP request on the network in order to obtain one if the access server unit does not have an IP address defined in NVRAM. Customers who do not wish to run IP on their access server, and, therefore, may wish to disable this feature, may issue the DEFINE INTERNET DISABLE command to explicitly disable it.

The parameters that the access server unit can obtain from the BOOTP server include the Internet (IP) address, subnet mask, default gateway address, and domain name server address. The BOOTP server stores the information for the default domain only; it will always store the IP address. The other parameters are BOOTP vendor extensions and may or may not be learned, depending on the capabilities of the BOOTP server used, and the configuration of data in the BOOTP server database.

Remote Connection Password

CNAS has a password feature for remote logins, similar to the main login password. CNAS uses a single value for the remote password server-wide that is separate from the main login password. The factory default value is the same, however, for both the remote login password and the main login password.

Each port enabled for remote or dynamic access, may have its remote password feature individually enabled or disabled. This feature is useful for both reverse LAT services or Telnet listeners. CNAS uses the remote password, in addition to the LAT service password, when the LAT service is password-protected. When a host initiates a login to a remote password-protected port on the server, the server displays the '-' prompt. The customer can use this feature in a variety of ways. For example, the customer can use this feature for creating password-protecting modem pools that can be accessed via a Telnet listener.

Upline Dumping

Introduction

The access server upline dumps its memory when:

- An unexpected failure occurs.
- You force a crash.

The access server always dumps to a load host with the protocol that was used for its download. After an upline dump, the access server automatically reinitializes.

Reference

To send a dump file to your authorized service provider for evaluation, follow the procedure described in the Cabletron *Network Access Software Problem Solving* guide.

Upline Dumps with MOP Hosts

If the access server uses the MOP protocol, check the Dump Address field in the display for the SHOW SERVER STATUS command. This 12-digit hexadecimal number is the Ethernet address for the load host that received the most recent upline dump.

If the dump host is running DECnet software, you can convert the Ethernet address of the dump host to the DECnet node address of the dump host. A formula for this conversion appears in the DECnet documentation for the operating system of the dump host.

When you use the Add option of DSV$CONFIGURE, the command procedure assigns a name for the access server dump file. When a dump occurs, MOP takes the data and creates the dump file. If the access server dumps more than once, MOP creates new versions of the file.

Upline Dumps with BOOTP/TFTP Hosts

Load hosts that use BOOTP and TFTP protocols store upline dumps in the file that you created when you configured the load host.

Refer to the Cabletron *Network Access Software Installation* guide.

Terminal Server Manager (TSM)

Introduction

TSM is a utility that runs on OpenVMS load hosts. TSM enables you to configure and manage the access servers on the same extended LAN.

TSM is not included in the access server software and must be purchased separately.

Reference

For more information about TSM, refer to the Terminal Server Manager Installation and Use manual.

For TSM Users

If you use TSM, do not use DSV$CONFIGURE or NCP to update the DECnet database. By not using DSV$CONFIGURE and NCP with TSM, you can avoid accidentally overwriting access server information from TSM.

Chapter 5

Managing Directed TFTP

Overview

Directed TFTP is a feature that allows the Access Server to load from a single, pre-specified TFTP server. Once configured for Directed TFTP, the Access Server ROM firmware downloads its operating image from the specified TFTP server rather than soliciting a response from a BOOTP server. Directed TFTP makes it easier for the Access Server to obtain an operating image over the wide area network (WAN).

In This Chapter

This chapter includes the following information:

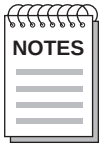
- How to configure Directed TFTP on an Access Server

Configuring Directed TFTP on an Access Server

Directed TFTP requires a minimum ROM code revision to be resident in the Access Server. The minimum revision of ROM firmware is V5.1 for the DECserver 90M and V7.1 for the DECserver 700, DECserver 900 models, and Cabletron Access Server models.

Before you start, you must know the following information:

- The IP address of the Access Server
- The IP address of the default gateway (for routed access)
- The IP address of the TFTP server
- The image name on the TFTP server (if it is not the default)
- If the Access Server has V2.3 (or later) software preloaded in FLASH RAM or if a BOOTP server for loading V2.3 (or later) software is available to the Access Server



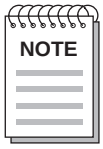
You will need the default gateway IP address if the TFTP server is not in the same IP LAN subnet as the Access Server.

If the Access Server did not ship from the factory with the required minimum revision of ROM firmware, and the Access Server has not been reset to the factory default parameters, then you must purge or redefine the existing default gateway information using the Access Server command line interface PURGE and DEFINE commands.

For an Access Server that is already running V2.3 (or later) software (e.g. from FLASH RAM) perform the following steps to configure the Access Server for Directed TFTP (DTFTP) loading using the Access Server command line interface:

Step	Action
1	Ensure that the Access Server has an IP address configured (SHOW INTERNET). If not, use the DEFINE INTERNET MASK nnn.nnn.nnn.nnn and DEFINE INTERNET ADDRESS nnn.nnn.nnn.nnn commands to define the IP address.
2	Ensure that the Access Server has a default gateway configured, if required by your network topology (SHOW INTERNET GATEWAY). If not, use the DEFINE INTERNET GATEWAY nnn.nnn.nnn.nnn ANY command to define one.

Step	Action
3	Define the Directed TFTP server host address using the DEFINE SERVER TFTP HOST nnn.nnn.nnn.nnn command. For example: Local> DEFINE SERVER TFTP HOST ADDRESS 192.444.10.2
4	Ensure that the Access Server load image name matches the filename used at the TFTP server's default directory location (LIST SERVER). If not, use the DEFINE SERVER SOFTWARE aaaaaaaaa command to modify the filename. For example: Local> DEFINE SERVER SOFTWARE MYDS900



You may also configure DTFTP using the Access Server Manager V2.3 (or later) user interface.

For an Access Server that is not already running V2.3 (or later)software, to perform a Directed TFTP image load, you must intervene in the boot process using the ROM firmware Mini-Monitor. Follow these steps:

Step	Action
1	Connect a terminal or terminal emulator to the Access Server console port, Port 1, at 9600 baud.
2	Boot the Access Server.
3	Once the boot status messages appear, enter Ctrl/B twice. You will receive a Mini-Monitor command prompt that looks like this: >>>.

4	Temporarily set the Access Server IP address, default gateway IP address, if required, and the TFTP server IP address, using the "S" command to set the Access Server IP address (ip=nnn.nnn.nnn.nnn), default gateway address (gw=nnn.nnn.nnn.nnn), and the TFTP server IP address (tftp=nnn.nnn.nnn.nnn). For example:
	
	`>>> s ip=192.444.2.3`
	`>>> s gw=192.444.5.1`
	`>>> s tftp=192.444.3.3`

Step	Action

5	Initiate a boot from using the Access Server's Ethernet interface, by entering the "B" command at the prompt. For example:
	
	`>>> b eth:mneng2 (for DECserver 90M)`
	`>>> b eth:wweng2 (for DECserver 700 or 900 or Access Server 316)`

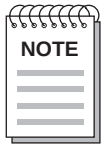
6	Once the software load is complete, follow the steps listed in the previous table to make the configuration of the DTFTP information permanent.

To permanently disable Directed TFTP from the DNAS command line prompt, DEFINE the TFTP HOST to NONE. For example:

```
Local> DEFINE SERVER TFTP HOST NONE
```

To temporarily disable Directed TFTP from the ROM firmware Mini-Monitor command line prompt, set the TFTP server IP address to zero. For example:

```
>>> s tftp=0
```



When DTFTP is configured on an access server and a network load is specified (excluding a FLASH RAM load), the Access Server ROM firmware will revert to loading from FLASH RAM after several unsuccessful retries of DTFTP loading.

Chapter 6

Initializing the Access Server

Overview

Introduction

This chapter describes how to initialize the access server. Initializing the access server reloads the software image.

Initializing the access server does not affect the configuration settings stored in NVRAM. To reset the access server to the factory-set defaults, you need to reboot the access server and press the appropriate switch on the hardware unit. For details about this procedure, refer to the hardware documentation provided with the access server.

In This Chapter

This chapter contains the following topics:

- Preparing LAT Services for Initialization
- Preparing Telnet Listeners for Initialization
- Initializing the Access Server
- Using NCP to Initialize the Access Server
- Booting from the Network
- Booting Using Console Commands

Preparing LAT Services for Initialization

Do This

If the access server offers LAT services, follow these steps before you initialize:

Step	Action
1	Enter the following command to disable queuing on the access server: `Local> SET SERVER QUEUE LIMIT 0`
2	Disable additional connections to local services. For example, the following command disables the service LASER: `Local> SET SERVICE LASER CONNECTIONS DISABLED`

3	Check that the queue is empty before starting the initialization procedure by entering one of the following commands:
	
	`Local> SHOW QUEUE ALL`
	or
	`Local> SHOW SERVER STATUS`

The time that it takes for the queue to empty depends upon the number of requests that it contains.

Preparing Telnet Listeners for Initialization

Do This

If the access server has Telnet listeners, follow these steps before you initialize:

Step	Action
1	Disable further Telnet connections. The network access server fails to execute the SET TELNET LISTENER CONNECTIONS DISABLED command if a session exists on the specified listener. **Example**: The following command disables Telnet connections on TCP port 2005: `Local> SET TELNET LISTENER 2005 CONNECTIONS DISABLED`
2	Log out the port. **Example**: The following command logs out port 5: `Local> LOGOUT PORT 5`

Initializing the Access Server

Using the INITIALIZE Command

To use the INITIALIZE command, log in to one of the following:

- A terminal attached to the access server
- The remote console port

Login Methods

You can use any of the following methods to log into the remote console port:

- NCP
- SET HOST/MOP
- CCR
- Telnet remote console

Refer to Remote Console Port section in Chapter 2 for additional information about the remote console port.

Default Mode for the INITIALIZE Command

To use the INITIALIZE command in its default mode of operation, enter the following:

```
Local> INITIALIZE
```

In this mode of operation, the following steps occur:

Step	Action
1	If the access server has Flash capabilities and the image name stored in NVRAM matches the image name stored in Flash, the access server loads the image from Flash RAM.
2	If there is no image in FLASH or the access server lacks FLASH capabilities, the access server loads the software image from a load host on the network.

If there is no image in FLASH or the access server lacks FLASH capabilities, the access server loads the software image from a load host on the network.

Specifying Initialization from a Load Host

To specify initialization from a network load host, use the following command:

```
Local> INITIALIZE FROM ETHERNET
```

This command causes the access server to request the image name stored in its NVRAM from a load host.

Specifying an Image Name When Initializing

You can specify the name of an image when initializing. For example, the following command causes the access server to request the image named WWENG2 from a load host:

```
Local> INITIALIZE FROM ETHERNET IMAGE WWENG2
```

Specifying Initialization from Flash RAM

If a access server has Flash capabilities, you can specify initialization from the image stored in Flash RAM by using the following command:

```
Local> INITIALIZE FROM FLASHRAM
```

Updating Flash RAM

If a access server has Flash capabilities, you can update the image stored in Flash RAM with an image from a network load host. Use the following command:

```
Local> INITIALIZE FROM ETHERNET UPDATE FLASHRAM
```

This command causes the access server to request the image name stored in NVRAM from a load host to update Flash RAM.

Specifying a Delay Value with INITIALIZE

When you enter the INITIALIZE command, you can specify a delay value as shown in the following example:

```
Local> INITIALIZE DELAY 10
```

This command causes the access server to wait 10 minutes before initializing.

The range for the delay value is from 0 to 1440 minutes. The default delay value is 1.

Using the DIAGNOSE Option with INITIALIZE

Using the DIAGNOSE option with INITIALIZE enables you to test the access server hardware. You can specify three types of tests as described in the INITIALIZE DIAGNOSE Option Tests.

The following example shows the DIAGNOSE option with INITIALIZE:

```
Local> INITIALIZE DIAGNOSE FULL
```

This command initializes the access server in the default mode and performs an extended test.

INITIALIZE DIAGNOSE Option Tests

The following table shows the tests that are available as part of the INITIALIZE DIAGNOSE option:

Test	Performs
Brief	Internal self-test only.
Full	Extended test including in-depth memory test
Normal (Default)	Standard self-test.

Specifying the DISABLE OPTION with INITIALIZE

Using the DISABLE option with INITIALIZE loads the software image, but disables the use of the CONNECT command and the AUTOCONNECT function. The following command shows how to use this option:

```
Local> INITIALIZE DISABLE
```

Using NCP to Initialize the Access Server

NCP Initialization Commands

The following table shows the NCP commands used to initialize the access server if you are on a load host:

NCP Initialization Commands	Description
LOAD	Ensures that the host at which you issue the command is the node that performs the load.
TRIGGER	Causes the access server to load the software image from any host on the network.

The NCP LOAD and TRIGGER commands do not have any automatic warning or delay options. However, you can warn users about an impending initialization by using the access server BROADCAST command.

NCP Reference

For more information about NCP, refer to the documentation provided with the host system.

Booting from the Network

Loading the Software Image

If your network server is configured with Flash RAM, but does not have the correct image, the access server performs a network load.

Determining Boot Protocols

During the network boot sequence, the access server searches for a load host. The access server tries both MOP and BOOTP protocols in a factory-defined order. The boot sequence includes a wait period after passing through all the boot protocols. Once the access server finds a load host, it records the protocol and load host in its permanent database. The software is then downline loaded from the load host.

Reference

For more information about installing the software, refer to the Cabletron *Network Access Software Installation* guide.

Booting Using Console Commands

Introduction

Console functions require access server ROM Version 4.0 or greater.

If you program Flash RAM with a nonstandard boot image name and a load host is not available, pressing the reset-to-factory button may leave the access server unbootable.

Procedure

To allow booting of a nonstandard boot image name, perform the following steps:

Step	Action
1	During the boot sequence of the access server initialization process, press Ctrl/B two times consecutively on the port defined as the console port. The boot process stops and the access server returns the following console prompt: >>>
2	At the >>> prompt, you can enter H to invoke help. Entering H provides help text to describe the interactive boot mode commands available. The Boot Command Options section in this chapter lists the boot mode commands and summarizes the help text that appears when you invoke H.
3	Choose one of the boot command options listed in the Boot Command Options section in this chapter.

Boot Command Options

The following table lists the command options you can select for the boot command:

Option	Definition	Associated Options
B	This command, without an argument, starts a new boot sequence to load the access server with an executable image using the default boot parameters.	-
B name	This command and the argument name specifies a nonstandard boot image. The access server looks for the software name; first from Flash RAM, then from the network.	B MNENG — This command instructs the access server to look for the MNENG2 software image first in Flash RAM, then from the network. b /tftp/serversw — This command instructs the access server to look for image /TFTP/SERVERSW; first in Flash RAM, then from the network. If you want lowercase letters, you have to use quotation marks. For example: `b "/tftp/serversw"` B "" — This command and the quotation marks (explicit null name) instruct the access server to search for any image in Flash RAM. If the access server is unable to find an image in Flash RAM, then it loads from the network. The network load host defines this software and is typically based on the Ethernet MAC address of the access server.

Option	Definition	Associated Options

B media:name	In this command, the media part of media:name specifies which boot media to use.	FLA: — Use Flash RAM. For example:
		`B FLA:MNENG2`
		ETH: — Use the network to find a load host. For example:
		`B ETH:MNENG2`
		FLA:ETH: — Use Flash RAM first, and if that does not work, then use the network to find a load host. For example:
		`B FLA:ETH:MNENG2`

B/M	This command boots the maintenance mode software for the access server. The network load host defines this software and is typically based on the Ethernet MAC address of the access server.	-
B/S	This command boots the standard system software for the access server. The network load host defines this software and is typically based on the Ethernet MAC address of the access server.	-
H	This command displays the help text that describes the interactive boot mode commands.	-
I	This command initializes the access server using the default boot parameters. The access server performs all normal self-tests.	-

Option	Definition	Associated Options
R	This command resets the factory-settings and initializes the access server. This command requires verification. Enter YES if you want to reset the access server to factory settings.	-

S	This command sets parameters for the current boot cycle only	`S ip=nnn.nnn.nnn.nnn`
		
		This command sets the IP address of the access server. Use it with the directed TFTP feature.
		
		`S gw=nnn.nnn.nnn.nnn`
		
		This command sets the IP default gateway address of the access server. Use it with the directed TFTP feature.
		
		`S tftp=nnn.nnn.nnn.nnn`
		
		This command sets the IP address of the TFTP server to be used to load the access server's operating image. This command also sets the directed TFTP feature to ENABLED.
		
		`S tftp=0`
		
		This command sets the directed TFTP feature to DISABLED.

Chapter 7

Configuring LAT Characteristics

Overview

In This Chapter

This chapter describes how to configure the LAT characteristics for the access server. This chapter contains the following topics:

LAT Characteristics

Preparing to Change LAT Characteristics

Before you change LAT characteristics, make sure to:

- Install the latest software image on the access server and all load hosts.
- Read the release notes.
- Know what devices and cables are connected at the various ports.
- Enter the SET PRIVILEGED command for the port.
- Check if the current values or default values are appropriate.

LAT Characteristic Summary

To modify a LAT characteristic, use the SET / DEFINE / CHANGE command for the appropriate characteristic. The following table summarizes the access server LAT characteristics:

Characteristic	Default	Range	Refer to Section
ANNOUNCEMENTS	Enabled	-	ANNOUNCEMENTS Characteristic
CIRCUIT TIMER	80 milliseconds	30 to 200	CIRCUIT TIMER Characteristic
IDENTIFICATION	None	-	IDENTIFICATION Characteristic
KEEPALIVE TIMER	20 seconds	–	KEEPALIVE TIMER Characteristic
MULTICAST TIMER	30 seconds	10 to 180	MULTICAST TIMER Characteristic
NAME	LAT_ethernet-address	-	SERVER NAME Characteristic
NODE LIMIT	200	1 to 1000	NODE LIMIT Characteristic
NUMBER	0	0 to 32,767	SERVER NUMBER Characteristic

Characteristic	Default	Range	Refer to Section
PASSCHECK	200	0 to 200	PASSCHECK Characteristic
QUEUE LIMIT	100	0 to 200	QUEUE LIMIT Characteristic
RESPONDER	Disabled	-	RESPONDER Characteristic
RETRANSMIT LIMIT	8	4 to 120	RETRANSMIT LIMIT Characteristic
SERVICE GROUPS	0 ENABLED, 1 to 255 DISABLED	0 to 255	Service Groups

Displaying LAT Characteristics

Command To Use

To display the current LAT characteristics, use the SHOW / LIST / MONITOR SERVER command as shown in the following example.

LAT Characteristics Display Example

The following example shows a typical display that appears when you use the SHOW SERVER command:

```
Local> SHOW SERVER
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 0 00:44:34

Address: 08-00-2B-26-AA-99                    Name: WWDOCMC Number: 0

Identification:
Circuit Timer:                  80              Password Limit:    3
Console Port:                    1              Prompt:          Local>
Inactivity Timer:               30              Queue Limit:     100
Keepalive Timer:                20              Retransmit Limit:   8
Multicast Timer:                30              Session Limit  :   64
Node Limit:                    200              Software:      WWENG1

Service Groups:          42, 46, 66

Enabled Characteristics:
Announcements, Broadcast, Dump, Lock, Server Responder

Local>
```

ANNOUNCEMENTS Characteristic

Introduction

The ANNOUNCEMENTS characteristic determines if the access server sends LAT multicast messages about local services over the Ethernet. The access server does not send any announcements if no local services are defined.

Configure Announcements Example

The following example shows how to enable and disable the announcements characteristic:

```
Local> CHANGE ANNOUNCEMENTS ENABLED
Local> CHANGE ANNOUNCEMENTS DISABLED
```

CIRCUIT TIMER Characteristic

Introduction

The CIRCUIT TIMER characteristic defines the interval at which the access server sends virtual circuit messages to the LAT service node. This value is important for balancing fast response time and network utilization against optimal service node performance.

The circuit timer value ranges from 30 to 200 milliseconds. The default is 80 milliseconds, which is recommended for normal interactive functions.

Changing the CIRCUIT TIMER

To change the circuit timer, use the command shown in the following example:

```
Local> CHANGE SERVER CIRCUIT TIME milliseconds
```

Increasing the CIRCUIT TIMER

As you increase the circuit timer value, the LAT protocol overhead decreases on the access server, service node, and network. A slower terminal response time, however, is the trade-off for any increased circuit timer value.

Decreasing the CIRCUIT TIMER

If you reduce the circuit timer value, the access server port buffers are less likely to fill between virtual circuit messages. If you have a file transfer with no flow control between a port and a device, a lower circuit timer value can mean fewer data overrun errors at the port. Therefore, a reduced circuit timer value may enable file transfers to run at increased speeds.

IDENTIFICATION Characteristic

Introduction

The IDENTIFICATION characteristic is a string that can be up to 40 characters long. This string displays:

- Under the welcome banner during a login procedure
- In the SHOW SERVER displays

The access server also uses the identification string when it multicasts messages about the availability of services.

Changing the Server Identification String

To change the server identification string, use the following command:

```
Local> CHANGE SERVER IDENTIFICATION "newID"
```

Removing an Identification String

To remove an identification string, specify a null string by using the following command:

```
Local> CHANGE SERVER IDENTIFICATION ""
```

The null string is the default identification string.

Identification String in a Login Procedure Display

The following example shows how the identification string Personnel Printers displays during a login procedure:

```
Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 0
00:16:58 Personnel Printers
(c) Copyright 1998, Cabletron Systems, Inc.  - All Rights Reserved
Please type HELP if you need assistance
Enter username>
```

KEEPALIVE TIMER Characteristic

Introduction

The KEEPALIVE TIMER characteristic maintains a virtual circuit between the access server and service node when no messages are exchanged over a period of time. If the keepalive timer expires, the access server sends a message to determine if the service node is still reachable. If the service node fails to respond, the access server can time out the virtual circuit.

Keepalive Timer Default Values

The keepalive timer value is a trade-off between fast circuit-down detection and unnecessary network traffic. The factory-set default value of 20 seconds represents a good compromise. For a heavily loaded Ethernet, use a value from 60 to 180. For applications that require quick notification of a service node failure, use 10 seconds.

Keepalive Timer Example

The following example shows how to change the keepalive timer to 10 seconds:

```
Local> CHANGE SERVER KEEPALIVE 10
```

MULTICAST TIMER Characteristic

Introduction

The MULTICAST TIMER characteristic determines the interval at which a service node sends service announcements.

Multicast Timer Default Values

You can specify a value from 10 to 180 seconds. The default value is 30 seconds.

Changing Multicast Timer Values Example

The following example shows how to change the multicast timer value:

```
Local> CHANGE SERVER MULTICAST TIMER 50
```

ACCESS SERVER NAME Characteristic

Introduction

The SERVER NAME characteristic is a string of 1 to 16 characters. This name must be unique on the LAT network. When the access server offers a service, it periodically multicasts the name over the local area network.

Default Access Server Name

The default access server name is LAT_ethernet-address. This value is the 12-digit hexadecimal Ethernet address of the access server. This address does not contain hyphens.

Changing the ACCESS SERVER NAME

Use the DEFINE/SET/CHANGE SERVER NAME command to change this characteristic. The following example shows how to change the access server name to “Printing”:

```
Local> CHANGE SERVER NAME PRINTING
```

NODE LIMIT Characteristic

Introduction

The NODE LIMIT characteristic specifies the maximum number of LAT service nodes that the access server maintains in its node database. The range is from 1 to 2000, and the default is 200.

You can also specify a node limit of NONE. This keyword indicates that the only limit is the available memory of the access server.

Changing the Access Server NODE LIMIT

Use the DEFINE / SET / CHANGE SERVER NODE LIMIT command to change this characteristic. The following example shows how to change the node limit to 300:

```
Local> CHANGE SERVER NODE LIMIT 300
```

Access SERVER NUMBER Characteristic

Introduction

Each access server has a number that uniquely identifies it.

Access SERVER NUMBER Values

This number is a value from 0 to 32,767. The default is 0.

When the access server offers a service, it periodically multicasts the number over the network.

Changing the Access SERVER NUMBER

Use the DEFINE / SET / CHANGE SERVER NUMBER command to change this characteristic. The following command shows how to change the access server number to 35:

```
Local> CHANGE SERVER NUMBER 35
```

PASSCHECK Characteristic

Introduction

The PASSCHECK characteristic determines whether a host is required to provide a password as part of a host initiated contact (HIC) request to a password-protected local service. With PASSCHECK disabled, HIC requests are not required to supply a password. With PASSCHECK enabled, HIC requests are required to supply a password.

Changing the PASSCHECK Characteristics

The factory default for the PASSCHECK characteristic is DISABLED. To change this characteristic, use the DEFINE/SET/CHANGE SERVER PASSCHECK command.

PASSCHECK Characteristic Example

The following example shows how to enable the PASSCHECK characteristic:

```
Local> CHANGE SERVER PASSCHECK ENABLED
```

QUEUE LIMIT Characteristic

Introduction

The LAT QUEUE LIMIT characteristic specifies the maximum number of outstanding connection requests for remote access to access server ports. The range is from 0 to 200, and the default is 100.

Special QUEUE LIMIT Values

Two values have special meaning:

- The value 0 disables the queue.
- The keyword NONE places no limit on connection requests.

Changing the QUEUE LIMIT

To change queue limit characteristic, use the DEFINE/SET/CHANGE SERVER QUEUE LIMIT command. The following example shows how to change the queue limit to NONE:

```
Local> CHANGE SERVER QUEUE LIMIT NONE
```

RETRANSMIT LIMIT Characteristic

Introduction

The RETRANSMIT LIMIT characteristic specifies the number of times that the access server resends a message without an acknowledgment. After the specified time limit, the access server times out the circuit. If other service nodes offer the same service that timed out, the access server attempts automatic failover.

RETRANSMIT LIMIT Values

The retransmit limit range is from 4 to 120. If traffic load is heavy or the network experiences noise problems, set the value higher than the default value of 8. On the other hand, if rapid error detection is important, you may want to specify a lower value.

Changing the RETRANSMIT LIMIT Characteristic

To change the RETRANSMIT LIMIT characteristic, use the DEFINE/SET/CHANGE SERVER RETRANSMIT LIMIT command. The following example shows how to change the retransmit limit to 100:

```
Local> CHANGE SERVER RETRANSMIT LIMIT 100
```

RESPONDER Characteristic

Access Server Mapping

In order to connect to other nodes on the LAN, the access server must be able to map node names, port names, and services to specific nodes.

Datagram Types

LAT provides the following specific types of datagrams that facilitate this mapping:

Datagram Name	Description
Service Announcement	A mulicasted datagram used by slave nodes to advertise services
Solicit Information	A multicasted or physically addressed datagram used by any node to solicit service information from another node
Response Information	A physically addressed datagram sent in response to a received Solicit Information message

LAT V5.2 nodes operating as LAT masters can address Solicit Information datagrams to V5.2 slave nodes and be almost assured of a direct response. However, nodes operating as V5.1 masters can only address Solicit Information datagrams to other V5.1 masters since V5.1 slaves do not enable multicast addresses for the reception of directory service datagrams. Therefore, V5.1 and V5.2 nodes are allowed to respond to Solicit Information datagrams for slave nodes that cannot respond for themselves.

The RESPONDER characteristic determines whether the access server may act as an agent for other nodes. By configuring one or more access servers to act as responders, the other access servers can operate with a node limit of 1 and still be assured access to LAT services. This frees up the dynamic memory and reduces the overhead that would otherwise have been required to maintain the LAT node database.

Changing the RESPONDER Characteristic

The factory default setting for the RESPONDER characteristic is disabled. To enable it, use the following command:

```
Local> CHANGE SERVER RESPONDER ENABLED
```

Use the SHOW SERVER command to determine the current setting. When the feature is enabled, “RESPONDER” is displayed as one of the enabled characteristics.

Along with enabling the RESPONDER characteristic, you must set the access server group codes so that they intersect those of all the nodes offering the service.

Enabling or disabling the RESPONDER characteristic has no affect on the access server ability to respond to Solicit Information messages for services it offers locally.

Service Groups

Introduction

A service group defines the access that service nodes and port users have to the network. Each service group has an identifying number from 0 to 255.

Viewing Service Groups

To view service groups that have access to services on the access server, use the SHOW SERVER command. (See the LAT Characteristics Display Example section in this chapter.)

Changing Access Server Service Groups

Use one of the following commands:

- To enable service groups on the access server, use the following command:

  ```
  Local> CHANGE SERVER SERVICE GROUPS group-list ENABLED
  ```

- To assign ports to a service group, use the following command:

  ```
  Local> CHANGE PORT port-list AUTHORIZED GROUPS group-list ENABLED
  ```

Changing Service Groups Examples

- The following example shows how to enable service groups 1, 16, and 18:

  ```
  Local> CHANGE SERVER SERVICE GROUPS 1,16,18 ENABLED
  ```

- The following example shows how to assign ports 2, 3, and 5 to service groups 1, 16, and 18:

  ```
  Local> CHANGE PORT 2,3,5 AUTHORIZED GROUPS 1,16,18 ENABLED
  ```

Chapter 8

TCP/IP Network Characteristics

Overview

Introduction

This chapter describes the configuration characteristics for a TCP/IP network. To enable the access server to operate on a TCP/IP network, you need to:

1. Configure the Internet address and subnet mask.
2. Configure the TCP/IP characteristics, for example:
   - List of commonly used Internet hosts
   - List of gateway addresses
   - List of ARP entries
   - TCP keepalive timer
3. Configure domain name characteristics.

In addition, you can configure the access server to automatically learn IP information from other types of servers on the network.

In This Chapter

This chapter contains the following topics:

- Displaying the Internet Counters
- Setting the TCP Keepalive Timer
- Learning IP Information From a BOOTP Server
- Learning IP Information From a DHCP Server
- Assigning WINS Server Addresses

Configuring the Internet Address and Subnet Mask

Tasks

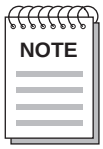
You can perform the following tasks:

- Set an Internet address.
- Set a subnet mask.
- Display the Internet address and subnet mask.

Alternative: Learning IP Information

You can configure the access server to learn IP configuration information from a BOOTP server or a Dynamic Host Configuration Protocol (DHCP) server on the network instead of configuring all of the IP information on the access server manually. See the following sections in this chapter:

- Learning IP Information From a BOOTP Server
- Learning IP Information From a DHCP Server



The access server will not acquire its own IP address from a DHCP server. Use a BOOTP server for this purpose.

Setting the Internet Address

Before the access server can operate on a TCP/IP network, you must assign a Class A, B, or C Internet address. To assign the address on the access server, use a command similar to the one shown in the following example:

```
Local> CHANGE INTERNET ADDRESS 195.1.1.60
```

If you do not intend to use the default subnet mask, you must set or change the subnet mask before you set or change the Internet address.

Setting an Internet Subnet Mask

The Internet subnet mask is used to partition the host section of an Internet address into subnets. The default subnet mask depends on the class of the Internet address that you assigned.

The following table lists these defaults:

Internet Address Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Do Not Define the Subnet Mask in the /etc/bootptab File

Although some BOOTP implementations allow you to define a subnet mask using the /etc/bootptab file, the network access server does not support this feature. For more information, refer to the network access server software installation documentation for your load host.

Changing the Subnet Mask

To change the subnet mask, use the CHANGE INTERNET SUBNET MASK command. The following example shows how to change the subnet mask to 255.255.255.0:

```
Local> CHANGE INTERNET SUBNET MASK 255.255.255.0
```

Changing the Subnet Mask to the Default Value

To return the subnet mask to its default value after changing it, do the following:

Step	Action
1	Enter the following command: `Local> DEFINE INTERNET SUBNET MASK NONE`
2	Reboot the access server.

Supernetted IP Addresses

The CNAS software supports the use of supernetted IP addresses. Supernetting allows you to configure the access server and its ports with a subnet mask shorter than the intrinsic subnet mask (for example, 255.255.255.0 for a Class C address). With supernetting, you can give a Class C subnet mask a range of 255.255.0.0 to 255.255.255.254. This allows you to address a block of Class C IP addresses as a "domain" or a single destination address with more than 254 hosts.

Displaying the Internet Address and Subnet Mask

To display the Internet address and subnet mask, use the SHOW / LIST / MONITOR INTERNET command.

Internet Address and Subnet Mask Display Example

The following example shows how to display the current Internet address and subnet mask for the access server:

```
Local> SHOW INTERNET

State                Enabled
Internet Address:    195.1.1.1
Subnet Mask:         255.255.255.0
DHCP:                Enabled
TCP Keepalive Timer: Disabled
TCP Keepalive Retry: 8
Local>
```

Configuring Domain Name System (DNS) Characteristics

Tasks

This section describes how to display and set the access server characteristics for the Internet domain name system (DNS) to resolve host names into Internet addresses.

You can perform the following tasks:

- Display DNS characteristics.
- Display DNS counters.
- Configure the default name resolution domain.
- Change the time limit.
- Change the retry limit.
- Change the name resolution mode.
- Configure a list of commonly used Internet hosts.
- Configure a list of Internet name servers.

Displaying DNS Characteristics

To display the access server characteristics for the DNS, use the SHOW/LIST INTERNET NAME RESOLUTION command.

Internet DNS Character Display Example

The following example shows how to display the characteristics for the Internet DNS:

```
Local> SHOW INTERNET NAME RESOLUTION
NetBIOS (WINS) Name Resolution:

Primary WINS Server:      16.20.44.55
Secondary WINS Server     wins-server-local (from DHCP)

Domain Name Resolution

Domain Name: finance.acme.com (from DHCP)

Resolution Host Limit:      32 Resolution Time Limit:  4
Resolution Mode:       Ordered Resolution Retry Limit: 3
```

```
Nameservers (Locally configured):
99.99.99.99            Local name.acme.com (from DHCP)

Nameservers (Learned):
99.99.99.99            Local         name.acme.com
88.88.88.88            Local          secondary.acme.com

DHCP server: 16.20.244.250
Local>
```

The following table describes the DNS characteristics that appear in the previous example. (See the Displaying WINS Characteristics section in this chapter for an explanation of the WINS characteristics in the display.)

Field	Description
Domain Name	Name of the access server default domain. If a DHCP server provides this information, the display includes "(from DHCP)" at the end of the line
Resolution Host Limit	Maximum number of host names that can be entered using the SET/DEFINE/CHANGE INTERNET HOST command. Note that this parameter is currently not functional.
Resolution Mode	DNS data retrieval preference: LOCAL, REMOTE, ORDERED, STUB or SLAVE. (See the Name Resolution Modes table in this chapter.)
Resolution Time Limit	Minimum time in seconds between name server retries.
Resolution Retry Limit	Maximum number of times DNS can retry the same name server when looking for a particular Internet host name.
Name Servers (Locally configured)	The Internet address, type (local or root), and absolute domain name of name servers entered by a user. If a DHCP server provides this information, the display includes "(from DHCP)" at the end of the line.
Name Servers (Learned)	The Internet address, type (local or root), and absolute domain name of name servers learned by DNS.

If a DHCP server provides the Domain Name information, the display includes "(from DHCP)" at the end of each line of information and the Internet address of the DHCP server.

Displaying the DNS Counters

To display the DNS counters, use the SHOW/LIST INTERNET NAME RESOLUTION COUNTERS command.

To reset the DNS counter, use the ZERO INTERNET NAME RESOLUTION COUNTERS command.

DNS Counter Display Example

The following example shows how to display the various DNS counters:

```
Local> SHOW INTERNET NAME RESOLUTION COUNTERS
Input Packets:   5 Duplicate Responses: 0
Output Packets:  7 Bad Responses:       0
Total Responses: 5 Truncated Responses: 0
OK Answers:      3 Fail Answers:        0
Total Queries:   2 FORMERR Answers:     0
                   Duplicate Queries:   0
```

The following table describes the information in the previous example:

Field	Description
Input Packets	Number of packets entering the access server from the DNS server.
Output Packets	Number of packets exiting the access server into the DNS server.
Total Responses	Total number of responses received by the access server from the DNS server. This total includes the bad responses, truncated responses, and duplicate responses, along with good responses.
OK Answers	Number of valid answers received from the DNS server.
Total Queries	Number of DNS queries sent by the access server.
Duplicate Responses	Number of identical responses to queries.
Bad Responses	Number of bad responses received. A bad response could be due to: 1. An unrecognizable response from the DNS server. 2. A fail response from the DNS server. 3. A response indicating that DNS could not understand the query from the access server.

Field	Description
Truncated Responses	Number of incomplete (truncated) responses from the DNS server. This is not necessarily an error condition.
Fail Answers	Number of fail answers received. This condition could be caused by a number of events, including: 1. Unable to find a name server to send particular query. 2. Unable to find the Internet address of a particular name server. 3. Sent a query and received more than maximum amount of responses. 4. Query is trapped in a loop of name servers that refer to each other.
FORMERR Answers	Number of answers received that were either not able to be decoded or states that DNS did not understand the query.
Duplicate Queries	Number of duplicate queries sent where the original query is on a pending queue to be sent to its destination.

Configuring the Default Name Resolution Domain

Configuring the default domain name characteristic enables you to abbreviate Internet host names in commands. To configure the Default Name Resolution Domain, use the DEFINE/SET/CHANGE INTERNET NAME RESOLUTION DOMAIN command.

Configuring and Using Default Name Resolution Domain Example

The following example shows the procedure for and results of configuring the default name resolution to FINANCE.ACME.COM:

Step	Action
1	Define the default name resolution domain as follows: `Local> **CHANGE INTERNET NAME RESOLUTION DOMAIN FINANCE.ACME.COM**`
2	Enter the following connect command: `Local> **CONNECT SALES**`

Step	Action
3	In this situation, the access server automatically appends the default name resolution domain to SALES. The access server behaves as if you had typed: `Local> CONNECT SALES.FINANCE.ACME.COM`

4	Enter a command with a higher level domain name:
	
	`Local> CONNECT SALES.REVENUE`
	
	Result: The access server tries a sequence in the following order, using parts of the default domain name:
	
	`SALES.REVENUE.FINANCE.ACME.COM`
	`SALES.REVENUE.ACME.COM`
	`SALES.REVENUE`
	
	The name is likely to be resolved correctly as the access server tries SALES.REVENUE.ACME.COM. The sequence terminates at that point.

Using Trailing Dots

The access server uses a sequence of name resolution attempts when you enter a host name without a trailing dot at the end of the domain name. If you end a name with a trailing dot, the access server does not use a sequence of name resolution attempts. Instead it uses the domain name as you enter it.

For example, suppose that you enter:

```
Local> CONNECT SALES.REVENUE.
```

Because this domain name ends with a dot, the access server does not append the default name resolution domain or any part of that domain.

Changing the Time Limit

The domain name resolution time limit specifies the time that the access server waits before it resends a query to a name server. The range is from 1 to 10 seconds, and the default is 4 seconds.

To change the time limit, enter the command shown in the following example:

```
Local> CHANGE INTERNET NAME RESOLUTION TIME LIMIT 5
```

Changing the Retry Limit

The domain name resolution retry limit indicates the number of times that the access server resends queries to the same name server when looking for an Internet host. The range is from 1 to 5, and the default is 3.

To change the retry limit, enter the command shown in the following example:

```
Local> CHANGE INTERNET NAME RESOLUTION RETRY LIMIT 2
```

Changing the Name Resolution Mode

The name resolution mode describes where the access server searches for host name and address information. To change the name resolution mode, use the command shown in the following example:

```
Local> CHANGE INTERNET NAME RESOLUTION MODE LOCAL
```

Name Resolution Modes

The following table lists and describes the name resolution modes:

Mode	When the access server attempts to resolve a host name or address, it searches:
Local	Local data, which is host name and address information that users previously entered with the SET/DEFINE/CHANGE INTERNET HOST command. Use local data when no name servers are configured.
Remote	Learned data and remote name servers. Learned data is name and address information that the access server receives from name servers and enters in its cache. If the access server fails to resolve the address with the learned data in its cache, it queries the network name servers for remote data.
Ordered (Default)	Local data, then learned data and remote data from the network name servers. Local data takes precedence.
Stub	Remote data only, using recursive name service. The access server performs no DNS caching.
Slave	Local data and remote data, using recursive name service. The access server performs no DNS caching. When conflicts occur, the local data takes precedence.

Configuring a List of Commonly Used Internet Hosts

You can optionally enter commonly used Internet host names and addresses in the access server cache.

The following command shows how to do this:

```
Local> CHANGE INTERNET HOST SALES ADDRESS 195.1.1.72
```

Two additional commands enable you to manage the list of commonly used Internet hosts:

- SHOW / LIST / MONITOR INTERNET HOST
- CLEAR / PURGE INTERNET HOST

If Using a Name Server

If you are using name servers—that is, if NAME RESOLUTION MODE is set to a value other than LOCAL—then you should define local host names and addresses only in exceptional cases. The names received from name servers reflect recent updates.

Also, they may include the hosts you are likely to define with CHANGE INTERNET HOST. Undesirable conflicts may result.

Configuring a List of Internet Name Servers

This section describes how to configure a list of Internet local and root name servers that the access server commonly uses.

Configuring a Root Name Server

A root name server is a name server at the top level domain. To enter a root name server, you must provide an absolute domain name. The following example shows how to enter a root name server:

```
Local> CHANGE INTERNET NAMESERVER C.NYSER.NET ADDRESS
192.33.4.12 ROOT
```

Configuring a Local Name Server

A local name server is any name server that is authoritative for the default domain of the access server. Before adding a local name server, you must first define the access server domain name. The following example shows how to enter a local Internet name server:

```
Local> CHANGE INTERNET NAMESERV NAMED.ACME.COM ADDRESS
99.99.99.99 LOCAL
```

You can use a relative domain name if you are defining a local name server for the default domain only.

Configuring a Name Server for a Different Domain

To enter a locally defined name server for a domain other than the access server default domain, follow these steps:

Step	Action
1	Use the SET INTERNET NAME RESOLUTION DOMAIN command to change the access server default domain name temporarily. Note: Temporarily changing the default name affects the ability of other users in resolving relative domain names.
2	Use the SET/DEFINE/CHANGE INTERNET NAMESERVER domain-name ADDRESS n.n.n.n LOCAL command to add the name server.
3	Change the access server default domain name back to the original domain name.

Name Resolution and Gateways

The access server uses the learned name servers to perform name resolution when using REMOTE or ORDERED name resolution modes. The list of learned name servers for a given domain are, in general, a superset of those explicitly entered with the CHANGE INTERNET NAMESERVER command. The access server primes the cache for the server's default domain by sending queries to the configured name servers. The queries request the names of all authoritative name servers for the default domain.

The access server may not be able to reach a learned name server because of subnet access restrictions on the access server itself. In this case, the access server flags the unreachable name server and stops using it for name resolution. The access server cannot reach a name server if it is not in the same subnet or there is no gateway to it.

If the access server cannot reach a learned name server because of gateway restrictions outside the server, it does not flag the unreachable name server. This can often cause name resolution to time out and fail. In this configuration use either the STUB or SLAVE name resolution mode.

Assigning DNS Server Addresses Automatically

The DNS autoconfigure feature on the access server allows dial-up clients to receive DNS configuration information automatically from the access server when establishing a remote PPP connection.

The access server assigns a primary and secondary DNS server to the remote PPP client. The access server uses an algorithm to obtain the addresses of the DNS servers from its database.

The access server assigns only local name servers to PPP clients. It makes two passes through a list of local nameservers. The following table describes how the access server determines which name servers to assign to the PPP client:

Pass	Description
1	a. The access server goes through a list of learned name servers and searches for name servers that are on its network (by using the access server's subnet mask) and have a positive time to live (ttl). b. The access server goes through a list of locally-configured name servers and searches for name servers that are on its network (by using the access server's subnet mask) and have a positive time to live (ttl). c. The access server assigns the first valid name server as the Primary Nameserver and the second valid name server as the Secondary Nameserver.
2	If the access server does not find two valid name servers: a. The access server goes through the list of learned name servers and searches for name servers with a positive time to live (ttl). b. The access server goes through the list of locally-configured name servers and searches for name servers with a positive time to live (ttl). c. The access server assigns the first valid name server as the Primary Nameserver and the second valid name server as the Secondary Nameserver.

Configuring a List of Internet Gateway Addresses

Introduction

If the access server users need to access hosts in different networks or subnets, you can define a database of Internet gateways. The access server uses gateways to route traffic to different networks and subnets.

Displaying a List of Gateway Addresses

To display a list of Internet gateway addresses, use the SHOW/LIST/MONITOR INTERNET GATEWAY command.

Internet Gateway Addresses Display Example

The following example shows how to display a list of Internet gateway addresses available to the access server for routing network traffic:

```
Local> SHOW INTERNET GATEWAY
Gateway: 16.20.0.3    Host:    16.30.22.35
Gateway: 16.20.48.56  Network: 16.30.0.0    Mask: 255.255.0.0
Gateway: 16.20.98.245 Network: Any
Gateway: 16.20.48.48  Network: 17.0.0.0     Mask:   255.0.0.0
```

Configuring a Default Gateway

The access server uses a default gateway to route a packet when its destination address:

- Is on a different subnet than the access server
- Does not match any of the known gateway network addresses

Default Gateway Definition Example

The following example shows how to define a default gateway:

```
Local> CHANGE INTERNET GATEWAY 195.1.1.72
```

Defining Networks Available Through a Specific Gateway

To indicate that the access server can reach a given network through a specific gateway, use the DEFINE/SET/CHANGE INTERNET GATEWAY command with the NETWORK parameter to do this.

Default Gateway Definition Example

The following example shows how to define the mapping of the default gateway to the network:

```
Local> CHANGE INTERNET GATEWAY 195.1.1.72 NETWORK 197.0.0.0
```

You can define multiple networks that can be reached through the same gateway with the same address. You must enter a separate command to each network with a gateway.

Defining Subnets Available Through a Specific Gateway

To indicate that the access server can reach a given subnet through a specific gateway, use the DEFINE/SET/CHANGE INTERNET GATEWAY command with the NETWORK and MASK keywords.

Subnet Definition Through a Specific Gateway Example

The following example shows how to define a subnet through a specific gateway:

```
Local> CHANGE INTERNET GATE 195.1.1.72 NETWORK 197.5.7.0
MASK 255.255.255.0
```

You can define multiple subnets that can be reached through the same gateway address. You must enter a separate command to associate each subnet with a gateway.

Defining Hosts Available Through a Specific Gateway

To indicate that the access server can reach a given host through a specific gateway, use the DEFINE/SET/CHANGE INTERNET GATEWAY COMMAND and the HOST parameter.

Host Definition Through a Specific Gateway Example

The following example shows the command to define the host through a specific gateway:

```
Local> CHANGE INTERNET GATEWAY 195.1.1.72 HOST 52.53.21.10
```

You can define multiple hosts that can be reached through the same gateway with the same address. You must enter a separate command to define each host with a gateway.

Configuring a List of Internet ARP Entries

Introduction

The list of address resolution protocol (ARP) entries maps Internet addresses to Ethernet hardware addresses for devices on the same network as the access server. You only need to enter the network hosts that do not support ARP.

Displaying the List of Internet ARP Entries

To display a list of ARP entries, use the SHOW / LIST / MONITOR INTERNET ARP ENTRY command.

Sample List of Internet ARP Entries

The following example shows a typical display list of ARP entries:

```
Local> SHOW INTERNET ARP ENTRY
Internet Address   Ethernet Address    Status
16.20.0.96         AA-00-04-00-21-10
16.20.0.173        08-00-2B-04-41-9B
16.20.0.96         AA-00-04-00-3B-11
6.20.48.48         AA-00-05-08-3B-20   No Purge
```

Defining an ARP Entry

To define an ARP entry in the list of entries, use the DEFINE / SET / CHANGE INTERNET ARP ENTRY command with the ETHERNET parameter.

ARP Entry Definition Example

The following example shows how to enter a definition in the list of ARP entries:

```
Local> CHANGE INTERNET ARP ENTRY 195.1.1.72 ETHERNET 08-54-
56-67-AC-89
```

This command maps the Internet address of 195.1.1.72 to the Ethernet hardware address 08-54-56-67-AC-89.

Setting the TCP Keepalive Timer

What the Timer Does

The TCP keepalive timer determines whether a TCP connection with a remote host is active and should remain open.

After the access server and a remote host establish a TCP connection, the access server waits a set amount of time and sends a keepalive probe to the remote host. If the access server receives a valid response from the remote host, it waits again and sends a new keepalive probe.

If the access server does not receive a response from the remote host, it continues to send keepalive probes until it reaches a set maximum. If the remote host does not respond after the access server sends the last keepalive probe, the access server drops the connection.

Setting the Timer

Use the SET / DEFINE / CHANGE INTERNET [TCP] KEEPALIVE TIMER command to set the amount of time (in minutes) the access server waits to send the first keepalive probe after establishing a TCP connection with an idle remote host. The range is from 1 to 1440 (one day) and the default is 120 (2 hours).

Timer Set Example

The following example shows how to set the TCP keepalive timer to wait one minute before sending the first keepalive timer:

```
Local> CHANGE INTERNET TCP KEEPALIVE TIMER 1
```

Disabling the Timer

By default, the TCP keepalive timer is enabled. Use the SET / DEFINE / CHANGE INTERNET [TCP] KEEPALIVE TIMER DISABLED command to disable it.

Setting Timer Retries

Use the SET/DEFINE/CHANGE INTERNET [TCP] KEEPALIVE RETRY command to set the number of keepalive probe retries. The TCP keepalive timer retry number indicates the number of times that the access server sends keepalive probes to the remote host when it does not receive a valid response. The access server sends a keepalive probe every minute until the host responds or it reaches the retry count value. The retry count value range is from 1 to 60 and the default value is 8. If the access server does not receive a valid response from the remote host after sending the last probe, the access server drops the connection.

Retry Set Example

The following example show how to set the maximum number of keepalive probes that the access server sends (10):

```
Local> CHANGE INTERNET TCP KEEPALIVE RETRY 10
```

Displaying Timer Characteristics

Use the SHOW/LIST INTERNET command to display the TCP keepalive timer characteristics.

Timer Characteristics Display

The following shows an example of the display. If you disable the timer, the value for the Keepalive Timer field is DISABLED.

```
Local> SHOW INTERNET
State                Enabled
Internet Address:    195.1.1.1
Subnet Mask:         255.255.255.0
DHCP:                Enabled

TCP Keepalive Timer:    60
TCP Keepalive Retry:    10
Local>
```

Displaying the Internet Counters

Using the SHOW Command

Use the SHOW / LIST / MONIITOR INTERNET command to display the Internet counters. To reset the Internet counters, use the ZERO INTERNET COUNTERS command.

To reset the Internet counters, use the ZERO INTERNET COUNTERS command.

Internet Counters Display Example

The following example shows a typical Internet counters display:

```
Local> SHOW INTERNET COUNTERS
TCP Segments:            146
 Transmitted              58 Bytes Transmitted:        182
  Data:                    0 Bytes Data:               182
  Data Retransmitted       0 Bytes Data Retransmitted    0
  Other:                  88 Bytes Received:          9894
 Received                144
 Segments Discarded:       0 Internet Connections:       0
IP Packets Transmitted:  146 Requested:                  2
IP Packets Received:     144 Accepted:                   0
IP Fragments Received:     0 Established:                2
IP Fragments Dropped:      0 Closed:                     1
IP Error in Header:        0 Dropped:                    0

ICMP Message                 UDP Datagrams
 Transmitted:              0 Transmitted:                0
  Received:                0 Received:                  00
  Dropped:                 0 Dropped:                    0
  Destination Unreachable: 0

Local>
```

Internet Counter Display Fields

The following table describes the fields in a typical Internet counters display:

Field	Description
TCP Segments	The following counters contain statistics on TCP segments:
Transmitted:	Total number of TCP segments transmitted by the access server. The following counters are a breakdown of this total: **Data**: Number of transmitted segments that contained data. **Data Retransmitted**: Number of transmitted segments that contained retransmitted data. **Other**: Number of transmitted segments that contained no data.
Received:	Received: Total number of TCP segments received by the access server.
Segments Discarded:	Number of received TCP segments that were discarded due to errors. These errors can include bad checksum and invalid length of TCP header.
Bytes Transmitted:	Total number of bytes of data transmitted in TCP segments, including bytes retransmitted. The following counters are a breakdown of this total: **Bytes Data**: Total number of bytes of data transmitted in TCP segments, not including bytes retransmitted. **Bytes Data Retransmitted**: Total number of retransmitted bytes of data transmitted in TCP segments.
Bytes Received:	Total number of bytes of data received in TCP segments.
IP Packets Transmitted:	Total number of IP datagrams transmitted.
IP Packets Received:	Total number of IP datagrams received.
IP Fragments Received:	Total number of IP fragments received.
IP Fragments Dropped:	Total number of IP fragments dropped due to either a lack of memory to store the fragment or received a duplicate fragment.
IP Error in Header:	Total number of IP datagrams received with errors in the header. These are discarded.
Internet Connections	The following counters contain statistics on connections:
Requested:	Number of outgoing Telnet connect attempts made by users.

Field	Description
Accepted:	Number of incoming TCP connections accepted by Telnet. This count includes those connections accepted by Telnet then dropped due to no physical port available.
Established:	Number of connections established by TCP. This count includes those connections accepted by Telnet then dropped due to no physical port available.
Closed:	Number of connections closed by a user or remote host.
Dropped:	Number of connections dropped, because of a reset from the remote host, unsuccessful retransmission, keepalive timeout, protocol error, or aborted by Telnet due to lack of available physical ports.
ICMP Messages	The following counters contain statistics on ICMP messages:
Transmitted	Total number of ICMP messages transmitted by the access server.
Received:	Total number of ICMP messages received by the access server.
Dropped:	Total number of ICMP messages dropped by the access server, because of an error in the ICMP message, such as incorrect code, checksum error, or incorrect length.
Destination Unreachable:	Total number of ICMP Destination Unreachable messages received by the access server. Usually received when a connect attempt fails because either the TCP or UDP port is unknown at the remote host, or the host (or the host's network) is unreachable.
UDP Datagrams	The following counters contain statistics on connections:
Transmitted:	Total number of UDP datagrams transmitted by the network access server.
Received:	Total number of UDP datagrams received by the network access server.
Dropped:	Total number of USDP datagrams dropped by the network access server, because of an error in the UDP header, checksum fails, or length is incorrect.

Learning IP Information From a BOOTP Server

Introduction

Instead of manually configuring IP information, you can have the access server learn its IP address and other IP configuration information from a BOOTP server on the network. If you use the BOOTP server to load the CNAS software on the access server, it can also learn its IP configuration from the BOOTP server during the load operation.

BOOTP Server Configuration

Refer to the CNAS installation instructions for information about configuring a BOOTP server.

Learning Operation

The following occurs when the access server learns IP configuration information from a BOOTP server:

- If you use a BOOTP server to load the software image on your access server, the access server learns the IP configuration information during the boot operation.
- If you use MOP to load the software image on your access server, the access server learns the IP configuration information after initialization.
- If you disable INTERNET, the access server does not learn its IP address and no IP functions work. You can enable INTERNET at any time to start the address learning process.
- If you enable INTERNET, you cannot disable it operationally (that is, using a SET command) because the access server cannot easily ensure that an Internet function is not pending or occurring. You must use the DEFINE INTERNET DISABLE command and reboot the access server.
- When the access server is learning an IP address, you can use the SHOW / MONITOR INTERNET command to display the status of the learning operation. If learning is occurring, the IP address displays as “(Learning)”.

Setting Up IP Configuration Learning

Do the following to set up your access server to learn IP configuration information from a BOOTP server on the network:

Step	Action
1	Set up the BOOTP server: a. Add an entry for the access server's Ethernet address. b. Associate the Ethernet address with an IP address. c. Optionally, associate the Ethernet address with a subnet mask and default gateway. **Reference**: The CNAS installation instructions provide details about configuring a BOOTP server.

2	Ensure that the access server does not have an IP address stored in NVRAM. Use the following command:
	`Local> LIST INTERNET`
	If the display shows an Internet address, clear it using the following command:
	`Local> DEFINE INTERNET ADDRESS NONE`

3	Ensure that the Internet characteristic is enabled. Use the following command:
	`Local> LIST INTERNET`
	If the Internet characteristic is not enabled, enable it using the following command:
	`Local> DEFINE INTERNET ENABLED`

Learning IP Information From a DHCP Server

Description

You can use the Dynamic Host Configuration Protocol (DHCP) to automatically configure TCP/IP characteristics on the access server and remote clients. DHCP provides dynamic assignment of IP addresses and discovery of IP configuration parameters (for example, subnet mask or default gateways). A DHCP client requests and receives this information from a DHCP server on the network.

Enabling DHCP on the access server allows it to learn some of its IP configuration information from a DHCP server. The access server does not receive its IP address from the DHCP server; you must manually configure it or use a BOOTP server.

Enabling DHCP on the access server also allows remote dial-up clients to receive dynamically assigned IP addresses and IP configuration parameters from the DHCP server. Depending on the situation, the access server acts as a DHCP client or proxy.

By default, the DHCP setting on the access server is ENABLED. If you do not have a DHCP server on your network, disable DHCP. (See the Enabling and Disabling DHCP section in this chapter.)

BOOTP and DHCP Differences

DHCP is an extension of BOOTP; however, using a DHCP server to obtain IP information differs from using a BOOTP server in the following ways:

Using a BOOTP Server	Using a DHCP Server
The access server can learn its IP address from a BOOTP server (or you can configure it directly on the access server).	The access server does not learn its IP address from a DHCP server. The access server can learn the following from a DHCP server: • Domain name • Default gateway • Domain Name System (DNS) servers • Windows Internet Naming Service (WINS) servers
You configure the IP information to be learned in the BOOTP server's database and associate it with the access server's hardware address.	You do not configure the DHCP server with any access server or client-specific information. You need only to configure the DECserver with network information (for example, a domain name) and a pool of IP addresses available for assignment.
The access server writes the information it learns from the BOOTP server to NVRAM.	The access server does not write the information it learns from the DHCP server to NVRAM. This ensures that the access server receives the most recent information from the DHCP server.

DHCP Client Operation

During initialization, the access server acts as a DHCP client to obtain IP configuration parameters (excluding the IP address; use a BOOTP server or the DEFINE INTERNET ADDRESS command to configure the IP address). The access server requests the following IP configuration parameters from a DHCP server:

- Default gateway
- Domain name
- Domain Name System (DNS) servers
- Windows Internet Naming Service (WINS) servers

Figure 8-1 shows what occurs when the access server acts as a DHCP client:

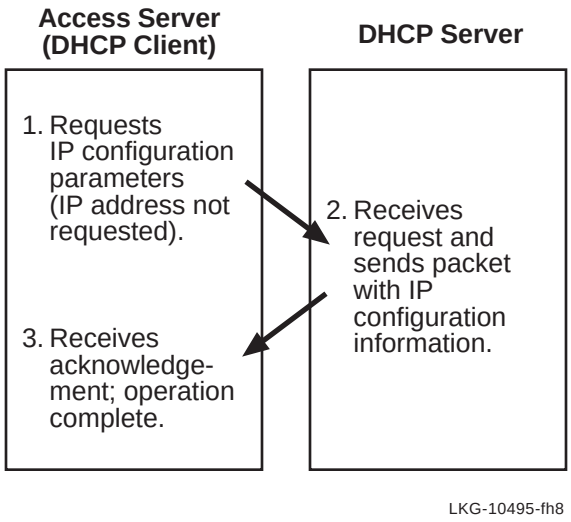


Figure 8-1. Access Server as a DHCP Client

DHCP Proxy Operation

The access server can act as a DHCP proxy to provide IP address assignment for most remote clients.

IP Address Assignment

When you enable DHCP, the access server sends requests for IP addresses to a DHCP server on behalf of the remote client if:

- You do not configure an IP address on the ports configured for remote access.
- You do not specify an IP address using RADIUS authentication.
- The remote client is not configured with an IP address for its PPP session.

When the access server receives the IP address from the DHCP server, it assigns the address to the remote client.

Figure 8-2 shows what occurs when the access server uses DHCP to assign IP addresses to remote clients:

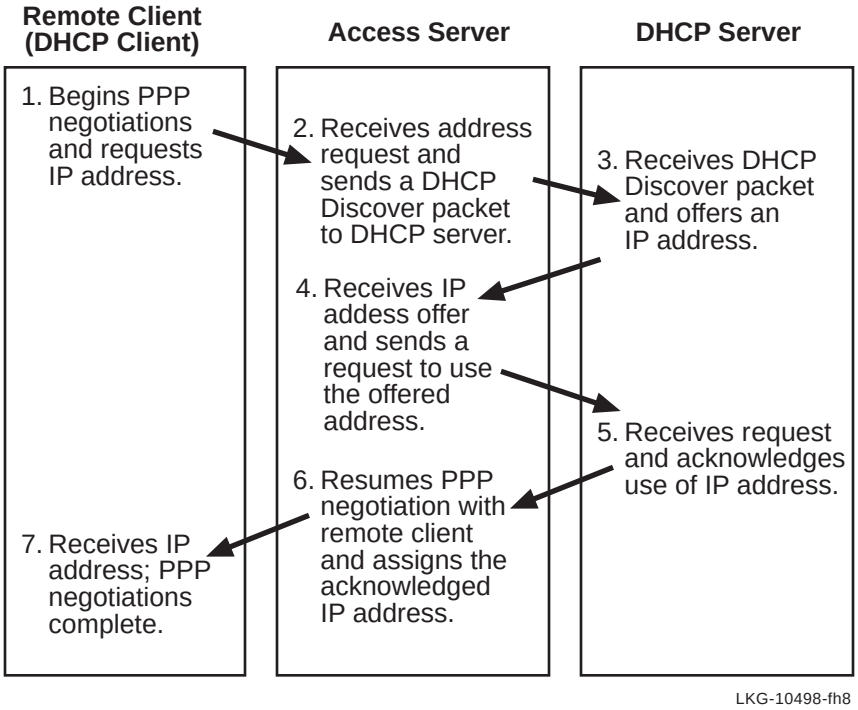


Figure 8-2. What Occurs When Access Server Uses DHCP to Assign IP Addresses to Remote Clients

IP Address Renewals

When the DHCP server assigns an IP address to a remote client, it "leases" the address to the remote client for a finite or infinite amount of time. If the lease is about to expire and the remote client still has a dial-up connection, the access server renews the lease on behalf of the remote client. The access server attempts to renew the lease as long as the remote client maintains a dial-up connection.

Enabling and Disabling DHCP

The default DHCP setting on the access server is DHCP ENABLED. The following table lists the commands that you use to enable and disable DHCP:

To Do This:	Use This Command:
Enable DHCP.	DEFINE / SET / CHANGE INTERNET DHCP ENABLED
Disable DHCP.	DEFINE INTERNET DHCP DISABLED

Displaying the DHCP Setting

Use the SHOW / LIST / MONITOR INTERNET command to display the current DHCP setting. The example in the Displaying the Internet Address and Subnet Mask section in this chapter shows a typical display.

Configuring Default Values

If you enable DHCP but also want the access server to function in the event that a DCHP server is not available, you can define default values for some of the DHCP-learned IP information in NVRAM using DEFINE commands. Follow the procedures in this chapter for setting the IP address, subnet mask, DNS values, WINS values, and gateways. You can also use the Access Server Manager to set these values. See the Access Server Manager's online help for details.

When the access server initializes, it writes the default values from NVRAM to RAM. If a DHCP server responds to the access server's request for information, the DHCP-learned values overwrite the default values in RAM. If a DHCP server does not respond, the access server uses the default values.

Overriding DHCP-Learned Values

To override DHCP-learned values, use SET commands after initialization completes. Follow the procedures in this chapter for setting the IP address, DNS values, WINS values, and gateways or use the Access Server Manager (see the Access Server Manager online help for details).

Assigning WINS Server Addresses

What Does WINS Do?

Windows Internet Naming Service (WINS) performs NetBIOS name and IP address resolution, similar to the Domain Name Service (DNS). WINS allows systems that use NetBIOS to communicate with each other over TCP/IP.

What Is WINS Autoconfigure?

The WINS autoconfigure feature on the access server allows dial-up clients to receive WINS configuration information automatically from the access server when establishing a remote PPP connection.

The access server provides the remote client with the addresses of WINS primary and secondary servers that it finds in its RAM.

Operation

The access server receives WINS server addresses in one of the following ways:

- From a DHCP server on the network, if the DHCP is enabled on the access server.
- From access server commands that you enter at a local or remote console.

Figure 8-3 shows how the remote client receives WINS server information from the access server:

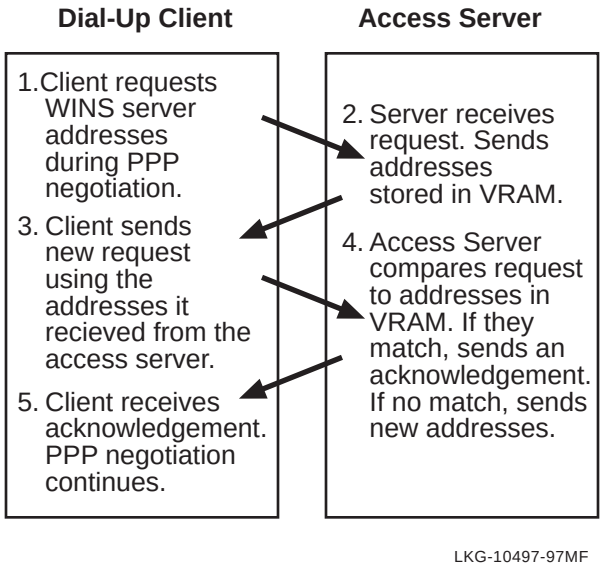


Figure 8-3. How the Remote Client Receives WINS Server Information from the Access Server

Assigning WINS Addresses

If you enable DHCP on the access server, it receives the WINS server addresses from a DHCP server on the network and writes the values to VRAM when you reinitialize the access server. When a remote client sends a request to the access server for WINS server addresses during PPP negotiation, the access server responds with the addresses it finds in VRAM.

If you disable DHCP, or need to change the WINS server addresses at a time when you do not want to reinitialize the access server, you can set the addresses manually. Use the SET/DEFINE/CHANGE INTERNET WINS [PRIMARY | SECONDARY] command for this purpose.

WINS Address Example

The following example shows how to set primary and secondary WINS server addresses on the access server:

```
Local> CHANGE INTERNET WINS PRIMARY 12.30.34.10
Local> CHANGE INTERNET WINS SECONDARY 12.150.25.5
```

Displaying WINS Characteristics

Use the SHOW/LIST INTERNET NAME RESOLUTION command to view the WINS server addresses stored in the access server's VRAM (or NVRAM).

WINS Display Example

The following shows a typical example of the WINS display:

```
Local> SHOW INTERNET NAME RESOLUTION

NetBIOS (WINS) Name Resolution:

Primary WINS server:    6.20.44.55
Secondary WINS server   16.125.14.235 (from DHCP)

Domain Name Resolution:

Domain Name:            finance.acme.com (from DHCP)

Resolution Host Limit:  32      Resolution Time Limit:  4
Resolution Mode:        Ordered Resolution Retry Limit: 3

Nameservers (Locally configured):
99.99.99.99           Local name.acme.com (from DHCP)

Nameservers (Learned):
99.99.99.99           Local name.acme.com
88.88.88.88           Local secondary.acme.com

DHCP server: 16.20.244.250
Local>
```

The following table lists the WINS characteristics displayed in the previous example. (See the Displaying DNS Characteristics section in this chapter for a description of the DNS characteristics shown in the example.)

Field	Description
Primary	The Internet address or host name for the primary WINS server.
Secondary	The Internet address or host name for the WINS server used when the primary WINS server is not available.

If a DHCP server provides the WINS servers and Domain Name information, the display includes “(from DHCP)” at the end of each line of information and the name of the DHCP server at the end of the display.

Chapter 9

Managing AppleTalk

Overview

Introduction

This chapter explains how to configure and manage the AppleTalk protocol suite on an access server.

In This Chapter

This chapter contains the following topics:

- Configuring AppleTalk on an Access Server
- Displaying AppleTalk Characteristics
- Displaying AppleTalk Counters
- Displaying AppleTalk Status
- Displaying AppleTalk Routes
- Displaying AppleTalk ARP Entries

Configuring AppleTalk on an Access Server

Introduction

You can configure an access server to act as an AppleTalk node on the network and many different components can then be monitored. The configuration of the AppleTalk characteristics can be done only in the NVRAM database. This means that the manager has to reinitialize the access server after making a change to any of the AppleTalk characteristics before the changes take effect. This chapter does not address managing asynchronous connections. For information about ATCP, see Chapter 19. This chapter assumes you have a basic understanding of the AppleTalk protocol suite.

AppleTalk Address Format

AppleTalk node addresses consist of two fields: a network number and a node number. A network number can be in the range 1 to 65534. A node number can be in the range 1 to 254. The network and node numbers are separated by a period (.).

Enabling AppleTalk

By default, AppleTalk is not enabled on an access server. In order for the access server to act as an AppleTalk node on the network, a privileged user has to enable AppleTalk explicitly with the following DEFINE command:

```
Local> DEFINE APPLETALK ENABLED
```

Then the access server has to be reinitialized. Upon reinitialization, the access server functions as an AppleTalk node by doing the following:

- Acquiring an AppleTalk address and zone
- Registering its AppleTalk name
- Acquiring and defending AppleTalk addresses for attached hosts
- Forwarding AppleTalk DDP packets
- Permitting hosts attached via asynchronous lines to participate in the AppleTalk protocol
- Responding to SNMP requests for AppleTalk information
- Responding to AppleTalk Echo packets

Disabling AppleTalk

If you decide that your access server should no longer act as an AppleTalk node, all AppleTalk capabilities can be turned off using the following privileged DEFINE command:

```
Local> DEFINE APPLETALK DISABLED
```

Reinitialize the access server to have this command take effect. Upon reinitialization, the access server no longer functions as an AppleTalk node. All of the SHOW AppleTalk commands then give you the following message:

```
Local -527- AppleTalk is not enabled, no operational
commands allowed
```

DIGITAL recommends that you disable AppleTalk when the access server is not used as an AppleTalk node. When you disable AppleTalk:

- The access server no longer responds to or monitors AppleTalk traffic on the network, freeing up CPU time.
- System resources are freed up since they are no longer allocated for AppleTalk operation.
- The access server rejects all SNMP queries for AppleTalk information. It transmits a No Such Name error message.

Setting AppleTalk Address Cache Size

An access server with AppleTalk enabled tries to acquire unused AppleTalk addresses for any potential hosts attached to the access server with asynchronous lines. It saves these addresses in a cache and defends them if any other host on the network tries to use them. When a host attaches to the access server via an asynchronous port, the access server assigns one of the addresses from the cache to the attached host.

A privileged user on the access server specifies how many AppleTalk addresses the access server should acquire on initialization using the following DEFINE command:

```
Local> DEFINE APPLETALK [address] CACHE [ size] n
```

As with the command to enable or disable AppleTalk, this command affects only the NVRAM database on the access server. The access server has to be reinitialized for the cache size to take effect operationally.

The supported range for n is 1 to the number of asynchronous ports. The access server always attempts to keep the number of available entries in the address cache equal to the smaller of either the cache size that you define or the number of ports that do not already have AppleTalk connections.

The default value for n is the number of access server asynchronous ports divided by 8. For instance, the default cache size on a 16 port access server would be 2.

The DEFINE APPLETALK ADDRESS CACHE command lets the access server manager trade off address use versus the probability of simultaneous Appletalk session requests.

- If the value of n is set too high, the access server can acquire too many addresses, exhausting the supply available for the rest of the network.
- The access server serializes address acquisition attempts, which typically require about 2 seconds each. If the access server pre-acquires too few addresses (the value of n is too low), some client AppleTalk session initiation attempts may fail if too many arrive at once. When this happens, the access server may not have enough addresses to assign to all the new sessions.

Displaying AppleTalk Characteristics

Commands

Use the LIST APPLETALK CHARACTERISTICS command to display the AppleTalk characteristics. This command is nonprivileged.

Use the SHOW / MONITOR APPLETALK STATUS command to see the values being used operationally.

Displaying AppleTalk Characteristics Example

The following example shows how to display the latest values configured by the DEFINE APPLETALK commands:

```
Local> LIST APPLETALK CHARACTERISTICS
AppleTalk Characteristics Server: LAT_08002B24F24F
State:                    Enabled
Cache Size:               2
```

Fields in the AppleTalk Characteristics Display

The following table describes the fields in the AppleTalk Characteristics display:

Field	Description
State	Indicates whether AppleTalk is enabled the next time you initialize the access server.
Cache	Shows the number of AppleTalk addresses that the access server will acquire in cache memory the next time you initialize the access server.

Displaying AppleTalk Counters

Command

Use the SHOW / MONITOR APPLETALK COUNTERS command to display the AppleTalk counters on an access server. The command is nonprivileged.

Displaying AppleTalk Counters Example

The following example shows a typical display when you enter the SHOW APPLETALK COUNTERS command:

```
Local> SHOW APPLETALK COUNTERS
AppleTalk Counters         Seconds Since Zeroed: 18207
AARP
Unsent Probes:           0 Unsent Responses:          0
DDP
 In Receives:         5510 Out Requests:            19
 In Local Datagrams:     1 Forwarded Requests:       0
 Too Short Errors:       0 Out Shorts:               0
 Too Long Errors:        0 Out Longs:               19
 No Protocol Handlers:   0 Out No Routes:            0
 Checksum Errors:        0 Hop Count Errors:         0
 Short DDP Errors:       0 Broadcast Errors:         0
NBP
 Lookups Received:    1850 Lookup Replies:          13
 In Errors:              0
RTMP
 Router Lost:            0 In Errors:                0
ZIP
 In GetNetInfo Response: 1 Out GetNetInfo Requests: 6
 In Errors: 0
```

Fields in the AppleTalk Counters Display

The following table describes the fields in the AppleTalk Counters display:

Field		Description
AARP	Unsent Probes	The number of AARP probes that could not be sent due to insufficient access server resources.
	Unsent Responses	Unsent Responses The number of AARP responses that could not be sent due to insufficient access server resources.
DDP	In Receives	The number of DDP datagrams the access server has received, including those received in error.
	Out Requests	The number of DDP datagrams DDP sent out on behalf of access server AppleTalk components.
	In Local Datagrams	The number of DDP datagrams the access server has received that were destined for the access server.
	Forwarded Requests	The number of DDP datagrams the access server received for which this was not their final destination. DDP made an attempt to forward these packets.
	Too Short Errors	The number of DDP datagrams dropped because their data length was less than the length specified in the DDP header or because their length was less than that of a DDP header.
	Too Long Errors	The number of DDP datagrams dropped because their data length exceeded the length specified in the DDP header or because their length was greater than the maximum DDP length.
	No Protocol Handlers	The number of DDP datagrams the access server received that were addressed to an upper layer protocol that the access server does not support.
	Checksum Errors	The number of input DDP datagrams dropped because of a checksum error.
	Short DDP Errors	The number of input DDP datagrams dropped because access server was not final destination and type was short DDP.
	Broadcast Errors	The number of input DDP datagrams dropped because the access server was not their final destination and they were addressed to the link level broadcast.
	Out Shorts	The number of short DDP datagrams transmitted.

Field		Description
	Out Longs	The number of long DDP datagrams transmitted.
	Out No Routes	The number of DDP datagrams dropped because a route could not be found.
	Hop Count Errors	The number of input DDP datagrams dropped because the access server was not their final destination and their hop count would exceed 15 if forwarded.
NBP	Lookups Received	The number of NBP Lookup Requests the access server has received.
	Lookup Replies	The number of NBP Lookup Replies the access server has sent.
	In Errors	The number of invalid NBP datagrams received.
RTMP	Router Lost	The number of times the access server lost contact with every AppleTalk router on its Ethernet.
	In Errors	The number of invalid RTMP datagrams received.
ZIP	In GetNetInfo Responses	The number of GetNetInfo responses the access server has received.
	Out GetNetInfo Requests	The number of GetNetInfo requests the access server has sent.
	In Errors	The number of invalid ZIP datagrams received.

AARP Values

Two important counter values are those for AARP. Unsent AARP probes or responses can indicate network problems. This happens when the access server is too overloaded to respond to AARP requests. When there are unsent probes, other AppleTalk nodes can acquire AppleTalk addresses used by the access server or its clients. There can be connectivity problems when there are unsent responses.

Displaying AppleTalk Status

Command

Use the SHOW / MONITOR APPLETALK STATUS command to display the AppleTalk status on the access server. The command is nonprivileged.

Displaying AppleTalk Status Example

The following example shows how to display the AppleTalk status on an access server:

```
Local> SHOW APPLETALK STATUS
AppleTalk Status     Server:              LAT_08002B24F24F
State:               Up
Address:             401.78
Network:             401-401
Name:
   Object:           LAT_08002B24F24F
   Type:             Access Server 316
   Zone:             LKG Littleton MA
Cache:               2
Attached Hosts:      0
Last Error:          <no error>
```

Fields in the AppleTalk Status Display

The following table describes the fields that appear in the AppleTalk Status display:

Field	Value	Description
State		The status of the access server AppleTalk implementation.
	Off	AppleTalk is not operating.
	Acquiring	The access server is acquiring an AppleTalk address.
	Learning	The access server is learning its AppleTalk zone.
	Reacquiring	The access server is getting itself a new AppleTalk address.
	Registering	Registering The access server is registering its name.

Field	Value	Description
	Up	AppleTalk is fully operational.
Address		The AppleTalk address of the access server, learned from the EtherTalk network at initialization. Its value is 0.0 until the Learning state.
Network		The AppleTalk network range the access server learned at initialization. If no AppleTalk router is on the access server's network, the value is 1-65534. The value is 0-0 until the Learning state.
Name		The full AppleTalk name of the access server consists of: object:type@zone.
	Object	The unique name of the access server (for example, LAT 08002B24F24F). You can configure this parameter with the SET/DEFINE/CHANGE SERVER NAME command.
	Type	The type of device (for example, DECserver 700-08). This parameter cannot be configured.
	Zone	The zone to which the access server belongs. This is a learned parameter and cannot be configured.
Cache		The current address cache size.
Attached Hosts		The number of AppleTalk hosts attached to the access server via asynchronous lines.
Last Error		The last AppleTalk error reported.

Displaying AppleTalk Routes

Command

Use the SHOW / MONITOR APPLETALK ROUTES command to display the available AppleTalk routes to an access server. The command is nonprivileged.

Displaying AppleTalk Routes Example

The following example shows how to use the SHOW APPLETALK ROUTES command to display available AppletTalk routes:

```
Local> SHOW APPLETALK ROUTES
AppleTalk Routes                Server:  LAT_08002B24F24F
Destination   Next Hop   Status   Interface      Seconds
                                                    since
                                                     Last
                                                Validated
12344-12350  12346.132   Up       Ethernet           159
<default>    12347.1     Up       Ethernet            20
12349.223    12346.132   Up       Asynch7             29
12348.144    12346.132   Up       Asynch3            116
```

Fields in the AppleTalk Routes Display

The following table describes the fields in the AppleTalk routes display:

Field	Value	Description
Destination		The route destination. This can be either an AppleTalk network number range or an AppleTalk host address. A host address indicates a route to a host attached to the access server by means of an asynchronous link. The destination <default> is distinguished from the others. If the server does not find an appropriate route for a DDP packet, it sends the packet to the route's next hop.
Next Hop		The AppleTalk router that is the "next hop" to a particular network. For the <default> destination, the next hop corresponds to an AppleTalk router. For all other destinations, the next hop is the access server's own AppleTalk address.
Status		The current state of the route, as follows:

Field	Value	Description
	Up	The route is known to be valid.
	Suspect	The route is thought valid, but has not been refreshed recently.
	Bad	The route has not been refreshed recently enough to warrant further use.
	Down	The route exists in the routing table, but is not being used.
Interface		The interface the access server uses to route packets to the destination.
Seconds Since Last Validated		This will be the time since: • The "first" RTMP data packet announcing the route arrived, for a network destination with a status of "Up" • A connection was established, for a host destination with a status of "Up" • The most recent RTMP data packet announcing it, for a network destination with a status of "Suspect," "Bad," or "Down"

Displaying AppleTalk ARP Entries

Introduction

When an attached host sends a message to an unknown AppleTalk node on the access server network, the access server creates an entry in the AppleTalk ARP cache and transmits an ARP request for the node's data link address. At this time, the access server does not know the address for the desired node. When it receives a reply, it fills in the node's corresponding Ethernet address.

Command

Use the SHOW / MONITOR APPLETALK ARP ENTRIES command to display entries that the access server creates in the AppleTalk ARP cache.

Displaying AppleTalk ARP Entries Example

The following example shows how to display the entries in the AppleTalk ARP cache:

```
Local> SHOW APPLETALK ARP ENTRIES
   AppleTalk ARP Entries         Server:LAT_08002B26AE00
     ATalk Address  Ethernet Address  Status   Interface
      12345.132     08-00-2B-26-AE-00 Local     Ethernet
      12345.28      08-00-2B-26-AE-00 Acquired  Ethernet
      12346.7       08-00-2B-26-AE-00 Local      Asynch3
      12347.18      08-00-2B-26-AE-00 Local     Asynch12
      12347.2       <resolving>       Remote    Ethernet
      12344.3       AA-00-04-11-21-10 Remote    Ethernet
```

Fields in the AppleTalk ARP Display

The following table describes the fields in the AppleTalk ARP Entries display:

Field	Value	Description
ATalk Address		The AppleTalk address of a node.
Ethernet Address		The corresponding Ethernet address for the AppleTalk node.
Status		The status of the AppleTalk ARP Entry.

Field	Value	Description
	Remote	The entry designates an ARP entry for a remote host on the access server Ethernet. Such an entry usually means the server recently forwarded a DDP packet to this host.
	Local	The entry designates either: 1. A host that is presently running AppleTalk over its asynchronous link to the access server or 2. The access server AppleTalk address
	Acquired	The entry has been pre-acquired for later use by an attached AppleTalk host. It is also possible that the address has already been used by one or more attached hosts, but has been returned to the address cache.
Interface		The interface with which the address is associated. The access server's own AppleTalk address, as well as any remote or acquired addresses, are always associated with the Ethernet. This field identifies the asynchronous line with which a local address might be associated.

Chapter 10

Configuring Basic Device Characteristics

Overview

Introduction

This chapter explains how to configure the basic characteristics for all types of devices that attach to the access server ports. These devices include:

- Standard ANSI video terminals such as the DIGITAL VT100 and VT220
- Printers
- Modems
- PCs
- Computers
- Nonstandard terminals

In This Chapter

This chapter contains the following topics:

Configuring Basic Device Characteristics

Introduction

If you attach a standard ANSI video terminal to an access server port, the basic device characteristics described in this chapter are the only ones that you need to consider.

If you are configuring a port to communicate with a modem, PC, computer interface, or nonstandard terminal, refer to the signal characteristics described in Chapter 10 in addition to the characteristics described in this chapter.

Command

To configure or modify a basic device characteristic, use the SET / CHANGE / MODIFY command for the appropriate characteristic.

Basic Device Characteristic Summary

The following table summarizes the basic device characteristics, and refers you to related information in this chapter:

Characteristic	Default	Allowed Values	Refer to Section
ACCESS	Local	Local, Remote, Dynamic, None	Configuring the ACCESS Characteristic
AUTOBAUD	Enabled	Enabled, Disabled	AUTOBAUD
CHARACTER SIZE	8	7, 8	CHARACTER SIZE
DSRLOGOUT	Disabled	Enabled, Disabled	Specifying DSRLOGOUT
FLOW CONTROL	XON	XON, DSR, CTS, DISABLED	Flow Control Types
INACTIVITY LOGOUT	Disabled	Enabled, Disabled	Specifying INACTIVITY LOGOUT
INPUT FLOW CONTROL	Enabled	Enabled, Disabled	FLOW CONTROL Direction
LONGBREAK LOGOUT	Disabled	Enabled, Disabled	Specifying LONGBREAK LOGOUT
OUTPUT FLOW CONTROL	Enabled	Enabled, Disabled	FLOW CONTROL Direction

Characteristic	Default	Allowed Values	Refer to Section
PARITY	None	Even, Odd, Mark, None	PARITY
SPEED	9600	75,110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 57600, 115200	SPEED
STOP BITS	Dynamically set	1, 2	STOP BITS
TYPE	ANSI	Hardcopy, Softcopy, ANSI	TYPE

Displaying Basic Device Characteristics

Command

To display basic device characteristics, use the SHOW PORT command.

Displaying Port Characteristics Example

The following example shows how to display the port characteristics for port 5:

```
Local> SHOW PORT 5
Port 5:                     Server:         LAT_123456789ABC

Character Size:       8       Input Speed:              9600
Flow Control:         XON     Output Speed:             9600
Parity:               None    Signal Control:       Disabled
Stop Bits:            Dynamic Signal Select: CTS-DSR-RTS-DTR

Access:               Local   Local Switch:             None
Backwards Switch:     None    Name:                   PORT_5
Break:                Local   Session Limit:               4
Forwards Switch:      None    Type:                     ANSI
Default Protocol:     LAT     Default Menu:             None
Autolink Timer One:12 Two:10
Preferred Service:  None
Authorized Groups:  25
(Current) Groups:   25

Enabled Characteristics:
Autobaud, Autoprompt, Broadcast, Failover, Input, Flow
Control, Lock, Loss Notification, Message Codes, Output Flow
Control, Verification

Local>
```

Configuring the ACCESS Characteristic

Description

The ACCESS characteristic determines which types of devices can use a port. The following table lists and defines the possible values for the port ACCESS characteristic:

Characteristic	Device Type	Examples
Local (default)	Interactive	Terminals
Remote	Noninteractive	Computers, printers
Dynamic	Both interactive and noninteractive	Personal computers, printers with keyboards
None	-	Prohibits access to the port

Command

To set the ACCESS characteristic for a port, use the DEFINE/SET/CHANGE PORT command with the ACCESS keyword.

Defining the ACCESS Characteristic Example

The following example shows how to set the access characteristic for port 5 to remote:

```
Local> DEFINE PORT 5 ACCESS REMOTE
```

Matching the Port and Device Characteristics

Introduction

You must ensure that the physical characteristics of the access server port match the physical characteristics of the device as described in this section. If these characteristics do not match, the device does not operate correctly. The characteristics that must match are:

- AUTOBAUD
- CHARACTER SIZE
- PARITY
- STOP BITS
- SPEED
- TYPE

AUTOBAUD

The AUTOBAUD characteristic determines if a port automatically detects a device's speed, parity, and character size when you log in.

AUTOBAUD Settings

The following table lists the AUTOBAUD settings and the types of devices associated with them:

Setting	For These Devices
Enabled	Interactive (default)
Disabled	Printers, modems, computers

CHARACTER SIZE and PARITY Settings

The AUTOBAUD characteristic functions only if the input and output speeds of the port device are the same and the character size and parity settings have the combinations listed in the following table:

Character Size	Parity
8	None
7	Even

Example: Disabling AUTOBAUD

The following example shows how to disable the autobaud characteristic:

```
Local> CHANGE PORT 5 AUTOBAUD DISABLED
```

CHARACTER SIZE

The CHARACTER SIZE characteristic indicates the number of bits in a data character. The access server supports character sizes of 7 or 8 bits, and the default is 8 bits.

Refer to the operator's guide for the port device to determine appropriate character size.

If you enable autobaud, the access server automatically adjusts the character size.

Example: Setting the CHARACTER SIZE

The following example shows how to set the character size:

```
Local> CHANGE PORT 5 CHARACTER SIZE 7
```

PARITY

The PARITY characteristic determines the type of parity checks that the access server performs. If you enable autobaud, the access server automatically adjusts the parity.

PARITY Settings

The following table lists the available parity checks:

Setting	Check Performed Per Character
Even	Even number of one bits
Odd	Odd number of one bits
Mark	A set parity bit
Space	A cleared parity bit
None (default)	No parity checking performed

Example: Changing the PARITY Settings

The following example shows how to change the parity:

```
Local> CHANGE PORT 5 PARITY ODD
```

SPEED

The SPEED characteristic enables you to configure the port for devices that operate at the following speeds: 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bits per second (bits/s).

If you enable autobaud, the access server automatically adjusts the port speed.

Example: Changing the Port SPEED

The following example shows how to change the port speed:

```
Local> CHANGE PORT 5 SPEED 2400
```

Example: Configuring Different Input and Output Speeds for a Port

The following example shows how to specify different input and output speeds for a port:

```
Local> CHANGE PORT 5 INPUT SPEED 2400
Local> CHANGE PORT 5 OUTPUT SPEED 1200
```

STOP BITS

The STOP BITS characteristic indicates the number of bits that mark the end of a character transmission. By default, the access server dynamically sets up the STOP BITS characteristic. The access server automatically uses 2 stop bits for port speeds up to and including 134 bits/s, and 1 stop bit for port speeds above 134 bits/s.

You can also specify 1 or 2 stop bits for each device.

Example: Setting the STOP BITS for a Device

The following example shows how to set the stop bits for a device:

```
Local> CHANGE PORT 5 STOP BITS 1
```

TYPE

The TYPE characteristic indicates the device attached to the port.

Device Types

The following table lists device types available for each port of the access server:

Device Type	Applies to:
Hardcopy	Printers
Softcopy	Non-ANSI video terminals
ANSI (default)	Most video terminals such as the VT100. This causes the screen to clear before each display and enables command-line recall.

Example: Changing the device TYPE

The following example shows how to change the device type:

```
Local> CHANGE PORT 5 TYPE HARDCOPY
```

Configuring the FLOW CONTROL Characteristic

Introduction

The FLOW CONTROL characteristic allows the access server to start and stop data transfer between the port and the attached device. Flow control prevents data losses due to lack of buffering space.

The FLOW CONTROL characteristic does not apply to data transfer between the access server and a network resource. For a particular session, however, the network resource might manage FLOW CONTROL between the port and the host.

Flow Control Types

The types of FLOW CONTROL that you can configure are:

- XON / XOFF
- DSR
- CTS
- No Flow Control
- Flow Control Direction

XON/XOFF

When the access server use XON / XOFF FLOW CONTROL on a port, it sends

- An XON character to start the data transfer between the port and the attached device
- An XOFF character to stop the data transfer between the port and the attached device

XON / XOFF is the type of FLOW CONTROL that Digital Equipment Corporation's terminals, personal computers, printers, and modems use.

When to Use

You must use XON / XOFF FLOW CONTROL when you use:

- DSR logout (See Specifying DSRLOGOUT in this chapter.)
- Signal check (See Specifying SIGNAL CHECK in Chapter 10.)

Example: Enabling XON/XOFF FLOW CONTROL

The following example shows how to enable XON/XOFF FLOW CONTROL:

```
Local> CHANGE PORT 5 FLOW CONTROL XON
```

DSR

DSR FLOW CONTROL operates as follows:

- If the access server receives data too quickly from the port device, it turns off DTR until it can accept more data.
- If the port device receives data too quickly from the access server, it turns off the DSR signal until can accept more data.

Do not enable DSR FLOW CONTROL if modem control, signal control, DSR logout, or signal check is enabled. DSR FLOW CONTROL overrides these characteristics.

Example: Enabling DSR FLOW CONTROL

The following example shows how to enable DSR FLOW CONTROL on a port:

```
Local> CHANGE PORT 5 FLOW CONTROL DSR
```

CTS

CTS is a form of FLOW CONTROL used with null modem (DTE) devices. The access server only transmits data to an attached device when the device asserts DTS.

CTS FLOW CONTROL operates as follows:

- If the access server receives data too quickly from the port device, the access server deasserts RTS until it can accept more data.
- If an attached device receives data too quickly from the access server, it deasserts CTS until it can accept more data.

You can enable CTS/RTS FLOW CONTROL for access servers with attached modems with a speed of 9600 bits/s or greater. This enables a faster response time from the access server hardware.

Example: Enabling CTS FLOW CONTROL

The following command shows how to enable CTS FLOW CONTROL on port 7 of an access server:

```
Local> CHANGE PORT 7 FLOW CONTROL CTS
```

Example: Disabling FLOW CONTROL

The following command shows how to disable FLOW CONTROL on port 5 of an access server:

```
Local> CHANGE PORT 5 FLOW CONTROL DISABLED
```

FLOW CONTROL Direction

The access server software allows you to specify flow input and output FLOW CONTROL:

- Input FLOW CONTROL refers to the data flow from the attached device to the access server.
- Output FLOW CONTROL refers to the data flow from the access server to the attached device.

By default, the access server enables FLOW CONTROL in both directions.

Example: Enabling Input FLOW CONTROL

The following command shows how to enable input FLOW CONTROL on port 5 of an access server:

```
Local> CHANGE PORT 5 INPUT FLOW CONTROL ENABLED
```

Example: Enabling output FLOW CONTROL

The following command shows how to disable output FLOW CONTROL on port 5 of an access server:

```
Local> CHANGE PORT 5 OUTPUT FLOW CONTROL DISABLED
```

Specifying the Automatic Logout Characteristics

Introduction

This section describes the characteristics that you can use to log out a port automatically when the device attached to the port is turned off or when there is no activity for a specified period of time.

Specifying DSRLOGOUT

The DSRLOGOUT characteristic causes the access server to logout a port device when the device deasserts DSR. You cannot enable DSR logout if you enable DSR FLOW CONTROL.

To use DSRLOGOUT, the device and cable must support DSR. For the wiring and cables that support DSR, refer to the hardware documentation for your terminal server. For more information about DTR and DSR signals, refer to Configuring DTR and DSR Signals in Chapter 10.

By default, for DSRLOGOUT is disabled.

Example: Enabling DSRLOGOUT

The following command shows how to enable DSRLOGOUT on port 5:

```
Local> CHANGE PORT 5 DSRLOGOUT ENABLED
```

Specifying LONGBREAK LOGOUT

The LONGBREAK LOGOUT characteristic causes access server to logout a port device when the device deasserts RxD for 2.5 to 3.5 seconds. You use this characteristic for devices that do not support the DSR signal.

Use the SHOW/LIST/MONITOR PORT STATUS command to determine if the RxD signal is valid. If the signal is valid, it appears in the Input Signals field.

By default, LONGBREAK LOGOUT is disabled.

Example: Enabling LONGBREAK LOGOUT

The following command shows how to enable LONGBREAK LOGOUT on port 5:

```
Local> CHANGE PORT 5 LONGBREAK LOGOUT ENABLED
```

Specifying INACTIVITY LOGOUT

The INACTIVITY LOGOUT characteristic allows you to enable or to disable automatic log out for the port. If INACTIVITY LOGOUT is enabled, the access server automatically disconnects the session and logs out the port if there is no input or output activity for the time specified by the INACTIVITY TIMER characteristic.

Example: Enabling INACTIVITY LOGOUT

The following example shows how to enable INACTIVITY LOGOUT on port 5:

```
Local> CHANGE PORT 5 INACTIVITY LOGOUT ENABLED
```

Specifying the INACTIVITY TIMER

The INACTIVITY TIMER characteristic specifies the timeout period for all ports. You use the INACTIVITY TIMER characteristic when you enable the INACTIVITY LOGOUT characteristic.

The range for the timeout is from 1 to 120 minutes. The default is 30 minutes.

Example: Changing the INACTIVITY Timeout Period

The following command shows how to change the timeout period:

```
Local> CHANGE SERVER INACTIVITY TIMER 15
```

Chapter 11

Configuring Modem Signals

Overview

Introduction

This chapter describes the various port characteristics that you can use to control the modem signals. You use modem signals to support devices that use these signals, such as modems, computers, and printers.

In This Chapter

This chapter contains the following topics:

DTE/DCE Device Configuration

Port Configuration

The role of the access server in the communication is determined by the configuration of the port and the port device:

- If the port access characteristic is set to local, the access server appears as a data terminal equipment (DTE) device to a dial-in modem connected as a port device, and as a data communication equipment (DCE) device to a personal computer or terminal.
- If the port access characteristic is set to REMOTE, the access server appears as a DCE device to the port device, such as a computer system interface.
- If the port access characteristic is set to remote, the access server operates as a DTE device to a dial-out modem connected as a port device.

Determining the Supported Modem Signals

Access Servers and MODEM CONTROL

Not all access servers support all modem signals. There are three types of access servers:

- Full MODEM CONTROL
- MODEM CONTROL

  Access servers that support MODEM CONTROL can use only one of two sets of modem signals.
- DTR/DSR support

Access Server Types and Supported Modem Signals

The following table lists the types of access servers and the modem signals that each type supports. To determine the type of access server that you have, refer to the software product description (SPD) for your access server.

Network Access Server Type	Modem Signals Supported
Full MODEM CONTROL (Example: DECserver 700-08 access server)	Request To Send (RTS) Clear To Send (CTS) Data Set Ready (DSR) Data Terminal Ready (DTR) Data Carrier Detect (DCD) Speed Mode Indicator (SMI) RING Indicator (RI) Data Signal Rate Selector (DSRS)
MODEM CONTROL (Example: Access Server 316 access server)	Supports one of two sets of signals (software selectable): • Set 1 — Request To Send (RTS) — Clear To Send (CTS) — Data Set Ready (DSR) — Data Terminal Ready (DTR) • Set 2 — Data Signal Rate Selector (DSRS) — RING Indicator (RI) — Data Carrier Detect (DCD) — Data Terminal Ready (DTR)
DSR/DTR support (Example: DECserver 90TL access server)	Data Set Ready (DSR) Data Terminal Ready (DTR)

Modem Signals Description

Types of Modem Signal

The following table describes the various modem signals:

Modem Signal	Description
Request To Send (RTS)	Asserted by the access server to indicate to the port device that the access server is ready to exchange further control signals with the port device to initiate the exchange of data. The RTS signal is the same state as the DTR signal unless CTS input flow control is enabled.
Clear To Send (CTS)	Monitored by the access server and asserted by the port device to indicate that the port device is ready to receive data.
Data Set Ready (DSR)	Monitored by the access server and asserted by the port device to indicate that the port device is ready to exchange further control signals with the access server.
Data Terminal Ready (DTR)	Asserted by the access server to indicate that the access server is ready to exchange further control signals with the port device to initiate the exchange of data. (DTR is accompanied by RTS and DSRS.)
Data Carrier Detect (DCD)	Monitored by the access server and asserted by the port device to indicate that the received line signal is within acceptable limits.
Speed Mode Indicator (SMI)	Monitored by the access server to detect whether the modem at the access server port has selected the higher or lower speed in its range for exchanging data with a remote modem. SMI allows the use of a primary and alternate (or fallback) speed.
Ring Indicator (RI)	Monitored by the access server. This indicates that a calling signal is being received by the port device.
Data Signal Rate Selector (DSRS)	Asserted by the access server to indicate the speed at which the modem should initiate communications. On a port configured for a multispeed modem (where both SPEED and ALTERNATE SPEED are specified), DSRS indicates the higher of the two speeds.

Specifying MODEM CONTROL and SIGNAL CONTROL

Introduction

The MODEM CONTROL and SIGNAL CONTROL characteristics are identical, except that MODEM CONTROL is only used with full MODEM CONTROL access servers, and SIGNAL CONTROL is used on all other access servers.

These characteristics enable or disable the use of MODEM CONTROL signals on a port. With MODEM CONTROL or SIGNAL CONTROL enabled, the access server automatically logs out the port whenever a loss of the DSR signal (if used) is detected or if the DCD signal (if used) is deasserted for more than 2 seconds. Furthermore, a user must log in to the access server successfully within 120 seconds, or the access server automatically disconnects the call. You should disable MODEM CONTROL or SIGNAL CONTROL when a port is connected to a device that does not use modem signals, or if the device cable does not support modem signals.

Logging Out the Port with DSRLOGOUT or LONGBREAK LOGOUT

With MODEM CONTROL or SIGNAL CONTROL disabled, you can enable the access server to log out a port when the attached device is turned off by enabling port characteristic DSRLOGOUT (see Specifying DSRLOGOUT in Chapter 9) or LONGBREAK LOGOUT (see Specifying LONGBREAK LOGOUT in Chapter 9).

Computer Interface

For computer interface connections, you need to enable MODEM CONTROL or SIGNAL CONTROL and configure the host to use the modem signals. This ensures that session status is passed between the access server and the host system, which is important to maintain security.

When a user connected to the access server logs out from a system, the computer terminates the session and deasserts the DTR signal. The access server interprets this condition as a loss of DSR and terminates the session.

However, when the access server terminates a session, the access server deasserts the DTR signal. The system interprets this condition as a loss of DSR and logs out the user. This occurs when you enter a DISCONNECT command from the access server user interface or turn the power off.

The MODEM CONTROL or SIGNAL CONTROL characteristic can only be configured in the permanent database; therefore, you cannot use the SET or CHANGE command to configure MODEM CONTROL or SIGNAL CONTROL.

Example: Enabling MODEM CONTROL

The following example shows how to enable MODEM CONTROL on port 5:

```
Local> DEFINE PORT 5 MODEM CONTROL ENABLED
Local> LOGOUT PORT 5
```

Example: Enabling SIGNAL CONTROL

The following example shows how to enable SIGNAL CONTROL on port 11:

```
Local> DEFINE PORT 11 SIGNAL CONTROL ENABLED
Local> LOGOUT PORT 11
```

Normally, you should disable SIGNAL CHECK when MODEM CONTROL or SIGNAL CONTROL is enabled.

Specifying SIGNAL SELECT

Introduction

The SIGNAL SELECT characteristic is used only with MODEM CONTROL access servers. This characteristic determines which of two sets of signals that the access server uses:

- CTS, DSR, RTS, and DTR

  or

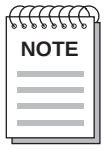
- RI, DCD, DSRS, and DTR

The port device must be cabled correctly to work with the set of signals that you choose.

Determining When to Use a Signal Set

The following shows when to use these signals:

- If the modem speed is below 9600 baud, configure the port SIGNAL SELECT characteristic to RI-DCD-DSRS-DTR.
- If the modem speed is 9600 baud or above, configure the port SIGNAL SELECT characteristic to CTS-DSR-RTS-DTR.



A maximum supported baud rate of 9600 on a modem is a guideline for signal set selection. The signals used are a factor of modem technology, not the actual baud rate for data tranfer.

Enabling CTS/RTS flow control for access servers with attached modems with 9600 baud or greater enables a faster response time from the access server hardware.

In order to enable SIGNAL CONTROL, you must configure SIGNAL SELECT.

Example: Enabling SIGNAL SELECT

The following example shows to configure SIGNAL SELECT to CTS-DSR-RTS-DTR on port 10:

```
Local> DEFINE PORT 10 SIGNAL SELECT CTS-DSR-RTS-DTR
Local> LOGOUT PORT 10
```

Specifying SIGNAL CHECK

Introduction

The SIGNAL CHECK characteristic allows the access server to check for any modem signal when a host requests a connection. If any one modem signal is present, the access server makes a connection; otherwise, a connection is denied. If all modem signals are dropped at the port once a connection is made, the access server disconnects the session and logs out the port. With SIGNAL CHECK disabled, the access server does not look for modem signals, and data might be lost. The factory-set default for SIGNAL CHECK is disabled.

Example: Enabling SIGNAL CHECK

The following example shows how to enable SIGNAL CHECK on port 7:

```
Local> CHANGE PORT 7 SIGNAL CHECK ENABLED
```

You should enable SIGNAL CHECK for ports with printers attached. If SIGNAL CHECK is disabled, data loss can occur when the device is turned off. However, you should not enable SIGNAL CHECK if you are using DSR or CTS flow control or if MODEM CONTROL or SIGNAL CONTROL is enabled.

You should enable SIGNAL CHECK along with either DSRLOGOUT or LONGBREAK LOGOUT and when the computer is turned off. This prevents users on the network from making a connection to the computer.

Specifying DTRWAIT

Description

When functioning with modems and computer interfaces, the access server port normally asserts the DTR signal at all times except during a disconnect sequence. However, there are instances when assertion of DTR is undesirable. For example, when a computer is offered as a service, the automatic reassertion of DTR after a disconnect sequence might cause the computer to act as if a session is in progress. If DTRWAIT is disabled, which is the factory-set default, the DTR signal is asserted on an idle port.

- When DTRWAIT is enabled, the access server can delay the assertion of DTR until a connection is detected from a modem when an interactive user logs in or when the access server receives a connection to the port from the network.
- With DTRWAIT enabled, the access server supports autoanswering equipment on a modem-control port. Upon detecting the RI signal from the modem, the access server asserts DTR and RTS, which allows the modem to answer the call. Then, upon detection of DSR, DCD, and CTS from the modem, the access server enables data transfer.
- DTRWAIT should be enabled for ports connected to computers and PCs. In order to enable DTRWAIT, you must enable MODEM CONTROL or SIGNAL CONTROL.

Enabling DTRWAIT Example

The following command shows how to enable DTRWAIT on port 3:

```
Local> CHANGE PORT 3 DTRWAIT ENABLED
```

Specifying RING

Description

The RING characteristic is supported only on those access servers that support the DSRS signal.

Certain terminal switches and computers need to detect a RING indicator signal (RI) before they activate. The access server can emulate the RI signal when the port is used with a BC22R or equivalent cable that crosses the DSRS signal of the access server over to the RI pin on the device. For information on this cable, refer to the access server hardware documentation.

When the port RING characteristic is set to enabled and MODEM CONTROL or SIGNAL CONTROL is enabled, the access server asserts and deasserts DSRS once every 2 seconds. This continues until either the access server detects DSR or 30 seconds have elapsed. Upon receiving DCD, the access server establishes the connection. DTR and RTS are asserted unless DTRWAIT is enabled.

Specifying ALTERNATE SPEED

Description

The ALTERNATE SPEED characteristic is only used with full MODEM CONTROL access servers.

Two speeds for a modem port can be defined in the access server database: primary and alternate (or fallback). The primary speed is defined with the speed characteristic; the ALTERNATE SPEED is defined with the ALTERNATE SPEED characteristic. You normally set up the primary speed as the high speed and the ALTERNATE SPEED as the low speed. For ALTERNATE SPEED to work, you must specify a single input/output speed for the speed characteristic.

If an ALTERNATE SPEED is specified, the access server asserts the DSRS signal along with DTR and RTS when receiving a connection. DSRS indicates that the higher primary speed should be used.

The access server monitors the SMI signal to determine whether to use the higher or lower speed. When SMI is asserted, the access server selects the higher speed; when SMI is deasserted, the communications selects the lower speed. The modem connected to the access server must support the SMI signal in order for ALTERNATE SPEED to work; otherwise, erroneous data transmission can occur. To determine whether the modem supports the SMI signal, refer to your modem's documentation.

The ALTERNATE SPEED feature can be used with dial-out (sends calls) modems. For dial-in (receives calls) modems, you should enable autobaud and disable ALTERNATE SPEED. This allows you to configure the dial-in modem to any speed supported by both the modem and the access server.

Specifying DIALUP

Description

The DIALUP characteristic is used to notify LAT service nodes that a port user connected to the service through a dial-in modem. The service node can use this information to implement system security. With DIALUP enabled, the access server sends DIALUP notification to service nodes. With DIALUP disabled (the default), the access server does not notify the service nodes. If you do not enable DIALUP, the service node could treat the user's service sessions as local connections at the service node itself. Ask the network manager and the service node system manager if they require this notification when there are dial-in modems at access server ports. The DIALUP characteristic is not used for resources on the TCP/IP network.

Sample Modem Configurations

Introduction

This section provides sample modem configurations for access servers that support full MODEM CONTROL.

Configuring a Dial-In Modem on a Full MODEM CONTROL Server

The following example provides a sample configuration for a dial-in modem operating at 57600 baud. Note that when the port password characteristic is enabled, you must have previously defined a server login password (refer to Specifying Passwords in Chapter 22).

```
Local> DEFINE PORT 6 ACCESS LOCAL ALTERNATE SPEED NONE AUTOBAUD ENABLED
Local> DEFINE PORT 6 INACTIVITY LOGOUT ENABLED MODEM CONTROL ENABLED
Local>
```

Configuring a Dial-In Modem on a MODEM CONTROL Server

The following example provides a sample configuration for a dial-in modem operating at 9600 baud and configured for the RI-DCD-DSRS-DTR signals. Note that when the port password characteristic is enabled, you must have previously defined a server login password (refer to Specifying Passwords in Chapter 22).

```
Local> DEFINE PORT 6 ACCESS LOCAL AUTOBAUD ENABLED SPEED 9600
Local> DEFINE PORT 6 INACTIVITY LOGOUT ENABLED SIGNAL CONTROL ENABLED
Local> DEFINE PORT 6 PASSWORD ENABLED SIGNAL SELECT RI-DCD-DSRS-DTR
Local> DEFINE PORT 6 SPEED 9600
```

Configuring a Dial-Out Modem on a Full MODEM CONTROL Server

The following example provides a sample configuration for a dial-out modem operating at 1200 baud with an ALTERNATE SPEED of 300 baud:

```
Local> DEFINE PORT 3 ACCESS REMOTE AUTOBAUD DISABLED
Local> DEFINE PORT 3 AUTOPROMPT DISABLED BREAK DISABLED
Local> DEFINE PORT 3 DSRLOGOUT DISABLED DTRWAIT ENABLED
Local> DEFINE PORT 3 MODEM CONTROL ENABLED SIGNAL CHECK DISABLED
Local> DEFINE PORT 3 SPEED 1200 ALTERNATE SPEED 300
Local> LOGOUT PORT 3
```

Configuring a Dial-In and Dial-Out Modem on a Full MODEM CONTROL Server

The following example provides a sample configuration for a dial-in and dial-out modem operating at 2400 baud:

```
Local> DEFINE PORT 4 ACCESS DYNAMIC AUTOBAUD DISABLED
Local> DEFINE PORT 4 DSRLOGOUT DISABLED FLOW CONTROL XON
Local> DEFINE PORT 4 INACTIVITY ENABLED MODEM CONTROL ENABLED
Local> DEFINE PORT 4 PASSWORD ENABLED SIGNAL CHECK DISABLED SPEED 2400
Local> LOGOUT PORT 4
```

Configuring a Dial-Out Modem on a MODEM CONTROL Server

The following example provides a sample configuration for a dial-out modem operating at 2400 baud and configured for the RI-DCD-DSRS-DTR signals:

```
Local> DEFINE PORT 3 ACCESS REMOTE AUTOBAUD DISABLED
Local> DEFINE PORT 3 AUTOPROMPT DISABLED BREAK DISABLED
Local> DEFINE PORT 3 DSRLOGOUT DISABLED DTRWAIT ENABLED
Local> DEFINE PORT 3 SIGNAL CONTROL ENABLED SIGNAL CHECK DISABLED
Local> DEFINE PORT 3 SIGNAL SELECT RI-DCD-DSRS-DTR
Local> DEFINE PORT 3 SPEED 2400
Local> LOGOUT PORT 3
```

Configuring a Dial-In and Dial-Out Modem on a MODEM CONTROL Server

The following example provides a sample configuration for a dial-in and dial-out modem operating at 115200 baud and configured for the CTS-DSR-RTS-DTR signals:

```
Local> DEFINE PORT 4 ACCESS DYNAMIC AUTOBAUD DISABLED
Local> DEFINE PORT 4 DSRLOGOUT DISABLED FLOW CONTROL XON
Local> DEFINE PORT 4 INACTIVITY ENABLED SIGNAL CONTROL ENABLED
Local> DEFINE PORT 4 PASSWORD ENABLED SIGNAL CHECK DISABLED
Local> DEFINE PORT 4 SIGNAL SELECT CTS-DSR-RTS-DTR
Local> DEFINE PORT 4 SPEED 115200
Local> LOGOUT PORT 4
```

MODEM CONTROL Sequences

Introduction

Modem-controlled communication requires that the access server recognize what type of device is on a port and detect when this device is ready to communicate and when the device has ceased to communicate. The following section describes the general sequences of modem signals involved in establishing, in monitoring, and in ending communications.

Establishing a Connection

When a connection is initiated at a port, the access server follows the signaling sequence described in this section.

1. First, the access server examines the DTRWAIT characteristic to determine whether to assert data terminal-ready signal (DTR) and the request-to-send signal (RTS) while the port is idle.

   If DTRWAIT is DISABLED, the access server asserts DTR and RTS while the port is logged out.

   If DTRWAIT is enabled, the access server delays assertion of DTR and RTS until either it detects any modem signal or a connection occurs. Then, the access server asserts DTR and RTS.

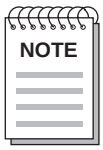
   When asserting DTR and RTS, if conditions require the data-signal-rate-selector signal (DSRS), the access server asserts DSRS at the same time.

2. After asserting DTR and RTS, the access server waits 2 seconds and monitors the data-set-ready signal (DSR), which helps the access server identify the type of device on the port. The presence of DSR indicates a null modem device. A delay of DSR indicates a modem.

   If DSR is delayed, the access server watches for one of the following situations:

   — A clear-to-send signal (CTS), which indicates a V.25/bis compatible modem.

   — The absence of a signal, which indicates a DIGITAL modem.



For dial-out modems, the access server enables data communication before detecting DSR. Otherwise, the access server waits until detecting DSR to enable data communication.

3. After first detecting DSR, the access server monitors the port for CTS and DCD. If it detects CTS and DCD within 30 seconds, the access server enables data flow on the line. If it does not detect CTS and DCD within 30 seconds, the access server disconnects the line.
4. At this point, if an ALTERNATE SPEED is defined, the access server examines the state of the SMI signal. The modem asserts SMI if it has accepted the higher port speed. When it requires a fallback speed, the modem does not assert SMI, and the access server sets the port to the fallback (lower) speed.
5. For dial-in lines, the user must log in to the access server successfully within 120 seconds, or the access server automatically disconnects the call.

Response to Momentary Loss of CTS

If the port device drops CTS (but not DCD), the access server suspends data transmission on the line until the port device reasserts CTS.

Disconnecting

The access server disconnects the sessions on a port when any of the following events occur on the port: DCD is lost for more than 2 seconds, DSR is lost, or a LOGOUT command is received.

Disconnecting involves the following series of events:

1. The access server disables data exchanges on the port and waits 300 milliseconds for the stop bit of the last transmitted character to be given to the port device.
2. The access server logs out the port, thereby disconnecting all sessions.
3. The access server drops DTR, RTS, and DSRS for 5 seconds.
4. After 5 seconds, the access server resumes the port device interaction as described in step 1 of the Establishing a Connection sequence in this section.

Configuring DTR and DSR Signals

Introduction

This section describes how to configure DTR and DSR signals for those access servers that do not support the other modem signals. DSR flow control must be disabled when you are using the various port characteristics to control the DSR and DTR signals. DSR flow control can override the port characteristics.

Port Characteristic Effects on the DTR and DSR Signals

The following table shows the enabled port characteristic effect on DTR and DSR signals:

Enabled Characteristic	DTR and DSR Actions
SIGNAL CONTROL	DTR is deasserted for 5 seconds as a consequence of a logout; otherwise, it is always asserted.
(SIGNAL CHECK and DTRWAIT disabled)	Solicited remote connection is established regardless of the state of DSR. Reception of asynchronous data is accepted once the connection is established. Port is logged out if DSR is deasserted after initial assertion.
DSRLOGOUT	DTR is always asserted.
(SIGNAL CONTROL and SIGNAL CHECK disabled	Solicited remote connection is accepted regardless of the state of DSR. Port is logged out if DSR is deasserted after initial assertion. Reception of asynchronous data is not be accepted unless DSR is asserted.
SIGNAL CHECK	DTR is always asserted.
(SIGNAL CONTROL disabled)	Solicited remote connection will not be accepted unless DSR is asserted. Port is logged out if DSR is deasserted after initial assertion. Port status indicates “Signal Wait” if connections cannot be accepted because DSR is deasserted.
DTRWAIT	Has no affect unless SIGNAL CONTROL is enabled.

Enabled Characteristic	DTR and DSR Actions
SIGNAL CONTROL and DTRWAIT	DTR is asserted only if there is a solicited remote connection.
(SIGNAL CHECK disabled)	Solicited remote connection is established regardless of the state of DSR. Reception of asynchronous data is accepted once the connection is established. Port is logged out if DSR is deasserted after initial assertion. DTR is deasserted for 5 seconds minimum as a consequence of a logout. DTR can only be reasserted when a connection is accepted. Reception of asynchronous data is not accepted unless DSR and DTR are asserted.
SIGNAL CONTROL and SIGNAL CHECK	DTR is deasserted for 5 seconds minimum as a consequence of a logout; otherwise, it is always asserted.
(DTRWAIT disabled)	Port is logged out if DSR is deasserted after initial assertion. Reception of asynchronous data is not accepted unless DSR and DTR are asserted. Port status indicates “Signal Wait” if connections cannot be accepted because DSR is deasserted. Solicited remote connection is not accepted unless DSR is asserted.
SIGNAL CONTROL, SIGNAL CHECK, and DTRWAIT	DTR will only be asserted if there is a solicited remote connection. Port is logged out if DSR is not asserted within 60 seconds of connection acceptance. Port is logged out if DSR is deasserted after initial assertion. DTR is deasserted for 5 seconds minimum as a consequence of a logout. DTR can only be reasserted when a connection is accepted. Reception of asynchronous data is not accepted unless DSR and DTR are asserted. Port status indicates “Signal Wait” if connections cannot be accepted because DSR is deasserted. Solicited remote connection is not accepted unless DSR is asserted.
SIGNAL CONTROL and DSRLOGOUT	Same as SIGNAL CONTROL.
SIGNAL CONTROL, SIGNAL CHECK, and DSRLOGOUT	Same as SIGNAL CONTROL and SIGNAL CHECK.

Enabled Characteristic	DTR and DSR Actions
SIGNAL CONTROL, DTRWAIT, and DSRLOGOUT	Same as SIGNAL CONTROL and DTRWAIT.
SIGNAL CONTROL, SIGNAL CHECK, DTRWAIT, and DSRLOGOUT	Same as SIGNAL CONTROL, SIGNAL CHECK, and DTRWAIT.
SIGNAL CHECK and DSRLOGOUT	Same as SIGNAL CHECK.

Chapter 12

Configuring and Managing Interactive Devices

Overview

Introduction

This chapter explains how to configure and manage interactive devices, such as terminals, terminal-like devices, and personal computers (PCs) in terminal emulation mode. Before you use the procedures in this chapter, you must:

- Connect and test the devices.
- Enable privileged status.
- Configure the port and device characteristics to match.

For More Information

For information about connecting device cables, refer to your access server hardware documentation.

In This Chapter

This chapter contains the following topics:

- Specifying the Telnet Client Session Profile
- Configuring Individual Telnet Client Session Characteristics
- Managing Access Server User Accounts
- Managing Users
- Managing Sessions

Configuring an Interactive Device for LAT Sessions

Configuring an Interactive Device for LAT Sessions

The following example shows a sample configuration of a device connected to LAT services:

```
Local> CHANGE PORT 6 ACCESS LOCAL AUTHORIZED GROUPS 10,24,46
Local> CHANGE PORT 6 AUTOBAUD ENABLED AUTOPROMPT ENABLED
Local> CHANGE PORT 6 BREAK LOCAL DEDICATED NONE DEFAULT PROTOCOL LAT
Local> CHANGE PORT 6 DSRLOGOUT ENABLED FLOW CONTROL XON
Local> CHANGE PORT 6 INACTIVITY LOGOUT ENABLED INTERRUPTS DISABLED
Local> CHANGE PORT 6 LIMITED VIEW DISABLED PASSWORD DISABLED
Local> CHANGE PORT 6 QUEUING ENABLED REMOTE MODIFICATION DISABLED
Local> SET PORT 6 GROUPS ALL ENABLED
```

Sample Network Configuration

Figure 12-1 shows the sample network configuration for LAT and Telnet sessions:

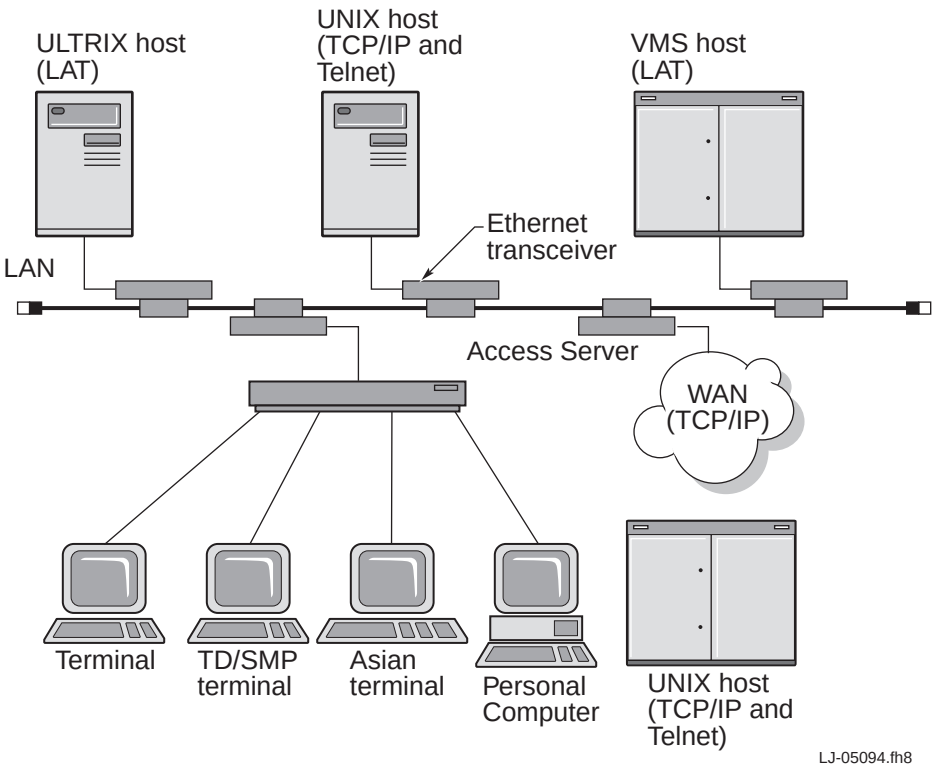


Figure 12-1. Sample Network Configuration for LAT and Telnet Sessions

Configuring LAT Group Codes for Interactive Devices

Group codes are subdivisions of a LAT network. Group codes are used to partition the network into combinations of service nodes, service-node services, and access server ports.

To configure group codes on an access server, perform the following steps:

Step	Action
1	Determine the group codes of the LAT services that a port user needs by entering the SHOW NODE STATUS command.

2	Enable the applicable groups on the port as illustrated by the following commands:
	
	`Local> CHANGE PORT 5 AUTHORIZED GROUPS 10,24,46`
	`Local> SET PORT 5 GROUPS ALL ENABLED`

3	If necessary, disable any unwanted group that was previously enabled. The following commands show how to disable group 0 on port 5:
	
	`Local> CHANGE PORT 5 AUTHORIZED GROUPS 0 DISABLED`
	`Local> SET PORT 5 GROUPS ALL ENABLED`

Specifying AUTOCONNECT

When you disable the AUTOCONNECT characteristic on a given port, the access server displays the local mode prompt after you log in. You can then enter the CONNECT command to use a network resource.

When you enable the AUTOCONNECT characteristic on a given port and a dedicated or preferred service is enabled, the port automatically connects a port to that service at log in. The port also attempts to reestablish the current session if the connection fails. You must enable AUTOCONNECT for a dedicated service port.

With preferred and dedicated service disabled, enabling AUTOCONNECT allows the access server to attempt to reestablish any service connection that terminates abnormally. If a service is not available when a connection attempt is made, the access server repeatedly retries to connect as specified by the CONNECT command. This feature is helpful when a user wants the access server to repeat connection attempts to a currently non-operational service node. When a session is established with the node, the access server notifies the user with a beep signal and a message.

Attempts to reconnect upon LAT session failure are made every 30 seconds. The attempts continue until the user enters local mode by using the Break key or the local switch key. Unless a dedicated service is in effect, a status message appears at the port device indicating that the access server is trying to restart a session. The new connection can be made to any service node that supplies the same service, unless a node or destination was supplied in the CONNECT command or when the preferred service was set up.

Example: Enabling AUTOCONNECT

The following example shows how to enable AUTOCONNECT on port 5:

```
Local> CHANGE PORT 5 AUTOCONNECT ENABLED
```

Specifying AUTOPROMPT

The AUTOPROMPT characteristic is only used with the LAT protocol. This characteristic controls the initiation of a login process on some service nodes when a session begins. The access server sends the status of the AUTOPROMPT characteristic whenever you establish a new LAT service session.

By default, AUTOPROMPT is enabled. If the service node supports AUTOPROMPT, the service node performs a system-specific login sequence, such as displaying a service announcement or login prompt.

If you disable AUTOPROMPT and the service node recognizes this, the service node does not perform any login sequence. Since devices without keyboards cannot respond to a login sequence, you should disable AUTOCONNECT for these devices.

Example: Disabling AUTOPROMPT

The following example shows how to disable AUTOPROMPT:

```
Local> CHANGE PORT 5 AUTOPROMPT DISABLED
```

Specifying the Default Protocol

The following options are available with the SET / DEFINE / CHANGE PORT DEFAULT PROTOCOL command:

- LAT — The access server defaults to the LAT protocol when the user does not specify a protocol in the CONNECT command.
- SLIP — The access server defaults to the SLIP protocol when the user does not specify a protocol in the CONNECT command.
- TELNET — The access server defaults to the Telnet protocol when the user does not specify a protocol in the CONNECT command.
- ANY — The access server first searches the network resources on the LAT network when the user does not specify a protocol in the CONNECT command. If unsuccessful, the access server then searches the network resources on the TCP / IP network. The AUTOCONNECT characteristic must be disabled when the default protocol is set to ANY.

- PPP — The access server defaults to the PPP protocol if the user does not specify a protocol with the CONNECT command.
- AUTOLINK — The access server passively examines characters received from the attached device. If the access server detects a PPP or SLIP connection, it attempts to change the current session into the appropriate data link session type, PPP or SLIP. If the access server cannot identify the data as PPP or SLIP, it starts and interactive session.

  An adjunct to the AUTOLINK protocol is AUTOLINK authentication. See Managing Dial-Up Access Security with AUTOLINK and AUTOLINK Authentication in Chapter 21 for details.

Specifying Failover

If a LAT service node suddenly becomes unavailable during a session, the access server searches for another LAT service node that offers the same service. If the access server finds one or more suitable nodes, it attempts to connect to the service on the node with the highest service rating. This process is called failover.

When used with a VAXcluster computer network, failover provides a flexible terminal connection to the VAXcluster service.

This feature can be disabled on each port.

Example: Disabling Port Failover

The following example shows how to disable failover on port 2:

```
Local> CHANGE PORT 2 FAILOVER DISABLED
```

Configuring Port Queuing

When a user on the access server tries to connect to a busy service on an access server, the Port Queuing characteristic allows the connect request to be queued. The service must be on an access server, either the same one as the user's or a different one.

The queuing of the connect request also depends on whether the access server offering the service has reached its queue limit or has queuing disabled. In this case, the connection is not queued and the user receives a message that indicates that service is not available.

If the access server offering the service has queuing enabled and has not reached its queue limit, the request is queued. If more than one access server offers the service, your access server will attempt to connect to the target access server that has the highest service rating. For access servers that offer queuing, service ratings are higher for access servers that have the greatest number of open positions in their connection queues.

If the port queuing characteristic is disabled, your access server cannot request a queue connection when a service is busy. Therefore, if the service is busy, your user receives a message that indicates that service is not available.

The factory-set default is disabled.

Example: Enabling Queuing on a Port

This example shows how to enable queuing on port 5:

```
Local> CHANGE PORT 5 QUEUING ENABLED
```

The Service Connections Characteristic

The service connections characteristic allows you to disable additions to the connection queue when a given service is busy. Changing this characteristic does not affect requests that are already in the queue.

Example: Disabling Port Queuing

The following example shows how to disable additional queued connections for the service LN03_PRINT:

```
Local> CHANGE SERVICE LN03_PRINT CONNECTIONS DISABLED
```

Server Queue Limit Characteristics

The server queue limit characteristic the maximum number of entries permitted at one time in the queue. The access server can queue up to 200 connection requests.

Example: Changing Queue Limit Characteristics

The following example shows how to change the queue limit to 150:

```
Local> CHANGE SERVER QUEUE LIMIT 150
```

Displaying Access Server Queue Entries

The SHOW / MONITOR QUEUE command displays the status of requests in the connection queue.

Options for the SHOW/MONITOR QUEUE Command

The following table lists the SHOW / MONITOR QUEUE commands:

Option	Displays Entries For
PORT *port-number*	A specific port
NODE *node-name*	A specific node
SERVICE *service-name*	A specific service
ALL	All types of requests

For example, to display information about the entries for the service LASER, enter the following command:

```
Local> SHOW QUEUE SERVICE LASER
```

The entry identification numbers in a SHOW / MONITOR QUEUE display can range from 1 to 9999. They are not related to the queue depth or the queue limit.

SHOW QUEUE ALL Display Example

The following example shows how to generate a queue display. For each queued request, the displays have one line of information arranged in columns under fixed headings.

```
Local> SHOW QUEUE ALL

Position  Entry  Source Node  Service      Port  Name
1         128    ORANGE       TIMESHARING4 2     PORT_NAME
2         130    BANANA       SALES        4     PORT_NAME
3         131    PEACH        ENGINEERING
```

Removing Entries from the Access Server Queue

Use the REMOVE QUEUE command to modify the connection queue by selectively removing entries from the queue. When you remove an entry from the access server queue, the access server notifies either the requesting service node (for a host-initiated request) or the terminal user (for a local-access request) that the request is being rejected.

No default entry exists for the REMOVE QUEUE command, and failure to specify what entry or entries are to be removed from the queue results in an error. The following sets of entries can be removed:

- A specific entry by using the REMOVE QUEUE ENTRY entry-number command for each entry
- The entries from a specific requesting node by using the REMOVE QUEUE NODE node-name command
- The entries for a specific requested service by using the REMOVE QUEUE SERVICE service-name command
- All queue entries by using the REMOVE QUEUE ALL command

Effect on the Queue

The REMOVE QUEUE ALL command deletes all queue entries, but it does not disable the queue; the next connection request takes position 1 in the queue.

Example: Remove Queue

The following example shows how you can remove entry number 10 by using the following privileged command:

```
Local> REMOVE QUEUE ENTRY 10
```

Configuring Port Characteristics

The port characteristic, remote modification, when enabled, allows a LAT node to modify particular access server port characteristics. These characteristics include speed, character size, parity, and LOSS NOTIFICATION. The LAT node must also support this feature. The factory-set default is disabled.

You should avoid enabling remote modification and security on the same port. Enabling these characteristics allows a secure user to modify the port from the host; normally the secure user cannot modify the port.

Example: Configuring Remote Modification for Port Characteristics

The following example shows how to enable remote modification on port 5:

```
Local> CHANGE PORT 5 REMOTE MODIFICATION ENABLED
```

Configuring an Interactive Device for Telnet Sessions

Introduction

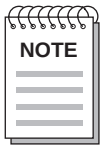
User-oriented characteristics, such as forward switch and VERIFICATION and the various Telnet session characteristics (see Configuring Individual Telnet Client Session Characteristics in this chapter), are not included in this example. Also, this example assumes that the port and device characteristics match. (See the Matching the Port and Device Characteristics section in Chapter 9.)

The following are variables that you should substitute with the appropriate value:

- Access server port number
- FLOW CONTROL (you cannot enable DSR FLOW CONTROL when the DSRLOGOUT characteristic is enabled, as described in FLOW CONTROL Types)

Reference

For a description of each command, refer to the Cabletron *Network Access Software Command Reference* guide.



Not all commands can be combined on one line.

Configuring a Device on Port 6 for Internet Hosts Example

The following example shows a sample configuration of a device connected to Internet hosts, which is illustrated in the Sample Network Configuration section in this chapter:

```
Local> CHANGE PORT 6 ACCESS LOCAL AUTOBAUD ENABLED
Local> CHANGE PORT 6 BREAK LOCAL DEDICATED NONE
Local> CHANGE PORT 6 DEFAULT PROTOCOL TELNET
Local> CHANGE PORT 6 DSRLOGOUT ENABLED FLOW CONTROL XON
Local> CHANGE PORT 6 INACTIVITY LOGOUT ENABLED INTERRUPTS DISABLED
Local> CHANGE PORT 6 LIMITED VIEW DISABLED PASSWORD DISABLED
Local> CHANGE PORT 6 TELNET CLIENT PROFILE CHARACTER
```

To connect to any host available on the TCP/IP network, the user enters the CONNECT, OPEN, or TELNET command.

Enable DSRLOGOUT or LONGBREAK LOGOUT (see Specifying DSRLOGOUT and Specifying LONGBREAK LOGOUT in Chapter 9) if you wish the access server to log out the port when the device is turned off. Note that the access server, device, and device cable must support the DSR signal if you use DSRLOGOUT.

Reference

For a description of the default protocol characteristic, refer to Specifying the Default Protocol in this chapter.

For a description of the Telnet client profiles, refer to Specifying the Telnet Client Session Profile in this chapter.

Configuring a Session Management (TD/SMP) Terminal

Introduction

The MULTISESSION characteristic allows a session management terminal using the terminal device / session management protocol (TD / SMP) to manage each terminal session at the terminal itself, not at the access server. A terminal session is a single session on an access server port that is operating under session management control.

Session management terminals can have more than one terminal session with the access server, but each terminal session can have one service session. A service session is a session between a network resource and the terminal session.

With session management terminals, TD / SMP maintains the context of a service session when the user switches to another terminal session. Session data from a service node continues even though the service session is currently inactive. You can visualize a session management terminal as two or more standard terminals using the same physical access server port. For terminals that do not implement TD / SMP, the access server suspends service session data until the user resumes the session.

How to Configure

Configure the session management terminal for a LAT session as described in the Configuring an Interactive Device for LAT Sessions section in this chapter. Configure a Telnet session as described in the Configuring an Interactive Device for Telnet Sessions section in this chapter. In addition you enable MULTISESSIONs on the port, as follows:

```
Local> CHANGE PORT 2 MULTISESSIONS ENABLED
```

Benefits and Restrictions Summary

The following is a summary of the benefits and restrictions for session management terminals:

- Context preservation for terminal sessions and their corresponding service sessions.
- Multiple local modes (one for each terminal session) to manage service sessions and port characteristics.

- Simultaneous data exchange with multiple service sessions.
- Management of terminal sessions using terminal commands.
- Restrictions on some access server commands (see the table in the Local Mode Command Restrictions During Session Management section in this chapter).
- The dedicated service characteristic must be disabled. (See the User Account Command Parameters section in this chapter.)

Local Mode Command Restrictions During Session Management

The following table list the restrictions on some of the access server commands:

Command	Description
CONNECT	Establishes a service session for any terminal session. You cannot use it to establish an additional service session. To do this, you must open another terminal session.
DISCONNECT DISCONNECT ALL	Either command disconnects the current service session but does not disconnect the terminal session. When a service session is disconnected, the terminal session remains in local mode.
LOGOUT LOGOUT PORT	LOGOUT closes your current terminal session only and disconnects the service session associated with it (if there is one). You are not logged out of the access server. You can open or switch to another terminal session. LOGOUT PORT does a full log out, logging you out of the access server, closing all terminal sessions and service sessions. It also ends session management.
SET PRIVILEGED	Applies to the port and to all terminal sessions on the port.
SET / DEFINE / CHANGE PORT	Changes the current characteristics for an access server port. Changes apply to all terminal sessions for that port. The preferred service characteristic behaves differently for terminal sessions. The preferred service is supported while you are in a terminal session when you use a CONNECT command without specifying a service. The preferred service also takes effect when you establish a terminal session if you do not specify a service name when the terminal prompts you for one. If you do not want to connect to the preferred service from your terminal session, enter the name “local” when your terminal prompts you for a service name.

Logging In with Multisessions

The following is a typical procedure for logging in at a session management terminal with MULTISESSIONS enabled at the access server port:

Step	Action
1	Press the Return key once or twice to obtain the introductory banner and username prompt. After the user optionally enters a user name, the access server invokes session management, and the terminal prompts the user for a network resource name. The access server then uses that name to create a session for the terminal session. If a preferred service is defined and AUTOCONNECT is enabled, the access server starts a session with the preferred service. If you do not enter a network resource name for a terminal session, the access server places the port in local mode.
2	Request additional terminal sessions (and associated sessions) by entering a terminal command. The terminal prompts the user again for a network resource name for each terminal session. The access server creates a session for each terminal session.
3	Switch among your terminal sessions by using a switch session key on the terminal keyboard.

In local mode, you can enter access server commands at the access server prompt. (The Local Mode Command Restrictions During Session Management table lists command restrictions that apply to session management terminals.) If you enter LOCAL as a service name for a terminal session, the access server places the port in local mode.

Configuring On-Demand Loading for Asian Terminals

Introduction

Asian terminals implementing the On-Demand Loading (ODL) font protocol can communicate with an OpenVMS load host through an access server. The access server software has an on-demand loading characteristic that enables the ODL protocol. When the on-demand loading characteristic is enabled on the access server, the ODL protocol overrides FLOW CONTROL during font loading to allow for Asian characters. This function is available only on a LAT network.

On-Demand Loading Configuration Example

The following shows how to enable on-demand loading on port 5:

```
Local> CHANGE PORT 5 ON-DEMAND LOADING ENABLED
```

Disable Switch Character

You should disable the access server switch characters to prevent interference with font requests from an Asian terminal.

Reference

See the following sections in this chapter: Specifying Keys to Switch Between Sessions, Defining the Break Key, and Specifying a Key to Switch to Local Mode.

Configuring for Block-Mode Terminals

Description

Block-mode terminals do not require any special setup to communicate with a host through an access server. The access server software automatically allows terminals that support block mode to transmit large blocks of data without using FLOW CONTROL.

Buffer Size

The maximum receive buffer size is 2048 bytes.

Specifying the Telnet Client Session Profile

Introduction

You can set various features for a Telnet client session. You can either choose a profile that has many of the characteristics predefined or set the characteristics individually (refer to Configuring Individual Telnet Client Session Characteristics in this chapter). Many of the characteristics have factory-set defaults.

Profiles Types

Each profile is a set of predefined Telnet client session characteristics. There are two basic profiles:

- CHARACTER — Typically used with interactive users at a terminal or similar device. All characters entered by the user are sent to the Internet host for handling. The host edits, ECHOes, and processes the user data. This is the factory-set default.
- BINARY — Used primarily with file transfers. All port and Telnet special characters, such as forward and backward switches and XON / XOFF FLOW CONTROL characters, are ignored by the access server and sent to the Internet host.

Profile Characteristics

You can customize a profile by first selecting a profile, then changing specific characteristics. However, the profile itself is invalidated. For example, you could select the BINARY profile, then enable FLOW CONTROL in the receive direction. To display the profile and client session characteristics, refer to Displaying Session Characteristics in this chapter.

Telnet Client Session Characteristics Predefined for Each Profile

The following table lists the Telnet client session characteristics that are predefined for each profile. Enabling a profile automatically sets all the characteristics to the value specified by the profile, except those listed as "use current value." Those characteristics keep their existing value.

	Profiles	
Session Characteristics	**Character**	**Binary**
ECHO	Remote	Use current access server value 1
BINARY	Disabled	Duplex
CHARACTER SIZE (Transmit)	Use current value	8
CHARACTER SIZE (Receive)	Use current value	8
SIGNAL REQUEST	Enabled	Disabled
AO, IP, AYT, SYNCH, EOR, BRK	Use current value	Not used
TOGGLE ECHO	Not used	Not used
QUOTE	Use current value	Not used
AUTOFLUSH	Use current value	Not used
AUTOSYNC	Use current value	Not used
NEWLINE FROM TERMINAL	Use current value	Not used
NEWLINE TO TERMINAL	Use current value	Not used
NEWLINE FROM HOST	Use current value	Not used
NEWLINE TO HOST	Use current value	Not used
FLOW CONTROL	Enabled	Disabled
MESSAGE VERIFICATION	Enabled	Disabled
SWITCH CHARACTERS	Enabled	Disabled
TERMINAL TYPE	Use current access server value	Use current access server value

[1] If ECHO is in local mode, the ECHO characteristics are suppressed, and characters are not echoed.

Configuring Individual Telnet Client Session Characteristics

Modifying Telnet Session Characteristics

You can modify the Telnet client session characteristics in two ways: at the port level or for the individual session using the SET SESSION command. Modifying the characteristics at the port level enables those values for Telnet client sessions at that port when sessions are created. Also, you can save the characteristics in the permanent database. The values you set with the SET SESSION command are lost once you log out of the session.

Specifying ECHO Characteristics

The user can specify whether characters entered at the port device are echoed at the access server (LOCAL) or at the remote Internet host (REMOTE). The factory-set default is REMOTE. The Example: Specifying ECHO Characteristics shows how to set ECHO CONTROL to LOCAL on port 5.

Example: Specifying ECHO Characteristics

```
Local> CHANGE PORT 5 TELNET CLIENT ECHO LOCAL
```

You can suppress local echoing by either selecting ECHO LOCAL and then selecting the BINARY profile or by selecting ECHO LOCAL and then using the toggle ECHO character (See Specifying ECHO Characteristics in this chapter).

Specifying the BINARY Characteristic

The BINARY characteristic allows the user to enable BINARY communication in either one or both directions (to or from the Internet host). The TRANSMIT characteristic enables BINARY communication in the access server to the Internet host direction. The RECEIVE characteristic enables BINARY communication in the Internet host to the access server direction. The DUPLEX characteristic enables BINARY communication in both directions.

The following example shows how to enable BINARY communication in the transmit direction on port 5:

Example: Enabling BINARY Characteristics

```
Local> CHANGE PORT 5 TELNET CLIENT BINARY TRANSMIT
```

Enabling the BINARY characteristic does some, but not all, of what a user might require to send and receive BINARY files over the Telnet connection. For BINARY transfers, you should use the BINARY profile instead of the BINARY characteristic.

The following example shows how to disable the BINARY characteristic:

Example: Disabling BINARY Characteristics

```
Local> CHANGE PORT 5 TELNET CLIENT BINARY DISABLE
```

Specifying CHARACTER SIZE

The CHARACTER SIZE characteristic allows the user to select the character size, 7- or 8-bit, that is used during a session with an Internet host. In addition, the character size can be specified in the transmit direction, receive direction, or both directions.

Example: Setting CHARACTER SIZE

The following example shows how to set CHARACTER SIZE to 7-bit in both directions for port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT CHARACTER SIZE 7
```

Example: Setting CHARACTER SIZE for a Specific Direction

The following example shows how to set CHARACTER SIZE to 7 in the transmit direction. To set the character size in the receive direction, use RECEIVE instead of TRANSMIT.

```
Local> CHANGE PORT 5 TELNET CLIENT TRANSMIT CHARACTER SIZE 7
```

Mapping Keyboard Characters to Telnet Functions

You can assign keyboard characters to various Telnet functions. The SIGNAL REQUEST characteristic can enable or disable all these functions. The factory-set default is ENABLED.

Example: Disabling SIGNAL REQUEST

The following example shows how to disable SIGNAL REQUEST on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT SIGNAL REQUEST DISABLED
```

Example: Mapping Keyboard Characters

The following example shows how to map the AO function to the Delete key:

```
Local> CHANGE PORT 5 TELNET CLIENT AO <DEL>
```

You can use the SET SESSION command to map a Telnet function to a key for a particular session. This mapping only lasts for the duration of the specified session. You cannot map a keyboard character to more than one function.

Telnet Keymapping Functions

The following table shows key function definitions mapped to specific keys. You can disable any of the Telnet commands in this table by using the keyword NONE. For example, to disable AO for port 5, you enter the following:

```
Local> CHANGE PORT 5 TELNET CLIENT AO NONE
```

Function	Description	Default
Abort Output (AO)	Aborts any output that is on its way to the user's terminal. If an Internet host hangs after an AO is sent, use the SEND RESUME OUTPUT command.	Ctrl/O
Interrupt Process (IP)	Aborts the process at the remote Internet host.	Ctrl/Y
Synch	Drops input on its way to the remote Internet host. This includes output queued by the access server and the host.	Ctrl/X
Are You There (AYT)	Verifies if the connection to the Telnet server is still active. You must resume the session to see the Telnet server's response.	Ctrl/T
Break (BRK)	Sends a Telnet Break command to the Internet host. The way that this command is interpreted depends on the host.	None
End of Record (EOR)	Sends a Telnet End of Record command to the Internet host. This command is only sent if the EOR option is enabled through negotiation with the peer.	None

Function	Description	Default
Quote	Causes the next character to be treated as ordinary data. To send a key mapped to a Telnet command as ordinary data, you precede the key with the Quote command.	None
Toggle Echo	Defines a character to enable or disable the echoed input when the ECHO option is local. You can use this command to suppress a local echo when you type a password.	Ctrl/E

Specifying AUTOFLUSH

The AUTOFLUSH characteristic automatically invokes the AO function whenever you enter the IP, SYNCH, AYT, EOR, or BRK characters. AUTOFLUSH aborts all output on its way to the user's terminal

By default, AUTOFLUSH is enabled for IP, and is disabled for SYNCH and AYT.

Example: Disabling AUTOFLUSH

The following example shows how to disable AUTOFLUSH for the IP character on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT AUTOFLUSH IP DISABLED
```

When you enter a SHOW PORT CHARACTERISTICS command, the -f and +f symbols indicate if AUTOFLUSH is disabled or enabled for a given character.

Specifying AUTOSYNCH

The AUTOSYNCH characteristic automatically invokes SYNCH function whenever you enter the IP, AO, or AYT characters. (Refer to Mapping Keyboard Characters to Telnet Functions in this chapter.) AUTOSYNCH causes all output on it way to the remote process to be dropped. This function allows IP, AO, or AYT to have a more immediate effect.

By default, AUTOSYNCH is enabled for IP, and disabled for AO and AYT.

Example: Specifying AUTOSYNCH

The following example shows how to disable AUTOSYNCH for IP and enable AUTOSYNCH for AO on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT AUTOSYNCH IP DISABLED
Local> CHANGE PORT 5 TELNET CLIENT AUTOSYNCH AO ENABLED
```

When you enter a SHOW PORT CHARACTERISTICS command, the -s and +s symbols indicate if AUTOSYNCH is disabled or enabled for a given character.

Specifying Telnet Client Newline

The NEWLINE characteristics allow the user to define a 1- or 2-character sequence that will be interpreted as a new line. This characteristic is useful for devices that generate or recognize sequences for a new line other than CRLF or CR. There are four different directions as follows. In this case, terminal specifies the user at the access server and host specifies the Telnet server at the remote end of the connection.

- NEWLINE FROM TERMINAL — When entered, the character sequence is interpreted as a new line. The factory-set default is <CR>.
- NEWLINE TO TERMINAL — When entered, the character sequence is sent to the user's terminal whenever a NEWLINE FROM HOST sequence is received. The factory-set default is <CRLF>.
- NEWLINE FROM HOST — When received from the Internet host, the character sequence is interpreted as a new line. The factory-set default is <CRLF>. Note that the Telnet protocol specifies that the CRLF sequence should be sent.
- NEWLINE TO HOST — When entered, the character sequence is sent to the Internet host whenever a NEWLINE FROM TERMINAL sequence is received. The factory-set default is <CRLF>. Note that the Telnet protocol specifies that the CRLF sequence should be sent.

You can define NONE if you do not want a character to be defined.

Example: Specifying Telnet Client NEWLINE

The following example shows how to define no character for NEWLINE TO TERMINAL and "AB" as a character string for Newline To Terminal on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT NEWLINE TO TERMINAL NONE
Local> CHANGE PORT 5 TELNET CLIENT NEWLINE TO TERMINAL AB
```

Specifying FLOW CONTROL

The FLOW CONTROL characteristic enables or disables the XON / XOFF FLOW CONTROL characters for any Telnet client session created at the port.

The access server supports the remote FLOW CONTROL feature, where the remote Telnet server can toggle on and off the XON and XOFF output FLOW CONTROL characters from the access server (client). This happens when an application on the Telnet server uses the XON and XOFF characters for a function other than FLOW CONTROL.

Example: Disabling FLOW CONTROL

The following example shows how to disable FLOW CONTROL on the Telnet client on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT FLOW CONTROL DISABLED
```

You can enable or disable FLOW CONTROL from the device to the access server (input) or from the access server to the device (output). By not specifying the keywords INPUT or OUTPUT, FLOW CONTROL is enabled in both directions.

Examples: Enabling FLOW CONTROL

The following example shows how to enable FLOW CONTROL from the device to port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT INPUT FLOW CONTROL
ENABLED
```

The following shows how to enable FLOW CONTROL from port 5 to the device:

```
Local> CHANGE PORT 5 TELNET CLIENT OUTPUT FLOW CONTROL ENABLED
```

Specifying MESSAGE VERIFICATION

The MESSAGE VERIFICATION characteristic controls the display of session information when an existing Telnet client session is started, stopped, or resumed. With VERIFICATION enabled (factory-set default), the access server displays the session number and the Internet address. With VERIFICATION disabled, no session information is displayed when a session is started, stopped, or resumed. This command does not affect existing sessions. To affect existing sessions, use the SET SESSION TELNET CLIENT MESSAGE VERIFICATION command.

Example: Configuring MESSAGE VERIFICATION

The following example shows how to disable VERIFICATION on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT MESSAGE VERIFICATION DISABLED
```

Specifying the SWITCH CHARACTER

The SWITCH CHARACTER characteristic determines how the access server handles SWITCH CHARACTERs. By default, if any SWITCH CHARACTER is defined on the port, it is recognized and intercepted by the access server during each session. However, any user can change or disable the access server from recognizing these SWITCH CHARACTERs for a specific Telnet session. (The sections Specifying Keys to Switch Between Sessions, Defining the Break Key, and Specifying a Key to Switch to Local Mode provide the procedures to define the SWITCH CHARACTERs.)

Example: Configuring SWITCH CHARACTER

The following example shows how to disable the SWITCH CHARACTERs on port 5:

```
Local> CHANGE PORT 5 TELNET CLIENT SWITCH CHARACTER DISABLED
Local> CHANGE PORT 5 LIMITED VIEW ENABLED
```

The limited view characteristic does not apply when you set privileges on the port.

Specifying a Preferred Terminal Type

The TERMINAL characteristic allows the user to specify a terminal type to be sent to the Telnet host during session startup. The available types are ANSI, UNKNOWN, and VT10 through VT999. This value is used as a starting point for terminal type subnegotiation between the access server and the host. The actual terminal type, as displayed by the SHOW PORT SESSION STATUS command, may be different if the Telnet host can not support the specified type. The order of negotiation is VTXXX, followed by ANSI, followed by UNKNOWN. For example, if the TERMINAL characteristic is set to VT321, the access server will negotiate for the following terminal types in the order listed:

DEC-VT32, VT321, DEC-VT300, VT300, DEC-VT200, VT200, DEC-VT100, VT100, ANSI, UNKNOWN

Example: Specifying Terminal Type

The following example shows the command for defining a terminal type for a VT321:

```
Local> CHANGE PORT TELENET CLIENT TERMINAL VT321
```

Managing Access Server User Accounts

Minimal Setup for Local User Accounts

A limited amount of storage is available for defining user account records within the access server volatile and nonvolatile memory.

Example: Setting the User Name

The following example establishes a user account named J_SMITH:

```
Local> SET USERACCOU J_SMITH
```

Example: Changing the User Password

The following example changes the password for the user account J_SMITH to the character string “SECRETSTUFF”. Quotes denote the password string in the command line.

```
Local> CHANGE USERACCOU J_SMITH PASSWORD "SECRETSTUFF"
```

Optional Setup for Local User Accounts

Example: Changing User Account Parameters

The following example shows how to change the user account parameters for the user J_SMITH to FRAMED access, and set his permissions to PRIVILEGED:

```
Local> CHANGE USERACCOU J_SMITH ACCESS FRAMED
Local> CHANGE USERACCOU J_SMITH PERMISSIONS PRIV
```

When the SHOW USERACCOUNT command is used, the above settings result in the following display:

```
Local> SHOW USER ACCOUNT J_SMITH
Username:          J_SMITH
Password:          (Entered)  User Status: ENABLED
Access:            FRAMED     Forced Callback: DISABLED
Max Connect Time: 0 02:00:00 Dialout Service: (NONE)
Dialback Number:  (NONE)
Dialout Number:  (NONE)
Permissions:      DIALBACK, DIALOUT, LAT, TELNET, SLIP, PPP,
PRIV
```

SHOW/LIST/MONITOR USERACCOUNT Display

The following table defines the values in the SHOW USSERACCOUNT display:

Field	Description
Username	Establishes a database for a user account for authentication / authorization.
Password	Specifies that a password has been set for the user account
Access	Specifies the default access mode this user is granted.
Max Connect Time	Indicates the maximum number of minutes the user can be logged in before being forcibly logged out.
Dialback Number	Contains a phone number used on dial-back.
Dialout Number	Contains a phone number used on dial-out.
Permissions	Defines what the user is allowed to do.
User Status	ENABLE / DISABLE this account for authentication / authorization.
Forced Callback	Specifies whether a user must be called back after login.
Dialout Service	Specifies the DIALER SERVICE to be used when attempting a dial-out.

Authorization Profile Information

The access server supports a variety of information in a user or realm default authorization profile. The following table gives the service types and access levels of this information.

Service Types and Access Levels

The following table defines the service type and access level:

Service	Type Description
Login	User will be connected to a dedicated host.
Framed	SLIP or PPP will be started on the session.

Service	Type Description
Local	User may utilize the access server commands.
None	The configuration value of the port access parameter or realm-wide access parameter determines user access to the realm.

Service Permissions Access

The following table shows the type of service permissions a user can have. A user can have more than one type of service permission. The user can also have more than one type of permission assigned at a time. There is no limit to the total number of permissions a user can have.

Service Type	User Access
Telnet	The user may make Telnet connections on the current session.
LAT	The user may make LAT connections on the current session.
Dial-Out	The user may invoke a dial-out connection on the current session.
Dial-Back	The user may invoke a dial-back on the current session.
SLIP	The user may invoke a SLIP connection on the current session.
PPP	The user may invoke a PPP connection on the current session.
Privileged-User	The user has a privilege level of PRIVILEGED.

User Account Command Parameters

The commands in the following table allow the security manager to manage a small local database to be used for authentication and authorization. The table shows the command keywords associated with user account variables.

Command Clause	Description	Variables	Comments
CLEAR / PURGE	Allows local data base entries to be deleted.		
SET / DEFINE / CHANGE	Permits entry addition and modification.	ENABLED / DISABLED	

Command Clause	Description	Variables	Comments
PASSWORD	Allows modification of the password field for the specified entry.	Clear the PASSWORD by setting it to null-string ("").	Max. length = 40 characters Case-sensitive, depending on authentication service (protocol). Case-insensitive only for the local access server user data base.
USERACCOUNT	User name of account.		Max. length = 40 characters
DIALOUT NUMBER	Contains a phone number used on dial-out.	Standard modem-dial strings	Max. length = 120 characters
DIALBACK NUMBER	Contains a phone number used on dial-back.	Standard modem-dial strings	Max. length = 120 characters
DIALOUT SERVICE	The DIALER SERVICE to be used when attempting a dial-out.	Values appear in uppercase.	Max. length = 16 characters
MAX CONNECT	CONNECT Indicates the maximum number of minutes the user can be logged in before being forcibly logged out.		Default = 0
USER STATUS	Specifies user status.	ENABLED / DISABLED	Setting DISABLED prevents any login using this user-name.
ACCESS	Specifies the default access mode this user is granted.	LOCAL FRAMED NONE	See the following table for a definition of the ACCESS clause variables.

Access Command Variables

The following table defines the ACCESS command parameter variables:

Variable	Definition
LOCAL	Local access (only) allowed.
FRAMED	Framed (PPP, SLIP) access (only) allowed.
NONE	No access specified; port characteristics or realm default access determine service.
LOGIN	Dedicated to a host.

Managing Users

This section describes various tasks for managing users.

Providing a Contact Name and Access Server Location

The SET / DEFINE / CHANGE SYSTEM command allows you to provide all access server users with a person's name to contact in case of problems. This command also allows you to specify the location of the access server.

Example: Providing a Contact Name and Access Server Location

The following example shows how to identify Bob G as the access server contact, and Building 2, Lab 3 as the location of the access server:

```
Local> CHANGE SYSTEM CONTACT "Bob G"
Local> CHANGE SYSTEM LOCATION "Building 2, Lab 3"
```

You can use the SHOW / LIST SYSTEM command to display this information.

Specifying Preferred Service for LAT or Telnet Resources

The following lists the results of enabling a preferred service on a port:

- Without AUTOCONNECT enabled (refer to Specifying AUTOCONNECT in this chapter), the port user connects to a particular resource by entering only the CONNECT command. With AUTOCONNECT enabled, the access server automatically connects the port to the preferred service at login.
- The user can switch to local mode at any time and make connections to other available services.

When you specify any LAT or Telnet resource to be a preferred service, the host or service name, node name, and port name are limited to 16 characters each.

For the LAT protocol:

To set a LAT service as a preferred service, the port's default protocol must be set to LAT.

Example: Enabling a Preferred LAT Service

The following example shows how to enable the LAT service, FILES, as the preferred service on port 5:

```
Local> CHANGE PORT 5 PREFERRED FILES
```

You can specify that the connection be made to a particular node and / or port name of the LAT service.

Example: Enabling a Preferred LAT Service on a Specific Node and Port

The following example shows how to specify that port 5 connects to port JAMES on node MARKETING for service FILES:

```
Local> CHANGE PORT 5 PREFERRED FILES NODE MARKETING
DESTINATION JAMES
```

For the Telnet Protocol

To set an Internet host as a preferred service, the port's default protocol must be set to TELNET. You can use the host's Internet address, domain name, or relative domain name if the host is defined in a name server; however, you cannot use the entire domain name if the name is more than 16 characters, including the dots.

Example: Enabling a Preferred Telnet Service

The following example shows how to enable a resource on the TCP/IP network, SALE.MKT.FOO.COM, as a preferred service on port 5:

```
Local> CHANGE PORT 5 PREFERRED SALE.MKT.FOO.COM
```

Specifying the Port USERNAME

By factory-set default, the Enter username> prompt appears when a user logs in to the access server port. The access server uses the user name as the string the user enters in response to the Enter username> prompt. However, the access server uses the port's name as the user name when the user enters Ctrl/Z instead of a user name.

You can use the USERNAME characteristic to establish a permanent user name (1 to 16 ASCII characters) for a port. In this case, the Enter username> prompt is not displayed when a user logs in to the access server. Always make an effort to specify a unique user name, since the access server does not prevent duplicate user names.

Examples: Configuring Port USERNAME

The following example sets the port 5 user name to "Barney":

```
Local> CHANGE PORT 5 USERNAME "Barney"
```

If you do not use the quotation marks in the command, the user name will appear in uppercase (for example, BARNEY instead of Barney).

To clear USERNAME, enter empty quotation marks as follows:

```
Local> CHANGE PORT 5 USERNAME ""
```

USERNAME is designed to accommodate interactive terminals that have one permanent user. Terminals that are usually shared should not have a permanent user name assigned, and the Enter Username> prompt should be entered upon login.

If AUTHENTICATION is enabled on the port, the port user name may be set to the Kerberos principal name of the port's permanent user.

Specifying Keys to Switch Between Sessions

Access server users can define keys as switches. These keys can switch from one session to another without having to return to local mode. When the user presses the key, the access server interprets the character and does not pass it to the service node.

Pressing the BACKWARD SWITCH character activates the user's previous session. The FORWARD SWITCH character activates the next session. These switches can be pressed either at the local prompt or in a session.

If the user has only two sessions, both of these switch characters restart the inactive session. You can configure any keyboard character as the FORWARD or BACKWARD SWITCH. Previously undefined control characters are recommended. Do not select characters that the port user is likely to enter routinely while using a service; otherwise, the current session is interrupted when that switch is pressed. Avoid the tilde (~) character if you use function keys on the VT-series terminals or PCs.

Switch characters can be temporarily disabled for a particular session by using the SET SESSION command for a LAT session or the Telnet client profile for a Telnet session. (Refer to Specifying the Telnet Client Session Profile in this chapter.) However, they remain in effect outside such a session.

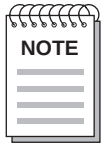
To define these keys as switches, select a different character for each switch.

Example: Defining Keys as Switches

The following example shows how to set Ctrl/F and Ctrl/B for the forward and backward switches on port 5:

```
Local> CHANGE PORT 5 FORWARD SWITCH ^F BACKWARD SWITCH ^B
```

To delete a switch character, use the NONE keyword instead of a character.



If you are using a session management terminal and your port has MULTISESSIONS ENABLED, switch sessions by using a terminal command rather than access server switch characters.

Defining the Break Key

The BREAK characteristic defines how the Break key is used. The Break key can be defined in three ways:

- LOCAL — Pressing the Break key switches the user from service mode to local mode. This is the factory-set default. The following shows how to set the Break key to LOCAL on port 5:

```
Local> CHANGE PORT 5 BREAK LOCAL
```

- REMOTE — The Break key is ignored by the access server and passed to the LAT service for the port's current session. BREAK is not sent to any host on a TCP/IP network. To send BREAK to a host on the TCP/IP network, refer to Mapping Keyboard Characters to Telnet Functions in this chapter. The following shows how to set the Break key to REMOTE on port 5:

```
Local> CHANGE PORT 5 BREAK REMOTE
```

- DISABLED — The Break key is ignored by the access server and not passed to the host on the network. The following shows how to set the Break key to DISABLED on port 5:

```
Local> CHANGE PORT 5 BREAK DISABLED
```

The Break key is ignored on a port with a dedicated service; however, you should disable BREAK along with all other switch characters. If you need to pass the break condition to the dedicated service for any application of the service, set BREAK to REMOTE. In this case, the break signal is not ignored but is passed to the LAT service node.

Specifying a Key to Switch to Local Mode

The LOCAL SWITCH characteristic identifies a character that, when entered by the user, switches the port to local mode from session mode. This character, like the FORWARD and BACKWARD SWITCH characters, is intercepted by the access server and is never transmitted to the network resource unless you set SET SESSION PASSALL or PASTHRU for a LAT session, or you set the Telnet client profile for a Telnet session. The Break key is also available for this function unless the BREAK REMOTE or the BREAK DISABLED option has been chosen. When you define a local switch character, the character you choose can be used in place of the Break key, or you can continue to use the Break key.

Example: Configuring a Key as a Switch

The following example shows how to identify "-" as the local switch for port 3:

```
Local> CHANGE PORT 3 LOCAL SWITCH -
```

Example: Disabling a Local Switch

The following example shows how to disable the local switch, which is also the factory-set default:

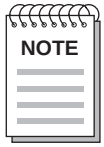
```
Local> CHANGE PORT 5 LOCAL SWITCH NONE
```

Specifying BROADCAST

There are three types of BROADCAST characteristics:

- BROADCAST — A port user uses this command to send messages.
- Port broadcast — Defines whether a particular port can receive broadcast messages.
- Access server broadcast — Defines whether all port users can send broadcast messages.

Disabling the port BROADCAST characteristic stops the port from receiving broadcast messages from other access server ports along with access server messages, such as shutdown. For this reason, you might want to recommend to users that they leave BROADCAST enabled on their ports.



The port user can still send messages with the access server BROADCAST enabled and the port BROADCAST disabled.

Example: Disabling BROADCAST Messages

The following example shows how to disable port 5 from receiving broadcast messages:

```
Local> CHANGE PORT 5 BROADCAST DISABLED
```

If any user tries to broadcast to a broadcast-disabled port, the access server enters the following message, which identifies the port or ports by port number:

```
Local -111- Port(s) with broadcast disabled not notified
Broadcast disabled at port n
```

When BROADCAST is enabled for both the access server and a port, port users can send and receive broadcast messages, by using the BROADCAST PORT command. When the access server BROADCAST is disabled, port users cannot send broadcast messages. Note that an individual port must have the port BROADCAST characteristic enabled to receive messages.

A user with privileges set can use the privileged BROADCAST ALL command to send a message to all interactive users.

Example: BROADCAST ALL

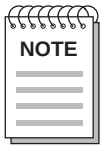
The following example shows a sample of a message broadcasted to all users:

```
Local> BROADCAST ALL "Server shut down at 12:15; back up at 1:00."
```

At a port with a session management terminal, broadcast messages are delivered to the current terminal session.

The factory-set default allows port users to send broadcast messages. Use the following command if you do not wish users to send broadcast messages:

```
Local> CHANGE SERVER BROADCAST DISABLED
```



Messages warning that the access server is going to initialize are unaffected by the access server-wide BROADCAST characteristic.

Ask users to inform you if they receive excessive or annoying broadcasts from other ports. If you receive complaints about such broadcasts, you can ask the sender of those broadcasts to stop broadcasting unnecessary messages, or you can enable security on the sender's port. This disables the BROADCAST command for the port.

Specifying LOSS NOTIFICATION

The LOSS NOTIFICATION characteristic signals a port user when characters entered by the user are lost, because of parity errors, framing errors, data overruns, or other reasons. The signal is a BEL character (an audible beeping sound), which the access server transmits to the port for each character that is lost. The factory-set default is enabled.

Example: Disabling LOSS NOTIFICATION

The following example shows how to disable LOSS NOTIFICATION on port 5:

```
Local> CHANGE PORT 5 LOSS NOTIFICATION DISABLED
```

Specifying Message Codes

Each access server message has a message code. In the following example, the number 750 is the message code:

```
Local -750- Another port has this name
```

With message codes disabled, the same message would look like:

```
Local - Another port has this name
```

The factory-set default shows the message codes. The following example shows how to disable reception of message codes on port 5:

```
Local> CHANGE PORT 5 MESSAGE CODES DISABLED
```

Specifying VERIFICATION

The VERIFICATION characteristic controls the display of session information when an existing session is started, stopped, or resumed. If you enable VERIFICATION (factory-set default), the access server displays the session number and the service name of the service. If you disable VERIFICATION, no session information is displayed when a session is started, stopped, or resumed.

Example: Disabling VERIFICATION

The following example shows how to disable VERIFICATION on port 5:

```
Local> CHANGE PORT 5 VERIFICATION DISABLED
```

Specifying Lock

The LOCK characteristic enables or disables the LOCK command for selected or all ports. If the LOCK command is enabled on the access server at the port, a user can enter the LOCK command at the terminal to prevent unauthorized access to an unattended terminal. The command prevents any input until the unLOCK password is entered.

The factory-set default is LOCK ENABLED. You can disable the LOCK command for all users as follows:

```
Local> CHANGE SERVER LOCK DISABLED
```

Example: Configuring LOCK

The following example shows how to enable LOCK on the access server, while disabling LOCK on ports 5 through 7:

```
Local> CHANGE SERVER LOCK ENABLED
Local> CHANGE PORT 5-7 LOCK DISABLED
```

Since anyone can LOCK any terminal, the LOCK facility can cause inconvenience in a situation where there are irresponsible users. If a user forgets the LOCK password, you have to log out the port with the LOGOUT command before the port can be used again. However, the LOGOUT command disconnects all sessions on that port. In that case, it may be best to disable LOCK on that port and rely on users to protect their sessions by disconnecting them when they must leave the terminal unattended.

Displaying Information About the Users

You can use the SHOW / MONITOR USERS command to do the following:

- Determine which ports are in use at any time.
- Identify the port users.
- Display information about active port users.

Example: SHOW USERS Display

The following example shows how to generate a users display. The display contains one line of information for each port that is logged in to the access server:

```
Local> SHOW USERS
Port         Username        Status      Service

1            Rich Smith      Connected   DOCUMENT2
2            Jane Brown      Locked      TIMESHARING
3            giovanni        Local       Mode
4            (Remote)        Connected   PRINTER
5            card            Connected   SLIP
```

SHOW/LIST/MONITOR USERS Display Headings

The following table provides an explanation of the information in the display in the previous example:

Heading	Description	
Port Number	Number of the port.	
Username	Any user name or the name of the port established by the PORT NAME characteristic. Note: Any port having the user name "(Remote)" designates a remote-access session in progress.	
Status	Status of the port, which can be one of the following:	
	Connected	Port is connected to a service.
	Connecting	Port is attempting to connect to a service.
	Disconnected	Session was terminated while dormant.
	Disconnecting	Session is disconnecting from a service.
	Signal Wait	The port failed to assert the DSR signal during a signal check controlled connection attempt.
	Idle	Port is not is use.
	Local Mode	Port is logged into the access server and is in local mode.
	Locked	The user has entered the LOCK command to LOCK the port.
Service	Name of the user's current session.	

Specifying User Groups

Nonprivileged users can choose the groups they require for their ports by using the SET PORT GROUPS command. Users must choose from the groups you authorized for their ports. The SET PORT GROUPS command limits user access to those services made available by the groups specified with the command. The command serves to shorten the node and service displays.

The SHOW PORT CHARACTERISTICS command displays the user-specified groups, listing them in the field labeled (Current) Groups. Current groups apply only to those ports with ACCESS set to LOCAL; current groups are ignored for those ports with ACCESS set to REMOTE.

Current groups (user-specified groups) are stored only in the operational database. Therefore, users must use the SET PORT command to configure these groups; users cannot use the DEFINE PORT or CHANGE PORT command.

Current groups are always equal to or a subset of the AUTHORIZED GROUPS. If a user enters SET PORT GROUPS ALL, the current groups consist of all the enabled authorized groups.

The access server uses the current groups for these functions:

- Checking authorization when the user enters a CONNECT command on the access server
- Displaying information with the SHOW NODES and SHOW SERVICES commands

Example: Assigning User Groups

The following example shows the command for nonprivileged users to assign groups from among their authorized groups:

```
Local> SET PORT GROUPS 5
```

If the authorized groups for the port were groups 4 to 7, the user can only access group 5 after executing the command. In addition, the SHOW SERVICES command shows only the information for services and nodes in group 5, and the SHOW PORT CHARACTERISTICS command shows the groups assigned to the port in the (Current) Groups field.

Managing Sessions

This section shows how to initiate and terminate sessions and how to display session information.

Initiating a Session to a LAT Service

To initiate a session to a LAT service, use the CONNECT LAT command with the service name. If the default protocol (refer to Specifying the Default Protocol in this chapter) is set to LAT or ANY, you can ignore the LAT keyword.

Example: Initiating a Session to a LAT Service

The following example shows how to initiate a session with LAT service SALES:

```
Local> CONNECT LAT SALES
```

You can use the CONNECT command to connect to any available LAT node or service at a specific service node and port. For example, if it is important for you to connect to a particular system associated with a service named ACCOUNTING, you can specify the service node where that system is attached.

Example: Connecting to a LAT Service on a Specific Node or Server

The following shows how to connect to LAT service SALES at node SERVER2:

```
Local> CONNECT LAT SALES NODE SERVER2
```

The following shows how to connect to LAT service SALES at node SERVER2, port 1:

```
Local> CONNECT LAT SALES NODE SERVER2 DESTINATION 1
```

Initiating a Session to an Internet Host

To initiate a session to an Internet host, use the CONNECT TELNET command with the Internet host name or address. If the default protocol (refer to Specifying the Default Protocol in this chapter) is set to TELNET, you can ignore the TELNET keyword. You can connect to the Internet host name or address. The host name can be either a relative or an absolute domain name.

Example: Initiating a Session with an Internet Host

The following three commands show how to initiate a session with the same host. The first command uses the relative domain name, SALES; the second command uses the absolute domain name SALES.MARKETING.FOO.COM; and the third command uses the Internet address, 129.122.30.11.

```
Local> CONNECT TELNET SALES
Local> CONNECT TELNET SALES.MARKETING.FOO.COM
Local> CONNECT TELNET 129.122.30.11
```

You can also use the OPEN or TELNET command instead of the CONNECT command to connect to an Internet host. The OPEN command does not accept the TELNET keyword.

```
Local> OPEN SALES
Local> TELNET SALES
```

Sending Telnet Functions to a Remote Telnet Server

To send a Telnet function such as AO, AYT, BRK, EOR, or SYNCH, you use the SEND TELNET command on a current session with a Telnet server. For example, the following command sends the Telnet abort output (AO) command:

```
Local> SEND TELNET AO
```

You can map Telnet functions to keyboard characters as described in Mapping Keyboard Characters to Telnet Functions. For a complete list of Telnet commands, refer to Telnet Keymapping Functions in this chapter.

In addition to the functions listed in Mapping Event Indications to Keyboard Characters in Chapter 13, you can also send the following:

- Request Status — Requests that the peer Telnet implementation responds with the current status of all Telnet options for this session. You must resume the session to see the Telnet server's response. The following shows how to send the REQUEST STATUS function:

  ```
  Local> SEND TELNET REQUEST STATUS
  ```

- Resume Output — If the Internet host appears to be hung after the AO function is sent, you send RESUME OUTPUT to cancel the AO. You only use this command to cancel an AO. The following shows how to send the RESUME OUTPUT function:

  ```
  Local> SEND TELNET RESUME OUTPUT
  Local> SEND TELNET SYNCH
  ```

- TEST INTERNET or PING - Sends an ECHO request message to the specified remote Internet host. You use this command to test for a valid connection. This command starts a PING session, which continues until the PING succeeds (and sends a VERIFICATION message) or until the timeout period of 30 seconds is exceeded. The following shows how to test the communication to an Internet host with an address of 22.46.72.167:

  ```
  Local> TEST INTERNET 22.46.72.167
  ```

  or

  ```
  Local> PING 22.46.72.167
  ```

Controlling the Number of Sessions

You can control the number of sessions at the individual port and the total number of sessions allowed for the access server. The combined number of sessions for all ports must be equal to or less than the access server session limit.

A high limit allows users to have more sessions but results in increased memory requirements. A low limit decreases the memory requirements but decreases the number of sessions. If the access server session limit is reached by some of the port users, the remaining port users cannot establish subsequent additional sessions. In this case, you need to increase the access server session limit value or decrease the port session limit value for some or all of the ports.

You can set the SESSION LIMIT for the access server to a value of 0 to 128 or to NONE. If you enter NONE, the access server maintains up to 128 sessions, potentially eight per port user. The factory-set default is 64 sessions.

Example: Changing the Server Session Limit

The following example shows how to change the access server session limit to 48:

```
Local> CHANGE SERVER SESSION LIMIT 48
```

The maximum number of sessions allowed on one port is eight. The factory-set default is four sessions. You can set the port session limit to a number from 0 to 8 or to NONE, where NONE allows eight sessions at the port. If you set a session limit to 0, the affected users cannot connect to any resources.

Example: Changing the Server Session Limit on a Specific Port

The following example shows the session limit being set to 6 on port 5:

```
Local> CHANGE PORT 5 SESSION LIMIT 6
```

For ports with session management terminals, the kind of terminal at the port further determines the port's session limit, where the access server port can support up to eight terminal sessions. However, terminal devices typically support a maximum of less than eight terminal sessions. The documentation for the terminal device should tell you how many terminal sessions the device can have. Set the port session limit to a value in that range.

Displaying Session Information

You can display a line of information about the current status of a port or ports and a list of the sessions on the port or ports. To display a summary of session information, use the SHOW SESSIONS command. If you wish to display a continuous update of the sessions, use the MONITOR SESSIONS command.

Use the ALL keyword instead of a port number to receive equivalent information about the sessions for all access server ports. For ports set up as a LAT service or Telnet listener, the user name is displayed as "(Remote)".

Example: SHOW SESSIONS Display

The following example shows how to generate a sessions display for ports 1 and 2. The first line of the sessions display begins with the port number and port user name. On the same line, the display shows the port mode (either Local Mode or Session Mode) and the current session number.

The next few lines in the display consist of active-session information. One line of information appears for each active session on the port. When a session is terminated, the information for the session is removed and replaced by the information below it in the display.

```
Local> SHOW SESSIONS PORT 1,2

Port 1: Rich Smith Local Mode Current Session: Session 2

- Session 1: Queued at 3   LAT                    TIMESHARE
- Session 2: Connected     TELNET                   DEVELOP
- Session 3: Connecting    TELNET                    BERGIL
- Session 4: Disconnected  LAT             DOCUMENT (PEAR)
- Session 5: Disconnecting LAT                       TEST

Port 2: card Session Mode
Current session: Session 1

- Session 1: Connected SLIP
```

SHOW/MONITOR SESSIONS Display Fields

The following table describes the information in the SHOW/MONITOR SESSIONS display:

Field	Description	
Session n	Number of the session.	
First Column	Status of a session, which can be one of the following:	
	Connected	Port is connected to the service.
	Connecting	Port is attempting to connect to a service
	Disconnected	Session was terminated while dormant.
	Disconnecting	Access serve is disconnecting the port from the service.
	Signal Wait	The port failed to assert the DSR signal during a signal check controlled connection attempt.
	Queued at *n*	Position in the connection queue of the connection request for a service. The request at position 1 is the next one to be dequeued and connected.
Second column	Displays which protocol (LAT or Telnet) the session is using.	
Third Column	Name of the LAT service or Internet host associated with the session, or SLIP for SLIP sessions. If the name of the LAT service differs from the name of the LAT service node supplying the service, the display includes the name of the LAT service node within parentheses. For a remote-access connection to the port, the LAT service name is the LAT service sought by the requesting node and the name within parentheses is the requesting LAT service node.	

Displaying Session Characteristics

You can display the characteristics of any current LAT or Telnet session.

Example: SHOW PORT SESSIONS CHARACTERISTICS Display for a LAT Session

The following example displays the characteristics of LAT session 1 on port 4:

```
Local> SHOW PORT 4 SESSIONS 1 CHARACTERISTICS
Port 4, Session 1, Protocol LAT
Transparency Mode: Interactive
```

There are only two lines in this display. The first line displays the port number, session number, and protocol used by the session. The second line displays the transparency mode, which can be Interactive, Pasthru, or Passall.

For an explanation of the characteristics for Telnet and 3270 sessions, refer to Specifying the Telnet Client Session Profile in this chapter and Chapter 18, respectively.

Displaying Session Status

You can display the status of any current Telnet session. If you have a LAT session, the SHOW/LIST/MONITOR PORT SESSION command displays the port number, session number, Protocol LAT, and the following message: (no status information available for LAT sessions)

Example: SHOW PORT SESSIONS STATUS Display for a Telnet Session

The following example shows how to display the status of a Telnet session on port 14:

```
Local> SHOW PORT 14 SESSION 1 STATUS

Port 14, Session 1, Protocol TELNET
Do-BINARY                Disabled
Will-BINARY              Disabled
Do-ECHO                  Enabled
Will-ECHO                Disabled
Do-SGA                   Enabled
Will-SGA                 Enabled
Do-Status                Disabled
Will-Status              Disabled
Do-End of Record         Disabled
Will-End of Record       Disabled
Do-Remote FLOW CONTROL   Disabled
Will-Remote FLOW CONTROL Disabled
Will-Terminal Type       Enabled             DEC-VT300
```

SHOW/MONITOR PORT SESSIONS STATUS Display Fields

The following table provides a description of the SHOW / MONITOR PORT SESSIONS STATUS display information:

Field	Description
Do-Binary	Enabled — Interpreting all data received as in a BINARY access server format. Disabled — Not interpreting all data received as in a BINARY format.
Will-Binary	Enabled — Sending data in a BINARY format. Disabled — Not sending data in a BINARY format.
Do-ECHO	Enabled — The remote peer will echo the output from the access server. Disabled — The remote peer will not echo the output from the access server.
Will-Echo	Enabled — The access server will echo the input from the remote peer. Disabled — The access server will not echo the input from the remote peer.
Do-SGA	Enabled — Receiving data in suppressed go-ahead (SGA) mode. This allows duplex communication. Disabled — Not receiving data in SGA mode. (The remote peer is sending go-aheads.)
Will-SGA	Enabled — Sending data in SGA mode. This allows duplex communication. Disabled — Not sending data in SGA mode.
Do-Status	Enabled — The access server has permission to send requests for the peer's status. Disabled — The access server does not have permission to send requests for the peer's status.
Will-Status	Enabled — The access server will respond to remote requests for status. Disabled — The access server will not respond to remote requests for status.

Field	Description
Do-End of Record	Enabled — The access server is enabled to receive EOR commands. Disabled — The access server is not enabled to receive EOR commands.
Will-End of Record	Enabled — The access server has permission to transmit EOR commands to the remote peer. Disabled — The access server does not have permission to transmit EOR commands to the remote peer.
Do-Remote FLOW CONTROL	Enabled — The access server will send remote FLOW CONTROL commands to enable and disable the peer's output FLOW CONTROL. Disabled — The access server will not send remote FLOW CONTROL commands to enable and disable the peer's output FLOW CONTROL.
Will-Remote FLOW CONTROL	Enabled — The network access server will accept remote FLOW CONTROL commands. Disabled — The access server will not accept remote FLOW CONTROL commands.
Will-Terminal Type	Enabled — The network access server will respond to SEND TERMINAL TYPE commands. Disabled — The network access server will not respond to SEND TERMINAL TYPE commands. The third column displays the terminal type negotiated between the access server and the host.

Terminating Sessions

There are two commands you can use to terminate a session on another port:

- The privileged LOGOUT PORT command allows you to manually log out any port, and all sessions terminate at the specified port. If the port device supports session management, the LOGOUT PORT command disconnects all the terminal sessions (and the associated sessions) then logs out the port.

  For example, to disconnect port 4 from all its sessions, enter the following command:

  ```
  Local> LOGOUT PORT 4
  ```

  The port that you specify can have local, remote, or dynamic access. Use caution when you log out a user's port. When you log out a port, you abruptly stop all sessions, and data may be lost. The port characteristics are also reset to the permanent values.

- The privileged DISCONNECT PORT command allows you to stop another port's session with a dedicated service. (You cannot use this command for ports with session management terminals, because these ports cannot have a dedicated service.)

  You can use the DISCONNECT PORT command to disconnect a nonkeyboard printer being used by a dedicated service that offers printers to the network. For example, to stop the session with a dedicated service at port 4, enter the following command:

  ```
  Local> DISCONNECT PORT 4
  ```

Chapter 13

Configuring and Managing LAT Services

Overview

Introduction

This chapter explains how to configure devices attached to the access server ports as LAT services. A LAT node can offer devices as LAT services to users on the port itself and other LAT nodes.

Prerequisites

Before you use the procedures in this chapter, you must:

- Connect and test the devices.
- Enable privileged status.
- Configure the port and device characteristics to match.

Reference

For information about connecting device cables, refer to the appropriate access server hardware documentation.

In This Chapter

This chapter contains the following topics:

- Configuring a Port to Offer a LAT Service
- Configuring Access to a LAT Service
- Configuration of Specific Types of Devices As LAT Services

- Configuring a Printer with Unannounced Availability
- Verifying the LAT Service
- Managing Your Access Server As a LAT Node Offering a Service

Configuring a Port to Offer a LAT Service

Configuration Parameters

After you attach a device to a port and ensure that the port and device characteristics match, you need to specify certain configuration parameters to enable all devices as LAT services.

The following table lists the configuration parameters. In addition to the parameters listed in the table, you need to configure certain parameters for specific types of devices as described in the Configuration of Specific Types of Devices As LAT Services section in this chapter.

For This Parameter:	**Use This Command:**	**And Refer to This Section and Chapter:**
Service Groups	CHANGE SERVER SERVICE GROUPS ENABLED	Changing Access Server Service Groups in Chapter 6
Authorized groups	CHANGE PORT AUTHORIZED GROUPS ENABLED	Configuring LAT Group Codes for Interactive Devices in Chapter 11
Service name	CHANGE SERVICE NAME CHARACTERISTIC[S]	Assigning a Service Name (in this chapter)
Port name	CHANGE PORT n NAME	Assigning a Port Name (in this chapter) ID string CHANGE SERVICE NAME Assigning an Identification String (in this chapter)
Modem control	CHANGE PORT n SIGNAL CONTROL ENABLED	Specifying MODEM CONTROL and SIGNAL CONTROL in Chapter 10
Signal control	CHANGE PORT n MODEM CONTROL ENABLED	Specifying MODEM CONTROL and SIGNAL CONTROL in Chapter 10
Service Password	CHANGE SERVICE NAME PASSWORD WORD	Specifying the Service Password (in this chapter)

Configuring Access to a LAT Service

Assigning a Service Name

A service name is a name you assign to the LAT service using the CHANGE SERVICE NAME command. When you assign a service name, the access server periodically multicasts the service's availability over the network. When you select a service name for a device, follow these guidelines:

- Service names must be 1 to 16 characters long and cannot be abbreviated.
- Allowable characters are A to Z, 0 to 9, $, - (hyphen), _ (underscore), and . (period).
- Ensure that the name is unique on the LAN.
- If two or more service nodes offer the same service name, access servers assume that all the services with that name are identical and are interchangeable.

Enabling Announcements

By default, announcements for a LAT service are enabled. To change the announcements characteristic, use the CHANGE ANNOUNCEMENTS ENABLED / DISABLED command as described in Chapter 4. You should also be aware of the multicast timer characteristic when announcements are enabled.

Assigning an Identification String

A service identification string helps users recognize and use the service. It can be up to 40 characters in length. The factory-set default is no identification string.

Example: Assigning the Service Name, to a Specific Port and Identification String

The following example shows how to assign a service name LN03_PRINT to the printers connected to ports 5, 6, 7, and 12. This example shows IDENTIFICATION abbreviated to ID and uses the identification string Production Printer.

```
Local> CHANGE SERVICE LN03_PRINT PORT 5-7,12 ID "Production Printer"
```

Example: Clearing the Identification String

To clear a previously set service identification string, enter the ID qualifier with empty quotations marks, as shown in the following example:

```
Local> CHANGE SERVICE LN03_PRINT PORT 5-7,12 ID ""
```

Assigning a Port Name

Assigning a port name to a service limits the service's availability. When you assign a port name to a service:

- The service is not listed in the access server multicast message.
- The service is available only to those users that know the port name.

Also, the access server transmits the port name to Telnet servers during Telnet sessions at the port.

Port Naming Guidelines

When you select a port name for a device, follow these guidelines:

- The factory-set default port name is PORT_n, where n is the port number.
- Port names must be a string of 1 to 16 characters long and cannot be abbreviated.
- Allowable characters are A to Z, 0 to 9, $, - (hyphen), _ (underscore), and . (period).
- Each port name must be unique to the access server.

Example: Changing the Port Name

The following example shows how to change the port name to PERSONNEL_PRINT for a printer on port 5:

```
Local> CHANGE PORT 5 NAME PERSONNEL_PRINT
```

Specifying the Service Password

An optional service password restricts access to a service. When a service contains a password, the access server prompts you for the password before allowing you to use the service.

There are two characteristics that you need to specify: SERVICE PASSWORD and PASSWORD LIMIT.

The service password can be up to 16 ASCII characters.

Example: Assigning a Service Password

The following example shows two ways to assign a password to the service

LN03_PRINT:

```
Local> DEFINE SERVICE LN03_PRINT PASSWORD
Password> BLIGH (not echoed)
Verification> BLIGH (not echoed)
Local>
```

or

```
Local> DEFINE SERVICE LN03_PRINT PASSWORD "BLIGH"
```

Do not specify passwords for services such as printers that you set up for host-initiated requests.

Example: Clearing the Service Password

To clear a previously set service password, use empty quotation marks as shown in the following example:

```
Local> CHANGE SERVICE LN03_PRINT PORT PASSWORD ""
```

The password limit characteristic determines the number of times that the access server prompts you for the correct password before it ends the connection requests. The password limit applies to all password-protected access server operations.

The range for the password limit characteristic is 0 to 10, and the factory-set default is 3. The following shows how to change the limit to 5:

```
Local> CHANGE SERVER PASSWORD LIMIT 5
```

Configuration of Specific Types of Devices As LAT Services

Introduction

This section provides examples of configuring the following types of devices as LAT services:

- A personal computer (as both a LAT service and a terminal)
- A computer
- A modem
- A printer

When you configure each type of device, you need to determine if the devices use SIGNAL CONTROL or MODEM CONTROL. For additional information, refer to Specifying MODEM CONTROL and SIGNAL CONTROL in Chapter 10.

Configuring a Personal Computer As a Terminal and LAT Service

The following example shows a sample configuration of a personal computer (PC) used as a terminal and a LAT service. With the port set to ACCESS DYNAMIC, the PC can switch between terminal emulation mode and file transfer mode.

When a PC is configured as a terminal, you can use the connect command to use a printer service. To do this, the PC must have an application program that provides file transfer capabilities.

Example: Configuring a PC As a Terminal and LAT Service

```
Local> DEFINE PORT 2 ACCESS DYNAMIC AUTOBAUD DISABLED AUTOCONNECT DISABLED
Local> DEFINE PORT 2 AUTOPROMPT ENABLED AUTHORIZED GROUPS 10,24,46
Local> DEFINE PORT 2 BREAK DISABLED DEDICATED NONE DEFAULT PROTOCOL LAT
Local> DEFINE PORT 2 DSRLOGOUT ENABLED FAILOVER ENABLED
Local> DEFINE PORT 2 INACTIVITY LOGOUT ENABLED INTERRUPTS DISABLED
Local> DEFINE PORT 2 LOCAL SWITCH ^L PASSWORD DISABLED PREFERRED NONE
Local> DEFINE PORT 2 SIGNAL CHECK ENABLED SIGNAL CONTROL DISABLED
Local> LOGOUT PORT 2
Local> CHANGE SERVER SERVICE GROUPS 10,24,46 ENABLED
Local> CHANGE SERVICE MICRO PORT 2 IDENTIFICATION "Personal computer 2"
```

Configuring a Computer As a LAT Service

By using multiple terminal interfaces and access server ports, you can use more than one access server port with a single computer system. Ensure that each access server port is assigned to a service.

Example: Configuring a Computer As a LAT Service on Port 2

The following example shows a sample configuration of a computer used as a LAT service:

```
Local> DEFINE PORT 2 ACCESS REMOTE AUTOBAUD DISABLED AUTOPROMPT DISABLED
Local> DEFINE PORT 2 DEDICATED NONE DIALUP ENABLED DSRLOGOUT DISABLED
Local> DEFINE PORT 2 DTRWAIT ENABLED INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 2 INTERRUPTS DISABLED LONGBREAK LOGOUT DISABLED
Local> DEFINE PORT 2 MODEM CONTROL ENABLED SIGNAL CHECK DISABLED
Local> LOGOUT PORT 2
Local> CHANGE SERVER SERVICE GROUPS 10,24,46 ENABLED
Local> CHANGE SERVICE NONDEC PORT 2 IDENTIFICATION "XYZ minicomputer"
```

Configuring a Modem As a LAT Service

The following example shows a sample configuration of a dial-out modem used as a LAT service:

```
Local> DEFINE PORT 3 ACCESS REMOTE AUTOBAUD DISABLED
Local> DEFINE PORT 3 AUTOPROMPT DISABLED BREAK DISABLED
Local> DEFINE PORT 3 DSRLOGOUT DISABLED DTRWAIT ENABLED
Local> DEFINE PORT 3 MODEM CONTROL ENABLED SIGNAL CHECK DISABLED
Local> DEFINE PORT 3 SPEED 1200
Local> LOGOUT PORT 3
Local> CHANGE SERVER SERVICE GROUPS 10,24,46 ENABLED
Local> CHANGE SERVICE MODEM1 PORT 3 IDENTIFICATION "Modem 123-4567"
```

Example: Configuring a Dial-In and Dial-Out Modem

The following example shows a sample configuration of a dial-in / dial-out modem used as a LAT service:

```
Local> DEFINE PORT 4 ACCESS DYNAMIC AUTOBAUD DISABLED
Local> DEFINE PORT 4 DSRLOGOUT DISABLED FLOW CONTROL XON
Local> DEFINE PORT 4 INACTIVITY ENABLED MODEM CONTROL ENABLED
Local> DEFINE PORT 4 PASSWORD ENABLED SIGNAL CHECK DISABLED
Local> DEFINE PORT 4 SPEED 2400
Local> LOGOUT PORT 4
Local> CHANGE SERVER SERVICE GROUPS 10,24,46 ENABLED
Local> CHANGE SERVICE MODEM2 PORT 4 IDENTIFICATION "MODEM 890-1234"
```

Configuring a Printer As a LAT Service

After you configure a printer as a LAT service, you need to set up the appropriate LAT remote print queue as described in the following sections of this chapter: Setting Up a LAT Remote Print Queue on an OpenVMS Host and Setting Up a LAT Remote Print Queue on an ULTRIX System.

Example: Configuring a Printer As a LAT Service on Port 4

The following example shows a sample configuration of a printer as a LAT service:

```
Local> DEFINE PORT 4 ACCESS REMOTE AUTHORIZED GROUPS 10,24,46
Local> DEFINE PORT 4 AUTOBAUD DISABLED AUTOCONNECT DISABLED DEDICATED NONE
Local> DEFINE PORT 4 DSRLOGOUT DISABLED INACTIVITY LOGOUT ENABLED
Local> DEFINE PORT 4 LONGBREAK LOGOUT DISABLED SIGNAL CHECK ENABLED
Local> DEFINE PORT 4 SIGNAL CONTROL DISABLED
Local> LOGOUT PORT 4
Local> CHANGE SERVER SERVICE GROUPS 10,24,46 ENABLED
Local> CHANGE SERVICE LASER PORT 4 IDENTIFICATION "LN03 laser printer"
```

Setting Up a LAT Remote Print Queue on an OpenVMS Host

To set up a LAT remote print queue on an OpenVMS host, the host must be running LAT software Version 5.1 or a later version. You use the LAT control program (LATCP) to perform the setup procedure.

Privileges for Running LATCP

The privileges that you need to run LATCP depends on the version of the operating system as shown in the following table:

Operating System	Privileges Needed
OpenVMS Version 5.1 through OpenVMS Version 5.4	CMKRNL
OpenVMS Version 5.4-1 and subsequent maintenance releases	OPER

Creating a Logical Device to Access a Printer Service

The following example shows how to run LATCP to create a logical device. This example configures the logical port LTA1925 to access the LAT service PRINT.

```
$RUN SYS$SYSTEM:LATCP
LCP> CREATE PORT LTA1925: /NOLOG
LCP> SET PORT LTA1925: /APPLICATION /NODE=LAT_08002B054DE0 /SERVICE=PRINT
LCP> EXIT
$COPY/LOG FILE.TXT LTA1925:
```

Configuring a Logical Device to Connect a Specific Port

You can configure a SET PORT /PORT = PORTNAME qualifier to connect to specific port as shown in the following example:

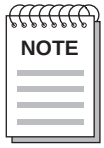
```
LCP> SET PORT LTA1925: /APPLICATION /NODE=LAT_08002B054DE0 /PORT=PORT 5
```

Using a Remote Printer Command File

The following example shows a remote printer command file, REMOTE_PRINT.COM. This command file sets up a remote printer and remote print queue. You can use this file as a template to set up subsequent remote printers.

You should enter the remote printer command file name in the LTLOAD.COM file.

This ensures that remote printers and remote print queues are set up automatically at system startup.



For OpenVMS Version 5.4-1 and later, use LAT$SYSTARTUP.COM instead of LTLOAD.COM.

```
$! This command procedure sets up the local characteristics of the
$! applications devices for remote printers and sets up the print
$! queues for these remote printers. These devices should have been
$! set up previously by the LTLOAD.COM command file. NOTE: The queue
$! manager must be running before executing this file.
$!
$! Set up local characteristics for the applications devices.
$!
$SET TERM LTA1925: /PERM /DEVICE=LNO3 /WIDTH=60 /NOBROAD- / SPEED=4800
$!
$! Set the protection on the devices so that only the symbiont can
$! access them. $! $SET PROT=(S:RWLP,O,G,W) /DEVICE LTA1925:
$!
$! Set the devices spooled
$!
$SET DEVICE LTA1925: /SPOOLED=(LN03_QUE,SYS$SYSDEVICE:)
$!
$DEFINE/FORM LN_FORM 10 /WIDTH=60 /STOCK=DEFAULT /TRUNCATE
$!
$! Initialize and start the print queue
$!
$INIT/QUE /START /PROCESSOR=LATSYM /RETAIN=ERROR- /DE-
FAULT=(NOBURST,FLAG=ONE) /RECORD_BLOCKING LN03_QUE/ON=LTA1925:
$EXIT
```

On a VAXcluster system, you can configure the applications ports on the local node only. However, you should do so on at least two nodes so that a redundant path to the printer is available in the event of a cluster node failure.

To set up a remote-printer applications port on a cluster node, include the LAT control program CREATE PORT and SET PORT commands for that port in the node's LTLOAD.COM file in the SYS$MANAGER directory. For complete information about setting up remote printing on VAXcluster systems, refer to the VMS VAXcluster manual in the OpenVMS documentation set.

Setting Up a LAT Remote Print Queue on an ULTRIX System

To set up a LAT remote print queue on an ULTRIX host, specify the access server name and the port name by using one of the following:

- An lcp command
- An entry in the /etc/printcap file

After you specify the access server name and the port name, set up a spool directory and test the printer.

Example: Configuring a LAT Remote Print Queue on an ULTRIX System

The following example provides a sample procedure for setting up a remote print queue for a laser printer. This example identifies the access server and port names to the with the /etc/printcap file.

```
lps|ln03|laser printer on LAT:
   :lp=/sdwv/tty42
   :sd=/usr/spool/lpd:\
   :ts=/LAT_08002B0540B7:\
   :op=PORT_7:\
   :br-19200:\
   :fc-0177777:fs-023\
   :xc-0177777:xs-040\
   :of=/usr/lib/lpdfilters/ln03of:\
   :if=/usr/lib/lpdfilters/ln03of:\
   :lf=/usr/lib/adm/lpd-errs:
# cd /usr/spool
# mkdir lpd
# chown daemon lps
# lpr -Plps test
```

Configuring a Printer with Unannounced Availability

Introduction

This section describes how to configure a printer with unannounced availability. The only users that know about the device's availability are those users that you tell about the device. By defining a port name and not a service name, you can configure a device on the access server for access by users on a LAT network.

Configuring a Printer with Unannounced Availability

The example in this topic shows a sample configuration of a printer with unannounced availability on a LAT network. You must configure the device and port characteristics, as described in Chapter 9, before performing this procedure. The following are variables in the example that you should substitute with the appropriate values:

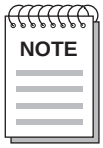
- Access server port number
- Authorized and service groups
- Port name

  You should change the port name to a descriptive term. This term should describe the resource provided (for example, printer or file transfer). The port name must be unique on the access server and follow the naming conventions described in the Cabletron *Network Access Software Command Reference* guide.

Substitute MODEM CONTROL for SIGNAL CONTROL if your access server supports MODEM CONTROL.

Reference

For a description of each command, refer to theCabletron *Network Access Software Command Reference* guide.



Not all commands can be combined on one line.

Example: Configuring a Printer with Unannounced Availability on a LAT Network on Port 4

```
Local> DEFINE PORT 4 ACCESS REMOTE AUTHORIZED GROUPS 10,24,46
Local> DEFINE PORT 4 AUTOBAUD DISABLED AUTOCONNECT DISABLED
Local> DEFINE PORT 4 DEDICATED NONE DSRLOGOUT DISABLED
Local> DEFINE PORT 4 INACTIVITY LOGOUT ENABLED LONGBREAK LOGOUT DISABLED
Local> DEFINE PORT 4 NAME PORT_4 SIGNAL CHECK ENABLED
Local> DEFINE PORT 4 SIGNAL CONTROL DISABLED
Local> LOGOUT PORT 4
```

For systems that need to access the printer, you must supply the system managers with the access server name, port name, and at least one group code that is enabled as an authorized group code on the port.

More Examples

The following sections in this chapter provide examples of setting up a remote print queue on OpenVMS and ULTRIX systems:

- Setting Up a LAT Remote Print Queue on an OpenVMS Host
- Setting Up a LAT Remote Print Queue on an ULTRIX System

Verifying the LAT Service

Do This

To verify whether the service is functioning, try connecting to the new service.

Once connected, you can assess whether the device responds appropriately. The appropriate response depends on what device is attached to the access server port.

When you have adequate information, return to local mode (press the Break key or a local-switch character) and disconnect the service by typing DISCONNECT at the `Local>` prompt.

For a computer, you may want to repeat this procedure to verify that your first session was disconnected by the host. You should receive the standard login procedure each time you connect to any computer offering a service.

Example: Verifying the LAT Service

The following example shows the command for verifying a previously defined LAT service A_DEVICE, and its port (port 5, named PORT_5):

```
Local> CONNECT LAT A_DEVICE DESTINATION PORT_5
```

Problem Solving

If you have any problem connecting to the service or using the device, use the following series of commands to review the service and port characteristics:

- Verify whether the service is set up correctly by using the SHOW SERVICE service-name CHARACTERISTICS command. For example, with the service A_DEVICE, the command appears as follows:

  ```
  Local> SHOW SERVICE A_DEVICE CHARACTERISTICS
  ```

  The service characteristics display shows all the ports assigned to a local service and indicates its other characteristics. For a sample of the service characteristics display, refer to Displaying Information About a Service in this chapter.

- Verify whether the port is properly configured by entering a SHOW PORT command and looking at the port characteristics display. For example, for port 5, the command is as follows:

  ```
  Local> SHOW PORT 5
  ```

- Verify the access server characteristics, for instance, that announcements are enabled and service groups are valid, by using the SHOW SERVER CHARACTERISTICS command as follows:

  ```
  Local> SHOW SERVER CHARACTERISTICS
  ```

Managing Your Access Server As a LAT Node Offering a Service

Introduction

By default, once there is a service, the access server functions as a service node by issuing multicast service announcements, which describe its available services to access servers on the network. These announcements contain information about the service node (such as its name and identification string) and about the available services. A single multicast service announcement is entered at the interval indicated by the multicast timer

Displaying Information About a Service

You can display information about services on the LAT network, including services on your access server, using the SHOW / MONITOR / LIST SERVICES command.

To display information on the services offered by your access server, use the SHOW / LIST SERVICES LOCAL command. To display information about a particular service, use the SHOW / LIST SERVICE command followed by the service name. To display information about all services, use the SHOW / LIST SERVICE ALL command.

There are three types of information you can display about the service:

- Characteristics

  The characteristics display is useful when you are changing operational and permanent values with the SET / DEFINE / CHANGE SERVICE command.

- Status

  You can obtain data on the operation of services by using the status display.

- Summary

  The summary display gives you capsule data on the services offered on the network or the local access server.

Displaying Services Characteristics

The LIST/SHOW/MONITOR SERVICES CHARACTERISTICS command generates a display of information on values that you can modify with the SET/DEFINE/CHANGE SERVICE command. With the LIST command, the characteristics display is the default display for the SERVICES and the SERVICES LOCAL entity specifications.

Example: SHOW SERVICE CHARACTERISTICS Display

The following example below shows how to generate a service characteristics display for the service named PRINTER:

```
Local> SHOW SERVICE PRINTER CHARACTERISTICS
Service: PRINTER
Identification: Printer Ports to PEACH
Ports: 1-3, 5, 7
Rating: 255
Enabled Characteristics:
Connections, Password, Queuing
Local>
```

SHOW/LIST/MONITOR SERVICE CHARACTERISTICS Display Fields

The following table describes the fields displayed in the service characteristics display:

Field	Description
Service	Name that identifies the network service.
Identification	Service identification string. This string is usually a short description of the service or of how to use it.
The following fields are displayed only for services offered by the access server (local services):	
Ports	Numbers of the ports at which the local service is offered.
Rating	Rating at which the access server offers this service. If any ports that offer the service are available, the rating is proportional to the number of available ports. If no ports are available that offer the service and if queuing is enabled for the service, the rating is proportional to the number of unused positions in the connection queue.
Enabled characteristics	Characteristics that can be enabled with the CHANGE SERVICE command. The access server displays only those characteristics that are enabled for local services.

Field	Description	
	Connections	Access server allows connections to this service.
	Password	Access server requires the requester of the service to supply a password before access to the service is allowed.
	Queuing	Access server places queued connection requests for this service in a queue if the request cannot be immediately satisfied.

Displaying Services Status

The SHOW / LIST / MONITOR SERVICE STATUS command displays information about the operational condition of the network and its services, including services offered by your access server. The display includes a list of the nodes that offer the selected service or services. Use the keyword LOCAL to restrict the information displayed to locally defined services. Without the keyword LOCAL or a particular service name, you get information on all network services, including local services.

The status display is the default display for the SHOW SERVICE service-name command.

For each selected service, an introductory line identifies the service for which status information is being displayed. The next line shows the headings for the status information. Under the headings, a line is displayed for each node offering the selected service.

The access server displays information about a service or services from data stored in its memory. If none of the ports can access a particular service, the access server does not retain any data about that service. Hence, no information about that service can be displayed.

Example: SHOW SERVICE STATUS Display

The following example shows how to generate a service status display for a service named DEVELOP:

```
Local> SHOW SERVICE DEVELOP STATUS
Service DEVELOP - Available
Node Name Status Rating Identification
ORANGE Reachable 27 Terminals
Development System
PEACH Unreachable 255 Engineering
Development System
TEST Unknown 150 High-powered
Performance Testing
```

SHOW/LIST/MONITOR SERVICE STATUS Display Headings

The following table describes the fields and the headings in the display:

Heading	Description	
Service	Name that identifies the network service.	
Node Name	Name of the service node, as stored in access server memory for each node that offers the service.	
Status	The accessibility of the service node as one of the following:	
	n Connected	Service node is reachable and the access server has n active sessions on the node.
	Reachable	Node is accessible.
	Unknown	No sessions are active, and the service node offering this service has not been heard from recently.
	Unreachable	Active service session has timed out, or attempt to connect has timed out. The node can also signal that it is unreachable.

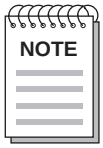
Heading	Description	
	Rating	Relative capability for a service node to process new sessions. The service rating is assigned by a service node for each service that it offers. With the higher rating, the capability of the service node to accept a new connection is greater. The access server uses service ratings to decide where to establish a service session when two or more service nodes offer the same service. The access server attempts to connect to the service on the node that advertises the highest rating for the service.
	Identification	Service identification string for this service node. This string may be different from the service node identification string.

Displaying Services Summary

The SHOW / MONITOR SERVICES SUMMARY command displays one line of information on each selected service or services. Use the keyword LOCAL to obtain information on locally defined services. Without the keyword LOCAL or a particular service name, you get information on all network services. For the SHOW / MONITOR commands, the summary display is the default display for the SERVICES, SERVICES ALL, and SERVICES LOCAL entity specifications.

The display contains one line of headings and, for each service known to the access server, one line of information describing each service.

The access server displays information about a service or services from data stored in its memory. If none of the ports can access a particular service, the access server does not retain any data about that service. Hence, no information about that service can be displayed.



Ports with the LIMITED VIEW command enabled cannot perform the SHOW SERVICES command.

Example: SHOW SERVICE SUMMARY Display

The following example shows how to generate a service summary display for all network services:

```
Local> SHOW SERVICES ALL SUMMARY

Service Name  Status        Identification

DEVELOP       Connected     Hardware Development System
DOCUMENT      Available     Documentation Timesharing
TEST          Unavailable   High-powered Performance Testing
TIMESHARING   Unknown       Accts. Payable Timesharing
```

SHOW/LIST/MONITOR SERVICE SUMMARY Display Headings

The following table describes the headings in the display:

Heading	Description	
Service Name	Name that identifies the network service.	
Status	Current availability of the service as one of the following:	
	Available	One or more service nodes that offer the service are accessible.
	n Connected	Service is available and n sessions are currently active with this service.
	Unavailable	All service nodes that offer the service are not accessible.
	Unknown	None of the service nodes that offer the service are accessible, and one or more is unknown.
Identification	Service identification string, which may describe the service or how to use the service.	

Chapter 14

Configuring and Managing Telnet Servers

Overview

Introduction

This chapter explains how to configure various types of devices as a Telnet or raw TCP server. A Telnet or raw TCP server is a resource on a TCP/IP network.

To use the procedures in this chapter, you must:

- Connect and test the devices
- Enable privileged status
- Configure the port and device characteristics to match

Refer to your access server hardware documentation for information about connecting device cables.

In This Chapter

This chapter contains the following topics:

- Managing Your Access Server As a Telnet Listener Node
- Supplying User Location Data to Telnet Servers
- Configuring a Raw TCP Listener

Sample Device Configurations

Introduction

This section provides examples of configuring the following types of devices for access through a Telnet listener:

- A printer
- A computer
- A modem

You must configure the device and port characteristics as described in Chapter 9 before performing the procedures described in this chapter.

The examples in this section do not include the various Telnet server characteristics.

Refer to Configuring Telnet Server Session Characteristics in this chapter to set up the Telnet server characteristics.

The following lists the variables in this chapter that you should substitute with the appropriate values:

- Access server port number
- Flow control type (printer only)
- Telnet listener-identifier (Must be 23 or between 2001 to 2032, inclusive.)
- Identification string (up to 40 characters)

Configuring a Printer for Access Through a Telnet Listener

For systems that need to access the printer, you must supply the system managers with the TCP port number. The section Configuring a Remote Print Queue in this chapter provides an example of setting up a remote print queue on an ULTRIX or UNIX system.

The following example shows a sample configuration of a printer used for access through a Telnet listener on port 4.

```
Local> DEFINE PORT 4 ACCESS REMOTE AUTOBAUD DISABLED BREAK DISABLED
Local> DEFINE PORT 4 DEDICATED NONE DSRLOGOUT DISABLED FLOW CONTROL XON
Local> DEFINE PORT 4 INACTIVITY LOGOUT ENABLED LONGBREAK LOGOUT DISABLED
Local> DEFINE PORT 4 SIGNAL CHECK ENABLED SIGNAL CONTROL DISABLED
Local> LOGOUT PORT 4
Local> CHANGE TELNET LISTENER 2010 PORTS 4 ENABLED
Local> CHANGE TELNET LISTENER 2010 IDENTIFICATION "PRINTER"
Local> CHANGE TELNET LISTENER 2010 CONNECTIONS ENABLED
```

Configuring a Computer for Access Through a Telnet Listener

The following example shows a sample configuration of a computer used for access through a Telnet listener on port 2:

```
Local> DEFINE PORT 2 ACCESS REMOTE AUTOBAUD DISABLED AUTOCONNECT DISABLED
Local> DEFINE PORT 2 BREAK DISABLED DEDICATED NONE DSRLOGOUT DISABLED
Local> DEFINE PORT 2 DTRWAIT ENABLED INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 2 INTERRUPTS DISABLED LONGBREAK LOGOUT DISABLED
Local> DEFINE PORT 2 MODEM CONTROL ENABLED SIGNAL CHECK DISABLED
Local> LOGOUT PORT 2
Local> CHANGE TELNET LISTENER 2010 PORTS 2 ENABLED
Local> CHANGE TELNET LISTENER 2010 IDENTIFICATION "XYZ minicomputer"
Local> CHANGE TELNET LISTENER 2010 CONNECTIONS ENABLED
```

Configuring a Modem for Access Through a Telnet Listener

This section contains examples that show how to configure a dial-out modem and a dial-in / dial-out modem.

Example: Configuring a Dial-Out Modem

The following example shows a sample configuration of a dial-out modem used for access through a Telnet listener on port 3:

```
Local> DEFINE PORT 3 ACCESS REMOTE AUTOBAUD DISABLED
Local> DEFINE PORT 3 AUTOPROMPT DISABLED BREAK DISABLED
Local> DEFINE PORT 3 DSRLOGOUT DISABLED DTRWAIT ENABLED
Local> DEFINE PORT 3 LONGBREAK LOGOUT DISABLED MODEM CONTROL ENABLED
Local> DEFINE PORT 3 SIGNAL CHECK ENABLED SPEED 1200 ALTERNATE SPEED 300
Local> LOGOUT PORT 3
Local> CHANGE TELNET LISTENER 2004 PORTS 3 ENABLED
Local> CHANGE TELNET LISTENER 2004 IDENTIFICATION "Modem 123-4567"
Local> CHANGE TELNET LISTENER 2004 CONNECTIONS ENABLED
```

Example: Configuring a Dial-In and Dial-Out Modem

The following example shows a sample configuration of a dial-out modem used for access through a Telnet listener on port 4:

```
Local> DEFINE PORT 4 ACCESS DYNAMIC AUTOBAUD DISABLED
Local> DEFINE PORT 4 DSRLOGOUT DISABLED FLOW CONTROL XON
Local> DEFINE PORT 4 INACTIVITY ENABLED MODEM CONTROL ENABLED
Local> DEFINE PORT 4 PASSWORD ENABLED SIGNAL CHECK ENABLED
Local> DEFINE PORT 4 SPEED 2400 ALTERNATE SPEED 1200
Local> LOGOUT PORT 4
Local> CHANGE TELNET LISTENER 2008 PORTS 3 ENABLED
Local> CHANGE TELNET LISTENER 2008 IDENTIFICATION "Modem 890-1234"
Local> CHANGE TELNET LISTENER 2008 CONNECTIONS ENABLED
```

Configuring a Personal Computer As a Terminal and for Access through a Telnet Listener

Sample Configuration

To configure a PC for access through a Telnet listener only, use the following example and:

- Substitute MODEM CONTROL for SIGNAL CONTROL if your access server supports modem control.
- Use LONGBREAK LOGOUT instead of DSRLOGOUT if your access server, device, or device cable does not support the DSR signal.

```
Local> DEFINE PORT 2 ACCESS DYNAMIC AUTOBAUD DISABLED BREAK DISABLED
Local> DEFINE PORT 2 DEDICATED NONE SIGNAL CONTROL DISABLED
Local> DEFINE PORT 2 DEFAULT PROTOCOL TELNET
Local> DEFINE PORT 2 DSRLOGOUT ENABLED INACTIVITY LOGOUT ENABLED
Local> DEFINE PORT 2 INTERRUPTS DISABLED LOCAL SWITCH ^L PASSWORD DISABLED
Local> DEFINE PORT 2 PREFERRED NONE SIGNAL CHECK ENABLED
Local> LOGOUT PORT 2
Local> CHANGE TELNET LISTENER 2010 PORTS 2 ENABLED
Local> CHANGE TELNET LISTENER 2010 IDENTIFICATION "Personal Computer"
Local> CHANGE TELNET LISTENER 2010 CONNECTIONS ENABLED
```

Switching Modes

With the port set to ACCESS DYNAMIC, the PC can switch back and forth from terminal-emulation mode, which allows the PC to access Access Server services on the LAT network, and file transfer mode, which allows the PC to transfer files with another computer as a transfer partner. Refer to Setting User Priority for Devices Using Dynamic Access in this chapter for further information on switching between terminal-emulation mode and file transfer mode.

Configuring Personal Computer Access to a Printer

Personal computers configured as a terminal can connect to a printer offered as a resource when a user enters a CONNECT command. However, for the user to access the printer, the PC must have an applications program capable of sending files to the printer. The person in charge of the PC must supply the appropriate applications program. The access server does not queue connection requests to a printer.

Setting User Priority for Devices Using Dynamic Access

You can enable interrupts if you want the owner or main user of the device to have full control over it. For example, the main user of a personal computer may require priority over other users that want to copy files from the computer disk. You can provide this control by setting the port to INTERRUPTS ENABLED and the Break key to LOCAL.

Setting the BREAK to LOCAL allows the user to use the Break key to return from session mode to local mode. Use caution when enabling interrupts, because they inconvenience people using the device as a service. For printers with keyboards, which can also be used as interactive terminals, you should have the interrupts characteristic disabled on the port.

The INTERRUPTS characteristic is governed by the following rules:

- With INTERRUPTS DISABLED, a potential user cannot interrupt an ongoing file transfer session between the PC and another system. The user can start a session only when all file transfer sessions have completed or are disconnected from the privileged port. The factory-set default is INTERRUPTS DISABLED.
- With INTERRUPTS ENABLED, a potential user can press the Break key to interrupt an ongoing file transfer session and start a local session. The access server logs out the file transfer session and allows the interactive user to log in. In this situation, any queued connection requests for the port remain queued and are processed when the user logs out of the port.
- A request from another system can never interrupt an ongoing local session.
- If there is no ongoing session, a session using either type of access (user at the PC or system accessing the PC) can be started, and the above rules apply.

Example: Enabling Interrupts for Devices Using Dynamic Access

The following example shows how to enable interrupts and set BREAK to LOCAL on port 5:

```
Local> CHANGE PORT 5 INTERRUPTS ENABLED BREAK LOCAL
```

Configuring a File Transfer Partner

The access server supports the file transfer capability of a personal computer on an access server port. This allows a user of a personal computer to send and receive files over the LAN. For a particular session, the access server permits a user to control whether flow control and other special characters are intercepted by the access server. Note that session nodes frequently control these characteristics for you.

To be available for file transfers, the PC must be logged out from the access server port. When a connection is made to the port, the port shifts to remote-access mode.

To transfer files, you must set up the access server port and the personal computer (local partner) to function as the initiator of a session with the remote partner in the transfer. The remote partner computer can be a session node or a personal computer that is available on the network. Once the initiator establishes a session to a partner, you can transfer files in either direction between the initiator and the partner. The computer serving as the file transfer partner might require some modifications before a file transfer. To learn what modifications are required, refer to the documentation for the computer and for the file transfer program.

Partner Guidelines

The following provides guidelines for setting up the partners:

- Remote partner — You need to disable such characteristics as message verification, forward switch, backward switch, and local switch when using binary or ASCII file transfers. If needed, also disable flow control for binary file transfers. Additionally for binary or ASCII file transfers, all Telnet indications should be set to none. Use the SET / DEFINE / CHANGE TELNET SERVER command.
- Local partner — Flow control should always be enabled on the access server port and disabled on a session-by-session basis. The Telnet client binary profile disables flow control (refer to Specifying the Telnet Client Session Profile in Chapter 11). If flow control is needed, you will need to use the SET SESSION TELNET CLIENT FLOW CONTROL command. Note that this command affects only the client partner.

Configuring a Remote Print Queue

Introduction

The following sections explain how to configure a print queue on an ULTRIX or UNIX system.

Configuring a TCP/IP Remote Print Queue on an ULTRIX System

An ULTRIX print spooler can be configured to access one or more access server ports through the access server Telnet listener. Thus, a file can be queued for printing using the host's lpr command. If a host print spooler attempts a connection to a Telnet listener port that is busy, the queue entry request is dropped at the host and will have to be resubmitted.

Printer Port Telnet Server Characteristics

The following table lists the recommended Telnet server characteristics for the printer port to facilitate printing of files. (Refer to Configuring Telnet Server Session Characteristics in this chapter.)

Characteristic	Setting
Xmit Char Size	8
Rcv Char Size	8
IP, AYT, AO, EOR, NOP, BRK, EC, EL	None
Newline From Terminal	<LF>
Newline To Terminal	None
Newline From Host	None
Newline To Host	<CRLF>

Procedure

The following procedure describes how to configure an ULTRIX (Version 4.0 or subsequent maintenance release) host's print system. The host will use the access server internet address and Telnet listener TCP port number to connect to the access server printer port.

It is assumed that you are familiar with configuring an ULTRIX print system. For more detailed description of the ULTRIX print system, refer to the ULTRIX Guide to System Environment Setup.

Step	Action

1	Use the lprsetup program to initially configure a remote access printer entry in the printcap file.
	Example: The following example creates printer ds0 with spooling directory /usr/spool/
	lpd1. Some of the questions are ignored by pressing the Return key.
	`# lprsetup`
	`ULTRIX Printer Setup Program`
	`Command <add modify delete exit view quit help>: add`
	`Enter printer name to add []: ds0`
	`Enter the FULL name of one of the following printer types:`
	`or press RETURN for [unknown]: remote`
	`Enter printer synonym:`
	`Set spooler directory 'sd' [] ? /usr/spool/lpd1`
	`Set remote system name 'rm' [] ?`
	`Set remote system printer name 'rp' []?`
	`Enter the name of the printcap symbol you wish to modify.`
	`Enter symbol name: q`
	`Are these the final values for printer 1 ? [y] y`
	The lprsetup program creates the following printcap entry for ds0:
	ds0|lp1:\
	:lp=:\
	:rm=:\
	:rp=:\
	:sd=/usr/spool/lpd1:

2	Modify the printcap entry:
	`ds0|lp1:\`
	`:lp=@tsb0c3/prds3:\`
	`:sd=/usr/spool/lpd1:`
	The **tsb0c3** entry identifies the access server internet address and is an entry in /etc/hosts for the access server. The **prds3** entry identifies the access server TCP port number and is an entry in **/etc/services**. For example:
	`16.20.48.43 tsb0c3.lkg.foo.com tsb0c3`
	`prds3 2010/tcp`

3	Print a file using the host's lpr command. The lpr command queues and submits a job for printing. For example: `# lpr -P ds0 file`

Configuring a Telnet Listener

Introduction

Perform the following steps to assign a Telnet listener to one or more devices attached to access server ports:

Step	Action
1	Assign a TCP port to the access server port. The access server uses 23, and 2001 to 2032 as TCP port numbers. The TCP port number is the number that users on the TCP/IP network use to connect to the device on the access server port.
2	Determine which access server port or ports are to be assigned to the Telnet listener.
3	Provide an identification string that helps users recognize and use the resource. It can be up to 40 characters in length. The factory-set default is no identification string.
4	Enable the listener to receive connections. The factory-set default for CONNECTIONS is DISABLED.
5	Specify the individual access server session characteristics, as described in the Configuring Telnet Server Session Characteristics section in this chapter.

Configuring Telnet Server Session Characteristics

Introduction

The following sections describe how to configure the various Telnet server session characteristics.

Mapping Event Indications to Keyboard Characters

You can map the event indications to keyboard characters. The factory-set default for each indication is that no character is sent to the device or application on the access server port set up as a Telnet server port.

In most cases, you would map an event indication to a character in order for the access server to forward that event indication to the application or device on the access server port. The mapped character is defined by the device or application. For example, if an application defines IP as Ctrl/G, then you need to map IP to Ctrl/G:

```
Local> CHANGE PORT 5 TELNET SERVER IP ^G
```

Event Indications

You can map the following event indications to keyboard characteristics:

Event Indication	Description
Abort Output (AO)	Occurs when the remote user of this connection requests that any output currently en route to the user's terminal be aborted.
Interrupt Process (IP)	Occurs when the remote user of this connection requests that the process at this access server be aborted.
Are You There (AYT)	Occurs when the remote user of this connection requests a response from the Telnet server to verify that the connection is active.
Break (BRK)	Occurs when the remote user of this connection sends a remote break.
End of Record (EOR)	Occurs when the remote user of this connection issues an EOR request.

Event Indication	Description
Erase Previous Character (EC)	Occurs when the remote user of this connection issues an EC request.
No operation (NOP)	Occurs when the remote user of this connection issues a NOP command.

Specifying Newline Characteristics

The NEWLINE characteristics allow the person managing the access server to define a new line as a 1- or 2-character sequence. In this case, TERMINAL specifies the user at the remote end of the connection (Telnet client) and HOST specifies the device connected to the access server (Telnet server).

- NEWLINE FROM TERMINAL — When entered by the remote user, the character sequence is interpreted as a new line. The factory-set default is CR. The following shows how to change the character sequence to @#:

  ```
  Local> CHANGE PORT 5 TELNET SERVER NEWLINE FROM TERMINAL @#
  ```

- NEWLINE TO TERMINAL — The character sequence is sent to the user's terminal whenever a NEWLINE FROM HOST sequence is received from the internet host. The factory-set default is CRLF.
- NEWLINE FROM HOST — When received from the internet host, the character sequence is interpreted as a new line. The factory-set default is CRLF. Note that the Telnet protocol specifies that the CRLF sequence should be sent.
- NEWLINE TO HOST — When entered by the remote user, the character sequence is sent to the internet host. The factory-set default is CRLF.
- Note that the Telnet protocol specifies that the CRLF sequence should be sent.

Specifying Character Size

The CHARACTER SIZE characteristic allows you to select the character size, 7- or 8-bit, that is used during a session. In addition, the character size can be specified in the transmit direction (server to Telnet client), receive direction (Telnet client to server), or both directions.

Example: Setting CHARACTER SIZE

The following example shows how to set CHARACTER SIZE to 7 in both directions for port 5:

```
Local> CHANGE PORT 5 TELNET SERVER CHARACTER 7
```

Erase Previous Line (EL) Occurs when the remote user of this connection issues an EL request.

Example: Setting Character Size in a Specific Direction

The following example shows how to set CHARACTER SIZE to 7 in the TRANSMIT direction:

```
Local> CHANGE PORT 5 TELNET SERVER TRANSMIT CHARACTER SIZE 7
```

To set the character size in the receive direction, use RECEIVE instead of TRANSMIT.

Managing Your Access Server As a Telnet Listener Node

Introduction

This section contains the procedures to display and remove Telnet listeners.

Displaying Telnet Listeners

The SHOW / LIST / MONITOR TELNET LISTENER command displays the Telnet listener characteristics. The ALL characteristic displays all the Telnet listeners. You can specify a specific Telnet listener by its TCP port number.

Example: SHOW TELNET LISTENER Display

The following example shows how to display the Telnet listener characteristics on TCP port 2010:

```
Local> SHOW TELNET LISTENER 2010
Listener TCP-port:          2010
Identification:             Printer
Ports:                      6,8
Connections:                Enabled
```

The first line displays the TCP port number; the second line displays the identification string; the third line displays the listener's access server port numbers; the last line displays whether connections to the listener are enabled or disabled.

Displaying Telnet Server Characteristics

The SHOW / LIST / MONITOR PORT TELNET SERVER CHARACTERISTICS command displays the Telnet server characteristics.

Example: SHOW PORT TELNET SERVER CHARACTERISTICS Display

The following example shows how to display the Telnet server characteristics on port 12:

```
Local> SHOW PORT 12 SESSIONS 1 CHARACTERISTICS
Xmit Char Size:    8       Newline From Term:       <CRLF>
Rcv Char Size:     8       Newline From Host:       <CRLF>
IP:                None    Newline To Term:         <CRLF>
AYT:               None    Newline To Host:           <CR>
AO:                None    EC:                        NONE
EOR:               None    EL:                        NONE
NOP:               None    BRK:                       None
Local>
```

Removing a Telnet Listener

You can remove a Telnet listener that was defined in either the permanent or operational databases. Use the privileged CLEAR TELNET LISTEN command (which acts on the operational database) or PURGE TELNET LISTEN command (which acts on the permanent database) to remove a defined Telnet listener and its associated characteristics.

Example: Removing a Telnet Listener

The following example shows how to remove Telnet listener 2010 from the access server permanent database:

```
Local> PURGE TELNET LISTENER 2010
```

Removing One of Many Devices Assigned to a Telnet Listener

To remove a device that is one of many devices assigned to a Telnet listener, perform the following steps:

Step	Action
1	Use the SET TELNET LISTEN CONNECTIONS DISABLED command to stop any future connections. The SET TELNET LISTEN CONNECTIONS DISABLED command is refused if a session exists. Example: The following example shows how to disable future connections to internet port 2005: `Local> SET TELNET LISTEN 2005 CONNECTIONS DISABLED`
2	If a session exists, use the LOGOUT command to log out the port.

Step	Action
3	Disable the port as follows (substitute your listener TCP port for 2005 and the listener physical port for 5): `Local> CHANGE TELNET LISTENER 2005 PORT 5 DISABLED`
4	Enable the Telnet listener. The following shows how to enable connections to internet port 2005: `Local> SET TELNET LISTEN 2005 CONNECTIONS ENABLED`

Reassigning a Port

This process allows you to manage a failed access server port that is configured as a Telnet listener. Use the following steps to reassign a port:

Step	Action
1	Use the LIST PORT n CHARACTERISTICS command to learn the values used in the existing configuration.
2	Disconnect the device from the port.
3	Select a new port and reattach the device at the new port.
4	Set the new port's values to those of the existing port. If the values are unavailable, you need to configure the device as described in Chapter 4.
5	Enable the Telnet listener on this port and disable the Telnet listener on the original port.

Supplying User Location Data to Telnet Servers

Introduction

When the access server creates a Telnet client connection, it automatically negotiates with the Telnet server to send port user data. If the server responds with a "send" message, the access server transmits the session port name and port number.

Appropriate software on the server can then use the location data for each session to generate statistics about Telnet use. In these negotiations, the access server functions only as a Telnet client, not as the Telnet server.

Each time the Telnet server transmits IAC DO, the client sends the location data. In this way, the server can poll anytime for the user's location. If the Telnet server does not respond with IAC DO, the session proceeds normally, but the client does not send the location data.

Example: TCP Messages to Poll Client User Location Data

The following example shows a series of TCP messages generated during negotiation between the Telnet client (the access server) and the Telnet server. The client starts the negotiation with IAC WILL SEND-LOCATION.

```
IAC WILL SEND-LOCATION
IAC DO SEND-LOCATION
IAC SB SEND-LOCATION ascii-location IAC SE
IAC DO SEND-LOCATION
IAC SB SEND-LOCATION ascii-location IAC SE
.
.
.
```

The *ascii-location* field comprises the Telnet user's port name and port number. The port number is stored in the access server NVRAM. The port name is also stored in NVRAM. It is the string specified by the DEFINE/CHANGE PORT NAME command, and it appears in the display for the LIST PORT command.

Configuring a Raw TCP Listener

Introduction

When you configure a Telnet listener to use raw TCP, the associated port sends data to a device or a remote host without any data manipulation or interpretation of control characters. Because raw TCP sends the data it receives to a port without any interpretation, sending data this way is faster than using the Telnet protocol. The raw TCP listener also allows an application program on a remote host to use single socket I/O (input/output) calls and bypass the Telnet protocol layer.

When To Use Raw TCP

Using raw TCP is beneficial when you need to maintain the control character definitions in the data you send to and from a port on the access server or when you need to send data without any Telnet processing. For example, when sending data to a printer, you may need to preserve the control characters sent to the printer or you may need to run socket I/O calls. In these cases, you want to configure the raw TCP protocol on the Telnet listener.

Configuring Raw TCP

To configure raw TCP on an access server, configure a Telnet listener that has a type of RAW. Use the CHANGE TELNET LISTENER TYPE RAW command to configure the Telnet listener. Then use the CHANGE TCP LISTENER or CHANGE TELNET LISTENER commands to define additional characteristics.

Example: Configuring Raw TCP

The following example shows how to a configure raw TCP listener on port 3:

```
Local> CHANGE TELNET LISTENER 2003 PORT 3
Local> CHANGE TELNET LISTENER 2003 TYPE RAW
Local> CHANGE TELNET LISTENER 2003 CONNECTIONS ENABLED
```

These commands:

- Create a Telnet listener on access server port 3 and assign TCP port 2003 to the port.
- Set the type for the Telnet listener to RAW.
- Enable the raw TCP listener.

Displaying Raw TCP Characteristics

Use the SHOW / LIST TELNET LISTENER command to view the raw TCP settings.

Example: Raw TCP Display

The following example shows a typical display for a Telnet listener configured for raw TCP:

```
Local> SHOW TELNET LISTENER 2003
Listener TCP-port: 2003 Listener Type: RAW TCP
Identification:
Ports: 3
Connections: ENABLED
IP address: 12.22.22.22
```

Chapter 15

Configuring LPD Printers

Overview

Introduction

The Line Printer Daemon (LPD) handles remote networking printing. It listens for print requests from remote hosts on the Local Area Network (LAN) and responds to these requests. The LPD software that the access server implements is similar in function to the LPR / LPD (Line Printer Remote / Daemon) on UNIX systems.

In This Chapter

This chapter contains the following topics:

- LPD Operation
- Configuring LPD

LPD Operation

Supported File Types

The access server's LPD implementation supports printing of ASCII text and PostScript header and trailer pages. The access server does not convert files from one format to the other. The host system must be configured with appropriate printer drivers to match the file formats supported by the printer.

Users must be aware of the type of file they want to print and select the appropriate printer and printer driver when submitting a print job.

Control and Data Files

During the printing operation, the access server receives control and data files from the remote host. The following table describes these files:

This File:	Contains:
Control	File format information and user information (for example, host and user name).
Data file	Total number of bytes in the file, the name of the data file, and the data.

Remote hosts can send control and data files in any order. The access server does the following:

- If the control file arrives first, the access server stores the file, waits for the data file to arrive, and then prints the data. The access server sends the user data in the control file as the last page of the print job.

If the Control File Arrives First and the:	Does the Header/ Trailer Print?	Does the User Information Print?
Header is enabled.	Yes	Yes
Header is disabled.	No	No
Header is optional.	Yes	Yes
Trailer is enabled.	Yes	Yes
Trailer is disabled.	No	No
Trailer is optional.	No	No

- If the data file arrives first, the access server sends the file to the printer according to the printer setup on the port. When the control file arrives, the access server sends the user data to the printer as the last page of the print job. In this situation, the access server cannot display or use user information from the control file while the file is printing.

If the Data File Arrives First and the:	Does the Header/ Trailer Print?	Does the User Information Print?
Header is enabled.	Yes	No
Header is disabled.	No	No
Header is optional.	No	No
Trailer is enabled.	Yes	Yes
Trailer is disabled.	No	No
Trailer is optional.	Yes	Yes

Operation

The access server receives print requests from remote hosts on TCP port 515. It uses LPD to send the file to a local printer through the access server's LAN interface and a serial port. Figure 15-1 shows what occurs when a host on the LAN uses LPD to send a print job to the access server:

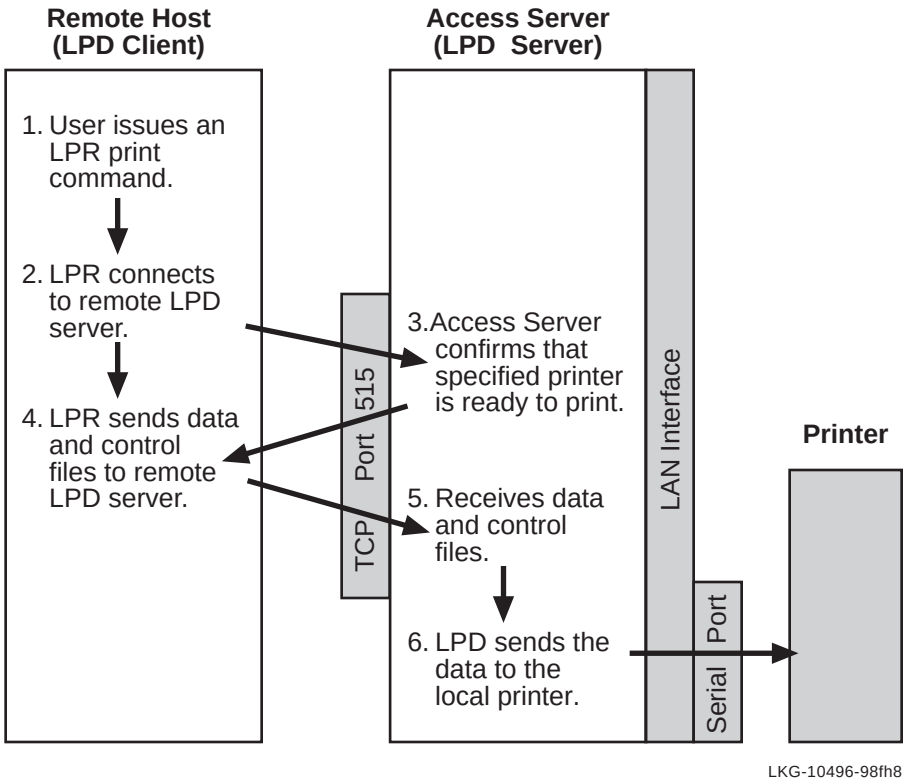


Figure 15-1. What Occurs When a Host on the LAN Uses LPD to Send a Print Job to the Access Server

Configuring LPD

Configuring Remote Hosts

Remote network printing using LPR/LPD requires that you set up the host system correctly. The following table describes the setup requirements for specific types of hosts:

If Printing From This Host:	**Then:**
UNIX	Create an entry in the /etc/printcap file that includes the name of the remote printer and the IP address of the access server (the LPD server). Refer to your system's LPR/LPD documentation for details. Users must convert files to either ASCII text or PostScript format before printing files.
Windows NT	1. Install a TCP/IP printing service. 2. Install a printer (use the Control Panel). 3. Choose an appropriate print driver for the printer. 4. Assign the LPR port that the TCP/IP printing service creates to the printer. This causes the system to prompt the user to enter the LPD server's IP address and remote printer name.
VMS UCX	1. Install the UCX software. 2. Run UCX$LPRSETUP.EXE to set up the LPR printer. 3. Follow the prompts to set up the printer.

Associating a Printer With a Port

To allow remote network printing with LPD, associate a printer with one or more ports.

This is similar to defining a Telnet or TCP listener; however, instead of specifying a port number, you specify a printer name. The printer name must be unique on the network. You can associate the printer with a single port or you configure it to be shared across multiple ports. This allows you to assign a single name to a collection of similar printers.

Use the DEFINE/SET/CHANGE PRINTER command to associate a printer with a port and configure print characteristics.

The following table lists the print characteristics that you can configure:

Characteristic	Description
AUTOCR	Automatically inserts a carriage return. When you enable this option, the access server inserts a carriage return after each line feed character if there is no existing carriage return. The AUTOCR option applies only to ASCII text files.
CONNECTIONS	Specifies whether a user can queue a print job to a printer. You use this option to disable access to a printer temporarily for reasons such as routine maintenance or adding paper.
FLAGPAGE	Specifies a message that prints on the flag page that prints before the file data.
HEADER	Specifies whether a header page prints before the file data. You can set this option so that no header page prints if the access server does not know the user name at the start of the print job (for example, if the access server receives the data file before it receives the control file).
IDENTIFICATION	Specifies a text string (40 characters or less) that is associated with a printer.
TRAILER	Enables or disables printing of a trailer page after file data prints. You can set this option so that no trailer page prints if the access server does not know the user name at the start of the print job (for example, if the access server receives the data file before it receives the control file).
TYPE	Specifies ASCII or PostScript. Use this option to determine the kind of flag page or pages to send to the printer.

Setting Port Characteristics

For LPD to communicate with your printers, you must set the following port characteristics:

- ACCESS REMOTE
- AUTOBAUD DISABLED
- FLOW CONTROL, PARITY, SPEED and STOP BITS to match the printer's settings

Use the DEFINE/SET/CHANGE PORT command to configure port characteristics.

Printer Configuration Example

The following example shows how to configure the access server to use LPD for remote network printing:

```
Local> DEFINE PRINTER LPS32_PS CONNECTIONS ENABLED HEADER
ENABLED PORTS 4,5 TRAILER DISABLED AUTOCR DISABLED
```

In this example:

- The name of the printer is LPS32_PS.
- The printer is set to allow users to submit print jobs to it.
- A header page prints at the start of each job.
- The ports associated with the printer are 4 and 5.
- No trailer page prints at the end of the job.

Displaying Printer Characteristics

Use the LIST/SHOW PRINTER command to display the printer characteristics. You can specify a printer name or display all of the configured printers.

Printer Display Example

The following shows a typical display when you enter the SHOW PRINTER ALL command:

```
Local> SHOW PRINTER ALL
Printer:         LPS32_PS             Header Page:   Enabled
Connections:     Enabled              Trailer Page: Optional
Flag Page Type:  Postscript           Auto C/R:     Disabled
Identification:  The PostScript Printer
Flag Page Note:
Ports: 4,5

Printer:         LPS32_ASCII          Header Page:   Enabled
Connections:     Enabled              Trailer Page: Optional
Flag Page Type:  ASCII                Auto C/R:     Disabled
Identification   The ASCII Text Printer
Flag Page Note:
Ports:           6

Local>SHOW PORT
Port 3:                        Server: LAT_08002BB767E3


Character Size:    8          Input Speed:             9600
Flow Control:      XON        Output Speed:            9600
Parity:            None       Signal Control:      Disabled
Stop Bits:         Dynamic

Access:            Remote     Local Switch:            None
Backwards Switch:  None       Name:                  PORT_3
Break:             Local      Session Limit:              4
Forwards Switch:   None       Type:                   Ansi
Default Protocol:  LAT        Default Menu:            None
Dialer Script:     None

Preferred Service: None

Authorized Groups: 0
(Current) Groups:  0

Enabled Characteristics:
Broadcast, Failover, Input Flow Control, Lock, Loss
```

```
Notification, Message Codes, Output Flow Control,
Verification

Local> SHOW PRINTER SPEEDY STATUS

Printer:          SPEEDY
Identification:   Fast Laser Printer
Print Jobs:       34               Total Bytes Sent: 459285

Printer Service Status:

Port   User   Status                  Bytes

4             Waiting for data file   3045
5             Waiting for LPD command 0
```

Chapter 16

Configuring and Managing SLIP Ports

Overview

Introduction

This chapter explains how to configure and manage access server ports for use with PCs and computers acting as serial line Internet protocol (SLIP) hosts. A SLIP host is an Internet host that uses SLIP as its data link over low-speed serial lines.

To use the procedures in this chapter, you must:

- Ensure that the devices support SLIP.
- Connect and test the devices.
- Enable privileged status.
- Configure the port and device characteristics to match.

This chapter provides information about configuring only the access server for SLIP communications. For information about configuring SLIP hosts, refer to the documentation provided with the host system.

In This Chapter

This chapter contains the following topics:

- Packet Forwarding to and from SLIP Hosts
- Displaying SLIP Characteristics
- Managing Internet Addresses for SLIP Hosts

- Managing the Maximum Transmission Unit
- Configuring a Port So That a PC Can Function as a Terminal or SLIP Host
- Configuring a Dedicated SLIP Port
- Configuring a Dial-In Modem for Use with a SLIP Host
- Establishing Terminal Sessions with a PC
- Establishing a SLIP Session
- Establishing a SLIP Session
- Compressed SLIP
- Displaying SLIP Counters
- Disabling SLIP

Packet Forwarding to and from SLIP Hosts

Description

During SLIP sessions, the access server forwards packets from an attached SLIP host through the Ethernet interface to the Internet. When the access server receives a packet addressed to an attached SLIP host, it forwards the packet to that host. The access server also directly forwards packets from one attached SLIP host to another attached SLIP host.

The access server acts like an ordinary IP router to an attached SLIP host. The access server appears like a multihomed IP host to the IP routers on the Internet. A multihomed host is an IP host with more than one IP address.

Network Configuration Containing SLIP Hosts

Figure 16-1 shows a sample network configuration that contains SLIP hosts:

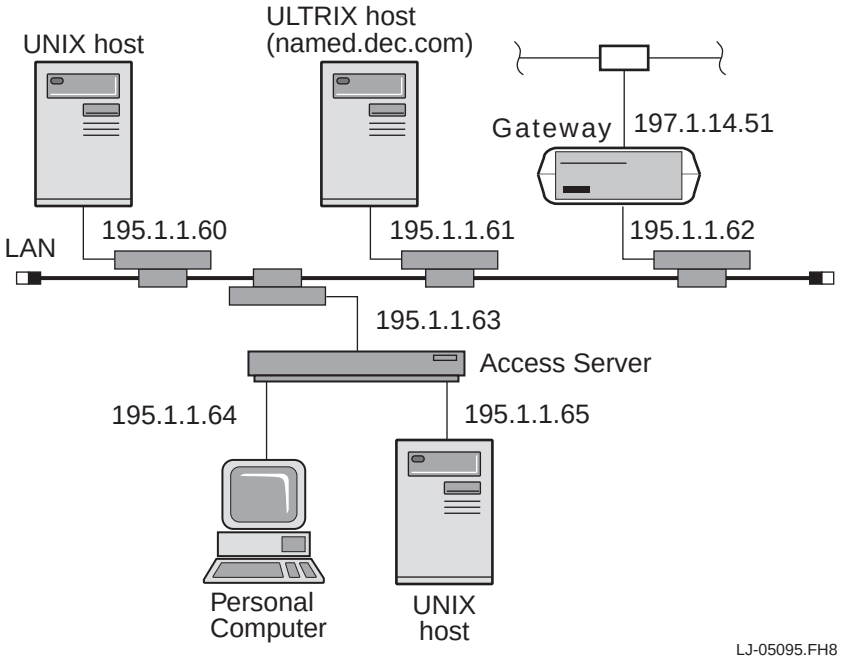


Figure 16-1. Sample Network Configuration That Contains SLIP Hosts

Displaying SLIP Characteristics

Introduction

The LIST / SHOW / MONITOR SLIP CHARACTERISTICS command enables you to display the SLIP configuration for a given port. The characteristics that you manage are the host address, the Maximum Transmission Unit (MTU) and the compression.

If you change SLIP characteristics while a SLIP session is already established, the changes have no effect until you start a new SLIP session.

Command

Use the SHOW PORT n SLIP CHARACTERISTICS command to display SLIP characteristics.

Displaying SLIP Characteristics Example

The following example shows a typical SLIP characteristics display:

```
Local> SHOW PORT 5 SLIP CHARACTERISTICS
Port 5: Rick Server: Servername
Host Address: 17.20.19.7 MTU: 1006
Header Compression: Disabled Compression States: 16
```

Managing Internet Addresses for SLIP Hosts

Introduction

The Internet address for the SLIP host must be unique on the subnet and must have the same subnet identifier as the access server. A subnet identifier is the result of a logical AND operation on the Internet address and the subnet mask.

For example, assume that you set:

1. The access server Internet address as follows:

   ```
   Local> CHANGE INTERNET ADDRESS 83.62.18.101
   ```

2. The subnet mask as follows:

   ```
   Local> CHANGE INTERNET SUBNET MASK 255.255.255.0
   ```

In this situation, the subnet identifier is 83.62.18.0.

In this example, the Internet address of the SLIP host must be 83.62.18.xx. The value xx is any number between 1 and 254, except 101. The value 101 is the access server Internet address.

How an Access Server Port Obtains the SLIP Host Internet Address

This section describes how an access server port obtains the SLIP host Internet address. The SLIP host port address must be contained in the access server subnet identifier. You can assign an address or you can allow the access server to automatically obtain the SLIP host address.

Assigning a Host Internet Address

To assign the Internet address to a port, use the SET/DEFINE/CHANGE PORT SLIP HOST ADDRESS command as shown in the following example:

```
Local> CHANGE PORT SLIP HOST ADDRESS 195.1.1.101
```

After you assign the address, you can enter the SHOW PORT SLIP CHARACTERISTICS command on the SLIP host to verify the change. You then need to assign the address to the attached host.

RADIUS Specified SLIP Host Address

If a user performs a RADIUS authentication, the SLIP host IP address may be specified in the user's authorization data. A RADIUS specified address of 255.255.255.254 means the IP address of the port is used. An address of 255.255.255.255 means the PC client's IP address is used (see below).

How a Port Automatically Obtains the SLIP Host Address

If you configure a port for SLIP communication and do not assign a host address, the access server does the following:

1. Reads the source address from the attached host's first output IP packet.
2. Automatically assigns this address to the port if it is valid.

The access server clears this address when the SLIP host logs out from the port.

Managing the Maximum Transmission Unit

Introduction

The maximum transmission unit (MTU) value specifies the maximum size of the datagram that a given access server port accepts. The range is 64 to 1500 bytes. The default is 1500 bytes.

Changing the MTU

You can change the MTU value using the SET / DEFINE / CHAGE PORT n MTU command. If you use the SET or CHANGE command, the new value does not affect an existing SLIP connection.

MTU Change Example:

The following example makes the access server compatible with attached hosts that have fixed MTU values other than 1006 bytes:

```
Local> DEFINE PORT 4 SLIP MTU 500
```

Relationship of the TCP Maximum Segment Size and the MTU

An attached host announces the TCP maximum segment size (MSS) at connection time. The MSS specifies the largest fragment of a datagram that the attached host is willing to receive. The MSS is normally based on the MTU of the network connection as recommended by RFC 879.

The MSS should always be smaller than the MTU value. The TCP and IP headers account for the difference between the two values.

Fragmentation

When the TCP MSS announced by the SLIP host exceeds the MTU on the SLIP line, IP fragmentation occurs. Therefore, an MSS value that greatly exceeds the MTU causes excessive fragmentation and downgrades performance.

Setting the MTU adjusts the point at which IP fragmentation occurs when sending datagrams. Setting the MTU also adjusts the maximum receive unit (MRU) packet size. Since the access server considers packets larger than the MTU as framing errors, it discards these packets.

Configuring a Port So That a PC Can Function as a Terminal or SLIP Host

Introduction

This section describes how to configure an access server port so that you can use an attached PC as a both a terminal and a SLIP host. With this configuration, port users can switch between terminal emulation and SLIP mode.

To configure the port so that the PC acts only like a SLIP host, refer to the Configuring a Dedicated SLIP Port section in this chapter.

Before you configure a port for SLIP communications as shown in the following example, you must configure the device and port characteristics as described in Chapter 9.

Example: Configuring a PC As a Terminal and SLIP Host

The following example shows a sample port configuration that enables a PC to act as both a terminal and a SLIP host:

```
Local> DEFINE PORT 2 ACCESS LOCAL AUTOBAUD ENABLED
Local> DEFINE PORT 2 BREAK LOCAL DEDICATED NONE
Local> DEFINE PORT 2 DEFAULT PROTOCOL SLIP DSRLOGOUT ENABLED
Local> DEFINE PORT 2 FLOW CONTROL CTS INACTIVITY LOGOUT ENABLED
Local> DEFINE PORT 2 INTERRUPTS DISABLED PASSWORD DISABLED
Local> DEFINE PORT 2 SIGNAL CHECK DISABLED SIGNAL CONTROL DISABLED
Local> DEFINE PORT 2 SLIP ENABLED
Local> DEFINE PORT 2 SLIP HOST 195.1.1.1
Local> DEFINE PORT 2 SLIP MTU 800 Local> LOGOUT PORT 2
```

Configuring a Dedicated SLIP Port

Introduction

The dedicated SLIP port allows a single SLIP session.

Before you perform this procedure, you must configure the device and port characteristics as described in Chapter 9.

Configuring a Device As a Dedicated SLIP Host

The following example shows a sample configuration of a dedicated SLIP port:

```
Local> DEFINE PORT 4 ACCESS LOCAL AUTOBAUD DISABLED AUTOCONNECT ENABLED
Local> DEFINE PORT 4 BREAK DISABLED DEDICATED SLIP
Local> DEFINE PORT 4 DEFAULT PROTOCOL SLIP
Local> DEFINE PORT 4 DSRLOGOUT DISABLED DTRWAIT DISABLED
Local> DEFINE PORT 4 FLOW CONTROL CTS INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 4 INTERRUPTS DISABLED PASSWORD DISABLED PREFERRED NONE
Local> DEFINE PORT 4 SIGNAL CHECK DISABLED SIGNAL CONTROL ENABLED
Local> DEFINE PORT 4 SLIP ENABLED
Local> DEFINE PORT 4 SLIP HOST 195.1.2.1
Local> DEFINE PORT 4 SLIP MTU 800
Local> LOGOUT PORT 4
```

Configuring a Dial-In Modem for Use with a SLIP Host

Introduction

Before you perform this procedure, you must configure the device and port characteristics as described in Chapter 9.

Configuring a Dial-In Modem on Port 6 for Use with a SLIP Host

The following example shows a sample configuration of a port using a dial-in modem for use with a SLIP host on a full modem control access server:

```
Local> DEFINE PORT 6 ACCESS LOCAL ALTERNATE SPEED NONE AUTOBAUD ENABLED
Local> DEFINE PORT 6 DEFAULT PROTOCOL SLIP
Local> DEFINE PORT 6 DSRLOGOUT DISABLED DTRWAIT DISABLED
Local> DEFINE PORT 6 FLOW CONTROL CTS INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 6 INTERRUPTS DISABLED PASSWORD ENABLED
Local> DEFINE PORT 6 SIGNAL CHECK DISABLED SIGNAL CONTROL ENABLED
Local> DEFINE PORT 6 SLIP ENABLED SPEED 57600 SLIP HOST 195.1.3.1
Local> DEFINE PORT 6 SLIP HOST 195.1.3.1
Local> DEFINE PORT 6 SLIP MTU 800
Local> LOGOUT PORT 6
Local> DEFINE PORT 6 SPEED 51600
```

Establishing Terminal Sessions with a PC

Prerequisites

Before you can use a PC to establish a terminal session with the access server, you must:

1. Configure the device and port characteristics as described in Chapter 9.
2. Enter the commands to set up SLIP operating characteristics as shown in the Example: Configuring a PC As a Terminal and SLIP Host, in this chapter.
3. If you want to authenticate a user, make sure that a terminal emulation program is installed and running on the PC. The terminal emulation program needs to be invoked after a connection is established so that the user can respond to prompts for authentication.

Refer to Managing Dial-Up Access Security with AUTOLINK and AUTOLINK Authentication in Chapter 22 for more information if you have enabled AUTOLINK authentication.

Once the terminal emulation program is running and the user is authenticated, the PC can access hosts on the TCP/IP and LAT networks through the access server by using the CONNECT command.

Establishing a SLIP Session

Enabling a SLIP Session from the PC

The following example shows how a nonprivileged user could configure and start a SLIP session. The example assumes that the port characteristics are configured as shown this example. The CHANGE PORT SLIP MTU command is optional.

```
Local> CHANGE PORT SLIP HOST 195.1.1.1 SLIP MTU 800
Local> CHANGE PORT SLIP MTU 800
Local> CONNECT SLIP
Local-561-Starting SLIP or PPP datalink session
```

If you previously configured the port with an Internet address and an MTU, then you only need to use the CONNECT SLIP command.

After Making a Connection

Once you enter the CONNECT SLIP command, the access server expects IP packets from the PC formatted as SLIP frames. Use the appropriate command to exit from terminal emulation mode on your PC and start the desired IP application program.

To transfer files, use any file transfer program that supports SLIP. You do not need to configure data transparency on the access server.

Compressed SLIP

Introduction

The access server has the ability to enable compressed SLIP (CSLIP). Enabling CSLIP compresses the lengthy headers of IP datagrams on low-speed asynchronous serial lines. Therefore, enabling CSLIP can improve performance.

Enabling CSLIP

Use the SET/CHANGE PORT n SLIP COMPRESSION command to enable or disable CSLIP. By default, compression is disabled. When you enable CSLIP, make sure that it is enabled at both ends of the communications link. If only one end of the link is running CSLIP, performance degrades.

Example: Enabling CSLIP

The following example shows how to enable CSLIP on port 5:

```
Local> CHANGE PORT 5 SLIP COMPRESSION ENABLED
```

Disabling CSLIP

The following example shows how to disable CSLIP on a port:

```
Local> CHANGE PORT 5 SLIP COMPRESSION DISABLED
```

Automatic CSLIP

You can enable a port to start CSLIP automatically if the port receives compressed data over an already existing SLIP session. The following example shows how to enable automatic CSLIP on a given port:

```
Local> CHANGE PORT 5 SLIP COMPRESSION AUTOCOMPRESS
```

Compression States

You can specify the number of connections that can be compressed over the data link at one time. The following example shows how to change the number of compression states on a port:

```
Local> CHANGE PORT COMPRESSION STATES 10
```

The default number of compression states is 16.

Displaying SLIP Counters

Commands

The SHOW / MONITOR PORT SLIP COUNTERS command displays the various SLIP counters. To reset the counters, use the ZERO COUNTERS PORT SLIP command.

SHOW PORT SLIP COUNTERS Display

The following example shows a typical SLIP counters display:

```
Local> SHOW PORT 5 SLIP COUNTERS
Port 1: Rick Server: Servername
Connect Time:         0 00:00:00
Bytes Received:       0 Bytes Sent:                    0
Packets Received:     0 Packets Sent:                  0
Receive Packets Lost: 0 Send Packets Lost:             0
Send Packets Queued:  0
```

SLIP COUNTERS Display Fields

The following table describes the information in the SLIP Counters display:

Field	Description
Connect Time	Length of duration of the SLIP session. This is 0 if there is no SLIP session.
Bytes Received	Number of bytes received by the access server from the SLIP host on the port.
Bytes Sent	Number of bytes sent by the access server to the SLIP host on the port.
Packets Received	Number of IP packets received by the access server from the SLIP host on the port.
Packets Sent	Number of IP packets sent by the access server to the SLIP host on the port.
Receive Packets Lost	Number of receive IP packets lost due to framing errors.

Field	Description
Send Packets Lost	Number of send IP packets lost due to lack of buffers.
Send Packets Queued	Number of IP packets in a queue to be sent to the SLIP host on the port.

Disabling SLIP

Command

Use the CHANGE PORT n SLIP DISABLED command to disable SLIP on a port.

Disable SLIP Example

The following example shows how to disable SLIP on port 2:

```
Local> CHANGE PORT 2 SLIP DISABLED
```

Chapter 17

Configuring for SNMP Access

Overview

Introduction

This chapter describes how to configure the access server simple network management protocol (SNMP) agent so that it can be controlled by a remote Network Management Station (NMS).

Reference

For complete information about managing SNMP on the access server, refer to the file snmp_survival.txt contained in the software installation kit. This file fully describes every SNMP-accessible variable and table in the access server. For example, the file describes:

- What values variables can take
- When and how variables and tables change
- How the user interface can access variables and tables

In This Chapter

This chapter contains the following topics:

- Supported SNMP Features
- Configuring the Access Server for SNMP Access
- Configuring the NMS

Supported SNMP Features

Supported Specifications

The access server supports the SNMP specifications listed in the following table:

Specification	Title
RFC 1155	Structure for Management Information for TCP/IP-Based Protocols
RFC 1157	A Simple Network Management Protocol (SNMP)

SNMP Community Names

An SNMP community name is a character string that the NMS uses as a password to gain access to the access server. A community name contains a maximum of 32 characters.

Due to memory constraints, the access server can have only a limited number of community names.

Community Name Reference

For more information about using community names, refer to the Configuring the Access Server for SNMP Access section in this chapter.

Supported SNMP Operations

The access server supports the SNMP operations listed in the following table:

Operation	Description	Default for All Community Names
GET	Fetches the value of a variable.	Enabled
GETNEXT	Fetches a value without knowing the variable's exact name.	Enabled
SET	Enables you to modify access server parameters and create and delete table entries.	Disabled
TRAP	Indicates the occurrence of an event.	Disabled

Supported MIBs

The access server supports the Management Information Bases (MIBs) listed in the following table. The release kit contains all supported MIBs. The network manager can enroll these MIBs in the appropriate NMS.

MIB	Description
RFC 1213	Management Information Base (MIB II) for Internet protocol suite management. This makes RFC 1158 obsolete.
RFC 1243	Definitions of Managed Objects for the AppleTalk MIB.
RFC 1284	Definitions of Managed Objects for the Ethernet-like interface types.
RFC 1158	Obsolete MIB II. Supported for backwards compatibility.
RFC 1316	Definitions of Managed Objects for Character Stream Devices, the Character MIB. The obsolete draft version dated March 19, 1991, is also supported for backwards compatibility.
RFC 1317	Definitions of Managed Objects for RS232-like Hardware Devices, the RS232-like MIB. The draft version dated March 19, 1991, is also supported for backwards compatibility.
RFC 1471	Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol.
RFC 1473	Definitions of Managed Objects for the IP Network Protocol of the Point-to-Point Protocol.
Accounting	Private MIB used to access the accounting data stored in volatile memory of the access server.
IPX	Private MIB used to manage the IPX protocol stack in the access server.
IPXCP	Private MIB used to manage the IPX Network Control Protocol of the Point-to-Point Protocol.

Supported MIB Variables

The standard Internet MIB contains approximately 200 variables. The meanings of many of these objects are device-specific.

For more information about MIB variables, refer to the file snmp_survival.txt contained in the software installation kit. This file provides explanations of the various SNMP (MIB) objects implemented on the access server.

Supported Management Information Base Variables

Figure 17-1 illustrates the access server implementation of MIB-II, the Character MIB, RS-232-like MIB, AppleTalk MIB, and Ethernet-like MIB variables. The objects described in this section are implemented as defined in RFCs 1213, 1243, 1284, 1316, and 1317.

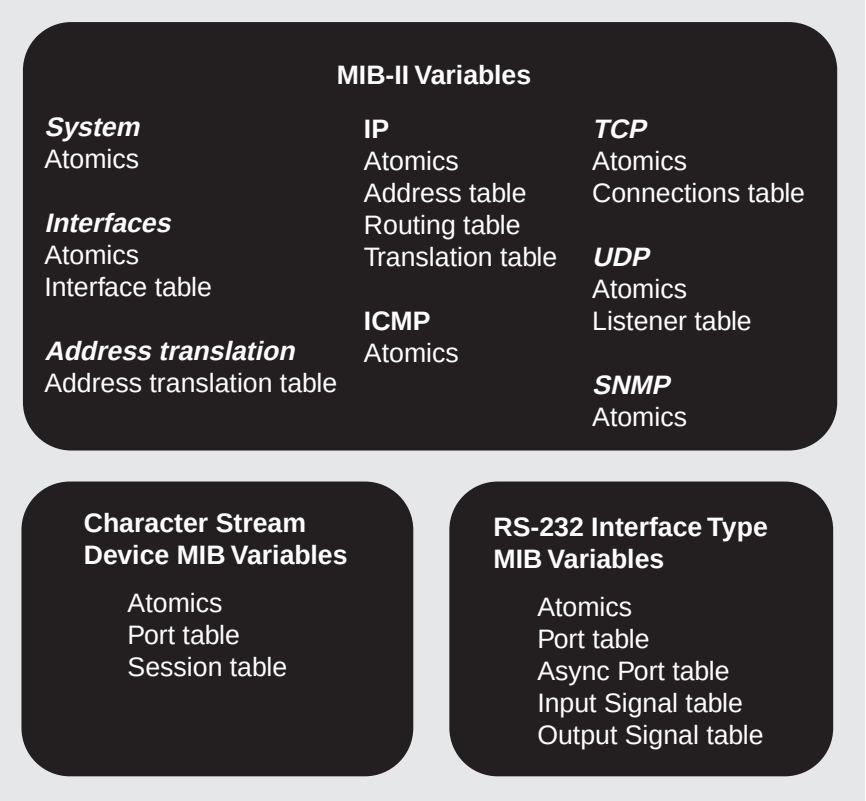


Figure 17-1. Access Server Implementations

Configuring the Access Server for SNMP Access

Enabling and Disabling SNMP

The access server must have an Internet address to enable SNMP. To enable SNMP, enter:

```
Local> CHANGE SNMP ENABLED
```

To disable SNMP, enter:

```
Local> CHANGE SNMP DISABLED
```

Displaying Information About SNMP

Use the SHOW SNMP command to display the access server's SNMP characteristics.

Example: Displaying SNMP Information

The following example shows how to display SNMP information on the access server:

```
Local> SHOW SNMP

SNMP State:   ENABLED      AUTHENTICATION FAILURES: ENABLED

Community Name      Address           GET GETNEXT SET TRAP
PUBLIC              ANY               ENA ENA     DIS DIS
SNUGS               ANY               ENA ENA     ENA DIS
BUGS                195.1.1.1         ENA ENA     ENA DIS
SERVER              195.1.1.2         ENA ENA     ENA ENA
```

Default Community Name PUBLIC

The CHANGE SNMP ENABLED command automatically configures the access server with the default community name PUBLIC. This community name follows the default behavior for the SNMP operations listed in the Supported SNMP Operations section in this chapter.

Configuring a Community Name for Access by Any NMS

Use the CHANGE SNMP COMMUNITY community-name SET ENABLED command to create a community name.

When you create a community name without specifying an address the access server assigns the default address ANY. The address ANY enables any NMS that knows this community name to GET or SET information about the access server.

Example: Configuring Community Names for Access by Any NMS

The following example shows how to create the community name SNUGS without specifying an address:

```
Local> CHANGE SNMP COMMUNITY "SNUGS" SET ENABLED
Local> CHANGE SNMP ENABLED
```

Configuring a Community Name with an Address

You can configure a community name so that only an NMS with a given address can access the access server with SNMP commands. Use the CHANGE SNMP COMMUNITY community-name ADDRESS command to configure the community name in this way.

Example: Configuring Community Names for Access from a Specific NMS

The following example shows how to create community name BUGS. Only the NMS with the address 195.1.1.1 can GET or SET information about the server:

```
Local> CHANGE SNMP COMMUNITY "BUGS" ADDRESS 195.1.1.1
Local> CHANGE SNMP COMMUNITY "BUGS" SET ENABLED
Local> CHANGE SNMP ENABLED
```

One IP Address for a Community Name

Each community name can have only one IP address assigned. The access server rejects the addresses 0.0.0.0 and 255.255.255.255. By default, GET and GETNEXT are enabled when you create a community name.

Configuring Community Names to Send TRAP Messages

You can optionally configure the access server to send TRAP messages to a specific NMS for each community name. The access server generates TRAP messages in response to the events listed in the following table:

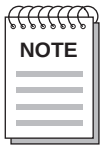
This Event:	Occurs When:
Cold start	The access server was reinitialized.
Line up	A network data link session was established on port n.

This Event:	Occurs When:
Line down	A network data link session was disconnected on port n.
Authentication	Unauthorized SNMP access was attempted

Example: Configuring SNMP TRAP Messages

The following example shows how to create the community name server. In this example, only NMS 195.1.1.2 can access community name SERVER. The access server sends TRAP messages to this NMS.

```
Local> CHANGE SNMP COMMUNITY "SERVER" ADDRESS 195.1.1.2
Local> CHANGE SNMP COMMUNITY "SERVER" SET ENABLED
Local> CHANGE SNMP COMMUNITY "SERVER" TRAP ENABLED
Local> CHANGE SNMP AUTHENTICATION ENABLED
Local> CHANGE SNMP ENABLED
```



TRAPS cannot be enabled for communities with the IP address ANY.

Sample SNMP Configuration

Figure 17-2 is a diagram of a network configuration that results from the commands in the Configuring a Community Name for Access by Any NMS, Configuring a Community Name with an Address, and Configuring Community Names to Send TRAP Messages sections:

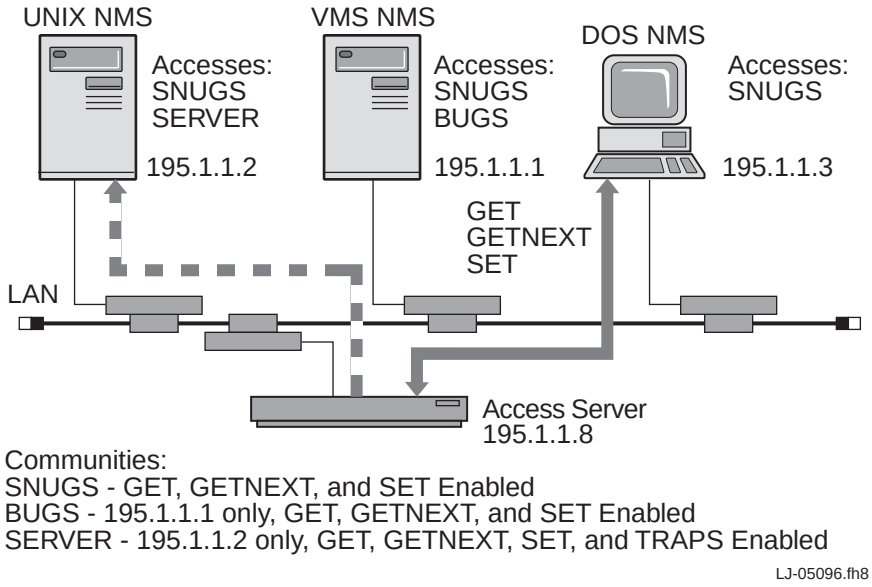


Figure 17-2. Diagram of a Network Configuration

Disabling TRAP Messages for a Community Name

To disable TRAP messages, use the CLEAR SNMP COMMUNITY community-name TRAP DISABLED command. The following is an example of disabling TRAP messages for the SERVER community:

```
Local> CLEAR SNMP COMMUNITY "SERVER" TRAP DISABLED
```

Removing Community Names

The access server allocates 80 bytes of NVRAM to store information about community names. If you attempt to define or modify a community name and there is insufficient memory, you see a message in this format:

```
Local -654- Insufficient space: total unused community characters left is n
```

In this situation, use the CLEAR or PURGE SNMP COMMUNITY command to remove one or more unused community names. You can also remove the default community name PUBLIC.

After you remove a community name, any NMS that used the community name is no longer able to communicate with the access server.

The following example shows how to remove community name BUGS:

```
Local> CLEAR SNMP COMMUNITY "BUGS"
```

Removing an Address from a Community Name

You can remove an NMS address from a community name by using the ANY keyword in the CHANGE SNMP COMMUNITY community-name ADDRESS command. This keyword allows any NMS that knows the community name to access the access server.

The access server, however, rejects an ADDRESS ANY command if TRAP access is enabled.

Example: Removing the Community Name Internet Address

The following example shows how to remove the Internet address from community name SERVER:

```
Local> CHANGE SNMP COMMUNITY "SERVER" ADDRESS ANY
```

Configuring the NMS

Procedure

To configure an NMS to manage an access server using SNMP, do the following:

Step	Action
1	Enter the access server management information bases (MIBs) in the NMS database (see Supported MIB Variables in this chapter). The software installation kit includes ASCII text files of these MIBs.
2	Enter the access server IP address, each appropriate community name, and desired access rights in the NMS database. If the community name is associated with an IP address, the address must be the Internet address of this NMS. The network manager must also associate the IP address of the access server with each such name. The exact procedure depends on the host-type of the NMS.
3	Configure the gateways to restrict unauthorized SNMP access by users from outside your network.

Chapter 18

Managing the Access Server

Overview

Introduction

The following lists the actions you perform to manage the access server. These actions should be done on an as-needed basis.

- Manage the access server as part of the LAT network.
- Manage the access server as part of the TCP/IP network.
- Manage access server characteristics.
- Check port status and counters.
- Reassign a port device (in case of port failure).

In This Chapter

This chapter contains the following topics:

- Managing Your Access Server As Part of the LAT Network
- Displaying Information About the Access Server
- Checking Port Status and Counters

Managing Your Access Server As Part of the LAT Network

Introduction

The network manager should coordinate the activities of service nodes and access servers. This section describes a set of configuration guidelines that helps maximize performance from your LAT network. All the guidelines presented are optional; however, failure to follow these guidelines might result in unnecessary performance degradation.

Distributing Devices on Access Servers

With the LAT protocol, the network bandwidth use is optimized when a high number of terminals (or other devices) are placed on every access server. If only one or two terminals are in use on each access server, the LAT protocol accounts for a higher proportion of the total Ethernet usage.

Controlling the Number of Known Service Nodes

Minimize the number of service nodes that are accessed from any one access server by keeping a single access server from accessing many different service nodes for its users. Having every access server user connecting to a different service node uses more of the data link bandwidth than many access server users connecting to few service nodes. To reduce the number of service nodes accessed from a particular access server, assign users to the access server based on their need for common services and then assign the appropriate authorized groups for the access server ports.

Checking LAT Service Accessibility

The node limit characteristic specifies the number of service nodes that can be simultaneously stored in the database for the access server. When the node limit is reached, messages from additional nodes are discarded. The node limit must be in the range of 1 to 2000. If you specify a node limit of NONE, there is no limit to the number of nodes stored. In this case, the node limit is subject to memory constraints. The default is 200 nodes.

If a user on the access server is experiencing response time problems with accessing LAT services, you can adjust the node limit characteristic. There is a faster connection when a user connects to a host that is defined in the access server database, as opposed to a host not in the database.

A higher node limit uses more of the access server memory. A lower node limit uses less memory. However, a lower node limit can potentially increase the time to make a connection to nodes that are not in the service database. You need to decide the optimal number for your needs.

The following example shows how to decrease the node limit to 100:

```
Local> CHANGE SERVER NODE LIMIT 100
```

Reducing Memory Usage

Set the node limit characteristic to a lower value. The access server automatically reduces the number of nodes in the database. This reduces the amount of memory used by the node database.

Viewing LAT Node Status Information

The SHOW / MONITOR NODE STATUS command displays information about the status of the selected nodes. This includes a list of the services offered by the nodes and information on each service. This display can help you track the availability and use of services.

Example: SHOW NODE STATUS Display

The following example shows how to generate a status display for the service node called PEACH:

```
Local> SHOW NODE PEACH STATUS
Node:            PEACH       Address            08-00-2B-00-2B-02
LAT Protocol:    V5.2        Data Link Frame Size:           1500

Identification:  Software Engineering Development

Node Groups:     20-50, 100-200

Service Name     Status      Rating               Identification

DEVELOP          2Connected  255      Hardware Development System
TEST             Available   150 High-powered Performance Testing
TIMESHARING      Available   27  Accts.Payable Development System

Local>
```

SHOW/LIST/MONITOR NODE STATUS Display Fields

The following table describes the information in the fields and headings of the node status display:

Field	Description
Node	Name of the service node.
LAT Protocol Vx.x	LAT protocol version number and update level of the service node software. LAT Version 5.2 protocol permits queued connection requests for printers connected to network access servers. LAT Version 5.2 protocol does not permit queued connection requests.
Address	Ethernet address of the service node.
Data Link Frame Size	Maximum Ethernet data link frame size used by the service node to receive messages.
Identification	Node identification string.
Node Groups	Group codes enabled for this service node. For a port to access the service node, at least one of these groups must.
Service Name column	Name of each service offered on this node. The same service might be offered on other service nodes. Use the SHOW SERVICE STATUS command to find the names of all the nodes offering a particular service.
Status column	• Available — Service is available to access server users. • n Connected — Service is available and n currently active sessions were requested with this service name. If the local access server is the service node specified in the display, sessions between two access server ports count as two sessions (one on the local port and one on the remote port). • Unavailable — All service nodes offering the service are unreachable. • Unknown.

Field	Description
Identification column	Service identification string.
Rating column	Value assigned to the service by the service node, indicating relative capacity to accept new connections or new queue connections. This value is the current load-balancing rating associated with the service. The rating varies from 0 to 255. With the higher value, the capacity of the service node to accept a new connection is greater.

Viewing LAT Node Counters Information

The SHOW / MONITOR NODE COUNTERS command displays the counters for messages transmitted between the access server and the selected LAT service nodes.

The counters apply only to the specified LAT service nodes. Some of these counters are also maintained for all the service nodes that the access server recognizes. When you enter a specific node name for the SHOW / MONITOR NODE node-name COUNTERS command, the counter values for only that service node appear in the display. To see the combined counters for all service nodes, use the SHOW SERVER COUNTER command.

Counters can help you estimate access server traffic on the network for specific time periods. For example, for information about daily access server usage, set the counters to zero at the start of each day.

You can also use counters data to calculate the average use of the Ethernet and the service nodes. By combining this data from the access server with the counters data from other access servers, you can calculate the network's capacity to handle more traffic.

Example: SHOW/LIST/MONITOR NODE COUNTERS Display

The following example shows how to generate a display of the counters for LAT messages between the access server and a service node named PEACH. Each counter displayed has a maximum value of 4,294,967,295. If a counter reaches that value, it remains at that value until either the counters are set to zero or the access server is initialized. Typically, the maximum values are not reached for several months.

```
Local> SHOW NODE PEACH COUNTERS
Node: PEACH
Seconds Since Zeroed: 961608  Multiple Node Addresses:    0
Messages Received:    687568  Duplicates Received:       21
Messages Transmitted: 558793  Messages Re-transmitted:   35
Slots Received:       509763  Illegal Messages Received:  0
Slots Transmitted:    532932  Illegal Slots Received:     0
Bytes Received:       13876620Solicitations Accepted:     0
Bytes Transmitted:    475427  Solicitations Rejected:     0
```

SHOW/LIST/MONITOR NODE COUNTERS Display Fields

The following table describes the information displayed in the previous example:

Field	Description
Node	Name of the node.
Seconds Since Zeroed	Number of seconds since the counters were last set to zero (maximum time exceeds 134 years).
Messages Received	Number of LAT virtual circuit messages that the access server received from this node.
Messages Transmitted	Number of LAT virtual circuit messages that the access server transmitted to this node.
Slots Received	Number of slots that the access server received from this node (slot represents a message segment for a particular session).
Slots Transmitted	Number of slots that the access server transmitted to this node.
Bytes Received	Number of data bytes that the access server received from this node.
Bytes Transmitted	Number of data bytes that the access server transmitted to this node.
Multiple Node Addresses	Number of times that a node advertised itself with a physical address different from that in a previous advertisement.
Duplicates Received	Number of messages the access server received from this node that were not in the correct sequence. This value should be less then 1/1000 of the value for Messages Received. This count usually indicates that the service node is retransmitting a message. If this value is higher than the guideline, the access server might not be handling the message traffic from the service node, causing the service node to retransmit messages.

Field	Description
Messages Retransmitted	Number of messages the access server retransmitted to this node. This value should be less than 1/1000 of the value for Messages Transmitted. If this value is higher than the guideline, the service node might not be handling the access server message load.
Illegal Messages Received	Number of illegally formatted messages the access server received from this node. This value should be zero. A count of nonzero indicates a possible software problem in either the access server or the service node.
Illegal Slots Received	Number of illegally formatted slots the access server received from this node. This value should be zero. A count of nonzero indicates a possible software problem in either the access server or the service node.
Solicitations Accepted	Number of queued connection requests that the access server has accepted, including queued requests and request that were immediately satisfied. The sum of the number of solicitations accepted and the number of solicitations rejected equals the number of queued connection requests that were received by the access server.
Solicitations Rejected	Number of queued connection requests that the access server has rejected. The sum of the number of solicitations accepted and the number of solicitations rejected equals the number of queued connection requests that were received by the access server. A rejected request might indicate a configuration problem at the access server or service node; for example, the port names do not match or a port has the incorrect access type.

Viewing LAT Node Summary Information

The SHOW NODE SUMMARY command produces a line of information for each selected service node. This display is useful to determine if a service node is reachable. The node summary is the default display class for the NODE and NODE ALL entity specifications.

Every service node name and access server name should be unique so as to allow other service nodes and users to distinguish among access servers. A unique access server name is necessary for an access server that is used for queued connection requests or for an access server to act as a service node.

The access server knows a service node by the node's Ethernet address and node name.

If you use the SET/DEFINE/CHANGE SERVER NAME command and you specify an access server name that is already being used by another node, other LAT nodes may replace your access server name with a default LAT name to make your access server name unique. The default is in the following format:

```
LAT_nnnnnnnnnnnn
```

The value nnnnnnnnnnnn is the unhyphenated, 12-digit Ethernet address of the second service node, which is used on the node summary displays.

Ports with LIMITED VIEW

Ports with LIMITED VIEW enabled cannot perform SHOW NODES.

Example: NODE SUMMARY Display

The following example shows how to generate a node summary display:

```
Local> SHOW NODE ALL SUMMARY

Node Name    Status        Identification

BANANA 2     Connected     Documentation System
ORANGE       Reachable     Terminals Development System
PEACH        Unreachable   Software Engineering Development
PEAR         Requesting    Printer Service
TEST         Unknown       High-powered Performance Testing

Local>
```

NODE SUMMARY Display Fields

The following table describes the information in the NODE SUMMARY display:

Heading	Description
Node Name	The name of the service node as defined in the access server node database.
Status	Reachability status of the service node shown as one of the following: • n Connected — Node is reachable and n sessions are active with services offered by the service node. • Reachable — No sessions are active, but the service node is accessible. • Requesting — Node that does not presently offer services has made remote connection requests to the access server (for printer access or for local services offered). • Unreachable — Active service session has timed out. The node can also signal that it is unreachable. • Unknown — No sessions are active, and the node has not been heard from recently.
Identification	Brief description about the service node as entered by the system manager.

Displaying Information About the Access Server

Introduction

The LIST / MONITOR / SHOW SERVER command displays information about the access server or about data maintained by the access server. You can obtain characteristics, counter, status, and summary displays for the access server.

Specifying the Prompt

The factory-set default access server prompt is `Local>`. You can change this prompt to any ASCII character, with a restriction of 1 to 16 characters. The following shows how to change this prompt to Engineering>. You should include a space at the end of the prompt, to leave space between the prompt and user commands.

```
Local> CHANGE SERVER PROMPT "Engineering> "
```

To go back to the default `Local>` prompt, enter the following command:

```
Local> CHANGE SERVER PROMPT ""
```

This command specifies the access server prompt displayed to all port users when in local mode, with the exception of the RCF management port.

Displaying Access Server Counters

The LIST / MONITOR / SHOW SERVER COUNTERS command displays the values for the global counters maintained by the access server. The counters display is useful for detecting network problems.

The first line displays the access server software version number and base level, LAT software version number, ROM version number, and the time that the access server has been running since the last downline load, expressed as days hours:minutes:seconds.

The COUNTERS data appear in two blocks:

- Ethernet data link counters — The upper block is for datagrams sent between the access server and all nodes on the Ethernet network. Some of the fields displayed are bit masks, the values of which tell the reasons for certain events.
- LAT protocol counters — The lower block is for messages transmitted between the access server and all LAT service nodes. The access server maintains some of these counters for each service node with which it communicates. Refer to

the node counters display descriptions in Viewing LAT Node Counters Information in this chapter.

Displaying Information About the Access Server

Each counter has a maximum value of 4,294,967,295. If a counter reaches that value, it latches (remains) at that value until either the counters are set to zero or the access server is initialized.

Example: SHOW SERVER COUNTERS Display

The following example shows how to generate an access server counters display:

```
Local> SHOW SERVER COUNTERS

Network Access SW Vx.x for DSxxx-xx BLxx-xx ROMx.x-x Uptime: 0 17:02:20

Seconds Since Zeroed:   1183161     Frames Sent: 1 Collision:         8377
Bytes Received:         811416880   Frames Sent,2+Collisions:        16344
Bytes Sent:             141519043   Send Failures:                       1
Frames Received:        8087172     Send Failure Reasons:         00000010
Frames Sent:            1572199     Receive Failures:                   47
Multicast Bytes Rcv'd:  1111005     Receive Failure Reasons:        000011
Multicast Bytes Sent:   215694      Unrecognized Destination:       193760
Multicast Frames Rcv'd: 66700       Data Overrun:                        0
Multicast Frames Sent:  2179        User Buffer Unavailable:             0
Frames Sent, Deferred:  96516       System Buffer Unavailable:           0
Messages Received:      1886375     Duplicates Received:               106
Messages Transmitted:   1569667     Messages Re-transmitted:           485
Solicitations Accepted: 0           Illegal Messages Rcv'd:              6
Solicitations Rejected: 0           Illegal Slots Rcv'd:                 0
Multiple Node Addresses:23591       Illegal Multicasts Rcv'd:            1

Local>
```

SHOW/LIST/MONITOR SERVER COUNTERS Display Fields

The following table defines the fields in the SHOW / LIST / MONITOR SERVER COUNTERS display:

Field	Description
Ethernet Data Link Counters:	
Seconds Since Zeroed	Number of seconds since the counters were last set to zero.
Bytes Received	Number of bytes contained in datagrams successfully received by the access server, excluding Ethernet header and CRC data.

Field	Description
Bytes Sent	Number of bytes contained in datagrams successfully transmitted by the access server, excluding Ethernet header and CRC data.
Frames Received	Number of datagram frames successfully received by the access server, including multicast frames.
Frames Sent	Number of datagram frames successfully transmitted by the access server, including multicast frames.
Multicast Bytes Rcv'd	Number of bytes received by the access server in multicast frames, excluding Ethernet header and CRC data.
Multicast Bytes Sent	Number of bytes transmitted by the access server in multicast frames, excluding Ethernet header and CRC data.
Multicast Frames Rcv'd	Number of multicast frames received by the access server.
Multicast Frames Sent	Number of multicast frames sent by the access server.
Frames Sent, Deferred	Number of times the access server deferred a frame transmission because the data link was in use. This value should be less than 20% of the value for Frames Sent.
Frames Sent, 1 Collision	Number of times the access server successfully transmitted a frame on the second attempt after a collision during the first attempt. This value should be less than 5% of the value for Frames Sent.
Frames Sent,2+ Collisions	Number of times the access server successfully sent a frame after collisions during the first two or more attempts. This value should be less than 5% of the value for Frames Sent.
Send Failures	Number of times the Ethernet interface aborted a transmission request. If this count is nonzero, refer to the Send Failure Reasons field for more information. This counter should be 0 or a low value such as 1 or 2 daily.

Field	Description
Send Failure Reasons	Mask providing information about the type or types of send failure encountered if the Send Failures counter is not zero. This is a cumulative mask.The following are the bits defined in the mask: Bit 0 1 4 5 8 9 If a reason for send failures is heartbeat errors and the access server characteristic HEARTBEAT is enabled for a transceiver that supports heartbeat, you can usually expect up to about 200 such errors daily. This number does not indicate a network problem. If a reason for send failures is heartbeat errors and the transceiver being used does not support heartbeat, check to see whether you have heartbeat enabled. The send failures count will reflect the heartbeat errors generated from the transceiver not responding to checks of its heartbeat circuitry. Disable the access server characteristic HEARTBEAT to eliminate the spurious generation of heartbeat errors.
Receive Failures	Number of packets that were received with an error condition. For more information, refer to the Receive Failure Reasons field. This counter should be 0 or a low value such as 1 or 2 daily.
Receive Failure Reasons	Mask providing information about the type or types of receive failure encountered if the Receive Failures counter is not zero. This is a cumulative mask. The following are the bits defined in the mask: Bit 0 1 2

Field	Description
Unrecognized Destination	Number of times a frame was passed through the hardware, but the access server did not recognize the multicast address and discarded the message. This value reflects multicast traffic or other traffic addressed to the access server from protocols not supported by the access server. The count will be high if the access server does not have an IP address and is connected to a network with ARP traffic. If this count is extremely high (greater than 10 for each second of uptime), the access server performance could be adversely effected.
Data Overrun	Number of times the access server hardware lost an incoming frame, because it was unable to keep up with the data rate. This value should be 0.
User Buffer Unavailable	Number of times the access server did not have a user buffer available to store an incoming frame that passed through the system buffer. This counter should accumulate at a rate of less than two counts per day. Note that the value of this counter could be high if there are a large number of LAT service multicast announcements on the network. Also, it is normal to experience some errors when nodes are added to the Ethernet.
System Buffer Unavailable	Number of times a system buffer was not available in the access server for an incoming frame. This counter should accumulate at a rate of less than two counts per day. It is normal to experience some errors when nodes are added to the Ethernet.
LAT Protocol Counters:	
Messages Received	Number of LAT circuit messages successfully received by the access server.
Messages Transmitted	Number of LAT circuit messages successfully transmitted by the access server.
Solicitations Accepted	Number of queued connection requests that the terminal server has accepted. This number includes requests that are queued and requests that were immediately satisfied without queuing. The sum of the number of solicitations accepted and the number of solicitations rejected equals the number of queued connection requests that the access server received.

Field	Description
Solicitations Rejected	Number of queued connection requests that the access server could not process and therefore rejected. The sum of the number of solicitations accepted and the number of solicitations rejected equals the number of queued connection requests that the access server received.
Multiple Node Addresses	Number of times a service node became available with different Ethernet addresses.
Duplicates Received	Number of LAT messages that the access server received more than once. This value should be less than 1/1000 of the value for Messages Received.
Messages Retransmitted	Number of LAT messages that the access server retransmitted, because they were not acknowledged by the service nodes. This value should be less than 1/1000 of the value for Messages Transmitted.
Illegal Messages Rcv'd	Number of LAT messages with an illegal format received by the access server. This value should be 0. A service node transmitting such messages might have a software problem.
Illegal Slots Rcv'd	Number of LAT messages with an illegal slot format received by the access server. This value should be 0. A service node transmitting such messages might have a software problem.
Illegal Multicasts Rcv'd	Number of illegally formatted multicast messages received from service nodes. This value should be 0. A service node transmitting such messages might have a software problem.

Displaying Access Server Status

The SHOW/LIST/MONITOR SERVER STATUS command displays the status of the access server. The information tells you how well the access server is working under the current load and also warns you of network trouble or of problems with ports on the access server. The display also lists current, highest, and maximum values for software and hardware resources.

If the status is not normal, then the following appears:

```
Selftest Status: Server:00-00-00 Service:00000
Port:0000000000000000

Software Status: PC=01234567 SP=01234567 SR=2300 M=01234567
```

The first line displays the access server software version number and base level, LAT software version number, ROM version number, and the time that the access server has been running since the last downline load, expressed as days hours:minutes:seconds.

Example: SHOW SERVER STATUS Display

The following example shows how to generate an access server status display:

```
Local> SHOW SERVER STATUS

Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM x.x-x Uptime: 0 17:05:57

Address: 08-00-2B-02-F2-BB Name: T_LAT06 Number: 65535

                        Cur   High  Max

Active Ports            8     8     16   Minutes to Shutdown:       N/A
Active Users:           8     8     16   Discarded Nodes:             0
Queue Entries:          0     0     100  Resource Errors:             0
Available Services:     89    92    N/A  Port Framing Errors:         0
Local Services:         2     2     20   Port Parity Errors:          0
Reachable Nodes:        75    78    200  Port Overrun Errors:         0
Boot Device: Ethernet:  0

Active Circuits:        4     7     32   Primary Host:            PEACH
Connected Nodes:        3     5     32   Load Address:AA-00-04-00-46-DC
Connected Sessions:     12    20    64   Dump Address:   None Available
% CPU Used:             15    36    100  Console User:   None Available
% Memory Used:          36    53    100  Boot Protocol:             MOP

Selftest Status: Normal
Software Status: Normal

Local>
```

SHOW/LIST/MONITOR SERVER COUNTERS Display Fields

The following table describes the fields and column headings in the access server status display:

Field	Description
Address	Address Ethernet address of the access server.
Name	Name of the access server. This string can be specified by using the SET/DEFINE/CHANGE SERVER NAME command.
Number	Number of the access server. This number can be specified by using the SET/DEFINE/CHANGE SERVER NUMBER command.

Field	Description
Cur column	Current running value of the resource. If the Max value is lowered during the Uptime, this value can exceed the Max value for counters.
High column	Highest value the resource attained, since the access server was last initialized. The length of time is shown in the Uptime field. If the Max value is lowered during the Uptime, this value can exceed the Max value for certain counters.
Max column	Maximum value that the resource can reach, given the physical restraints or the value specified for a access server characteristic.
Active Ports	Ports that have either interactive sessions or remote access connections.
Active Users	Ports that have interactive sessions.
Queue Entries	Queued connection requests that are in the access server queue.
Available Services (LAT protocol only)	Network services that the access server recognizes as being available to users on the access server. (The information about these services is stored in access server memory.)
Local Services (LAT protocol only)	Number of LAT services offered by the access server.
Reachable Nodes (LAT protocol only)	Computers or other access servers that offer services on the network and that are reachable for service connections.
Active Circuits	LAT virtual circuits on which the access server has active connections with service nodes.
Connected Nodes	Service nodes with which the access server has established LAT virtual circuits.
Connected Sessions	Total number of LAT, Telnet, and SLIP sessions on the access server. Total number of LAT, Telnet, and SLIP sessions on the access server.
% CPU Used	Percentage of processing time the access server used. This value is calculated every second.
% Memory Used	Percentage of the general memory pool being used.
Minutes to Shutdown	Number of minutes remaining on the initialize timer. If no INITIALIZE command is in effect, N / A is displayed to indicate not applicable.

Field	Description
Discarded Nodes	Number of nodes that could not be entered into the access server database, because of the value set for the node limit characteristic or because of a lack of memory. If this count is nonzero, the access server might be experiencing resource problems. The memory used for storing service and node information is shared with that used for handling multiple sessions and queued connection requests. If the access server receives information on a greater number of nodes than specified in the node limit access server characteristic, it discards that information and increments the Discarded Nodes counter. However, if the node limit is not reached but the access server could not find memory to store the information, it discards the information and increments both the Resource Errors and the Discarded Nodes counter. You can either reduce the value of the SESSION LIMIT access server characteristic, adjust the value of the node limit access server characteristic, or use Authorized Groups to logically subdivide the network for use by a discrete set of users.
Resource Errors	Number of times an internal data structure could not be created due to the lack of system memory.
Port Framing Errors	Sum of bytes received at the access server ports with illegally formatted data characters. Values other than 0 might indicate a problem with one of the ports. Use the port counters display to isolate the port or ports generating the errors accumulated in this counter.
Port Parity Errors	Sum of bytes received at the access server ports with parity errors. Values other than 0 might indicate a problem with one of the ports. Use the port counters display to isolate the port or ports generating the errors accumulated in this counter. Values other than 0 might indicate a problem with one of the ports. Use the port counters display to isolate the port or ports generating the errors accumulated in this counter.
Port Overrun Errors	Sum of characters lost at the access server ports, because the access server input buffers were full.
Primary Host	Name or IP address of the host from which the access server was last loaded.
Load Address	Ethernet address of the node or the gateway from which the access server was last loaded. Some access servers display all zeroes if a downline load occurs using BOOTP and TFTP.
Dump Address	Ethernet address of the node or gateway that received the last up-line dump. Some access servers display all zeroes if a dump is to an Internet host.

Field	Description
Console User	Address of the node at which the Remote Console Facility (RCF) is being used to access the access server. The access server indicates “none available” if the RCF is not in use.
Boot Protocol	This is the protocol used to downline load the software.
Selftest Status	Shows internal information if the result of self-test at the most recent access server initialization is other than: Normal: Server: 00-00-00 Service: 00000 Port: 0000000000000000 If a nonfatal error occurs during self-test, the access server displays information about the error. The following describes the information that appears in the display: Selftest Status: 00-00-00: The leftmost two numbers are always 00. The third number is a hexadecimal representation of a bit map in which a bit set indicates status as follows: Bit 1 2 4 8 20 40 80 Each number represents a bit map in which a bit set indicates a problem with the port. Bit 1 2 4 Service:00000: This value is a hexadecimal representation of a bit map in which a bit set indicates which service or services contained a checksum error. Bit 1 2 4 8 10 20 40 80 100 200 400 800 1000

Field	Description
Selftest Status (continued)	2000 4000 8000 10000 20000
Selftest Status (continued)	40000 80000 Port: 0000000000000000: This value is a hexadecimal number that corresponds to ports 1 to 16 from left to right. Note: If more than one bit is set in a bit map, the value shown is the sum of the values for each bit. For example, if the Service Status value is 18C (hexadecimal), this is the sum of 100, 80, 8, and 4.
Software Status	Display shows internal information if the status displayed is other than Normal, that is, if a fatal software error occurs. For example: PC=01234567 SP=01234567 SR=2300 M=01234567 C=217 A status other than Normal indicates that a fatal bugcheck error has occurred. More information is found in the Cabletron *Network Access Software Problem Solving* guide.

Displaying Access Server Summary Information

The LIST / SHOW / MONITOR SERVER SUMMARY command displays the access server groups you defined.

The first line displays the access server software version number and base level, LAT software version number, ROM version number, and the time that the access server has been running since the last downline load, expressed as days hours:minutes:seconds.

Use this display to determine which group codes the access server recognizes when it processes service announcement messages from other nodes on the network. These group codes are the sum of the authorized group codes of the ports on the access server.

Example: SHOW SERVER SUMMARY Display

The following example shows how to generate an access server summary display:

```
Local> SHOW SERVER SUMMARY
Network Access SW Vx.x for DSxxx
Address: 08-00-2B-02-F2-BB     Name: T_LAT06    Number: 6
Identification: Number 6 LAT Server
Server Groups: 0,4,10-20
Local>
```

SHOW/LIST/MONITOR SERVER SUMMARY Display Fields

The following describes the access server summary display fields:

Field	Description
Address	Ethernet address of the access server.
Name	Name of the access server as defined with the SET/DEFINE/CHANGE SERVER NAME command.
Number	Number of the access server as defined with the SET/DEFINE/CHANGE SERVER NUMBER command.
Identification	An ASCII string describing the access server supplied in multicast service node announcement messages and issued to interactive access server users at access server login.
Server Groups	List of assigned groups across all the access server ports. The group list includes the current groups for every port on the access server. A group is current for any port if it appears in this group list. The access server uses this information to filter incoming multicast messages from other nodes.

Checking Port Status and Counters

Introduction

The LIST / MONITOR / SHOW PORT command displays information about one or more ports on the access server. You can obtain characteristics, counter, status, and summary displays for ports.

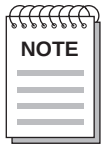
Displaying Port Characteristics

The LIST / MONITOR / SHOW PORT CHARACTERISTICS command displays the values of the characteristics of the selected ports. The bottom of the display lists all the enabled port characteristics. Use the characteristics display when you are changing settings.

The port number n in the display indicates that the port device is connected to connector JN on the hardware unit. The server name is configured with the SET / DEFINE / CHANGE SERVER NAME command. The other values can be changed with the SET / DEFINE / CHANGE PORT command.

Reference

Refer to Cabletron *Network Access Software Command Reference* guide for information on each command.



Some access servers have Modem Control instead of Signal Control. Also, Signal Select is not available on all access servers.

Example: SHOW PORT CHARACTERISTICS Display

The following example shows how to generate a port characteristics display:

```
Local> SHOW PORT 1 CHARACTERISTICS

Port 1: Joe Smith                Server:                Servername

Character Size:    8       Input Speed:                       9600
Flow Control:      XON     Output Speed:                      9600
Parity:            None    Signal Control:                Disabled
Stop Bits:         Dynamic Signal Select:          CTS-DSR-RTS-DTR
Access:            Local   Local Switch:                      None
Backwards Switch:  None    Name:                           PORT_1
Break:             Local   Session Limit:                      4
Forwards Switch:   None    Type:                           Ansi
Default Protocol:  LAT     Default Menu:                      None
                           Dialer Script:                     None
Preferred Service: TEST Node: PEACH Destination: LTA15
Authorized Groups: 0-10, 20-50, 200-255
(Current) Groups:  0-10, 20-50, 200-255
Enabled Characteristics:
Autobaud, Autoconnect, Autoprompt, Broadcast, DSRlogout, Inactivity
Logout, Input Flow Control, Interrupts, Limited View, Loss
Notification, Message Codes, Multisessions, Output Flow Control, On-
Demand Loading, Password, Queuing, Security, Signal Check,
Verification

Local>
```

Displaying Port Counters

The SHOW / MONITOR PORT COUNTERS command displays the counters associated with each of the selected ports. Use this command to discover the source of any problems between the port device and the port. Typically, network problems can be detected with errors recorded in the access server status display.

The maximum value possible for the port counters is 4, 294, 967, 295. If a counter reaches that value, it remains at that value until either the counters are set to zero or the access server is initialized.

Three counters in the port counters display can indicate possible problems. The access server status display gives values for port framing, parity, and overrun errors for the access server. Usually Framing Errors, Parity Errors, and Overrun Errors are zero. If the access server status display indicates nonzero values for any of these errors, you can use the port counters display to find the port or ports that are causing the errors.

Example: SHOW PORT COUNTERS Display

The following example shows how to generate a port counters display:

```
Local> SHOW PORT 1 COUNTERS

Port 1:                  Joe Smith     Server:   Servername

Seconds Since Zeroed: 1182768 Local Accesses:            17
Framing Errors:             0 Remote Accesses:            0
Parity Errors:              0 Overrun Errors:             0
```

SHOW/MONITOR PORT COUNTERS Display Fields

The following table describes the information in the port counters display:

Field	Description
Port n	Number n of the port. The text that follows the number of the port is any associated user name or the name of the port as established for the port characteristic NAME, if no user name was supplied.
Server	Specifies a 1- to 16-character name for the access server.
Seconds Since Zeroed	Number of seconds since the counters were last set to zero.
Framing Errors	Number of bytes received at the port with illegally formatted frames. If this value accumulates to greater than about 20 errors per day on any one port, you might have port line problems. Refer to the troubleshooting procedures in the *Network Access Software Problem Solving* manual.
Parity Errors	Number of bytes received with parity errors at the port. If this value accumulates to greater than about 20 errors per day on any one port, you might have port line problems. Refer to the troubleshooting procedures in the *Network Access Server Problem Solving* manual.
Overrun Errors	Number of characters lost because the access server input buffers were full. If this value accumulates more than 10 errors daily on any one port, you might have flow control problems. If the port device supports flow control, ensure that the access server flow control and the flow control in the hardware for that device are set the same way. To check the FLOW CONTROL setting, use the SHOW PORT CHARACTERISTICS command.

Field	Description
Local Accesses	Number of times an access server login occurred on the port.
Remote Accesses	Number of times a remote access connection was established on the port.

Displaying Port Status

The SHOW / MONITOR PORT STATUS command displays information about the operational condition of the selected port.

Example: SHOW PORT STATUS Display

The following example shows how to generate a port status display:

```
Local> SHOW PORT 1 STATUS

Port 1:         Joe Smith  Server:                SERVERNAME
Access:         Remote     Current Service:             TEST
Status:         Connected  Current Node:              PEACH
Sessions:       1 Current  Port:                      LTA15
Input XOFFed:   No         Output Signals:          DTR RTS
Input Signals:  DSR RXD    Output XOFFed:               Yes
```

SHOW/MONITOR PORT STATUS Display Fields

The following table discusses information displayed by the PORT STATUS command:

Field	Description
Port n	Number n of the port. The text that follows the number of the port is any associated user name or the name of the port established for the port characteristic NAME, if no user name was supplied.
Server	Specifies a 1- to 16-character name for the access server.

Field	Description
Access	Current setting of the ACCESS port characteristic. Access determines how a port can access a service node or how a port can be accessed by other interactive users and service nodes. Access is shown as one of the following: • Dynamic — Access server allows access on the port to alternate between local and remote. • Local — Access server allows only interactive use of the port. • None — Access server prevents any use of the port. • Remote — Access server allows only remote connections on the port. Port access is specified by using the SET/DEFINE/CHANGE PORT command.

Field	Description
Status	Current status of the port, which can be one of the following: • Connected — Port is connected to a service. • Connecting — Port is attempting a connection to a service. • Disconnected — Session was terminated while dormant. • Disconnecting — Session is disconnecting from a service. • Idle — Port is not in use. • Local Mode — Port is logged in to the access server and is not connected to or connecting to a service. • Locked — LOCK command was executed on the port. • Signal Wait — The port failed to assert the DSR signal during a signal check controlled connection attempt. • Sessions — Number of active sessions at the port. • Current Service — Active service session or the service session interrupted when the user last entered local mode.
Current Node	Node to which the current session is connected. If the access is remote, this is the name of the node from which the connection originated.
Current Port	Identification of the port at the service node or at the requesting node.
Input or Output XOFFed	Status of the data flow for the specified direction for the port.
Input or Output Signals	Modem signals either currently asserted by the access server or currently monitored by the access server.

Displaying Port Summary

The LIST/MONITOR/SHOW PORT SUMMARY command displays one line of general information for each selected port. The port summary display is useful for obtaining information about how the ports are being used. This is the default display for the PORTS ALL entity specification.

Example: SHOW PORT SUMMARY Display

The following example shows how to generate a port summary display:

```
Local> SHOW PORTS ALL SUMMARY

Port       Access       Status            Services Offered

1          Local        Connected
2          Remote       Connected            LA50, PRINTER
3          Dynamic      Idle                      HARDCOPY
4          Local        Local Mode
5          Remote       Connected            LA50, PRINTER
6          Local        Connecting
7          Remote       Disconnected           TIMESHARING
8          Local        Idle
9          Local        Idle
10         Local        Idle
11         Local        Idle
12         Local        Idle
13         Local        Idle
14         Local        Idle
15         Local        Idle
16         Local        Idle
```

SHOW/LIST/MONITOR PORT SUMMARY Display Fields

The following table describes the information under the headings in the SHOW/LIST/MONITOR PORT SUMMARY display:

Heading	Description
Port	Number n of the port.
Access	Current setting of the ACCESS port characteristic. Access determines how a port can access a service node or how a port can be accessed by other interactive users and by service nodes. Access is shown by one of the following: • Dynamic — Access server allows access to the port to alternate between local and remote. • Local — Access server allows only interactive use of the port. • None — Access server prevents any use of the port. • Remote — Access server allows only remote connections on the port. Port access is specified by using the SET/DEFINE/CHANGE PORT command.
Status	Current status of the port, which can be one of the following: • Connected — Port is connected to a service. • Connecting — Port is attempting a connection to a service. • Disconnected — Session was terminated while dormant. • Disconnecting — Session is disconnecting from a service. • Idle — Port is not in use. • Local Mode — Port is logged in to the access server and is not connected to or connecting to a service. • Locked — LOCK command was executed on the port. • Permanent — Status that appears for the LIST command. • Signal Wait — The port failed to assert the DSR signal during a signal check controlled connection attempt.
Services Offered	The local services that the access server offers on the port. Host-initiated requests can be made for these services.

Chapter 19

Configuring and Managing 3270 Terminal Emulation (TN3270)

Overview

Introduction

This chapter explains how to configure and manage the 3270 Terminal Emulator (TN3270) software for the access server. This software enables ASCII terminals and PCs to access IBM applications.

The TN3270 software enables an ASCII terminal to emulate an IBM 3278 Display Station Model 2. The display screen of this model has 80 columns and 24 rows.

The TN3270 software performs the following tasks:

- Translates the ASCII terminal data stream into the 3270 data stream and transmits it to the IBM host.
- Receives the 3270 data stream from the IBM host and translates it into the ASCII terminal data stream.

The access server uses Telnet over TCP/IP to access applications on IBM hosts.

This chapter assumes a basic understanding of applications for IBM 3270 Information Display Systems and terminal emulation. This chapter also assumes that the system manager at the host site configures the appropriate TCP/IP software.

Supported ASCII Terminals

Definition

TN3270 supports the following models of DIGITAL ASCII terminals:

- VT100 with Advanced Video Option
- VT102
- VT220, VT240, and VT241
- VT320, VT330, VT340, and VT341
- VT420

In the remainder of this chapter, the term ASCII terminal refers to all the models listed above and any compatible terminal emulation package.

Definition and Description of a Keyboard Map

3278 Keyboards

Because the IBM 3278 keyboard differs greatly from those on ASCII terminals, TN3270 provides keyboard maps. A keyboard map assigns the functions on the IBM 3270 keyboards to keys or key sequences on the ASCII terminals. For example, Ctrl/Z on an ASCII keyboard by default maps to the IBM 3270 EXIT function when you use the VT100 keyboard map.

Server-Specific Keyboard Maps

You can have server-wide keyboard maps that all server ports can access, or you can set them up on a port-by-port basis. For information on displaying and customizing keyboard maps, refer to Displaying and Customizing Keyboard Maps in this chapter.

Configuring Basic 3270 Terminal Emulation

Once the IBM system administrator has configured the IBM host with TCP/IP, you need to do the following:

1. Set up the ASCII terminal.
2. Indicate the model number of the IBM 3270 Information Display Station that a terminal emulates.
3. Specify the type of ASCII terminal attached to the port.

Once you complete these tasks, you can connect to an IBM application as described in the Connecting to an IBM Host section in this chapter. These are the minimal tasks required to configure a port for 3270 emulation. This section describes these tasks.

Setting Up an ASCII Terminal

To enable an ASCII terminal for 3270 emulation, you need to change the setup parameters as described below. To change these parameters, use the setup procedure described in the documentation provided with the terminal.

When you connect to an IBM host or resume a 3270 session, TN3270 automatically:

- Configures the terminal to:
  - — Designate the ASCII character set as GO graphics set/invoke GO in GL.
  - — Position the cursor in column 1 of row 24.
  - — Set autowrap enabled except for ANSI.
  - — Set application keypad except for ANSI and VT100.
  - — Set local echo off except for ANSI, VT100, VT220.
- Detects if the cursor keys operate in normal or application mode.
- Detects 7- or 8-bit controls.

Terminal Setup Parameters

The following table provides information on terminal setup for the various DIGITAL terminal models:

Terminal Model	Terminal ModelSetup Parameters
VT100	ANSI mode AUTO XON / XOFF = ON
VT2xx, VT3xx, V4xx	General: • VT100 through VT400 mode • 7-bit or 8-bit controls Communications: • XOFF at 64 or 128 • No local echo

Indicating the 3270 Model Number

To enable 3270 emulation on a port, you must specify the 3270 model number as follows:

```
Local> CHANGE PORT 2 TN3270 MODEL 2
```

This command enables port 2 to emulate an IBM 3278 Model 2 display station.

When the access server establishes a session to an IBM host, the host negotiates for an IBM 3278 display station. If the IBM host does not negotiate for an IBM 3278, then the access server defaults to a standard Telnet connection.

To disable 3270 emulation on port 2, enter the following:

```
Local> CHANGE PORT TN3270 NONE
```

By default, 3270 emulation is disabled on all ports.

Specifying the Type of ASCII Terminal Used for Emulation

After you indicate the 3270 model number, you need to specify the type of ASCII terminal. For example, to indicate that a VT220 is attached to port 2, you enter:

```
Local> CHANGE PORT 2 TN3270 TERMINAL VT220
```

To display the list of terminal types and their associated keyboard maps, enter the SHOW TN3270 TERMINAL command. The default terminal device is VT100.

IBM Host Communications

Introduction

This section describes IBM host communications with a terminal attached to the access server.

Connecting to an IBM Host

After you complete the basic configuration of a port for 3270 emulation, you can use the CONNECT, OPEN, or TELNET commands to access an IBM host. The following example shows a connection to an IBM host that uses the host's Internet address:

```
Local> CONNECT 195.20.0.15
```

When the access server connects, follow the prompts that appear on the screen to log onto the host system.

To display the keyboard map defined for a session, enter the 3270 HELP function.

Entering and Editing Data

TN3270 supports the following data entry and editing features:

- Unformatted and formatted screens
- Normal and insert modes

For information about IBM 3270 data entry and editing, refer to the documentation provided with your IBM application.

Status Line Indicator

The status line indicator is a reverse video strip that displays messages on the bottom line of the terminal screen during a 3270 session. This indicator emulates the status line that appears on the bottom line of an IBM 3270 Display Station.

To turn the status line indicator on and off, enter the 3270 STATUS function.

The status line is overwritten when:

- The IBM application moves the cursor to the last line on the screen.
- You enter data on the last line of the screen.

The status line is restored when:

- You use the STATUS function.
- You send data to the host.
- The IBM application clears the screen.

Status Line Messages

The following table describes the messages that appear on the status line indicator:

Message	Description
EXTEND	You have pressed the EXT function.
HIDDEN	The status line is covering some screen data that you have not yet seen. This indicator turns off when you enable the status display after viewing the hidden data.
INSERT	The terminal is in insert mode.
INHIB	The application has suspended input from the keyboard. This condition can occur when: • You try to enter data in a protected field. • You try to enter the wrong type of data.
O	You are using the numeric lock override function. This indicator turns off when you enter the NUM OVR function again.
ONLINE	You are successfully communicating with the IBM host.
X	The IBM system is unavailable for input. For example, the message X displays after your use the ENTER function to send data to the IBM host.
7171	You are using 7171 mode to transmit embedded nulls as spaces.

Status Line Indicator Display

Figure 19-1 shows the position of the status line indicator on the screen:

LKG-7423-fh8

Figure 19-1. Position of the Status Line Indicator

Displaying and Customizing Keyboard Maps

Introduction

Although the default TN3270 keyboard maps are sufficient for most users, some may want to customize keyboard maps for specific applications. This section describes the default keyboard maps and the options for displaying and customizing them.

There are two ways to manage customization of keyboard maps: on a server-wide basis and a port-by-port basis. Server-wide customization may be preferred because it addresses multiple users' needs and makes more efficient use of the access server NVRAM. The server-wide customization must be set up by the privileged user, while port-by-port customization can be done by the port user.

Server-Wide Keyboard Maps Customization

Server-wide customization of keyboard maps depends upon the fact that each keyboard map is associated with a terminal type. The privileged user can create a new terminal type and associate a new keyboard map with it. Then he or she can customize the new map, which changes the key assignments that go with IBM 3270 functions.

A port user can then associate a port with the new terminal type. This automatically sets up the port to use the new keyboard map (see the following figure).

Figure: Port Access to Server-Wide Keyboard Maps

Default Server-Wide Terminal Types and Keyboard Maps

This section discusses the default server-wide keyboard maps and then explains how to define and customize new keyboard maps. The Selecting and Customizing Keyboard Maps for a Port section discusses keyboard maps for ports.

By default, the access server offers five different terminal types. Each terminal type is associated with one of two default keyboard maps, VT100 and VT220.

You can display the default terminal types and keyboard maps with the following command:

```
Local> SHOW TN3270 TERMINAL
```

Default Server-Wide Terminal Type and Keyboard Maps

The following table shows the default keyboard map and the associated terminal type:

Predefined Terminal Type	Default Keyboard Map
ANSI	VT100
VT100	VT100
VT220	VT220
VT320	VT220
VT420	VT220

These particular associations between terminal types and keyboard maps are fixed. You cannot reassign any of the five default terminal types to different keyboard maps. You cannot customize any of the individual key assignments for either of the two default keyboard maps on an access server-wide basis. These default terminal types and keyboard maps are intended for users who do not need any customization.

You can display the key assignments for the default keyboard map (VT220, in this example) with this command:

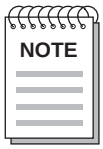
```
Local> SHOW TN3270 KEYMAP VT220
```

Defining New Server-Wide Terminal Types and Keyboard Maps

The privileged user can set up new terminal types and keyboard maps; up to six of each. New terminal types can be associated with one of the default keyboard maps or with a new keyboard map that has customized individual key assignments.

The first of the following two commands below creates a new terminal type called PC_100_DCA and associates it with the default VT100 keyboard map. You might want to do this, for example, if you have PCs that emulate VT100 terminals. The key assignments for the PC_100_DCA terminal type would look exactly like those for the VT100 keyboard map.

The second command reassigns PC_100_DCA to an entirely new keyboard map, called NEW_KEYS. NEW_KEYS starts out looking like the default VT100 keyboard map until you customize the key assignments (if you choose to do so). Customizing Server-Wide Keyboard Maps, in this chapter, discusses customization.



You cannot customize the predefined VT100 keyboard map that you set up with the first command.

```
Local> CHANGE TN3270 TERMINAL PC_100_DCA KEYMAP VT100
Local> CHANGE TN3270 TERMINAL PC_100_DCA KEYMAP NEW_KEYS
```

You can carry out a similar process for terminal devices that use the VT220 keyboard map—the other default map.

```
Local> CHANGE TN3270 TERMINAL PC_220_DCA KEYMAP VT220
Local> CHANGE TN3270 TERMINAL PC_220_DCA KEYMAP NEW_KEYS2
```

Customizing Server-Wide Keyboard Maps

After executing the CHANGE commands as shown in the Defining New Server-Wide Terminal Types and Keyboard Maps section in this chapter, you can customize the individual keymapping assignments in the new keyboard map NEW_KEYS. The goal is to have key assignments that fit the needs of the port users who can select the terminal type that goes with a new keyboard map.

The following command changes the keymapping assignment for the TN3270 function CLEAR. Instead of the default VT100 keymapping EXT ENTER, the manager assigns the CLEAR function to Ctrl/W.

```
Local> CHANGE TN3270 KEYMAP NEW_KEYS CLEAR <CTRL/W>
```

In a display, the customized keymapping assignment is marked with an asterisk (*).

The privileged user can show the new keymapping with this command:

```
Local> SHOW TN3270 KEYMAP NEW_KEYS
```

Rules for Customizing Keyboard Maps

The following rules apply to customizing keyboard maps:

- You can assign each 3270 function to only one ASCII key sequence.
- If you attempt to assign a 3720 function to an ASCII key sequence that is already in use, the access server:

  — Issues a warning message.

  — Assigns the requested key definition.

  — Assigns the 3270 function previously assigned to this sequence to NONE.

- You cannot assign an ASCII key sequence that is a subset of a key sequence already assigned to a 3270 function. For example, the assignment of "KPDOT" to a 3270 function is disallowed if "KPDOT F20" is already assigned to a 3270 function.

Selecting a Server-Wide Terminal Type and Keyboard Map for a Port

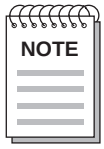
A port user who wants to establish a TN3270 session using a server-wide keyboard map can do the following:

Step	Action

1	Check to see what terminal types (and associated keyboard maps) are available with the following command:
	`Local> **SHOW TN3270 TERMINAL**`
	`Server: LAT_08002B26D0DE`
	`Terminal Keymap`
	`VT100 VT100`
	`VT220 VT220`
	`VT320 VT220`
	`VT420 VT220`
	`ANSI VT1000`
	`PC_100_DCA NEW_KEYS`
	`PC_220_DCA NEW_KEYS2`

2	Choose a keyboard map for one of the terminal types (for example, NEW_KEYS) and check its associated keymapping: `Local> **SHOW TN3270 KEYMAP NEW_KEYS**`
3	If the keymapping is what the users require for TN3270 applications, they set up the port to use the access server-wide terminal type: `Local> **SET PORT TN3270 TERMINAL PC_100_DCA**`

4	The user can now confirm what terminal type and key assignments TN3270 sessions will use at the port:
	`Local> **SHOW PORT TN3270 CHARACTERISTICS**`
	`Local> **SHOW PORT TN3270 KEYMAP**`
	The port user has set up the port to use an access server-wide customized set of keymapping assignments without any added memory or complexity.



Port users cannot customize access server-wide keyboard maps. The port users can customize only the default keyboard maps. See the Customizing a Default Keyboard Map for a Port section in this chapter.

Selecting and Customizing Keyboard Maps for a Port

Server-wide keymapping is the recommended method for customizing users' TN3270 keymapping assignments. It uses access server memory efficiently and provides a common customized environment across all TN3270 ports. Port-by-port keymapping is also possible, but uses additional access server resources.

A user can set up unique keymapping assignments for use only on his or her port.

Individual port users have the following choices for selecting the keyboard maps that are most appropriate for their TN3270 applications:

- Select and use one of the predefined default terminal types and its associated keyboard map. The predefined terminal types are VT100, VT220, VT320, VT420, and ANSI.
- Select one of the predefined default terminal types, and then customize its keyboard map. Customizing a Default Keyboard Map for a Port discusses this customization.
- Select and use one of the server-wide customized terminal types and its keyboard map. These terminal types have been defined and customized for all ports by the server manager. The users cannot customize the keymaps associated with these terminal types on a port-by-port basis.

The following sections discuss these options.

Selecting a Default Terminal Type and Keyboard Map for a Port

A port user can forego access to any server-wide keymappings that may be available. Instead the user can choose the default terminal types and keyboard maps.

Reference

For a printed copy of these keyboard maps, refer to the Cabletron *Network Access Software Command Reference* guide.

Keyboard Map and Terminal Type

The following table lists the two default keyboard maps and their associated terminal devices:

Predefined Terminal Device	Associated Keyboard Map
VT100, ANSI	VT100
All ASCII terminals other than the VT100	VT220

You can list the defaults with this command:

```
Local> SHOW TN3270 KEYMAP "KEYMAPNAME"
```

The defaults are shown in the Default Server-Wide Terminal Type and Keyboard Maps and the Keyboard Map and Terminal Type.

You can display the keyboard mappings associated with a default keyboard map (VT220 in this example, for a VT420 port device) with this command:

```
Local> SHOW TN3270 KEYMAP VT220
```

If this keymapping is the best choice for the port user, you can set up the port to use the VT420 terminal type, which is associated with the VT220 keyboard map. Execute the following command to choose the VT220 keyboard map for port 2:

```
Local> CHANGE PORT 2 TN3270 TERMINAL VT420
```

The user can now confirm the terminal type and keyboard mapping assignments:

```
Local> SHOW PORT 2 TN3270 CHARACTERISTICS
Local> SHOW PORT 2 TN3270 KEYMAP
```

Customizing a Default Keyboard Map for a Port

As a port user, you can customize any of the key definitions on the default keyboard map to suit your keyboard. For example, the following command defines the ASCII code for the IBM 3270 NEWLINE function:

```
Local> CHANGE PORT TN3270 KEYMAP NEWLINE <Ctrl/J>
```

In this example, the ASCII sequence Ctrl/J maps to the NEWLINE function.

See the Rules for Customizing Keyboard Maps section in this chapter for rules about customizing keyboard maps.

To display a customized keyboard map for a port, use the SHOW PORT TN3270 KEYMAP command.

For each IBM 3270 function, a given keyboard map definition indicates:

- The defined mnemonics for the ASCII codes that the access server associates with each IBM 3270 function
- An optional text description of the keystrokes used to produce the ASCII codes

Example: SHOW PORT TN3270 KEYMAP Command

The following example shows a partial display of a keymap:

```
Local> SHOW PORT 2 TN3270 KEYMAP

Port 1: john
3270 function       ASCII

Keystroke           mnemonic   description
CLEAR               F12        “Alt F2”

.

.

.
```

ASCII-to-EBCDIC and EBCDIC-to-ASCII Translation Tables

Commands

The following table lists and describes the commands that enable you to display and modify the ASCII-to-EBCDIC and EBCDIC-to-ASCII translation tables. These tables use ASCII codes 0 to 255.

When you display or change a given translation, you must enter the codes in hexadecimal format. Any changes to the translation tables take effect in new sessions on the access server, but do not affect current sessions.

Command	Enables You to Display and Modify
SHOW / SET TN3270 ATOE	The ASCII-to-EBCDIC translation table.
SHOW / SET TN3270 ETOA	The EBCDIC-to-ASCII translation table.

Guidelines for Managing the Use of NVRAM for TN3270

Introduction

There is a pool of approximately 2.5 KB of shared NVRAM for the customization of the following TN3270 characteristics:

- Keyboard maps for the ports
- ASCII-to-EBCDIC and EBCDIC-to-ASCII translation tables

This section provides guidelines on managing the available memory pool.

Storage Requirements for TN3270 Definitions in NVRAM

The following table lists the TN3270 storage requirements for TN3270 definitions in NVRAM:

Definition Description	Storage Requirements
Keyboard map definition for a port	8 bytes
Optional description text for a port	8 bytes for increments of 7 bytes of text
Each ASCII-to-EBCDIC and EBCDIC-to-ASCII customized translation	8 bytes

TN3270 Commands That Free NVRAM Space

The following table lists the commands used to free NVRAM space:

Command	Frees NVRAM Space Used By
DEFINE [PORT] TN3270 KEYMAP 3270-Function DEFAULT	The ASCII mnemonic and key sequence definition for the specified 3270 function.
DEFINE [PORT] TN3270 KEYMAP ALL DEFAULT	All customized keyboard maps.

Command	Frees NVRAM Space Used By
DEFINE TN3270 ETOA E-CODE A-CODE DEFAULT	The specified EBCDIC-to-ASCII translation.
DEFINE TN3270 ATOE A-CODE E-CODE DEFAULT	The specified ASCII-to-EBCDIC translation.

Limiting NVRAM Usage

To limit the number of NVRAM keyboard maps that the port user can customize, use the command shown in the following example:

```
Local> DEFINE PORT TN3270 NVRAM LIMIT 5
```

The default limit is 0.

Commands to Manage TN3270 Terminal Emulation

Introduction

This section summarizes the commands to manage 3270 emulation.

Reference

For a complete description of these commands and the correct syntax, refer to the Cabletron *Network Access Software Command Reference* guide.

TN3270 Access Server Characteristics

The following table summarizes the TN3270 commands that configure access server characteristics:

Command	Description	Default
SET / DEFINE / CHANGE TN3270 ATOE	Changes the ASCII-to-EBCDIC translation for the code specified.	For the default ASCII-to-EBCDIC translation table, refer to the Cabletron *Network Access Software Command Reference*. guide
SET / DEFINE / CHANGE TN3270 ETOA	Changes the EBCDIC-to-ASCII translation for the code specified.	For the default EBCDIC-to-ASCII translation table, refer to theCabletron *Network Access Software Command Reference* guide
SET / DEFINE / CHANGE TN3270 TERMINAL	Creates an access server-wide customized TN3270 terminal or renames an existing keymap for a terminal.	For the default KEYMAP, refer to the Cabletron *Network Access Software Command Reference*.
CLEAR / PURGE TN3270 TERMINAL	Clears dynamic or permanent memory of a customized 3270 terminal.	None
SET / DEFINE / CHANGE TN3270 KEYMAP	Customizes keymappings for an existing access server-wide keymap.	None

TN3270 Port Characteristics

The following table provides information on port characteristics and their defaults:

SET/DEFINE/ CHANGE PORT TN3270	Description	Default
MODEL	Specifies the model of IBM 3270 Information Display Station the ASCII terminal emulates.	NONE Nonprivileged
TERMINAL	Indicates the type of ASCII terminal and associated keymap attached to the port.	VT100 Nonprivileged
KEYMAP	Enables you to change a definition in the keyboard map.	-
KEYMAP NVRAM LIMIT	Specifies the number of keyboard maps in NVRAM that the nonprivileged user is allowed to define.	0 Privileged
NULLS	Determines how TN3270 treats the transmission of null characters to the host.	3179 Nonprivileged
FLOW CONTROL	Allows you to enable and disable input and output flow control for the port.	Enabled Secure
SWITCH CHARACTER	Controls whether the port detects port local, forward, or backward switch characters for a session.	Enabled Secure
Verification	Specifies whether the access server displays messages when you connect, disconnect, or switch sessions.	Enabled Secure

SHOW Commands

The following table provides information on the SHOW Commands for port characteristics:

SHOW	Description
PORT TN3270 KEYMAP	The TN3270 keyboard map for a specified port.
PORT TN3270 CHARACTERISTICS	The TN3270 port characteristics for a specified port.
TN3270 ATOE	The ASCII-to-EBCDIC translation table.
TN3270 ETOA	The EBCDIC-to-ASCII translation table.
TN3270 TERMINAL	The terminal types available on the access server and their associated keyboard maps.
TN3270 KEYMAP	The keymap assignments associated with a specified keymap.
PORT SESSION TN3270 KEYMAP	All keyboard maps for all sessions on the specified port.
PORT SESSION CHARACTERISTICS	The TN3270 characteristics for all sessions on the specified port.
PORT SESSION STATUS	The status for all sessions on the specified port.

Chapter 20

Configuring and Managing Point-to-Point Protocol (PPP) Ports

Overview

Introduction

This chapter explains how to configure and manage access server ports for use with PCs and computers acting as Point-to-Point Protocol (PPP) hosts. A PPP host uses PPP as its data link over low-speed asynchronous serial lines.

Prerequisites

Before you use the procedures in this chapter, you must:

- Ensure that the devices support PPP.
- Connect and test the devices.
- Configure the port and device characteristics to match.

For information about device cables, refer to the access server hardware documentation.

In This Chapter

This chapter contains the following topics:

- Displaying PPP Status
- Displaying PPP Counters

Enabling PPP on an Access Server Port

Introduction

To check if PPP is enabled on a given port, use the SHOW PORT command. When enabled, the keyword PPP displays in the list of enabled characteristics at the bottom of the screen.

The section provides examples of enabling PPP on an access server port.

Enabling PPP for Mixed Traffic

For basic operation of PPP, the only required commands are:

- DEFINE PORT MULTISESSIONS DISABLED
- DEFINE PORT PPP ENABLED

Example: Enabling PPP for Mixed Traffic

The following example shows a series of commands used to configure a port to support mixed character-cell and PPP traffic.

```
Local> DEFINE PORT 3 ACCESS LOCAL AUTOBAUD ENABLED AUTOCONNECT DISABLED
Local> DEFINE PORT 3 BREAK LOCAL DEFAULT PROTOCOL PPP DSRLOGOUT ENABLED
Local> DEFINE PORT 3 INTERRUPTS DISABLED MULTISESSIONS DISABLED
Local> DEFINE PORT 3 PREFERRED NONE SIGNAL CHECK DISABLED
Local> DEFINE PORT 3 SIGNAL CONTROL DISABLED
Local> DEFINE PORT 3 PPP ENABLED
Local> DEFINE PORT 3 PPP IPCP HOST ADDRESS 1.2.3.4
Local> LOGOUT PORT 3
Local>
```

Enabling Dedicated PPP Traffic

The following example shows a series of commands used to dedicate a port to PPP.

```
Local> DEFINE PORT 5 ACCESS LOCAL AUTOBAUD DISABLED
Local> DEFINE PORT 5 AUTOCONNECT ENABLED BREAK DISABLED DEDICATED PPP
Local> DEFINE PORT 5 DEFAULT PROTOCOL PPP DSRLOGOUT ENABLED
Local> DEFINE PORT 5 DTRWAIT ENABLED INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 5 INTERRUPTS DISABLED MULTISESSIONS DISABLED
Local> DEFINE PORT 5 PREFERRED NONE SIGNAL CHECK DISABLED
Local> DEFINE PORT 5 SIGNAL CONTROL DISABLED
Local> DEFINE PORT 5 PPP ENABLED
Local> DEFINE PORT 5 PPP IPCP HOST ADDRESS 1.2.3.4
Local> LOGOUT PORT 5
```

Enabling Ports with Modems for PPP

The following example shows a series of commands used to dedicate a port with an attached modem to PPP.

```
Local> DEFINE PORT 5 ACCESS LOCAL ALTERNATE SPEED NONE
Local> DEFINE PORT 5 AUTOBAUD ENABLED AUTOCONNECT DISABLED
Local> DEFINE PORT 5 BREAK DISABLED DEDICATED PPP DEFAULT PROTOCOL PPP
Local> DEFINE PORT 5 DSRLOGOUT DISABLED DTRWAIT DISABLED
Local> DEFINE PORT 5 FLOW CONTROL CTS INACTIVITY LOGOUT DISABLED
Local> DEFINE PORT 5 INTERRUPTS DISABLED MULTISESSIONS DISABLED
Local> DEFINE PORT 5 PREFERRED NONE SIGNAL CHECK DISABLED
Local> DEFINE PORT 5 SIGNAL CONTROL ENABLED SPEED 2400
Local> DEFINE PORT 5 PPP IPCP HOST ADDRESS 1.2.3.4
Local> DEFINE PORT 5 PPP ENABLED
Local> LOGOUT PORT 5
```

Establishing and Ending a PPP Session

Using the CONNECT PPP Command

If PPP is configured, you can start a PPP session on a port by entering the following secure command:

```
Local> CONNECT PPP
```

You can stop a PPP session by:

- Logging out of the port
- Generating a BREAK to the access server if the login is interactive, followed by the DISCONNECT command causing the peer to negotiate an end to the link

The exact mechanism for causing a peer to negotiate the end of a link depends on the PPP package used on the access server peer.

Displaying PPP Characteristics

Introduction

This section describes the commands used to display characteristics for LCP, IPCP, and ATCP.

Displaying LCP Characteristics

Use the SHOW PORT n PPP LCP CHARACTERISTICS command to display LCP characteristics for a port. This command is nonprivileged. The fields shown in the LCP display show the latest values configured by the SET PORT n PPP LCP characteristic commands. Use the SHOW / MONITOR PORT n PPP LCP STATUS command to see the values actually used on the link.

Example: Displaying LCP Characteristics

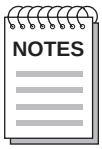
The following example shows the command to display the LCP configuration for port 5.

```
Local> SHOW PORT 5 PPP LCP CHARACTERISTICS

Port 5:                              Server: LAT_08002B26D0E7

LCP Characteristics:

LCP:                  Enabled Passive Open:        Disabled
Restart Timer:                             3 seconds
Max Configure:                            10 transmissions
Max Terminate:                             2 transmissions
Max Failure:                              10 transmissions


LCP Options:           Local:
MRU:                     1500
Character Map:       FFFFFFFF
Link Quality:        Disabled
Magic Number:        Disabled
PF Compress:         Disabled
ACF Compress:        Disabled
FCS Size:              16 Bit
Callback             Disabled
```

Fields in the LCP Characteristics Display

The following table explains the fields in the LCP characteristics display.

Field	Description	Values	Default
LCP	Indicates if LCP is enabled.	Enabled Disabled	Enabled
Passive Open	When enabled, LCP negotiation does not begin until initiated by the attached device.	Enabled Disabled	Disabled
Restart Timer	Indicates the amount of time between LCP configure- or terminate-request retransmissions when there is no response.	1 to 5 attempts	3
Max Configure	The number of times that LCP sends a configure-request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	10
Max Terminate	The number of times that LCP sends a terminate-request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	2
Max Failure	The number of times that LCP sends a negative acknowledgment for the peer's proposed options before deciding to reject the options.	1 to 15 seconds	10
MRU	The current MRU value.	64 to 1500	1500
Character Map	The current character map.	0 to FFFFFFFF	FFFFFFFF
Authentication	The current authentication configuration.	Disabled, PAP, CHAP	Disabled
Link Quality*	The current link quality.	Disabled	Disabled
Magic Number*	The current magic number.	Disabled	Disabled
PF Compress	Indicates if the access server negotiates to allow its peer to omit the extra protocol field byte from packets sent over the link.	Enabled Disabled	Disabled
ACF Compress	Indicates if the access server negotiates to allow its peer to omit the HDLC address and control fields from packets sent over the link.	Enabled Disabled	Disabled
FCS Size*	The size of the FCS that the access sever is configured to negotiate.	16-bit	16-bit
Callback**	Indicates that the access server negotiates to request a call-back.	Enabled Disabled	Enabled



**FCS Size has a fixed value in this software release.*

*** If you enable PPP call-back negotiation on a port, it is strongly recommended you also enable some sort of authentication (PAP, CHAP, etc.) on the port. Without authentication, any user who happens to discover the phone number for that port's modem could potentially request a call-back and run up unlimited phone charges. To enable authentication on a port, refer to Chapter 22.*

Displaying IPCP Characteristics

The SHOW / LIST / MONITOR PPP IPCP CHARACTERISTICS command displays the IPCP configuration for a given port. The fields in the display show the latest values configured by the SET PORT n PPP IPCP characteristic commands. Use the SHOW / MONITOR PORT n PPP IPCP STATUS command to see the values actually used on the link.

Example: IPCP Characteristics Display

The following example shows a sample IPCP characteristics display.

```
Local> SHOW PORT 5 PPP IPCP CHARACTERISTICS
IPCP Characteristics:
IPCP:                                Disabled
Passive Open:                        Disabled
Restart Timer:                              3 seconds
Max Configure:                             10 transmissions
Max Terminate:                              2 transmissions
Max Failure:                               10 transmissions
IPCP Options: Local:
Negotiate Address: Disabled
Remote IP Address: 0.0.0.0
Compress Header: Disabled
Compress States: 16
```

IPCP Characteristics Display Fields

The following table explains the fields in the IPCP characteristics display.

Field	Description	Values	Default
IPCP	Indicates if IPCP is enabled.	Enabled Disabled	Disabled
Passive Open[1]	When enabled, IPCP negotiation does not begin until initiated by the attached device.	Disabled	Disabled

Field	Description	Values	Default
Restart Timer	Indicates the amount of time between IPCP configure- or terminate-request retransmissions when there is no response.	1 to 5 seconds	3
Max Configure	The number of times that IPCP sends a configure- request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	10
Max Terminate	The number of times that LCP sends a terminate-request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	2
Max Failure	The number of times that IPCP sends a negative acknowledgment for the peer's proposed options before deciding to reject the options.	1 to 15 attempts	10
Negotiate Address	Indicates if IP address negotiation is enabled for this link.	Enabled Disabled	Disabled
Remote IP Address	Indicates the address that the access server should negotiate to use for the peer and the source of the port's remote IP address.		0.0.0.0
Compress Header	Indicates that TCP/IP header compression is to be used.	Enabled Disabled	Disabled
Compress States	Indicates the maximum number of TCP/IP sessions that can be compressed at any given time.	4 to 16	16

[1] This field has a fixed value in this software release.

ATCP Characteristics

The SHOW/LIST/MONITOR PPP ATCP CHARACTERISTICS command displays the ATCP configuration for a given port. The fields in the display show the latest values configured by the SET PORT n PPP ATCP characteristic commands. Use the SHOW/MONITOR PORT n PPP ATCP STATUS command to see the values actually used on the link.

Example: ATCP Characteristics Display

The following example shows a sample ATCP characteristics display:

```
Local> SHOW PORT 5 PPP ATCP CHARACTERISTICS

Port 5:                              Server: LAT_08002B26AA94

ATCP Characteristics:

ATCP:              Enabled       Passive Open:       Enabled
Restart Timer:     3 seconds
Max Configure:     10 transmissions
Max Terminate:     2 transmissions
Max Failure:       10 transmissions
```

ATCP Characteristics Display Field Values

The following table explains the fields in the ATCP characteristics display:

Field	Description	Values	Default
ATCP	Indicates if ATCP is enabled.	Enabled Disabled	Enabled
Passive Open [1]	When enabled, ATCP negotiation does not begin until initiated by the attached device.	Enabled Disabled	Enabled
Restart Timer	Indicates the amount of time between ATCP configure- or terminate-request retransmissions when there is no response.	1 to 5 seconds	3
Max Configure	The number of times that ATCP sends a configure-request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	10
Max Terminate	The number of times that ATCP sends a terminate-request packet to the peer without receiving an acknowledgment.	1 to 15 attempts	2
Max Failure	The number of times that ATCP sends a negative acknowledgment for the peer's proposed options before deciding to reject the options.	1 to 15 attempts	10

[1] This field has a fixed value in this software release.

Displaying PPP Status

Introduction

This section describes how to display the PPP LCP and IPCP status.

Displaying LCP Status

Use the SHOW PORT n LCP STATUS command to display LCP characteristics. This command is nonprivileged. This command shows the actual state of the LCP implementation on the access server. Because of the nature of PPP negotiations, the display can differ from the configured characteristics shown on the SHOW PORT n PPP LCP CHARACTERISTICS display.

The display fields fall into two categories:

- General link status (LCP Status section)
- Status of the LCP options (LCP Options section)

Example: LCP Status Display

The following example shows the LCP status display for port 5:

```
Local> SHOW PORT 5 PPP LCP STATUS

Port 5:                              Server: LAT_08002B26D0E7
LCP Status:

State:                    Initial
Negotiation Time:      0 00:00:00
Since Open:            0 00:00:00
Failure Reason:              None
Authentication:           Initial

LCP Options:                Local:    Remote:

MRU:                        1500           1500
Character Map               FFFFFFFF    FFFFFFFF
Authentication:             Disabled    Disabled
Link Quality:               Disabled    Disabled
Magic Number:               Disabled    Disabled
PF Compress:                Disabled    Disabled
ACF Compress:               Disabled    Disabled
FCS Size:                   16 Bit        16 Bit
Callback:                   Disabled     Enabled
```

Fields in the LCP Status Display

The following table describes the fields in the LCP status display:

Field	Description
State	The LCP state as defined in RFC 1331.
Negotiation Time	The number of seconds required by the PPP negotiation procedure the last time LCP renegotiated.
Since Open	The number of seconds since LCP last attempted to negotiate the link.
Failure Reason	Provides a brief reason if LCP cannot complete negotiations.
MRU	Maximum Receive Unit. Indicates the largest number of characters each peer would like to receive in a packet.
Character Map	Specifies which characters require special encapsulation or "byte stuffing."
Authentication	Indicates whether authentication is required. PAP is supported for this release.
Link Quality	The link quality is disabled in this release.
Magic Number	Local — Indicates if the access server has negotiated to respond to magic numbers from the peer. These numbers can be used to detect loopback. The local magic number is disabled in this release. Remote — Indicates if the peer has negotiated to respond to magic numbers from the access server. The remote magic number is disabled in this release.
PF Compress	Indicates whether Protocol Field compression has been negotiated.
ACF Compress	Indicates whether Address and Control Field compression has been negotiated.
FCS Size	Always 16-bit CRC.
Callback	Indicates that call-back has been negotiated.

Displaying IPCP Status

Use the SHOW PORT n PPP IPCP STATUS command to display IPCP status. This command shows the actual state of the IPCP implementation in the access server.

Because of the nature of PPP negotiations, this display can differ from the configured characteristics shown on the SHOW PORT n PPP IPCP CHARACTERISTICS display.

The display fields in fall into two categories:

- General IP status over the link (IPCP Status section)
- Status of each IPCP option (IPCP Options section)

Example: IPCP Status Display

The following example shows the IPCP status display for port 5:

```
Local> SHOW PORT 5 PPP IPCP STATUS

Port 5:                                Server: LAT_08002B26D0E7
IPCP Status:
State:                        Initial
Negotiation Time:          0 00:00:00
Since Open:                0 00:00:00
Failure Reason:                  None

IPCP Options:                  Local:          Remote:

Negotiate Address:           Disabled        Disabled
IP Address:                   0.0.0.0         0.0.0.0
Compress Header:             Disabled        Disabled
Compress States:                    0               0
```

Fields in the IPCP Status Display

The following table explains the fields in the IPCP status display:

Field	Description
State	The IPCP state as defined in RFC 1331. The possible states are Initial, Starting, Closed, Stopped, Closing, Stopping, Req Sent, Ack-Rcvd, Ack-Sent, Opened, and DHCP Req. DHCP Req (which is not part of RFC 1331) indicates the negotiations are waiting for DHCP to assign an IP address.
Negotiation Time	The number of seconds required by the PPP negotiation procedure the last time IPCP negotiated.
Since Open	The number of seconds since IPCP last attempted to negotiate IP over the link.
Failure Reason	Provides a brief reason if IPCP cannot negotiate IP over the link.

Field	Description
Negotiate Address	Indicates if address negotiation should take place. This characteristic is disabled in this release.
IP Address	Local — The IP address that the access server is using for itself on the link. This value is the address used with the access server's own Ethernet. Remote — The value that the access server is using to identify the peer on the link.
Compress Header	Indicates whether compression is turned on.
Compress States	Indicates the maximum number of TCP/IP connections that can be compressed at any time.

Displaying ATCP Status

Use the SHOW PORT n PPP ATCP STATUS command to display ATCP status. The

This command shows the actual state of the ATCP implementation in the access server. Because of the nature of PPP negotiations, this display can differ from the configured characteristics shown on the SHOW PORT n PPP ATCP CHARACTERISTICS display.

The display fields in fall into two categories:

- General ATCP status over the link (ATCP Status section)
- Status of each ATCP option (ATCP Options section)

Example: ATCP Status Display

The following example shows the ATCP status display on port 5:

```
Local> SHOW PORT 5 PPP ATCP STATUS

Port 5:                                Server: LAT_08002B26AA94

ATCP Status:
State:                        Opened
Negotiation Time:         0 00:00:10
Since Open:               0 00:08:10
Failure Reason:                 None
ATCP Options:                 Local:              Remote:
Appletalk Address:            401.20               401.12
Routing Protocol:           RTMP                   RTMP
Suppress B_Cast:            Disabled             Disabled
Compression:                Disabled             Disabled
Connect Time:               Disabled             Disabled
Server Info:                Disabled             Disabled
Default Router:             401.249                   0.0
Zone Info:                             LKG Littleton MA
```

Fields in the ATCP Status Display

The following table explains the fields in the ATCP status display:

Field	Description
State	The ATCP state as defined in RFC 1331. The possible states are Initial, Starting, Closed, Stopped, Closing, Stopping, Req Sent, Ack-Rcvd, Ack-Sent, and Opened.
Negotiation Time	The number of seconds required by the PPP negotiation procedure the last time ATCP negotiated.
Since Open	The number of seconds since ATCP last attempted to negotiate IP over the link.
Failure Reason	Provides a brief reason if ATCP cannot negotiate IP over the link.
ATCP Options:	Local — Refers to the access server. Remote — Refers to the attached PPP hosts.
AppleTalk Address	The access server Appletalk address and the AppleTalk address that the access server has acquired and assigned to the attached host.

Field	Description
Routing Protocol	The type of routing protocol information that may be sent across the link.
Suppress B_Cast	Indicates whether broadcasts are suppressed.
Compression	Indicates whether compression is being used on AppleTalk packets.
Connect Time	Indicates whether connect time information is passed.
Server Info	Indicates whether server information is passed.
Default Router	The current AppleTalk router that the access server and client are using.
Zone Info	The zone in which the access server and client reside.

Displaying PPP Counters

Introduction

The section describes PPP counters.

Displaying LCP Counters

Use the SHOW PORT n LCP COUNTERS command to display LCP counters for a port. The display shows all the counters relevant to LCP protocol operation. Most of this information is useful as a diagnostic aid. The CONNECT or DISCONNECT command zeroes each of the counters.

Example: Commands to Display LCP Counters

The following example shows the command to display LCP counters for port 5:

```
Local> SHOW PORT 5 LCP COUNTERS

Port 5:        Server:       LAT_08002B26D0E7

LCP Counters:

Negotiation Successes:          0
Negotiation Failures:           0

Configures in:          0       Configures out:           0
Acks in:                0       Acks out:                 0
Naks in:                0       Naks out:                 0
Rejects in:             0       Rejects out:              0
Terminates in:          0       Terminates out:           0
Term Acks in:           0       Term Acks out:            0
Code Rejects in:        0       Code Rejects out:         0
Echo Reqs in:           0       Echo Reqs out:            0
Echo Resps in:          0       Echo Resps out:           0
Prot Rejects in:        0       Prot Rejects out:         0
Discards in:            0       Discards out:             0
```

Fields in the LCP Counters Display

The following table describes the fields in the LCP counters display:

Field	Description
Negotiation Successes	The number of times that LCP successfully entered a round of negotiations since the link was brought up. Ordinarily, this counter is 1. However, you can reconfigure LCP and then cause LCP to renegotiate This changes the performance characteristics for the link.
Negotiation Failures	The number of times that LCP tried to negotiate the link, but failed.
Configures in	The number of LCP configure-requests received from the peer.
Configures out	The number of LCP configure-requests sent to the peer from the access server.
Acks in	The number of LCP configure-acks received from the peer.
Acks out	The number of LCP configure-acks sent to the peer from the access server.
Naks in	The number of LCP configure-naks received from the peer.
Naks out	The number of LCP configure-naks sent to the peer from the access server. This counter should always be zero in this release.
Rejects in	The number of LCP configure-rejects received from the peer.
Rejects out	The number of LCP configure-rejects sent to the peer from the access server.
Terminates in	The number of LCP terminate-requests received from the peer.
Terminates out	The number of LCP terminate-requests sent to the peer from the access server.
Term Acks in	The number of LCP terminate-acks received from the peer.
Term Acks out	The number of LCP terminate-acks sent to the peer from the access server.
Code Rejects in	The number of LCP code-rejects received from the peer.
Code Rejects out	The number of LCP code-rejects sent to the peer from the access server.
Echo Reqs in	The number of LCP echo-requests received from the peer.

Field	Description
Echo Reqs out	The number of LCP echo-requests sent to the peer from the access server. This number should always be zero in this version.
Echo Resps in	The number of LCP echo-replies received from the peer.
Echo Resps out	The number of LCP echo-replies sent to the peer from the access server.
Prot Rejects in	The number of LCP protocol-rejects received from the peer.
Prot Rejects out	The number of LCP protocol-rejects sent to the peer from the access server.
Discards in	The number of LCP discard packets received from the peer. A discard packet is the PPP equivalent of a “no op” instruction.
Discards out	The number of LCP discard packets sent to the peer from the access server. This number should always be zero in this version.

Displaying IPCP Counters

Use the SHOW PORT n IPCP command to display the IPCP counters for a port. This command requires no privileges. The display shows all the counters relevant to IPCP protocol operation. Most of this information is useful as a diagnostic aid. The CONNECT or DISCONNECT command zeroes each of these counters.

Example: Command to Display the IPCP Counters

The following example shows how to display the IPCP counters for port 5:

```
Local> SHOW PORT 5 IPCP COUNTERS

Port 5:        Server:         LAT_08002B26D0E7

IPCP Counters:

Negotiation Successes:           0
Negotiation Failures:            0

Configures in:        0  Configures out:                0
Acks in:              0  Acks out:                       0
Naks in:              0  Naks out:                       0
Rejects in:           0  Rejects out:                    0
Terminates in:        0  Terminates out:                 0
Term Acks in:         0  Term Acks out:                  0
```

Fields in the IPCP Counters Display

The following table describes the fields in the IPCP counters display:

Field	Description
Negotiation Successes	The number of times that IPCP has successfully entered a round of negotiations to bring up IP since the link was brought up. Ordinarily the value of this counter is 1. However, you can reconfigure IPCP and then cause IPCP to renegotiate. This changes the performance characteristics for the link.
Negotiation Failures	The number of times that IPCP tried to negotiate the link, but failed.
Configures in	This is the number of IPCP configure-requests received from the peer.
Configures out	The number of IPCP configure-requests sent to the peer from the access server.
Acks in	The number of IPCP configure-acks received from the peer.
Acks out	The number of IPCP configure-acks sent to the peer from the access server.
Naks in	The number of IPCP configure-naks received from the peer.
Naks out	The number of IPCP configure-naks sent to the peer from the access server. This counter should always be zero in this release.
Rejects in	The number of IPCP configure-rejects received from the peer.
Reject outs	The number of IPCP configure-rejects sent to the peer from the access server.
Terminates in	The number of IPCP terminate-requests received from the peer.
Terminates out	The number of IPCP terminate-requests sent to the peer from the access server.
Term Acks in	The number of IPCP terminate-acks received from the peer.
Term Acks out	The number of IPCP terminate-acks sent to the peer from the access server.

Displaying ATCP Counters

Use the SHOW PORT n ATCP Counters command to display ATCP counters for a port. This command requires no privileges. The counters display shows all the counters relevant to ATCP protocol operation. Most of this information is useful as a diagnostic aid. The CONNECT or DISCONNECT command zeroes each of these counters.

Example: Command to Display the ATCP Counters

The following example shows how to display the ATCP counters:

```
Local> SHOW PORT 5 ATCP COUNTERS

Port 5:        Server:       LAT_08002B26AA94

ATCP Counters:

Negotiation Successes:           0
Negotiation Failures:            0
Configures in:        8 Configures out:                 12
Acks in:              6 Acks out:                        6
Naks in:              0 Naks out:                        1
Rejects in:           6 Rejects out:                     1
Terminates in:        0 Terminates out:                  0
Term Acks in:         0 Term Acks out:                   0
```

Fields in the ATCP Counters Display

The following table describes the fields in the ATCP counters display:

Field	Description
Negotiation Successes	The number of times that ATCP has successfully entered a round of negotiations to bring up AppleTalk since the link was brought up. Ordinarily the value of this counter is 1. However, you can reconfigure ATCP and then cause ATCP to renegotiate. This changes the performance characteristics for the link.
Negotiation Failures	The number of times that ATCP tried to negotiate the link, but failed.
Configures in	This is the number of ATCP configure-requests received from the peer.
Configures out	The number of ATCP configure-requests sent to the peer from the access server.
Acks in	The number of ATCP configure-acks received from the peer.

Field	Description
Acks out	The number of ATCP configure-acks sent to the peer from the access server.
Naks in	The number of ATCP configure-naks received from the peer.
Naks out	The number of ATCP configure-naks sent to the peer from the access server. This counter should always be zero in this release.
Rejects in	The number of ATCP configure-rejects received from the peer.
Rejects out	The number of ATCP configure-rejects sent to the peer from the access server.
Terminates in	The number of ATCP terminate-requests received from the peer.
Terminates out	The number of ATCP terminate-requests sent to the peer from the access server.
Term Acks in	The number of ATCP terminate-acks received from the peer.
Term Acks out	The number of ATCP terminate-acks sent to the peer from the access server.

Chapter 21

Managing IPX

Overview

Introduction

This chapter describes how to configure and manage IPX on an access server.

In This Chapter

This chapter contains the following topics:

- IPX Description
- Getting Started
- Hardware and Software Requirements
- Setting Up Your PC
- Setting Up the Network Access Server
- Summary of DECserver IPX Management Commands
- Modem Considerations
- Novell Client/Server Operation
- Operational Checkout and Diagnosis
- Disabling IPX
- Frame Types
- Displaying IPX Characteristics
- Displaying IPX Status

- Displaying IPX Counters
- Displaying IPX Routes
- Resetting Counters

IPX Description

Introduction

The purpose of IPX is to allow Novell NetWare clients to dial in to (or directly attach to) the network access server via asynchronous lines. Each remotely connected Novell client looks and acts as if it was directly connected to the LAN.

The network access software provides PPP / IPXCP as the underlying data link on the asynchronous lines. This allows multiprotocol support (IP / IPX / AppleTalk) over the same asynchronous lines simultaneously.

Access Server Configuration

The access server can be set up to provide access for remote PC users to dial in over standard telephone lines to establish an IPX connection to a Novell network. The remote PC can access network resources such as file servers, printers, and electronic mail. Once connected, the PC becomes a remote node on the network. The access server facilitates IPX client-server communications between PC and NetWare file servers over the standard telephone line.

The remote node service provides the same functions and features to remote PCs as locally connected LAN users. The main difference between the remote node connection and a local connection using Ethernet is the data transfer speed. However, dial-in connections that use high-speed modems provide excellent performance.

The PC gains access to the IPX network through the access server by using any third-party remote node access software that supports the point-to-point protocol (PPP) for IPX. The remote access software must also facilitate the use of Novell NetWare workstation software, which is used to communicate with the Novell network over the dial-up connection.

By default, the access server will simultaneously communicate with all four frame types on the LAN: Ethernet II, 802.2 SAP, 802.2 SNAP, and Novell 802.3. When IPX is enabled on the access server, the network addresses for all four types will automatically be learned.

Login Procedures

One or more serial ports of the access server can be configured for Novell dial-up access. Depending on your requirements, different login procedures for IPX can be configured including:

- The remote PC user can choose to activate a connection to the Novell network after login to the access server local user interface. This allows the user to take advantage of other non-IPX services from the access server before connecting to the Novell network.
- The remote PC user can automatically connect to the Novell network after login.
- Login and/or PPP password authentication is configurable. For PPP password, the PC client software must support PPP/PAP authentication.

Getting Started

Checklist

The following is a checklist for using this chapter to perform the basic steps to perform remote node access to a Novell network through a network access server:

Step	Action
1	Determine your hardware/software requirements (Hardware and Software Requirements).
2	Configure your PC (Setting Up the Network Access Server).
3	Configure your network access server (Setting Up the Network Access Server).
4	Check your configuration (Operational Checkout and Diagnosis).

Hardware and Software Requirements

Introduction

This section describes the hardware and software necessary to run IPX.

There must be at least one NetWare fileserver version 3.xx or greater on the network. If a fileserver is not directly attached to the same LAN as the network access server, there must be a NetWare router on the LAN.

Software Requirements

The following software is required to run IPX:

- Network Access Software version 1.4 or greater.
- Remote node access software for the PC, which must support NetWare IPX using Point-to-Point Protocol (PPP). (Can be acquired from a third-party network software communications vendor.)
- Novell NetWare workstation software for the PC. (Can be acquired from your Novell NetWare or third-party remote node access software kit.)
- Novell NetWare utilities on the PC. (Can be acquired from your Novell NetWare or third-party remote node access software kit.)

Hardware Requirements

The following hardware is required to run IPX:

- PC with a high-performance Universal Asynchronous Receiver / Transmitter (UART) on the COM port. Either standard 16450 or 16550 UART or equivalent may be used.
- Dial-out modem for PC; dial-in modem for network access server. Minimum 9600 baud recommended. Highest speed modem available preferred.

References

For a comprehensive list of the server hardware platforms necessary to run IPX, refer to the Cabletron *Network Access Software Release Notes*.

Refer to Appendix A for the cable and adapter requirements.

Setting Up Your PC

PC Remote Access Software

Ensure you know whether the network access server port you are dialing in to requires you to enter a login password or logs directly in to the local user interface. If this is the case, you will need to use terminal emulation to communicate with the access server following modem connection.

Ensure you know whether the network access server port requires a PPP / PAP password. If so, you will have to configure the password on your remote node access software.

Reference

Refer to the documentation included with your PC remote node access software for installation and setup procedures.

Novell Workstation Software

Novell NetWare workstation software (or equivalent) must be installed on your PC. This makes it possible to establish and maintain IPX network connections.

Reference

Refer to your Novell Installation Guide for Workstations and the documentation included with your PC remote node access software for more information.

Novell Utilities for Local Execution

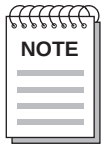
After a remote node access connection is made to a Novell fileserver, ensure that the Novell utilities you need are stored locally on your PC. This is because activating large executables from a network disk can result in long load times due to the relatively slower speed of the serial line. See the Novell Operation section in this chapter for more information.

Setting Up the Network Access Server

Enabling IPX

By default, IPX is not enabled on the access server. A privileged user must enable IPX with the following commands:

```
Local> CHANGE IPX INTERNAL ipx-net
Local> CHANGE IPX ENABLED
```



The ipx-net value must be a unique Novell network number on the network.

Configuring the Port for an Attached Device

To configure a port for PCs dialing in through a modem or directly connected to the network access server, use the following commands:

```
Local> CHANGE PORT n ACCESS DYNAMIC
Local> CHANGE PORT n ALTERNATE SPEED NONE
Local> CHANGE PORT n INACTIVITY LOGOUT ENABLED
Local> CHANGE PORT n FLOW CONTROL CTS
Local> DEFINE PORT n SIGNAL CONTROL ENABLED DSRLOGOUT ENABLED
Local> DEFINE PORT n SIGNAL SELECT CTS
Local> LOGOUT PORT n
```

Considerations

When configuring IPX, consider the following:

- ALTERNATE SPEED is not applicable to the DECserver 90M and DECserver 90TL hardware (Ignore warning messages).
- FLOW CONTROL should match the flow control configured for the attached device. For access server platforms with either full or partial modem control signals, flow control can be configured either CTS / RTS or XON / XOFF. CTS is recommended. For access server platforms with limited modem control signals (i.e., DTR / DSR), only XON / XOFF is supported. If the attached device does not support XON flow control, configure flow control DISABLE. This means flow control is not used. Although operation is possible without flow control, poor performance or unexpected behavior with your Novell connection can result.

- SIGNAL SELECT should match signals used by the attached device (for example, a modem) when the SIGNAL SELECT feature is supported on the access server. SIGNAL SELECT is not applicable for some access server platforms. SIGNAL SELECT can be configured either CTS (CTS-DSR-RTS-DTR) or RI (RI-DCD-DSRS-DTR). Based on configuration, correct adapter must be chosen (see Appendix A). Current high-speed modems (>9600 baud) typically use CTS.

Configuring the Port for the Login Method

You can configure a port to log in to a local user interface prompt or to be exclusively dedicated to PPP. To configure a port for login to a local user interface prompt, refer to the Configuring the Port for Login to the Local Prompt section in this chapter. To configure a port to be exclusively dedicated to PPP, refer to the Configuring the Port Dedicated to PPP section in this chapter.

Configuring the Port for Login to the Local Prompt

Following modem connection, the PC user will log in to the local interface with or without password authentication. Then, the user will have the option to activate PPP using user interface commands.

Activating PPP

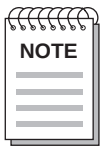
To configure the port with login password authentication required, use the following commands:

```
Local> CHANGE SERVER LOGIN PASSWORD xxxxxx
Local> CHANGE PORT n PASSWORD ENABLE
Local> CHANGE PORT n AUTOBAUD ENABLE SPEED 9600
Local> CHANGE PORT n DEDICATED NONE
```

Configuring the Port With No Login Password Authentication Required

To configure the port with no login password authentication required, use the following commands:

```
Local> CHANGE PORT n PASSWORD DISABLE
Local> CHANGE PORT n AUTOBAUD ENABLE SPEED 9600
Local> CHANGE PORT n DEDICATED NONE
```



Both login password authentication and PPP/PAP password authentication use the same password. One or both can be enabled at the same time.

Configuring the Port Dedicated to PPP

Following modem connection, the PC user will log in with or without password authentication. Then, PPP will automatically be activated to pass IPX network packets.

Configuring the Port With Login Password Authentication Required

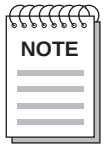
To configure a port with login password authentication required, use the following commands:

```
Local> CHANGE SERVER LOGIN PASSWORD xxxxxx
Local> CHANGE PORT n PASSWORD ENABLE
Local> CHANGE PORT n AUTOBAUD ENABLE SPEED 9600
Local> CHANGE PORT n DEDICATED PPP
Local> CHANGE PORT n DEFAULT PROTOCOL PPP
```

Configuring the Port With No Login Password Authentication Required

To configure a port with no login password authentication required, use the following commands:

```
Local> CHANGE PORT n PASSWORD DISABLE
Local> CHANGE PORT n AUTOBAUD DISABLE SPEED speed
Local> CHANGE PORT n DEDICATED PPP
Local> CHANGE PORT n DEFAULT PROTOCOL PPP
```



With AUTOBAUD DISABLEd, serial port speed must be explicitly configured for both the modem and the access server port.

Configuring the Port for PPP/IPXCP Data Link

To configure a port for PPP / IXPCP data link, use the following commands:

```
Local> CHANGE PORT n LCP MAP A0000
Local> CHANGE PORT n LCP PASSIVE DISABLE
Local> CHANGE PORT n LCP ENABLE
Local> CHANGE PORT n IPXCP ENABLE
Local> CHANGE PORT n PPP ENABLE
```

Enabling PPP/PAP Password Authentication

To enable the optional PPP / PAP password authentication, use the following commands:

```
Local> CHANGE SERVER LOGIN PASSWORD xxxxxx
Local> CHANGE PORT n LCP AUTHENTICATION PAP
```

Disabling PPP/PAP Password Authentication

To disable the optional PPP / PAP password authentication, use the following command:

```
Local> CHANGE PORT n LCP AUTHENTICATION DISABLE
```

Passwords

Both login password authentication and PPP / PAP password authentication use the same password. One or both can be enabled at the same time. For PAP, verification of the password is case sensitive. If PAP is enabled, the password must also be supported and configured using your remote node access software on the PC.

Summary of DECserver IPX Management Commands

The following are the network access server commands you can use to manage IPX.

Port PPP IPX Commands for LCP

The following table explains the PORT PPP IPX commands for LCP.

SHOW/LIST/MONITOR PORT n LCP	**Description**
CHARACTERISTICS	Display the current values for the LCP characteristics.
SHOW/MONITOR PORT n LCP	**Description**
COUNTERS	Display the current values of the IPXCP counters.
STATUS	Display the current values of the IPXCP counters and characteristics.
CHANGE/SET/DEFINE PORT n LCP	**Description**
ACFC	Address and Control Field Compression for PPP datagram.
AUTHENTICATION	Password authentication is enabled.
ENABLE	Enable LCP.
DISABLE	Disable LCP.
MAP	Specifies characters that may not be sent in the clear.
MAXFAILURE	Number of times LCP sends NAK before rejecting option.
MAXTERMINATE	Number of times LCP sends terminate request without ACK.
MRU	Maximum receive units.
PASSIVE	When enabled, LCP must be initiated by attached device.
PFC	Protocol Field Compression for PPP datagram.
RESTART	Restart a suspended session.

Port PPP IPX Commands for IPXCP

The following table explains the PORT PPP IPX commands for IPXCP:

SHOW/LIST/MONITOR Port n IPXCP	**Description**
CHARACTERISTICS	Display the current values for the IPXCP characteristics.
SHOW/MONITOR PORT n IPXCP	**Description**
STATUS	Display the values of the IPXCP counters and characteristics.
COUNTERS	Display the values of the IPXCP counters.
CHANGE/SET/DEFINE PORT n IPXCP	**Description**
ENABLE	Enable IPXCP.
DISABLE	Disable IPXCP.
MAXCONFIGURE	Number of times IPXCP sends configure request without ACK.
MAXFAILURE	Number of times IPXCP sends NAK before rejecting option.
MAXTERMINATE	Number of times IPXCP sends terminate request without ACK.
RESTART	Restart a suspended session.

Port PPP Commands for PPP Negotiation Status

The following table defines the PORT PPP commands for PPP negotiation status:

SHOW/MONITOR PORT n PPP	**Description**
COUNTERS	Display the values of the IPXCP counters.
STATUS	Display the values of the PPP counters and characteristics.

Server IPX Commands

The following table defines the server IPX commands:

SHOW/LIST/MONITOR IPX	**Description**
CHARACTERISTICS	Display the current values for the characteristics.
SHOW/MONITOR IPX	**Description**
COUNTERS	Display the values of the IPXCP counters.
RIP	Display the RIP entries known to the server.
ROUTES	Display the routes known by the server.
STATUS	Display the counters, RIP entries, and routes.
CLEAR IPX	**Description**
RIP	Clear all unique networks from the RIP database.
SAP	Clear all the SAP service entries known to the server.
ZERO	**Description**
IPX COUNTERS	Zero all IPX counters.
PORT n PPP COUNTERS	Zero all PPP counters associated with port n.
CHANGE/SET/DEFINE IPX	**Description**
ENABLE	Enable IPX.
DISABLE	Disable IPX.
CHANGE/SET/DEFINE IPX FRAME	**Description**
ETHERNET	Standard Ethernet V2.
RAW802	Novell standard 802.3 RAW.
SHOW/MONITOR PORT n PPP	**Description**
SAP802	IEEE 802.2 standard.
SNAP802	IEEE 802.2 with SNAP SAP format.

CHANGE/SET/DEFINE IPX FRAME frametype NETWORK	Description
ipx-net	Specify explicit internal network number.
LEARN	Learn internal network number from LAN.
DISABLED	Internal network disabled.

CHANGE/SET/DEFINE IPX INTERNAL NETWORK	Description
ipx-net	Specify ipx-net as the internal network number.
NONE	There is no IPX address for the internal network.

Modem Considerations

Dial-In Modems

Keep the following in mind when using dial-in modems attached to the network access server:

- Flow control for the dial-in modem and the access server port must match. CTS is recommended for access server platforms that support CTS/RTS. XON/XOFF is recommended for access server platforms that do not support CTS/RTS.
- Serial speed for the modem can be configured as high as 115,200 bits/s on some access server platforms and as high as 57,600 bits/s on others. The access server port will autobaud up to this speed when the port is configured for autobaud.
- When autobaud is enabled, in most cases, typing a carriage return once per second is sufficient to autobaud into the access server when the modem dial-in connection is complete. In some cases (AppleTalk, for example), it may be necessary to type a series of three carriage returns at a faster rate for a successful autobaud.
- Modem DSR must be configured to cycle on modem hang-up. The access server port is configured to log out the port when DSR cycles, making sure that the Novell network connection goes away when the PC user is finished.
- Use the fastest modem available. Error-correcting modems that are currently available provide up to 28,800 bits/s carrier speeds and serial port speeds to 115,200 bits/s. The access server serial ports will autobaud up to 115,200 bits/s.

Dial-Out PC Modems

Keep the following in mind when using dial-out modems attached to the PC:

- The PC should have a high-performance UART chip capable of high speeds (16450 or 16550). The serial port baud rate of the modem is dependent on the UART and the type of modem used.
- Normally, set the serial port baud rate of the modem to two to four times the speed of your modem. The 8250 and 16450 UART chips can be more susceptible to lower performance due to errors when run at higher speeds.

Recommended Serial Port Baud Rate

The following table lists guidelines for setting the serial port baud rate:

UART Type	Maximum Modem Speed	Maximum Recommended Serial Port Baud Rate
8250	9600	Up to 9600
16450	9600 to 14400	9600 to 19200
16450-A	9600 to 14400	9600 to 19200
16550	Up to 28800	Up to 115200

Novell Client/Server Operation

Establishing Remote Node Access Connection to Novell Network

Vendors of PC remote node access software for Novell may have different procedures for dialing in and establishing a remote access connection to a Novell LAN through the access server. However, the following are generally the expected steps:

Step	Action
1	Dial in to the network access server. Activate your remote node access software on your PC so that a phone call is made to the access server.
2	Log in to the access server. If the dial-in access server port requires login password authentication, type carriage returns until you see the # prompt, then type your password followed by another carriage return.
3	Activate the PPP connection. If the access server port is configured for dedicated PPP connection, your PC remote node access software will offer an indication that PPP has been negotiated with the access server dial-in port. If the access server port is configured for login to the access server local user interface, type several carriage returns and enter a user name to get the local prompt and type CONNECT PPP at the prompt. The PC remote node access software indicates that PPP has been negotiated.
4	Activate Novell workstation software. Refer to the documentation included with your PC remote node access software for instructions on loading and activating the Novell workstation software to establish a connection to a Novell fileserver.

Novell Operation

Refer to the documentation included with your PC remote node access software for a discussion of considerations associated with Novell operation from a remote dial-in node including:

- Make sure to store and run Novell utilities locally. Large executables activated from a network disk can experience long load times due to the relatively slower speed of the serial line. If the desired executables are not local, copy them from the network disk after a Novell fileserver connection is established. They may also be available from your remote node access software kit.
- Use DOS batch files with all the commands necessary to load and activate the remote node access software and Novell software for establishing an IPX

connection. Refer to the remote node access software installation guide for additional information.

- Use local Novell login scripts to facilitate logging in to a Novell fileserver.
- If Novell packet burst is used, specify a maximum of 3 for PB BUFFERS in NET.CFG. Using PB BUFFERS > 3 may cause access server buffers to be depleted for PPP at the port causing poor performance. In some cases, it may be better to disable packet burst by defining PB BUFFERS=0 in NET.CFG. You can determine if packets are being dropped by the access server by using the SHOW PORT n PPP COUNTERS command from a access server management port, where n is the port with the Novell connection.

Operational Checkout and Diagnosis

Verifying Configuration

To verify proper configuration, at a access server management port, type SHOW IPX at the local user interface prompt:

- At least one LAN frame should have a corresponding network number.
- IPX should be enabled and the internal network should be defined with a unique network number.

Reference

If you have problems with your dial-in connection, refer to the Cabletron *Network Access Software Problem Solving* guide.

If your PC has a problem establishing a modem connection or negotiating PPP protocol to the access server, you can diagnose the problem from the access server side.

Disabling IPX

Using the DEFINE Command

If you decide you no longer need IPX support, you can disable IPX by using the following privileged command:

```
Local> DEFINE IPX DISABLED
```

Reinitialize the access server to have this command take effect.

Frame Types

Introduction

To support a broad base of network stations, the access server supports four different frame formats for encapsulating IPX packets on the LAN. The four frame types supported by the access server can be enabled simultaneously:

- Ethernet
- RAW802
- SAP802
- SNAP802

A LAN frame is enabled when a unique NetWare network number is associated with the frame. The network number can be automatically “learned” or explicitly configured. By default, all four frame types attempt to learn their network number by monitoring frames on the network.

Standard Ethernet

This packet format is the standard Ethernet V2 packet format (protocol type 8137).

RAW802

This mode uses IEEE 802.3 format frames without an IEEE 802.2 LLC header. This mode is often called “raw” 802.3.

SAP802

This mode encapsulates IPX frames using IEEE 802.2 LLC standard header formats. The SSAP and DSAP for IPX is E0.

SNAP802

This mode uses the IEEE 802.2 LLC format with the SNAP SAP format. The SNAP protocol ID for IPX is 00-00-00-81-37.

Displaying IPX Characteristics

Using the SHOW command

Use the SHOW IPX CHARACTERISTICS command to display IPX characteristics, including IPX network and node numbers. The command is nonprivileged.

IPX Characteristics Display

The following example shows the command to display IPX characteristics on an access server:

```
Local> SHOW IPX CHARACTERISTICS
IPX Characteristics:
IPX: Enabled
LAN Node Address: 08002B24F2DD  Internal Network         2B24F2DD
LAN Frame:             ETHERNET  LAN Network:               Learn
LAN Frame:               RAW802  LAN Network:            Disabled
LAN Frame:               SAP802  LAN Network:            Disabled
LAN Frame:              SNAP802  LAN Network:            Disabled
```

IPX Characteristics Display Fields

The following table describes the fields in the IPX characteristics display:

Field	Description
IPX	Enabled or Disabled. The default is Disabled.
LAN Node Address	Maximum of 12 hexadecimal numbers (no leading zeroes) representing the Ethernet interface's hardware address.
Internal Network	None or up to 8 hexadecimal numbers (no leading zeroes, 1 to FFFFFFFE). This entry configures the IPX internal network number for the access server. It is used by the serial ports for configuring a common network number for all PC client dial-ins when PPP/IPXCP is negotiated. This occurs when the PC client requests the access server to configure the network through PPP. A higher network number offered by the PC client takes precedence over the internal network number. This number must also be unique. It is recommended that the internal network number be used to limit the number of unique networks in the IPX Routing Information Protocol (RIP) database of fileserver and routers.

Field	Description
LAN Frame	LAN frame types: ETHERNET, RAW802, SAP802, or SNAP802.
LAN Network	Learn, Disable, or up to 8 hexadecimal numbers (no leading zeroes, 1 to FFFFFFFE). “Learn” means that the access server will monitor the LAN to determine the network number of the corresponding frame.

Displaying IPX Status

Using the SHOW IPX Command

Use the SHOW IPX command to display IPX status. The command is nonprivileged.

IPX Status Display

The following example shows the command to display IPX status on an access server:

```
Local> SHOW IPX STATUS
IPX Status:
Route entries:          6
RIP entries:            6
SAP entries:            5
LAN Frame:    ETHERNET    LAN Network:                AAA1
LAN Frame:      RAW802    LAN Network:            Learning
LAN Frame:      SAP802    LAN Network:                BBB1
LAN Frame:     SNAP802    LAN Network:            Disabled
```

Fields in the IPX Status Display

The following table describes the fields in the IPX Status display:

Field	Description
IPX Status	Enabled or Disabled.
RIP entries	Number of current RIP networks known by the server.
SAP entries	Number of current SAP services known by the server.
Route entries	Number of current routing table entries.

Field	Description
LAN Frame	The frame type: Ethernet, RAW802, SAP802, or SNAP802.
LAN Network	Learning — The network number for the corresponding LAN frame has been configured to “learn.” The access server is currently attempting to learn the network number. XXXXXXXX — Either the network number for the corresponding LAN frame has been configured to “learn” and the network number has been automatically learned, or an explicit network number has been configured. The number is up to 8 hexadecimal digits (no leading zeroes). Disabled — The network number for the corresponding LAN frame has been configured as “disabled.”

Displaying IPX Counters

Use the SHOW IPX COUNTERS command

Use the SHOW IPX COUNTERS command to display the IPX counters. The command is nonprivileged.

IPX Counters Display

The following example shows the command to display IPX counters on an access server:

```
Local> SHOW IPX COUNTERS
IPX Counters                        Seconds Since Zeroed: 18207
IPX
 Total Packets Transmitted   0 Unknown Sockets:                 0
 Total Packets Received:     0 Receive Discards:                0
 Local Transmits:            0 Transmit Discards:               0
 Local Receives:             0 Hop Count Errors:                0
FORWARD CACHE
 Packets Received:           0 Packets Transmitted:             0
 Receive Discards:           0 Transmit Discards:               0
 Overruns:                   0 Timeouts:                        0
RIP
 Requests Transmitted:       0 Responses Transmitted:           0
 Requests Received:          0 Responses Received:              0
 Requests Discarded:         0 Responses Discarded:             0
 Request Resource Errors:    0 Response Resource Errors:        0
SAP
 Requests Transmitted:       0 Responses Transmitted:           0
 Requests Received:          0 Responses Received:              0
 Requests Discarded:         0 Responses Discarded:             0
 Request Resource Errors:    0 Response Resource Errors:        0
```

IPX Counters Display Fields

The following table describes the fields in the IPX Counters display:

Field	Description
Seconds Since Zeroed	Time, in seconds, since the counters were last zeroed.
IPX Total Packets Transmitted	Total number of data packets transmitted.

Field	Description
IPX Total Packets Received	Total number of data packets received.
IPX Local Transmits	Number of data packets transmitted, originating from the access server.
IPX Local Receives	Number of data packets received that were destined for the access server.
IPX Unknown Sockets	Number of data packets with unknown socket addresses.
IPX Receive Discards	Number of data packets that were received and discarded.
IPX Transmit Discards	Number of data packets discarded that were ready for transmission.
IPX Hop Count Errors	The number of input datagrams dropped because the access server was not their final destination and their hop count would exceed 15 if forwarded.
FORWARD CACHE Packets Received	If there is no existing route to a destination network, the packet is cached and a routing information request is sent out for the network. This field shows how many such data packets have been received.
FORWARD CACHE Receive Discards	The field shows how many discarded data packets were received for the cache.
FORWARD CACHE Overruns	This field shows how many cached data packets were discarded.
FORWARD CACHE Packets Transmitted	This field shows how many packets were transmitted from forward cache after the route was learned.
FORWARD CACHE Transmit Discards	This field shows how many packets were discarded that were ready for transmission from the cache.
FORWARD CACHE Timeouts	This field shows how many packets were discarded because the route was not learned.
RIP / SAP Requests Transmitted	Number of RIP / SAP request packets transmitted.

Field	Description
RIP / SAP Requests Received	Number of RIP / SAP request packets received.
RIP / SAP Requests Discarded	Number of RIP / SAP request packets discarded.
RIP / SAP Request Resource Errors	Number of RIP / SAP request packet resource errors.
RIP / SAP Responses Transmitted	Number of RIP / SAP response packets transmitted.
RIP / SAP Responses Received	Number of RIP / SAP response packets received.
RIP / SAP Responses Discarded	Number of RIP / SAP response packets discarded.
RIP / SAP Response Resource Errors	Number of RIP / SAP response packet resource errors.

Displaying IPX Routes

Using the SHOW IPX ROUTES Command

Use the SHOW IPX ROUTES command to display IPX Routes. This command is nonprivileged.

IPX Routes Display

The following example shows the command to display IPX routes:

```
Local> SHOW IPX ROUTES
IPX Routes
    Destination       Next Hop              Interface Ticks Hops
2B24F2DD.020000000001 2B24F2DD.08002B24F2DD ASYNC4    134      0
     911.000000000000 21000001.00608C114E4A ETHER0      2      1
21000001.FFFFFFFFFFFF 21000001.08002B24F2DD ETHER0      1      0
 EEE8022.FFFFFFFFFFFF EEE8022.08002B24F2DD  SAP0        1      0
 EEE8023.FFFFFFFFFFFF EEE8023.08002B24F2DD  RAW0        1      0
1BEAD017.000000000000 1BEAD017.08002B24F2DD ASYNC3    134      0
Local>
```

IPX Routes Display Fields

The following table describes the fields in the IPX routes display:

Field	Description
Destination	NetWare address of final destination.
Next Hop	NetWare address of next hop in the transmission.
Interface	Interface type for next hop.
Ticks	This field indicates how much time, in ticks, that the packet takes to reach the network number associated with this field entry. A tick is approximately 1/18 of a second.
Hops	This field indicates the number of routers that must be passed through to reach the network number associated with this field entry.

Resetting Counters

Using the ZERO Command

Use the ZERO command to reset IPX counters.

ZERO Command Options

The following table contains the options that you can use on the command line to reset specific counters or sets of counters:

Option	Description
ALL	Zeroes server IPX counters
IPX	Zeroes server IPX counters
PORT *port-list PPP*	Zeroes PPP port counters for the specified port including LCP and IPXCP counters

Chapter 22

Managing Dial Services

Overview

Introduction

Configuring dial services is similar in concept to configuring a LAT service or Telnet listener. You define a service with a specified configuration that dictates how the user can operate the dialer.

Before you begin any dialer management, be sure to:

- Install the latest software image on the access server and all load hosts.
- Read the release notes.
- Know what devices and cables are connected at the various ports.
- Enter the SET PRIVILEGED command for your port.
- Check if the current values or default values are appropriate.

In This Chapter

This chapter contains the following topics:

Dial Services Command Groups

Command Groups

To configure and manage the dial services, use the SET / DEFINE / CHANGE DIALER and SHOW / LIST / MONITOR DIALER command groups.

Reference

For more detailed information about commands used in this chapter, refer to the Cabletron *Network Access Software Command Reference* guide.

Entering the SET PRIVILEGED command

Before changing any other parameter, make sure you have the authority to make such changes. The SET PRIVILEGED command allows you to make changes that require special access. At the password prompt, type the privileged password. (DNAS does not echo the password as you type it.)

```
Local> SET PRIVILEGED
Password> (hidden)
```

Checking the Current Server Settings

Introduction

Before you configure dialer services, determine the current server configuration. Use the SHOW SERVER command to display the server configuration.

Server Configuration Display

The following example shows a typical access server configuration display:

```
Local> SHOW SERVER

Network Access SW Vx.x for DSxxx-xx BLxx-xx ROM Vx.x-x Uptime: 000:44:34

Address:      08-00-2B-26-AA-99     Name: WWDOCMC Number: 0

Identification:

Circuit Timer:                    80 Password Limit:              3
Console Port:                      1 Prompt:                  Local>
Inactivity Timer:                 30 Queue Limit:                100
Keepalive Timer:                  20 Retransmit Limit:             8
Multicast Timer:                  30 Session Limit:               64
Node Limit:                      200 Software                 WWENG2
Service Groups:                   42, 46, 66

Enabled Characteristics:
Announcements, Broadcast, Dump, Lock, Server Responder

Local>
```

Defining a Dialer Script

Introduction

The first step in configuring a dial service is creating a dialer script. A dialer script tells the access server what text strings to use to control a modem on a specific port. These text strings are also known as “modem strings.”

Defining Dialer Script Strings

Use the SET, DEFINE, and CHANGE DIALER SCRIPT commands to define the modem strings that make up various modem commands in a dialer script. Each associated string can be up to 40 characters in length.

Characteristics that you set using the DEFINE command take effect after you initialize the access server. Characteristics that you set take effect immediately, but are replaced when the access server initializes. Characteristics that you set using the CHANGE command take effect immediately and when the access server initializes.

The size of the dialer script modem strings is restricted by the amount of remaining unallocated NVRAM for the modem pool (total of 256 bytes for 8 and 16 port servers, and 512 bytes for 32 port servers) and by the command line restrictions. The script name can be a maximum of 16 characters.

Dialer String Descriptions

The following table lists the dialer script strings you can define, their default values and usage:

String Type	Default Value	Usage
COMMAND	"AT"	Appended to all other command strings.
INIT	None	Before initiating an outbound connection.
PREFIX	"DT"	Before digits of phone number.
CONNECTED	"CONNECT"	Verifies successful connection.
RESET	"H0Z"	After session is disconnected.

Example: Set Dialer Script Name

The following example illustrates how to modify dialer script strings in a dialer script called “dickens” in order to set unique dialer characteristics:

```
Local> DEFINE DIALER SCRIPT dickens COMMAND "AT"
Local> SET DIALER SCRIPT dickens INIT NONE
Local> SET DIALER SCRIPT dickens RESET NONE
Local> CHANGE DIALER SCRIPT dickens PREFIX "DT"
Local> DEF DIALER SCRIPT dickens RESET NONE
Local> SET DIALER SCRIPT dickens TIMEOUT NONE
```

Assigning the Dialer Script to a Port

Steps

After configuring the dialer strings in a dialer script, assign the script to a specific port. Do the following:

Step	Action
1	Are you defining the dialer script to the port for the first time? • If yes, go to step 2. • If no, use the SHOW PORT n command to determine the current dialer script by showing the port (optional). If you assign a dialer script to a port that already has an assigned dialer script, the access server overwrites the first dialer script. When you change or set a dialer script, it is a good idea to check to see if one is in use.
2	Assign the new dialer script to the desired port using the DEFINE PORT n DIALER SCRIPT command.

Determining the Current Dialer Script

Use the SHOW PORT n command to display information about specific ports and their current configuration. The SHOW PORT command helps you to determine how a port is configured before you begin making changes to that port.

Example: The Show Port Command Display

The following example shows the resulting display for the SHOW PORT command. In this example, the preferred dialer service is CALL_HOME and the dialer script name is Generic_14400.

```
Local> SHOW PORT 2

Port 2:                          Server: user10_DS700-16

Character Size:         8  Input Speed                      57600
Flow Control:         XON  Output Speed:                    57600
Parity:              None  Signal Control:                Enabled
Stop Bits:        Dynamic  Signal Select:         CTS-DSR-RTS-DTR

Access:           Dynamic  Local Switch:                     None
Backwards Switch:    None  Name:                          PORT_2
Break:              Local  Session Limit:                      4
Forwards Switch:     None  Type:                           Ansi
Default Protocol:    DIAL  Default Menu:                    None
                           Dialer Script:           Generic_14400
Preferred Service: CALL_HOME

Authorized Groups:   0
(Current) Groups:    0

Enabled Characteristics:
Autoconnect, Autoprompt, Broadcast, DSRlogout, Failover,
Inactivity Logout, Input Flow Control, Lock, Loss Notification,
Message Codes, Output Flow Control, PPP, SLIP, Verification
Local>
```

Assigning a Dialer Script to a Port

Use the SET/DEFINE/CHANGE PORT n DIALER SCRIPT command to assign a dialer script to a port.

Example: Defining the Dialer Script

The following example shows how to assign the dialer script dickens to port 2. After you enter this command and initialize the access server, the SHOW PORT display for port 2 will reflect this change.

```
Local> DEFINE PORT 2 DIALER SCRIPT dickens
```

Verifying Dialer Script Configuration

Use the SHOW PORT n command to verify any changes you make to dialer script assignments for a port. The change appears in the Dialer Script field of the display.

Example: Show New Port Configuration

The following example shows the display after using the CHANGE PORT n DIALER SCRIPT command to change the dialer script from Generic_14400 to dickens:

```
Local> CHANGE PORT 2 DIALER SCRIPT dickens
Local> SHOW PORT 2

Port 2:                    Server:               user10_DS700-16

Character Size:        8   Input Speed:                   57600
Flow Control:        XON   Output Speed:                  57600
Parity:             None   Signal Control:              Enabled
Stop Bits:       Dynamic   Signal Select:        CTS-DSR-RTS-DTR

Access: Dynamic    Local   Switch:                        None
Backwards Switch:   None   Name:                       PORT_2
Break:             Local   Session Limit:                   4
Forwards Switch:    None   Type:                        Ansi
Default Protocol:   DIAL   Default Menu:                  None
                           Dialer Script:               dickens
Preferred Service: CALL_HOME

Authorized Groups:   0
(Current) Groups:    0

Enabled Characteristics:
Autoconnect, Autoprompt, Broadcast, DSRlogout, Failover,
Inactivity Logout, Input Flow Control, Lock, Loss Notification,
Message Codes, Output Flow Control, PPP, SLIP, Verification
Local>
```

Defining the Dialer Service

Steps

After you define the dialer script and assign the dialer script to a port, define the dialer service. A dial service is used to establish a dial-back session. Do the following:

Step	Action
1	Display information (characteristics, status, and counters) about currently configured dialer services and system status.
2	Define or modify the dialer service using the SET/DEFINE/CHANGE DIAL SCRIPT SERVICE command.

Showing the Current Dialer Service Characteristics

Use the SHOW/LIST/MONITOR DIALER SERVICE service-name CHARACTERISTICS command to display dialer service characteristics. These commands are similar to the SHOW SERVICES LOCAL family of commands in usage and syntax.

The examples in this section show instances of using the SHOW command only. The use of the LIST and MONITOR commands is implied, since these commands produce similar results in the screen display. They differ in the effect that they have on storage of data in VRAM and NVRAM.

Reference

For more information on command line syntax, see the Commands to Display and Change Configuration Settings section in Chapter 1.

Example: Show Dialer, Port Security Enabled

In this example, a user on a port with SECURITY enabled would not have access to the STATUS display since it might provide access to unlisted or sensitive phone numbers and other information received from the modem.

```
Local> SHOW DIALER AT_TRADESHOW CHARACTERISTICS

Dial Service:        AT_TRADESHOW
Identification:      Dial-back from tradeshow

Connections:         Enabled
Ports:               1,2,9-14
Phone number:        555-6766
Delay (seconds):     15
Mode:                PPP
Username:            None
Password:            None

Local>
```

Showing Dialer Service Status

Use the SHOW / LIST / MONITOR DIALER SERVICE service-name STATUS command to display dialer service status. These commands are similar to the SHOW SERVICES LOCAL family of commands in usage and syntax.

Example: Show Dialer Status

In following example, port 10 is currently available; the last phone number it dialed was found to be busy. Ports 9 and 11 are presently in use. Port 13 is actually dialing a phone number, while port 14 is waiting for a response from the modem. When the dialer port is initialized prior to making a phone call, the Last Connection Status field is cleared.

```
Local> SHOW DIALER AT_TRADESHOW STATUS

Dial Service: AT_TRADESHOW - Available Identification: Dial-back
from tradeshow

Port:   User          Status                Last Connection Status

9       (remote)      Connected               CONNECTED 14400/LAPM
10      Available     BUSY
11      Raymond       Connect                       CONNECTED 9600
12                    Available                          NO ANSWER
13      Jim Dialing                                      No answer
14      Bob           Waiting

Local>
```

SHOW DIALER STATUS Display Fields

The following table lists values for the status field in the SHOW DIALER display:

Status	Meaning
Initializing	Sending dialer command and authorization strings.
Dialing	Sending the phone number string.
Waiting	Waiting for the expected response from mode.
Connected	Dialer call completed, port is in use.
Available	Dialer is not in use.

Displaying Dialer Counters

Use the SHOW DIALER service-name COUNTERS command to display the counters for a dialer service.

Example: Show Dialer Counters

The following example shows the dialer service counters display for the dialer service AT_TRADESHOW:

```
Local> SHOW DIALER AT_TRADESHOW COUNTERS

Dial Service:        AT_TRADESHOW

Seconds Since Zeroed:  1989692   Failures:               17
Connections Attempted: 113       Busy:                   10
Connections Completed: 96        No Answer:               0
No Dial Tone:          0         No Response:             0
No Carrier:            0         Authentication:          7
Unknown:               0

Local>
```

Modifying the Dialer Service

Use the SET / DEFINE / CHANGE DIALER SERVICE dialer-service-name command to define the dialer service. The dialer-service-name characteristic is a string of 1 to 16 characters.

The dialer service name must be unique to the server. Before you create a new dialer service, use the SHOW DIALER SERVICE command to verify that the new name does not conflict with that of an existing dialer service.

For a detailed explanation of command keywords used to mange dialer services, see the Command Definitions section in Chapter 2.

Example: Change Dialer Name

The following example uses many of the keyword options in the command line:

```
Local> CHANGE DIALER on_the_road PORT 4-9 IDENT "Dial-back"
Local> CHANGE DIALER on_the_road NUMBER "*" MODE *
```

Dialer Service Characteristics

The following table describes the dialer service characteristics:

Characteristic	Description	Comments
IDENTIFICATION	Allows an identifying string to be associated with a given service.	Maximum length = 40 characters
CONNECTIONS	Specifies whether a user may connect to the current dial service.	Variables: ENABLED / DISABLED
PORTS	One or more physical ports that are to offer this dial service.	-
NUMBER	Indicates the allowable phone number(s) for use with this service.	Maximum length = 48 characters Variables: "*" / ONLY Default = "*" • "*" — Means users may use any number within their security constraints, and are prompted to enter a phone number when initiating a dialer session. • ONLY — Designates the sole phone number that may be dialed using this service.

User Account Characteristics

The following table explains the user account characteristics:

Characteristic	Description	Comments
DELAY	Indicates the delay in seconds before the dialer engine should attempt to initiate the dial-back.	Default = 30 seconds Minimum = 15 seconds Maximum = 3600 seconds (1 hour)
USERNAME	Defines the user name to be supplied to a peer that requires the access server to be authenticated.	Maximum length = 1 to 16 characters
PASSWORD	Indicates the password to be supplied to a peer that requires authentication from the access server.	Maximum length = 1 to 16 characters • May be entered either on the command line within quotes or at a prompt. • If PASSWORD is the last word on the command line, the user is prompted for a password. • DNAS masks the password string upon entry.
MODE	Indicates the type of session the dial service will create after successfully completing the modem connection.	Variables: LOCAL / LOGIN / PPP / SLIP / *

MODE Command Variables

The following table explains the MODE command variables:

Variable	Definition
LOCAL	Interactive nondedicated session.
LOGIN	Interactive dedicated session to a host.
PPP	Dedicated PPP session.
SLIP	Dedicated SLIP session
*	Any mode allowed

Configuring Interactive Dial Requests

Configuring for Interactive Dial-Back

The following example sets the access server to a predefined phone number:

```
Local> CHANGE DIALER AT_HOME PORT 1-16 IDENT "DIALS YOU AT HOME"
```

The dialer service AT_HOME is set up to allow any phone number to be dialed, but the user's security profile allows for a connection to be made using only one number.

The ports are all set up to be ACCESS DYNAMIC, so they can be used for dial-in and also dial-back.

The user dials in, enters his user name and password, and is successfully authenticated.

As a result, the security component creates and maintains an authorization profile for this user. This authorization profile, which is also known as the active user database, contains among other things the phone number(s) that the user is authorized to use on a dial-back request.

Security Profile Information

For more information about user security profiles, see the user accounts information in the Determining Security Configuration section in Chapter 22.

Interactive Dial-Back (Dial Service) Example

The following example shows how the user specifies a dialer service and how the service operates:

```
Local> DIAL AT_HOME
Local -019- Dial request queued, will be attempted in 30 seconds
Local> LOGOUT
Local -020- Logged out port 10 on server NAS700
```

In this example, the access server uses a security realm (RADIUS, or local profile) for authorization when the user logs in. The user's RADIUS/local profile is maintained while the user is logged in. The profile is checked to see if the user is authorized for dial-back. In this particular example, the authorization database has but a single phone number that the access server would use when calling back this particular user.

Framed Dial Requests

Introduction

Dial-back requests can also be queued from a client that connects to the server using PPP. Unlike PPP, the SLIP protocol does not include a method of negotiating connection options including whether a call-back should be attempted and the phone number to which the call-back should be placed. Therefore, only PPP clients can request a call-back.

Changing PPP Characteristics Examples

In the following paragraphs, the default protocol for the access server's port is assumed to be set to PPP.

Configuring Dynamic Access

If the modem on that port will be used for both the incoming and the outgoing calls, the port must allow dynamic access, as shown in the following example:

```
Local> CHANGE PORT n DEFAULT PROTOCOL PPP
Local> CHANGE PORT n ACCESS DYNAMIC
```

Configuring Call-Back

To request a call-back using a PPP client, the access server's port must first allow the call-back negotiation to be started. This is done using the command:

```
Local> CHANGE PORT n LCP CALLBACK ENABLED
```

If the PPP client and the access server successfully negotiate the use of call-back, the access server will attempt to queue a dial request. The port must be set dedicated to the dialer service to be used in placing the return phone call.

```
Local> CHANGE PORT n DEDICATED SERVICE dialer-service-name
```

Guidelines

1. If you do not specify a service name, the port's preferred service is used. If the preferred service contains "*" as the number specified in the dialer service, the access server prompts the user to enter a telephone number.

2. For a PPP connection, the port is usually set to have a dedicated service name of PPP. However, as long as the port's default protocol is set to PPP, you can specify any dedicated service name.

3. If you enable PPP call-back negotiation on a port, DIGITAL strongly recommends that you also enable some sort of authentication (for example PAP or CHAP) on the port. Without authentication, any user who happens to discover the phone number for that port's modem could potentially request a call-back and run up unlimited phone charges.

4. To enable authentication on a port, use the SET/DEFINE/CHANGE PORT LCP AUTHENTICATION PAP/CHAP command.

5. If the PPP client specified a phone number to which the return call is to be placed, this phone number is also included in the dial request along with the name of the dialer service. If the PPP client did not specify a phone number, the phone number to be used is determined by the dialer service or the user's authorization information.

6. If a service name is specified that does not match an existing dialer service, the call-back will fail and an accounting event will be generated.

7. Whether the phone number to be dialed comes from the PPP client or the dialer service definition, the user making the request must be authorized to dial that number. Likewise, the user must be allowed to create sessions of the mode defined by the dialer service, either interactive or framed. If the user is not authorized to either dial the selected phone number or create sessions of the mode specified by the dialer service, the call-back fails and an accounting event is generated.

8. Unlike interactive dial requests, which require the user to log off the server and hang up the client's modem in anticipation of a return call from the server, successful PPP call-back negotiation results in the initial PPP session being automatically disconnected. This also breaks the modem's connection and results in the PPP client hanging up the phone, making it available for the return call from the server.

Chapter 23

Managing Access Server Security

Overview

Introduction

The Cabletron Network Access Software (CNAS) supports the following authentication services:

- RADIUS
- SecurID
- Local User Accounts
- Kerberos V4

In This Chapter

This chapter contains the following topics:

Security Type Descriptions

Introduction

This section describes the types of security that the access server supports.

Kerberos

Kerberos is a user authentication system designed for open network computing environments. It provides for the authentication of a user name and password pair, by means of a host system accessible over the network. Once the user name and password pair is verified, the access server assigns any default authorization that identify the access server services allowed for that user's session.

Realm Definition

Associated with a Kerberos login, a user specifies a realm. A realm is known by its realm name, a printable string of characters. The realm name identifies an administrative domain, and a set of realm parameters that are needed to administrate the logins for that realm. The administrator can also associate many other access server related parameters with a realm name.

The SHOW KERBEROS REALM realm-name command displays all the assignable parameters for all Kerberos realms. Realm definition and usage is the same for all other security methods supported by the access server, as are the characteristics that realms allow the administrator to define.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a security method that provides authorization information during the authentication procedure. Authorization information is a means for tailoring most of the configurable features of the access server to a particular user name. The authorization characteristics are not stored on the access server, but are embedded in the database that exists on the security host serving as the RADIUS authenticator. This chapter describes the RADIUS authorization attributes that the access server supports. See the Managing RADIUS section in this chapter.

For more information about the DECserver's implementation of RADIUS Accounting RFC 2139, see the DECserver RADIUS Survival Guide that is included as an ASCII text file in your media distribution kit.

SecurID

SecurID is a system of authentication from Security Dynamics Technologies, Inc. There is no authorization information at the SecurID authentication host. Like Kerberos, the SecurID realm provides values for realm-defined parameters.

Once the password has been accepted, its processing is analogous to the Kerberos method. However, the resulting “authorization” parameters with SecurID, are the combination of the realm parameters and the port configuration parameters.

User Accounts

User accounts provide a method of defining user name and password pairs, and associated authorization parameters. User account information resides on the access server. This is convenient method for supporting multiple administrative roles that are fully self-contained on the access server.

Local user accounts support the Password Authentication Protocol (PAP) and the Challenge Handshake Authorization Protocol (CHAP) Point-to-Point Protocol (PPP). The local user accounts also support interactive username and password authentication. Limited authorization information may also be configured for each account. This feature is designed for small sites or for back-up access by the network administrator.

Common Terminology Across Security Realms

Introduction

This section briefly defines the terms that are common to all of the security methods that the access server supports.

Accounting Host

A security server that accepts and records accounting information from the access server.

Authentication Host

A security server that provides authentication or authorization information to the access server.

Default Realm

One realm in the access server can be specified to be the default realm. The only advantage of the default realm is that, when logging in, the user can omit the @realm-name portion of the login identification. There is no other special meaning to be the default realm. To change the default realm name, you must first set any current (default) realm name to be NODEFAULT. Then assign another as DEFAULT.

Login Retries and Timeouts

The access server allows you to configure the number of times to retry contacting a server before timing out a login attempt.You can specify the maximum number of retries to potentially alternate authentication hosts. Hosts are tried round-robin fashion until the login attempt times out. Each realm can point to its own list of security hosts.

Secrets

A text string or value that ensures that the data exchanged between the access server and the security host is valid. You must configure a secret on the access server for RADIUS. You can also configure one for Kerberos. The secret for SecurID will automatically be assigned by the SecurID authentication host.

Once configured, the secret is never displayed on the access server. There are privileged access server commands to erase and to reenter secrets. The secret is assigned as a realm parameter, and applies to all security hosts in the realm.

Security Server

The remote host with which the access server communicates in order to request authentication clearance during the login process. Each security method (other than user accounts) defines one or more host processors that can support the authentication procedure.

RADIUS Accounting

The RADIUS security method supports logging of accounting information. The accounting information is sent to what is called the accounting host by means of the accounting service port.

UDP Ports

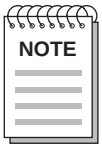
Each security method has a well-known port (or two) that must be specified to the access server in order for the UDP connection to be established. When you create a new realm, it is not usable until you define a secret (and at least one authentication host) for it. However, the realm will be created with default values (the well-known ports) for the UDP ports.

Managing Kerberos

Introduction

This section describes Kerberos security features and explains how to configure and manage these features on the access server. To use the procedures in this section, you must:

- Ensure that the access server can communicate with a host running Kerberos V4 software.
- Connect and test the devices.
- Enable privileged status.
- Configure the port and device characteristics to match.



Refer to the access server hardware documentation for information about connecting device cables. This section assumes that you have a basic understanding of Kerberos.

Configuration Prerequisites

This section describes the prerequisites for configuring the Kerberos security features on an access server.

Kerberos Host Requirements

- To use Kerberos authentication, the access server must be able to communicate over the network with a host that functions as a Kerberos V4 key distribution center (KDC). The key distribution center is an UNIX host that runs Kerberos software and contains a database of valid user names and passwords. The access server does not authenticate using the Kerberos V5 protocol.
- To operate with the highest level of security, the access server must be registered with all KDCs within the Kerberos realms in which user authentication will take place. A realm refers to a group of hosts that share a common administrative domain for purposes of user authentication.
- Each realm has one master KDC that contains a write-enabled database. The master KDC propagates its database to any slave KDCs in the same realm.

  A basic mode of operation is also available in which the access server does not need to be registered in any of the realms. This mode of operation is less secure, but easier to configure.

Network Access Server Requirements

Before configuring security-specific parameters, make sure that:

- You have entered the correct Internet address and subnet mask. (See the Configuring the Internet Address and Subnet Mask section in Chapter 7.)
- There is an Internet gateway to the KDC if the KDC is not on the access server subnet. (See the Defining Networks Available Through a Specific Gateway section in Chapter 7.)
- The DNS parameters are set correctly if Internet hosts are not explicitly configured on the access server. (See the Displaying the DNS Counters section in Chapter 7.)

Configuration of User Authentication

The configuration of user authentication on the access server involves entering several commands shown in the examples in this section. For details about command syntax, refer to the Cabletron *Network Access Software Command Reference* guide.

Case Sensitivity

Kerberos user names, instances, realms, and passwords are case sensitive.

Configuring Kerberos Settings

When you set up the access server for user authentication, you need to complete the following steps:

Step	Action
1	Specify a realm and a KDC.
2	If the default is incompatible with the KDCs in your realm, specify the TCP port numbers on the KDC to which the access server sends messages for password changes and ticket requests.
3	Change the default timeout if you want to do so.

Example: Definition of Kerberos Settings

The following example shows a sample of the commands used to change these settings:

```
Local> CHANGE KERBEROS DEFAULT REALM finance.acme.com SECRET
Secret> (not echoed)
Verification> (not echoed)
Local> CHANGE KERBEROS REALM finance.acme.com MASTER HOST security.acme.com
Local> CHANGE KERBEROS REALM finance.acme.com HOST atlas.acme.com
Local> CHANGE KERBEROS PASSWORD SERVICE PORT 89
Local> CHANGE KERBEROS TICKET PORT SERVICE PORT 88
Local> CHANGE KERBEROS TIMEOUT 20
```

This example shows the more secure Kerberos configuration. The access server itself is registered in the realm:

```
finance.acme.com
```

The access server user name is always “rcmd” while its instance is the same as its server name. In previous example, if the server name is LAT_08002B010203, then the Kerberos principal name is:

```
rcmd.LAT_08002B010203@finance.acme.com
```

The access server Kerberos password is the value of SECRET:

```
thisiswhereallthemoneyis
```

To perform authentication, the Kerberos system administrator must register the access server Kerberos user name, instance, and password in the master KDC for each of the realms. If the administrator does not specify a SECRET value in the access server database, then the access server can perform user authentication without being registered in the realm.

Displaying Kerberos Settings

The following example shows a sample display of Kerberos settings:

```
Local> show kerb characteristics

Retransmit Interval:                Retransmit Timeout: 0 00:00:08
Ticket service port: 750            Password service port:     751

Realm:              mfg.acme.com
 Secret:            (None)
 Authorization Defaults:
  Access:           (None)         Forced Callback:      DISABLED
  Max Connect:      (None)         Dialout Service:        (None)
  Dialback Number:  6111
  Dialout Number:   (None)
  Permissions: DIALBACK, DIALOUT, LAT, TELNET, SLIP, PPP, NOPRIV
```

Port Configuration

You need to configure user authentication on the access server on a port-by-port basis. To enable the authentication on a given port, you enter a command such as:

```
Local> DEFINE PORT 2 AUTHENTICATION ENABLED
```

Example: Sample SHOW PORT Command

After enabling authentication on a port, you can then display the port settings to verify that user authentication is enabled as shown in the following example:

```
Local> SHOW PORT 1

Port 1:          smith          Server:           TSM700
.
.
.
Enabled Characteristics:
Authentication, Autoconnect, Autoprompt, Broadcast,
Failover, Input Flow Control, Lock, Loss Notification,
Message Codes, Output Flow Control, Lock Notification,
Verification
```

User Authentication Procedure

When the system administrator configures Kerberos security features for a given access server port, you need to enter a valid user name and password when you log on to the access server. A complete Kerberos principal name has the following format:

user-name[.instance]@realm-name

To abort the authentication process, press the Break key or the Local Switch key. By default, Kerberos allows you three attempts to enter a valid user name and password. After three unsuccessful attempts to enter a user name and password, the access server disables the authentication procedure on the port for a period of 1 minute.

To change the default number of invalid authentication attempts, use the SET PASSWORD LIMIT command.

Example: Authentication with a Complete User Name

The following example shows a typical user authentication that uses the complete form of the Kerberos principal name. This session assumes that the Kerberos administrator has entered your user name and password in the Kerberos database.

```
Username> smith.su@finance.acme.com
Password> (not echoed)
Local - 450 - Attempting to authenticate user:smith.su@finance.acme.com
Local - 451 - Authentication successful
Local>
```

Example: Authentication Using the First Portion of the User Name

If a default realm is configured, you have to enter only the first portion of the user name as shown in the following example:

```
Username> smith
Password> (not echoed)
Local - 450 - Attempting to authenticate user: smith@finance.acme.com
Local - 451 - Authentication successful
Local>
```

Changing a User Name and Password

Once the network manager has set up the access server, users can change their own passwords on the master KDC for their realm.

Example: Sample Kerberos User Authentication Session

The following example shows a sample session for changing a password. The way that message 468 wraps may appear differently on your terminal screen.

```
Local> kpasswd
Username> smith
Old password>  oldpassword (not echoed)
New password>  newpassword (not echoed)
Verification>  newpassword (not echoed)
Local -468- Attempting to change Kerberos password for user smith@finance.acme.com
Local -469- Kerberos password has been changed
Local>
```

Alternative Password Command

Instead of the KPASSWD command, you can also use the DEFINE KERBEROS PASSWORD COMMAND as described in the Cabletron *Network Access Software Command Reference* guide.

User Authentication Counters

This section describes the user authentication counters. These counters display information that is useful for detecting problems.

Network Access Server User Authentication Counters

The following example shows how to display the user authentication counters for the access server:

```
Local> SHOW SERVER AUTHENTICATION COUNTERS
                                                  Total    Total
                                                  attempts failures

User authentication (all realms):                    16       0


                                      Total       Valid    Error
                                      Packets     Packets  Packets
                                      Sent        Received Received
Realm: mfg.acme.com                     8           8          0
Realm: sales.acme.com                   7           6          1
Realm: finance.acme.com                 1           1          0
Time since counters last zeroed:                       1 01:55:14
```

Port User Authentication Counters

The following example shows how to display the authentication counters for a given port:

```
Local> SHOW PORT 1 AUTHENTICATION COUNTERS

Port 1:         j_smith              Server:          Finance_server

                        Cur. login   Cur. login  Total     Total
                        attempts:    failures:   attempts: failures:
User authentication:       1            0           4          0
Time since last user authentication success:                0 00:52:32
Time since last user authentication failure:                     never
Time since counters last zeroed:                          1 01:50:28
```

Setting the User Authentication Counters to Zero

The user authentication counters add up until you explicitly reset them. To reset user authentication counters for the server to 0, use the following command:

```
Local> ZERO SERVER AUTHENTICATION COUNTERS
```

You can reset the user authentication counters for an individual port, a group of ports, or all ports. For example, the following command resets the user authentications counters to 0 for ports 2, 3, and 5:

```
Local> ZERO PORT 2,3,5 AUTHENTICATION COUNTERS
```

Managing RADIUS

Introduction

A RADIUS server must be operational on the network. The RADIUS server can include accounting capability, but the RADIUS accounting can be in a separate server, on a different node. In addition, there can be multiple RADIUS servers on the network, and RADIUS provides a method for using a second server should the attempt with the first server result in no response.

A node that has the RADIUS server is considered an authentication host. A node that has a RADIUS accounting server is considered an accounting host.

RADIUS security involves the definition on the access server of one or more RADIUS realms. A realm is an administrative domain for the purpose of authentication which can supply default values for many attributes associated with RADIUS access and usage. Each RADIUS realm points to its own associated RADIUS authenticating host and accounting host.

Minimal Setup for RADIUS

The minimal configuration requires the following commands to set up the remote ports used for communication with the RADIUS server(s). These features must be assigned in order for any communication with a RADIUS server or a RADIUS accounting server to take place.

- The following example shows the commands used to set up RADIUS security:

  ```
  Local> CHANGE RADIUS REALM JONAS.COM
  ```

- This command defines/initializes a new RADIUS realm:

  ```
  Local> CHANGE RADIUS REALM JONAS.COM AUTHEN HOST ip-addr
  ```

- This command defines RADIUS server authentication node:

  ```
  Local> CHANGE RADIUS REALM JONAS.COM SECRET " secret_string"
  ```

Variables

Words in examples in italics indicate user-supplied variables. In this case, the variable `JONAS.COM` is the name of the specific realm on which you want to perform this action.

Optional Setup for RADIUS

You can use the commands in the following examples to configure additional security parameters for RADIUS servers. The commands in these examples define a RADIUS server accounting node, the maximum timeout period for RADIUS server reply, and the interval between retries of an authentication request.

- The following command defines a RADIUS server accounting node:

  ```
  Local> CHANGE RADIUS REALM JONAS.COM ACCOUNTING HOST ip-addr
  ```

- This command defines the maximum timeout for RADIUS server reply:

  ```
  Local> CHANGE RADIUS TIMEOUT seconds
  ```

- This command defines how much time elapses before using an alternate server:

  ```
  Local> CHANGE RADIUS INTERVAL seconds
  ```

  Setting the INTERVAL variable defines the time period (in seconds) that the system is to wait before repeating an authentication request to an alternate authentication server.

- This command causes the realm name to be included as part of a user name sent to the RADIUS server:

  ```
  Local> CHANGE RADIUS REALM JONAS.COM INCLUDE
  ```

  Realm name inclusion is used for RADIUS proxy authentication service.

Reference

See the Cabletron *Network Access Software Command Reference* guide for more information on these commands.

Example: Including the Realm Name

If your realm name has to be included when the access server sends messages to the RADIUS server, issue the command shown in the following example:

```
Local> CHANGE RADIUS REALM JONAS.COM INCLUDE
```

For most usage, you will not want to include the realm name. If you do, each entry in the RADIUS server's users file will have to appear as "user-name@realm-name" instead of simply "user-name".

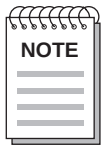
If a user has to be called back, this value is derived from User-Service-Type when specified. If it is not specified, then realm defaults / port defaults can apply:

Example: Defining Realm Default Authorization Attributes

```
Local> CHANGE RADIUS REALM JONAS.COM PERMISSIONS (DIALBACK)
Local> CHANGE RADIUS REALM JONAS.COM CALLBACK ENABLED DIALBACK NUMBER "1-800-555-1111"
```

Example: Defining Password Authentication Type

```
Local> CHANGE RADIUS REALM JONAS.COM ACCESS FRAMED
```



The value NONE should be read as unspecified. This allows the port configuration to determine the access whenever the RADIUS server's user entry does not specify one or more authorization attribute.

RADIUS Authorization

When a user attempts to log in using a realm, the user enters a string in the following format:

```
user-name@realm-name
```

The following occurs:

Stage	Description
1	The access server used the realm name to determine the security method to use when authenticating the login.
2	If the realm name is for a RADIUS server, the access server sends the login information to a RADIUS authentication host.
3	Upon completing authentication successfully, the RADIUS authentication host sends a list of authorization parameters to the access server after authentication completes successfully. These parameters are the intended settings for the user's session.

Since the set of attributes that the RADIUS authentication host sends to the access server can be incomplete, you can set default realm authorization parameters that provide missing values to complete the authorization set. If a parameter is missing from both the RADIUS authorization parameters and from the realm's default parameters, and the parameter is defined within the port configuration information, the port supplies the value for the parameter. This resulting set of parameters is the "authorization" information used for this session.

RADIUS User Authorizations

The ultimate value for an authorization attribute may come from one of three sources: the RADIUS server, the realm defaults, or port characteristics, in that order of precedence. The choices for such features are:

1. For each RADIUS realm name you define, you can set various authorization attributes for that realm. These values serve as defaults at the realm level. This means, that when a RADIUS user tries to login to the access server, these values will be assigned to authorization attributes if the user entry in the RADIUS server's users file does not assign a value for the corresponding attribute. If the user does not provide the attribute default in the realm, and the corresponding attribute is not provided in the RADIUS server's users file, then the access server's port characteristics are used if they have been previously defined.

2. One of the legal settings of the attributes in the realm is NONE. This special value connotes unspecified. In this case, when a user attempts to log in, if the value is not specified in the RADIUS server's entry for the user name, and has the value NONE in the REALM, then the PORT configuration parameter assigns the corresponding value.

   The resulting value may still be unspecified, if the corresponding port characteristic is unspecified or does not exist. Only a portion of the RADIUS authorization attributes have a corresponding realm default or corresponding port attribute.

User Access to the Access Server

The primary way to define a user's type of access is to use the RADIUS server attribute called "User-Service-Type". The following table shows User-Service-Type values that the access server supports:

Value	Description
Login	LAT/TELNET, depending on the Login-Service attribute or DEFAULT PROTOCOL value in PORT.
Framed	PPP/SLIP, depending on the Framed-Protocol attribute or DEFAULT PROTOCOL value in PORT.
Callback-Login	User is first called back, then gets login.
Callback-Framed	PPP/SLIP user is first called back.
Administrative-User	NAS prompt with automatic privilege.

Value	Description
NAS-Prompt	Access server's command or menu prompt.
Callback-NAS-Prompt	Callback first, then NAS prompt.

Setting User Permissions

Permissions are explicitly given by the authorizations that were in the user-name entry in the RADIUS server's authentication entry. When any attributes that may be appropriate are missing, an attempt is made to find a specified value in the realm defaults. When these are still missing, the port configuration can supply its specified values (for attributes having a corresponding representation in the port).

Permissions are from a DIGITAL vendor-specific RADIUS attribute. The following is a list of RADUIS permissions:

DIALOUT NODIALOUT

LAT NOLAT

TELNET NOTELNET

SLIP NOSLIP

PPP NOPPP

PRIVILEGED NOPRIVILEGED (level of access server command privilege)

For each of the these attributes, the default is NOxxx or DISABLED.

Additional RADIUS Attributes

The tables in this section contain lists of additional RADIUS attributes that the access server supports.

General Session Attributes

The following table defines the general session RADIUS attributes:

General Session Attributes	Definition
Service-Type	Type of link requested, or change in type of link. Used in both Access-Request and Access-Accept packets. • Login — Delivers a dedicated connection to the specified host, using the specified protocol (Telnet, rlogin, LAT). • Framed — Delivers a network (framed) protocol connection (PPP, SLIP). • Callback-Login. • Callback-Framed. • Administrative User — Delivers a NAS prompt with automatic privilege status. • NAS-Prompt — Delivers the NAS user interface. • Callback-NAS-Prompt.
Session-Timeout	Indicates the maximum number of seconds of service to be provided to the user, before (mandatory) termination of the session. Used in Access-Accept packets.
Idle-Timeout	Indicates the maximum number of consecutive seconds of idle connection allowed to the user before (mandatory) termination of the session. Used in Access-Accept packets.

Framed Session Attributes

The following table defines the framed session attributes:

Framed Session Attributes	Definition
Framed-Protocol	Type of framed protocol used for session. Used in Access-Accept packets. Values: • PPP • SLIP
Framed-IP-Address	IP address to be configured for the user (in lieu of DHCP, or similar). Used in Access-Accept packets. Note: Two values of this address require special action: • The value 255.255.255.255 means that the PPP client should be allowed to negotiate the use of its local IP address via IPCP, subject to the access server's subnet containment rules. • The value 255.255.255.254 means that PPP or SLIP client should be assigned the port's PPP address, if one exists. Nonspecial cases would equate to: `SET PORT SLIP HOST ADDRESS` *`ip-addr`* `SET PORT IPCP HOST ADDRESS` *`ip-addr`*
Callback-Number	Indicates the phone number to be called, after the user has been disconnected. This attribute is formatted as a printable ASCII string, typically containing the characters that would follow the “ATDT” modem command.

Interactive Session Attributes

The following table defines the interactive session attributes:

Interactive session attributes	Definition
Login-IP-Host	The IP address of the host system with which the user is to be automatically connected. Used in Access-Accept packets.
Login-Service	The type of service to which the user is to be automatically connected. Used in Access-Accept packets. Values: • Telnet • LAT

Interactive session attributes	Definition
Login-Port	Indicates the TCP (or LAT) port number to which the user is to be automatically connected. Used in Access-Accept packets.
Login-LAT-Service	Indicates the LAT service name to which the user is to be automatically connected, via LAT. Used in Access-Accept packets, when the Login-Service type is LAT.
Login-LAT-Node	Indicates the node, within the specified service, to which the user is to be automatically connected, via LAT. Used in Access-Accept packets, when the Login-Service type is LAT, and a Login-LAT-Service is specified.
Login-LAT-Groups	Indicates the LAT group codes which the user is authorized to use. Used in Access-Accept packets, when the Login-Service type is LAT.

RADIUS General Non-Session Attributes

The following table defines the RADIUS general non-session attributes:

RADIUS Overhead Attributes	Definition
NAS-IP-Address	IP address of the NAS. Used in Access-Request packets.
NAS-Port	NAS Port Number. Used in Access-Request packets.
Reply-Message	ASCII text, that the NAS may optionally display. Used in Access-Accept, Access-Reject, or Access-Challenge packets.
State	Opaque data sent from the server to the client in an Access-Challenge packet, to be sent back to the server by the client in a new Access-Request packet. Needed to support challenge / response forms of authentication.
Class	Opaque data sent from the server to the client in a Access-Accept packet, to be sent to the accounting server by the client in a Accounting-Request packet. Needed to support RADIUS accounting.
Vendor-Specific	Vendor-specific data, prefixed by the assigned vendor OID. Used in all but Access-Reject packets. Please refer to the following table for a list of the vendor-specific attributes.

DIGITAL Vendor-Specific Attributes

The following table defines the vendor-specific attributes implemented in CNAS:

DIGITAL Vendor-Specific Attributes	
Service Permissions(1)	V-Type — 1 for service permissions. V-Length >= 3 Integer — The value field is 4 octets. The value is formatted as a bit map.
Dialout Number (2)	V-Type — 2 for dialout number. V-Length >= 3 String — Any printable ASCII characters.
Dialback Number (3)	V-Type — 3 for dialback number. V-Length >= 3 String — Any printable ASCII characters.
Dialout Service (4)	V-Type — 4 for dialout service name. V-Length >= 3 String — Uppercase ASCII printable characters, starting with a letter.

RADIUS Accounting Attributes

The following table defines the RADIUS accounting attributes:

RADIUS Accounting Attributes	Definition
Acct-Status-Type	One of the following types of accounting information: • Start • Stop • Accounting-On • Accounting-Off • Checkpoint
Acct-Delay-Time	The amount of relative time from the origination of the accounting information until the transmission (or retransmission) of the accounting packet.
Acct-Input-Octets	The number of bytes received on the port during the delivery of service.
Acct-Output-Octets	The number of bytes transmitted on the port during the delivery of service.

RADIUS Accounting Attributes	Definition
Acct-Session-Id	A unique accounting session ID, preferably related to the access server accounting log.
Acct-Authentic	An indication of the means of authentication for this user: • RADIUS • Local (the User Data Base) • Remote (the Kerberos or SecurID client)
Acct-Session-Time	The number of seconds for which the service was delivered to the user.

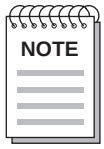
The Cabletron Network Access Software now reports a number of termination reason codes to the RADIUS Server when user sessions are completed. Termination reason codes can be helpful for network troubleshooting and include informational messages, such as:

- Lost carrier
- Idle time
- User request
- NAS error

Optional RADIUS User Attributes

The RADIUS attributes that the access server supports are as follows:

Session-Timeout	Login-Port
Idle-Timeout	Login-LAT-Service
Framed-Protocol	Login-LAT-Node
Framed-IP-Address	Login-LAT-Groups
Callback-Number	NAS-IP-Address
Login-IP-Host	NAS-Port
Login-Service (Telnet, LAT)	Vendor-Specific



Other RADIUS attributes (particularly accounting attributes) are utilized internally between the RADIUS server or accounting server and the access server, which are independent of authorization attributes.

Managing SecurID

Introduction

The Security Dynamics ACE/Server software performs dynamic two-factor SecurID authentication. Dynamic two-factor authentication combines something the user knows—a memorized personal identification number (PIN)—with something the user possesses—a randomly generated access code that changes every 60 seconds. The second factor is the tokencode generated by the SecurID token. This combination of PIN and tokencode represents a one-time passcode and is transmitted to the ACE/Server software for verification.

The ACE/Server security environment is composed of four components. These are:

1. ACE/Server software running on a UNIX platform
2. (Optional) slave ACE/Server software running on a UNIX platform
3. Access server running CNAS V2.0 or greater
4. SecurID tokens utilized by users when they attempt to access the ACE/Server protected ACE/Clients

SecurID utilizes two types of hosts: master and slave. When setting up a SecurID realm, specify the master host by using the command SET PRIMARY host-name. You can specify the slave host using the command SET HOST host-name. Although the access server does allow you to configure multiple slave hosts, you should not do this.

Using the SECRET Keyword

The SECRET in the SecurID REALM is not specified by the user, but rather is filled in the first time the realm is used to authenticate a user. After that, you can clear it by using the NOSECRET qualifier in the CHANGE SECURID REALM command. If you clear it or if you delete the realm and then re-create it, you must reset the client on the authentication server side using the SecurID server administrator program.

SecurID Prompts

The default prompt for SecurID is ENTER PASSCODE>. This default is set when you create a new realm. This is the standard SecurID prompt.

SecurID Ports

Normally, you do not need to change the SecurID master and slave SERVICE PORT. If the default values do not match with those assigned on your hosts, then change the values in the access server to match those on the hosts.

SecurID Realms

SecurID servers do not provide any authorization data; therefore, any authorization information comes from the SecurID realm or the port characteristics.

If a SecurID card is in a new PIN mode and the new PIN is coming from the access server, the new pin is displayed for 10 seconds and then erased.

Minimal Setup for SecurID

The minimal configuration requires the following commands to set up the remote ports used for communication with SecurID. These features must be assigned in order for any communication with SecurID or SecurID accounting to take place.

- The following example shows the command used to set up SecurID security:

  ```
  Local> CHANGE SECURID REALM realm-name
  ```

- This command defines and initializes a new SecurID realm:

  ```
  Local> CHANGE SECURID REALM JONAS.COM AUTHEN HOST ip-addr
  ```

Optional Setup for SecurID

The commands in the following example can be used to configure additional security parameters for SecurID. The commands in these examples will define a SecurID accounting node, define the maximum timeout period for SecurID reply, and define the interval between retries of an authentication request.

```
Local> CHANGE SECURID TIMEOUT seconds
```

This command defines the maximum timeout for SecurID reply.

```
Local> CHANGE SECURID INTERVAL seconds
Local> CHANGE SECURID REALM realm-name INCLUDE
```

This command causes the realm name to be included as part of a user name sent to SecurID. Realm name inclusion is used for SecurID proxy authentication service. See the Cabletron *Network Access Software Command Reference* guide for more information on this command.

Example: Including the Realm Name

If your realm name has to be included when the access server sends messages to SecurID, issue the command shown in the following example:

```
Local> CHANGE SECURID REALM realm-name INCLUDE
```

For most usage, you will not want to include the realm name. If you do, each entry in the SecurID users file will have to appear as “user-name@realm-name” instead of simply “user-name”.

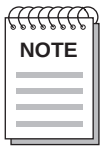
If a user has to be called back, this value is derived from User-Service-Type when specified. If it is not specified, then realm defaults / port defaults can apply:

Example: Defining Realm Default Authorization Attributes

```
Local> CHANGE SECURID REALM JONAS.COM PERMISSIONS (DIALBACK)
Local> CHANGE SECURID REALM JONAS.COM CALLBACK ENABLED DIALBACK NUMBER "1-800-555-1111"
```

Example: Defining Password Authentication Type

```
Local> CHANGE SECURID REALM JONAS.COM ACCESS FRAMED
```



The value NONE should be read as unspecified. This allows the port configuration to determine the access whenever the SecurID realm default does not specify one or more authorization attribute.

SecurID User Authorizations

Optional authorizations can come from the SecurID user description which is defined specifically for a particular SecurID implementation. It is possible to define realm defaults, within the access server. The ultimate value for an authorization attribute may come from one of three sources: the SecurID, the realm defaults, or port characteristics, in that order of precedence. The choices for such features are:

- For each SecurID realm name you define, you can set various authorization attributes for that realm. These values serve as defaults at the realm level. This means, that when a SecurID user tries to login to the access server, these values will be assigned to authorization attributes. If the user does not provide the attribute default in the realm, then the access server’s port characteristics are used if they have been previously defined.

- One of the legal settings of the attributes in the realm is NONE. This special value connotes unspecified. In this case, when a user attempts to log in, if the value is not specified in the SecurID entry for the user name, and has the value NONE in the REALM, then the PORT configuration parameter assigns the corresponding value.

Setting User Permissions

Permissions are explicitly given by the value in the realm defaults. When these are still missing, the port configuration can supply its specified values (for attributes having a corresponding representation in the port).

Permissions are CNAS vendor-specific. The following is a list of SecurID permissions:

DIALOUT	NODIALOUT
LAT	NOLAT
TELNET	NOTELNET
SLIP	NOSLIP
PPP	NOPPP
PRIVILEGED	NOPRIVILEGED (level of access server command privilege)

For each of the above attributes, the default is NOxxx or DISABLED.

Managing Local Access Server Security

Introduction

The tasks described in this section cover the configuration of the local access server realm and setup of local user accounts.

Configuration of server security involves:

- Access server realm configuration
- Local user account configuration parameter

Defining the Realm

Realm names must be unique within a given type of authentication.

In the case of the server realm, the realm name indicates local (or NAS) authentication.

The SET/DEFINE/CHANGE CLEAR/PURGE REALM realm-name command family sets up and tears down the various realms used to identify particular administrative domains.

Example: Setting the Server Realm

In the following example, the command defines a new server realm. The keyword realm-name is the proper name of the newly defined realm. Before using this new realm, you must assign additional realm parameters to it.

```
Local> SET SERVER REALM JONAS.COM
```

Determining Security Configuration

Displaying RADIUS, SECURID, and KERBEROS Characteristics

The SHOW {RADIUS | SECURID | KERBEROS} CHARACTERISTICS command displays all configured realm names, along with any pertinent configuration parameters. This command is privileged. It shows the various RADIUS and SecurID servers that are configured for the access server as well as the Kerberos KDCs. It also shows the existing local server security database.

Example: Showing RADIUS Characteristics

The following example shows the resulting display for the SHOW RADIUS CHARACTERISTICS command:

```
Local> SHOW RADIUS
Retransmit Interval:         00:00:01   Retransmit TimeOut:       00:00:20
Authentication Service Port: 1645       Account Service Port:         1646

Realm:                       XXX.YYY.XXX.COM
 Realm Inclusion:            EXCLUDE
 Prompt:                     Password>
 Secret:                     (Entered)
 Accounting Host:            16.20.55.66
 Authentication Host:        16.20.55.77
Authorization Defaults:
 Access:                     None        Forced Callback:          ENABLED
 Max Connect:                00 08:00:00 DialOut Service:        DIAL14400
 DialBack Number:            555-1234
 DialOut Number:             (Any)
 Permissions:                DIALBACK, DIALOUT, LAT, TELNET, SLIP, PPP,
                             NOPRIVILEGE
```

Example: Showing SecurID

The following example shows the resulting display for the SHOW SECURID CHARACTERISTICS command:

```
Local> SHOW SECURID
Retransmit Interval: 00:00:02        Retransmit TimeOut: 00.00.20
Service Port:        755
Realm:               AAA.BBB.CCC.COM
 Realm Inclusion:    EXCLUDE Encoding Format: DES
 Prompt:             Enter Passcode>
 Secret:             (Entered)
 Primary Host:       16.20.55.66
Authorization Defaults:
  Access:            INTERACTIVE Forced Callback: DISABLED
  Max Connect:       00 08:00:00 DialOut Service: DIAL28800
  DialBack Number:     555-1234
  DialOut Number:      (Any)
  Permissions:         DIALBACK, DIALOUT, LAT, TELNET, SLIP, PPP,
                      NONPRIVILEGED, NOPRIVILEGED
```

Example: Showing the Server Realm

```
Local> SHOW SERVER REALM
Realm:                local.NAS
Max Fails:            3
Authorization Defaults:
 Access:               INTERACTIVE   Forced Callback:     DISABLE
 Max Connect:          00 08:00:00   DialOut Service:    DIAL9600
 DialBack Number:      555-1234
 DialOut Number:       (Any)
 Permissions:         DIALBACK, DIALOUT, LAT, TELNET, SLIP, PPP,
                      NONPRIVILEGED, NOPRIVILEGED
```

Example: Displaying Kerberos Characteristics

The following example shows the resulting display for the SHOW KERBEROS CHARACTERISTICS command:

```
Local> SHOW KERBEROS
Retransmit Interval:  00:00:01 Retransmit TimeOut: 00:00:20
Ticket service port:  750 Password service port: 751
Default Realm:        33H.LKG.FOO.COM
  Secret:             (None)
  Primary Host:       prowlr.lkg.foo.com
  Master Host:        ds900.lkg.foo.com
  Host:               foo.bar.foo.com
  Authorization Defaults:
    Access:           INTERACTIVE Forced Callback:       DISABLED
    Max Connect:      00 08:00:00 DialOut Service:      DIAL14400
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT, TELNET, SLIP, PPP, DIALBACK, DIALOUT
```

Displaying Security Summary

To show the security summary, use the SHOW SECURITY SUMMARY command. This command displays all of the currently configured security realms. It provides a subset of the data produced by the SHOW SECURITY command.

Example: Showing the Security Summary

```
Local> SHOW SECURITY SUMMARY
Logout Warning ------------------------------------------------
Interval              0         Times         0
Kerberos ------------------------------------------------------
Default Realm:        33H.LKG.FOO.COM
Realm:                kerberos.realm.somewhere
RADIUS --------------------------------------------------------
Realm:                realmname1
SecurID -------------------------------------------------------
Realm:                realmnam2
Server --------------------------------------------------------
Realm:                realmname3
```

Showing the Authentication Counters

This access server can display the counters for all realms (local, RADIUS, KERBEROS). Any session authenticated by RADIUS attempts to send accounting data to the RADIUS Server. Sessions authenticated by other methods may be configured to send accounting packets to a RADIUS accounting server as well (if one exists).

Reference

See SHOW AUTHENTICATION COUNTERS in the Cabletron *Network Access Server Command Reference* guide for a sample of this display.

Showing the User Port Authorization Profile

The SHOW AUTHORIZATION command shows the user profile being used for the specified port(s).

Example: Showing the User Port Authorization Profile

The following example shows the resulting display for this command for a port that was authenticated:

```
Local> SHOW PORT 7 AUTHORIZATION

Port 7: user1          Server: ACCESS1
Username: user1@finance_realm
Access:           LOCAL Forced CallBack:                 DISABLED
Max Connect:      00 08:00:00  DialOut Service:          DIAL14400
Remaining Time:   00 00:33:24  Framed IP Address:     16.22.33.44
Login IP Host:    16.20.22.33  Login LAT Service:       LATSERVICE
Login Service Type:       LAT  Login Port:                     15
Authenticated By: 16.129.42.15 Authentication Type:         RADIUS
Login LAT Node:   MONEY
DialOut Number:   (Any)
DialBack Number:  1-802-767-8345
Login LAT Groups: 1,2,5,66-68,133,135,139,172,206,230-250

Permissions:      LAT, TELNET, SLIP, PPP, DIALACK, DIALOUT,
                  NONPRIVILEGED
```

Showing Security Counters

The SHOW / LIST / MONITOR SECURITY COUNTERS command displays all port-related security counters. This display is very similar to results from the SHOW PORT AUTHENTICATION COUNT command shown in the previous example.

Example: Showing Security Counters

```
Local> SHOW PORT 8 SECURITY COUNTERS
```

Managing Dial-Up Access Security with AUTOLINK and AUTOLINK Authentication

Introduction

AUTOLINK lets PC clients log in using SLIP, PPP, and character cell terminal mode.

AUTOLINK AUTHENTICATION provides a flexible and secure method for clients to authenticate when using AUTOLINK. A single port can support authenticated logins from different types of PPP clients, which may have different LCP authentication capabilities. For SLIP or PPP clients that do not support PAP or CHAP authentication, an interactive or script-based login will be used. When you enable AUTOLINK AUTHENTICATION, only one form of authentication is required during any port login.

When you use AUTOLINK authentication, a successful user login requires a user name/password authentication. The user name/password authentication requirement is independent of how you configure port characteristics (PORT AUTHENTICATION and LCP AUTHENTICATION).

To use AUTOLINK authentication, you need to set the DEFAULT PROTOCOL and DEDICATED SERVICE for the port to use the AUTOLINK protocol, and then enable the AUTOLINK AUTHENTICATION port characteristic.

Activating AUTOLINK

The port begins the AUTOLINK search protocol when the port has begun its login process. AUTOLINK examines the characters arriving on the port and determines if a PC is using PPP, SLIP, or a character-cell terminal emulation (which may be a login script).

If AUTOLINK does not detect a PPP or SLIP start frame character within a user-set timeout, it chooses character-cell mode. Note that a user or the login script can expedite the choice of character-cell mode by entering a carriage return character.

Example: Configuring the Port

The following example shows how to set the port's default protocol and dedicated service to AUTOLINK:

```
Local> DEFINE PORT DEFAULT PROTOCOL AUTOLINK
Local> DEFINE PORT DEDICATED SERVICE AUTOLINK
```

Enabling AUTOLINK Authentication

If you want authenticated logins, you must separately configure the port to require AUTOLINK AUTHENTICATION. The authentication can be by PPP PAP, PPP CHAP, or interactively by terminal emulation (which could be a script). The PC client is required to provide one authentication. SLIP users are treated as if they are character-cell users.

Once authentication is successful, the protocol identified by AUTOLINK (PPP, SLIP, or local login) starts.

Example: Enabling AUTOLINK Authentication

The following example shows how to enable AUTOLINK authentication:

```
Local> DEFINE PORT AUTOLINK AUTHENTICATION ENABLE
```

The SHOW PORT CHARACTERISTICS command shows AUTOLINK authentication enabled in the ENABLED CHARACTERISTICS section.

Specifying an Authentication Method

The following table describes the authentication method used when you enable AUTOLINK AUTHENTICATION and specify an LCP authentication method, and an interactive authentication was not already performed prior to LCP negotiation.

LCP Authentication	Results
PAP USERNAME	PC clients that connect immediately using PPP will be authenticated using PPP PAP authentication. This setting is required when you use Kerberos or SecurID authentication. For Kerberos authentication, you must set the Kerberos realm default ACCESS to NONE. For other forms of authentication, such as RADIUS, CHAP USERNAME may be used. If you user the PAP NOUSERNAME options with the PORT LCP AUTHENTICATION command, the login fails.

LCP Authentication	Results
Disabled	PC clients that connect immediately using PPP will be authenticated using either CHAP or PAP authentication. If the LCP negotiation for CHAP is not acknowledged, the access server requires PPP PAP authentication.
CHAP USERNAME	PC clients that connect immediately to PPP will be authenticated using PPP CHAP authentication. If you user the CHAP NOUSERNAME options with the PORT LCP AUTHENTICATION command, the login fails.

If you use either the PAP NOUSERNAME or CHAP NOUSERNAME options with the PORT LCP AUTHENTICATION command when you enable AUTOLINK authentication, the login fails.

Note if you configure the default protocol and dedicated service for the port as AUTOLINK and you disable AUTOLINK authentication, SLIP and character-cell users may be connected without authentication. This will occur even if PPP users are authenticated because of the port's LCP AUTHENTICATION characteristics.

Setting AUTOLINK Timers

You can set an AUTOLINK timer to specify how long the port waits to detect the protocol of the user session. If the port does not detect a valid PPP frame, a valid SLIP frame, or a single carriage return character, the session defaults to character cell terminal.

AUTOLINK makes two passes to determine the authentication style and the protocol of the user session:

1. If authentication is required, the first pass determines the authentication style. Either PPP authentication or character-cell authentication can be used. You can set the timer for the first pass to be between 10 and 60 seconds. If no authentication is required, AUTOLINK determines the session style.
2. If there has been an authentication pass, the second pass determines the protocol of the user session. The protocol can be SLIP, PPP, or character-cell terminal. You can set the timer for the second pass to be between 0 and 60 seconds. If the timer expires, AUTOLINK assumes a character-cell terminal.

Example: Setting AUTOLINK Timers

The following example shows how to set AUTOLINK timers:

```
Local> DEFINE PORT AUTOLINK TIMER PASS ONE 30
Local> DEFINE PORT AUTOLINK TIMER PASS TWO 50
```

Timeouts

The following are the properties of AUTOLINK timeouts:

- A user has one minute to complete an interactive login successfully. The clock starts from the time the USERNAME> prompt is displayed. This includes the time for the user name/password request to be processed by the authentication server. After one minute elapses, the port is logged out and the modem is disconnected.
- When a terminal emulation window first appears, it is blank. Entering a carriage return produces a USERNAME > prompt. If you do not enter a carriage return, the prompt is displayed after a user-set timeout (AUTOLINK PASS ONE). At this point the one minute time limit is initiated.
- If a user authenticates successfully in a terminal window (or a script), a single carriage return or a lapse of a user-set timeout (AUTOLINK PASS TWO) produces a local prompt. The user or the script can enter C PPP or C SLIP to begin framed operation.

Using a Login Script

If you use a login script on the remote client, your script must include the following:

Stage	Description
1	The script must send a carriage return character. Alternatively, the script can send no characters for [AUTOLINK TIMER PASS ONE] seconds (note that this is not the preferred method).
2	The script searches for Username> and responds with the user's user name and a carriage return.
3	The script searches for Password> and responds with the user's password and a carriage return.

Stage	Description
4	The script searches for: `Local -451- Authentication successful`
5	The script exits and allows the framed protocol to run. Note that the key phrase to search for is “Authentication successful”.

Specifying Other Security Features

Introduction

This section describes various security features on interactive ports.

Specifying Dedicated Service for LAT or Telnet Resources

The results of specifying a dedicated service on a port are as follows:

- The device on the port appears hard-wired to a specific resource.
- The access server establishes only one session for the port.
- Local mode cannot be entered on that port, although login and service passwords can still be defined for the user on that port.
- The access server automatically enables AUTOCONNECT for that port. AUTOCONNECT is not cleared when the dedicated service is cleared.

Kerberos Requirement

For Kerberos, the server name must be unique.

When you specify any LAT or Telnet resource to be a dedicated service, the host or service name, node name, and port name are limited to 16 characters each.

LAT Protocol Requirement

To set a LAT service as a dedicated service, the default protocol must be set to LAT. The following shows how to enable the LAT service, FILES, as the dedicated service on port 5:

```
Local> CHANGE PORT 5 DEDICATED FILES
```

You can specify that the connection be made to a particular node and/or port name of the LAT service. The following shows how to specify that port 5 connects to port JAMES on node MARKETING for service FILES:

```
Local> CHANGE PORT 5 DEDICATED FILES NODE MARKETING
DESTINATION JAMES
```

Telnet Requirement

To set an Internet host as a dedicated service, the default protocol must be set to TELNET. You can use the host's Internet address, domain name, or relative domain name if the host is defined in a name server; however, you cannot use the entire domain name if the name is more than 16 characters, including the dots.

The following shows how to enable a host on the TCP/IP network, SALE.MKT.FOO.COM, as a dedicated service on port 5:

```
Local> CHANGE PORT 5 DEDICATED SALE.MKT.FOO.COM
```

Normally, the user must press the Return key to connect to the LAT or Internet host. However, if SIGNAL CONTROL or MODEM CONTROL is enabled, the port automatically connects to the host. The following shows how to enable SIGNAL CONTROL on port 5:

```
Local> CHANGE PORT 5 SIGNAL CONTROL ENABLED
```

Specifying Passwords

There are two password characteristics that you need to set: SERVER LOGIN PASSWORD and PORT PASSWORD. SERVER LOGIN PASSWORD defines the password for the access server. PORT PASSWORD enables the login password on a particular port.

A single login password is used for the whole access server although the password is enabled on a port-by-port basis. This password is most likely to be useful when you wish to reserve access to a terminal located in a public place. For example, in a widely used computer center, you want to keep a terminal open for your computer-services staff. Enabling the login password would prevent your general user population from using that terminal.

You can enable the login password for a port with a session management terminal.The terminal user must enter the password when initially logging in to the access server.

If you plan to enable the login password at one or more ports, you should take care in selecting with whom you share the password. In addition, you should change the password on a regular basis and inform those selected users of the new password.

The login password can be 1 to 16 ASCII characters. The factory-set default login password is ACCESS.

Login Password Definition Example

The following example shows how to define TOTAL as the login password:

```
Local> CHANGE SERVER LOGIN PASSWORD "TOTAL"
```

or

```
Local> CHANGE SERVER LOGIN PASSWORD
Password> TOTAL (not echoed)
VERIFICATION> TOTAL (not echoed)
Local>
```

You must enable the PASSWORD characteristic at the port level. The following shows how to enable PASSWORD at ports 5, 6, and 7:

```
Local> CHANGE PORT 5,6,7 PASSWORD ENABLED
```

Once the PASSWORD characteristic is enabled at a port, the login prompt (#) appears at the port device accompanied by a beep signal when the user logs in to the port. The user must enter the login password to gain access to the port.

You can change the login password, but you cannot clear the password. If you specify NONE or type a null string ("") on the command line, you receive an error message.

To reset the default ACCESS, specify "ACCESS" on the command line or ACCESS at the Password> prompt.

Specifying PASSWORD LIMIT

The PASSWORD LIMIT characteristic specifies the following:

- The number of times that a port user with the PASSWORD and / or AUTHENTICATION port characteristic enabled can incorrectly enter the login password before the port is automatically logged out. If the port user fails to type the correct password within the number of allowed attempts, that user is not allowed to complete the login sequence for 1 minute. After 1 minute, the user can attempt to log in again.
- The number of times that a port user can incorrectly enter the privileged password before the port is automatically logged out by the access sever.
- For services that are password protected, the number of times that a user is prompted for the correct password before a connection request is denied. The value must be in the range of 0 to 10 attempts. If you specify 0, no attempts are allowed. The factory-set default is 3.

Example: Changing the Server Password Attempt Limit

The following example shows how to change the password limit to 6:

```
Local> CHANGE SERVER PASSWORD LIMIT 6
```

Chapter 24

Managing Remote Login

Overview

The remote login client (Rlogin) is supported by Cabletron Network Access Software. The Rlogin protocol, described in informational RFC 1282, allows users to log onto a remote computer (similar to Telnet). Rlogin supports pre-authenticated sessions on hosts that have been configured with trust relationships. This allows users to connect to those hosts without needing to enter a username and password.

In This Chapter

This chapter includes the following topics:

- Rlogin features
- Rlogin characteristics
- Configuring a Rlogin client

Rlogin Features

The following is a list of Rlogin features implemented in this release of the Cabletron Network Access Software:

- Rlogin runs over TCP/IP. Once a TCP/IP connection to the target system is established, the Rlogin client sends two frames to the Rlogin server. The first consists of a null. The second contains the username at the client side, the username at the server side, and the terminal type and speed. The server responds with a request for the terminal window display size at the client side, and then begins sending data (usually the banner a user sees once logged in). The client side replies to the window size request, then starts transmitting data, character by character.
- Rlogin conforms to all urgent data commands specified in RFC 1282, namely:

  — Flush (02)

  — RAW mode (10)

  — COOKED mode (20)

  — Request for window size (80)
- A Rlogin session operates in one of two modes. The Rlogin server controls when the session is in RAW or COOKED mode. In RAW mode, all user input is passed directly to the Rlogin server. In COOKED mode, the Access Server processes XON/ XOFF flow control chargers (STOP is Ctrl/S and START is Ctrl/Q) and does not pass them on to the Rlogin server. For this to work properly, turn off the XON/ XOFF flow control on your terminal.
- Security Realm permissions added for Rlogin include RLOGIN and NORLOGIN.
- Support for RADIUS-specified Rlogin sessions — If the login type is 1 (Rlogin) or the vendor specific attribute (VSA) is detected, the user will see a Rlogin session upon authentication.
- Existing port counters are used to indicate if data is lost while suspending input to the Rlogin server.
- The meaning of the Access Server's port setting of default protocol ANY is extended to include Rlogin. The CONNECT command attempts to connect to the server in this order: LAT, Telnet, and Rlogin.

Rlogin Characteristics

The following is a list of Rlogin characteristics:

- Client username — The client username sent to the Rlogin server is the username at the Rlogin client that is stored in the port's authorization information. This means the Access Server user has been authenticated and the username given during that process is the first choice for the rlogin protocol. If there is no authorization information available, the Access Server's port username is used.
- Server username — The server username sent to the Rlogin server is the username at the Rlogin server and is provided when entering the Rlogin command. If one is not provided, the server username is the name that is stored in the port's authorization information. If there is no authorization information available, the Access Server's port username is used.
- Terminal type — The terminal type sent to the Rlogin server is the one specified by the port Rlogin terminal type. You can set, define, or change the terminal type. The default is unknown, if no terminal type is specified.
- Terminal speed — The terminal speed sent to the Rlogin server is the Access Server port output speed.
- Display size — The display size sent to the Rlogin server is 24 lines by 80 columns. You cannot change the display size.
- Escape character — The default Rlogin escape character is ~ (a tilde) and is only recognized at the beginning of a line. The escape character can be modified.
- There are two character sequences that will cause the Access Server to quit the Rlogin session immediately:

  — These are the escape character followed by Ctrl/D, for example ~ Ctrl/D.

  — The escape character followed by a period, for example ~.

  To close the Rlogin session gracefully, use the Rlogin server's EXIT command.
- Suspend input — To suspend input to the server, use the escape character followed by Ctrl/Y. The server's output is not affected. This character will toggle the feature on and off. The default is Ctrl/Y, but can be modified.
- Suspend output — To suspend both input to the server and output from the server, use the escape character followed by Ctrl/Z. The default is Ctrl/Z, but can be modified.

Configuring a Rlogin Client

The Rlogin component implemented in the Cabletron Access Server Network Access Software is a Rlogin client. A user can initiate a Rlogin session from an Access Server, but a user cannot Rlogin onto an Access Server by means of a connection over a LAN.

Follow these steps to configure a Rlogin client:

Step	Action
1	Turn off the terminal's XON / XOFF flow control. (This is not the Access Server's flow control.)
2	Set the port Rlogin terminal to the appropriate VTxxx value. For example: `Local> SET PORT RLOGIN TERMINAL type` If you want this change to be permanent, you can use the DEFINE / CHANGE PORT command if you are a privileged user. If VTxxx does not describe your terminal, then skip this step, but verify that you have the correct terminal type specified once you have made a Rlogin connection. If it is not set correctly, modify your environment on the remote system.
3	Configure the remote system to accept your Rlogin request. • If you are configuring Rlogin for DIGITAL UNIX, see Step 4 in this table. • If you are configuring Rlogin for OpenVMS, See Step 5 in this table. Refer to your local system documentation for more information about configuring remote systems.

Step	Action
4	There are two ways you can configure Rlogin for DIGITAL UNIX: 1. In the user's home directory, add an entry to the .rhosts file, specifying the Access Server's name or IP address, and the client username. For example: `myserver.foo.com smith` or 2. Add an entry specifying the Access Server's name or address to the /etc/hosts.equiv file in the root directory. See Rlogin manpages for restrictions and syntax.

5	To configure Rlogin for OpenVMS, enter the following command:
	`UCX> SET PROXY user /HOST=hostname /REMOTE_USERNAME=username`
	`UCX> ENABLE SERVICE RLOGIN`
	Where hostname gives the Access Server's address or name.
	See UCX Help for more information.

Chapter 25

Accounting

Overview

Introduction

This chapter describes the network access server accounting component. The basis of an accounting facility is the logging of events related to user access. These events can be useful to support audit trails, billing, capacity planning, and connection trouble-shooting.

In This Chapter

This chapter contains the following topics:

- Accounting Description
- What Events Are Logged?
- When Events Are Logged
- Managing Accounting
- Using the Accounting Console Logging Feature

Accounting Description

Introduction

The configuration of the accounting feature is supported using SNMP and the user interface. The accounting log itself is also accessible by both mechanisms. There is also a facility for sending accounting events to the access server console port as they occur.

Accounting Log File

The accounting component stores information about significant user events (for example, logins) in an accounting log file. The size of the log file is defined by the administrator (see the Defining the Accounting Log Size section in this chapter) and if set to zero, no logging will occur. The log file can be viewed as a circular buffer with entries added in chronological order. When the end of the buffer is reached, a newly created entry will overwrite the oldest existing entry.

Since the access server offers limited mass storage, preserving the accounting information requires the use of the console logging feature (see the Using the Accounting Console Logging Feature section in this chapter) or a “harvester” application running on a management station. To facilitate this harvest application, the accounting component can be configured to send notifications when checkpoints (thresholds) have been crossed in the log file. These notifications are in the form of SNMP traps.

What Events Are Logged?

Contents of Log Entry Types

The following table shows the fields that are logged in each accounting log entry type:

Log Entry Type	Event	Time	Port	ID	Port	Access	Peer	Reason	Tx	Rx	User
Port Login	X	X	X			X					X
Port Logout	X	X	X						X	X	X
Session Connect Attempt	X	X	X	X	X	X	X				X
Session Disconnect	X	X	X	X	X			X	X	X	X
Kerberos Password Fail	X	X	X								X
Privilege Password Fail	X	X	X								X
Maintenance Password Fail	X	X	X				X				
Login Password Fail	X	X	X								
Remote Password Fail	X	X	X								
SNMP Community Fail	X	X			X	X					
Privilege Password Modified	X	X	X								X
Maintenance Password Modified	X	X	X								X
Login Password Modified	X	X	X								X
User Privilege Level Modified	X	X	X								X
SNMP Community Modified	X	X	X								X
Remote Password Modified	X	X	X								X

Event Field Descriptions

The following table describes the fields in the accounting log entries:

Field	Description
Event	Provides the ability to distinguish the event type. The valid event types are listed in the previous table.
Time	Current server system uptime when entry was created.
Port	• For session connect / disconnect events: - Local Access: The port the session connect or disconnect occurred on. If the connection is initiated from a physical port, this field will have the physical port number. If the connection is initiated from an existing remote console connection, the port number will be one higher than the maximum physical port number. - Remote Access: For a remote console connection (MOP or Telnet), the port will be one higher than the maximum physical port number. For a connection to a LAT service or Telnet listener (other than listener 23), the port will be the destination physical port the connection is made to. If no port is available, the port field will be zero. Note: If a connection is created from a physical or remote console port to a Telnet listener or LAT service on the same server, two session connect events will be logged: one for the local access from the source port and one for the remote access to the destination port. Two disconnect events will also be logged when the session is torn down. In each log entry, the port number will follow the rules stated above. • For nonsession events, the port that the event occurred on.
ID	The internal ID associated with an active session (not those that are displayed in the SHOW SESSION displays). The session IDs are always unique across the server at any given time (though they may be reused after a session is disconnected).

Field	Description
Port	• Session connect / disconnect: The protocol associated with the session attempt or disconnect. These values can be: - LAT - TELNET - MOP - TN3270 - SLIP - PPP - AUTOLINK - PING Note: For a TN3270 session, the protocol type may appear as TELNET for the connect event and TN3270 for the disconnect event. For an AUTOLINK session, the protocol may appear as AUTOLINK for the connect event and either AUTOLINK, SLIP, or PPP in the disconnect event, depending on what protocol was used last. • SNMP Community Fail: SNMP_IP (representing SNMP over IP).
Access	The access type, either Local or Remote.

Field	Description
Peer	The value of this field varies depending on the protocol field, as follows: • LAT - Local Access: For nondedicated / preferred case, whatever you type following the CONNECT [LAT] command. For example, C CLUSTER1 (peer is CLUSTER1); C CLUSTER1 NODE NODE1 (peer is CLUSTER1 NODE1). If dedicated / preferred service is defined, the peer field will contain the service name. - Remote Access: The local service name followed by the remote node name. • Telnet - Local Access: For nondedicated / preferred case, whatever you type following the CONNECT / Telnet command. For example, TELNET NODE1 (peer is NODE1); TELNET NODE1.finance.acme.com (peer is NODE1.finance.acme.com). If dedicated / preferred service is defined, the peer field will be the service name. - Remote Access: The remote node's IP address followed by the remote TCP port number. • PING: Whatever you type following the PING command. For example, PING NODE1 (peer is NODE1); PING NODE1.finance.acme.com (peer is NODE1.finance.acme.com). • MOP (maintenance password fail event): The Ethernet address of the remotely connected device. • SLIP: The peer field is SLIP. • PPP: The peer field is PPP. • AUTOLINK: The peer field is AUTOLINK. • SNMP_IP (SNMP community fail event): The IP address of the SNMP management station.
Reason	The reason for the disconnect, either Normal or Error. Normal represents the session being brought down by user action (you log out of the session or do a DISCONNECT SESSION at the local prompt). Error refers to cases where the session is refused by the protocol for some reason (insufficient resources, not authorized for group code in case of LAT, or couldn't resolve name in case of Telnet).

Field	Description
Tx	• Session Disconnect Event: The number of bytes of successfully transmitted user data on this session at the time of session termination. This field will always be zero for MOP remote console connections. • Logout Event: The number of bytes output to the port during the life of the associated login.
Rx	• Session Disconnect Event: The number of bytes of successfully received user data on this session at the time of session termination. This field will always be zero for MOP remote console connections. • Logout Event: The number of bytes input to the port during the life of the associated login. Subtracting the sum of all the session disconnect Tx/Rx fields during the life of a login from the Tx/Rx values in the logout event will yield the Tx/Rx count of bytes sent and received while the user was in local mode.
User	This field is a variable length string as follows: • Login Events: When authentication is enabled on the port, this field will contain the entire Kerberos user name string (for example, jones@finance.acme.com). • All Other Events: This field will contain the user name string associated with the port (the string in the first field of the SHOW PORT display). The SET PORT USERNAME command may change a port's user name from the string stored at login. This can cause entries associated with a particular login to have different user name fields. The login entry, when Kerberos is enabled, is the only trusted source for the user name.

When Events Are Logged

Introduction

This section describes when each specific event type is logged.

Login Events

Login events are logged at the time of the successful login (just before the user gets the `Local>` prompt). Unsuccessful login attempts are handled by Kerberos Password Fail, Login Password Fail, or Remote Password Fail events.

Logout Events

Logout events are stored when the port is logged out. There is always an associated login event.

Session Connect Attempt Events

Session connect attempt events are stored when a session connect is being attempted (either user-initiated or dedicated). All attempts are logged whether they are successful or not.

Session Disconnect Events

Session disconnect events are logged when a session connect attempt fails or when an existing session is terminated. There is always an associated session connect attempt event. Use the disconnect reason or bytes Tx/Rx to determine whether the connection attempt was successful.

Password Fail Events

Password fail (Kerberos, Privilege, Maintenance, Login, Remote) events are logged for every attempt to enter the associated password.

SNMP Community Fail Events

SNMP community fail events are logged whenever an SNMP access attempt is made with a community name and/or source IP address that is not enabled on the access server.

Password Modified Events

Password modified events (Privilege, Maintenance, Login, Remote) are logged whenever the associated password is modified with a SET/DEFINE/CHANGE command. A single event is logged for each UI command (only one event is logged for a CHANGE command). SET commands cannot be distinguished from DEFINE commands. If a user sets the password to the existing value, an event is still logged.

User Privilege Level Modified Events

User privilege level modified events are logged whenever a user does a SET PRIV command and successfully provides the privilege password at the Password> prompt. If the user is already privileged, the event is still logged.

SNMP Community Modified Events

SNMP community modified events are logged whenever a user adds or deletes an SNMP community string on the access server. They are also logged if an existing community's access capabilities are modified (SET SNMP COMMUNITY PUBLIC SET ENABLE). If the user sets the community to existing values, an event is still logged. A single event is logged for each UI command (only one event will be logged for a CHANGE command). SET commands cannot be distinguished from DEFINE commands. If a user does a CLEAR/PURGE SNMP COMMUNITY ALL, a single event will be logged.

Managing Accounting

Introduction

You can manage the accounting feature fully by using SNMP or the user interface. You can access the accounting log itself using both mechanisms. This section describes the user interface commands you can use to manage the accounting feature.

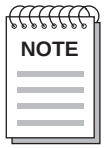
Reference

Refer to SNMP Survival Guide (located on the CNAS distribution media) for instructions on managing the accounting component with SNMP.

Defining the Accounting Log Size

Use the DEFINE ACCOUNTING LOGSIZE command to control the amount of memory allocated at initialization to create the log file. Valid values for the LOGSIZE variable are 0, 4, 8, 16, 32, 64, 128, 256, and 512 (units are kilobytes). If the accounting component cannot allocate the specified amount of memory at the time of initialization, the value displayed for LOGSIZE in the SHOW ACCOUNTING CHARACTERISTICS display will be set to zero.

If this occurs, define a smaller value for LOGSIZE. This characteristic can only be modified with a DEFINE command. Note that a newly defined value will not take effect until the next time the server is reinitialized.



An access server configured with 2 megabytes of memory may not have sufficient resources to allow for the creation of an accounting log.

Example: Defining the Accounting Log Size

The following shows how to set the size of allocated memory to 512 KB:

```
Local> DEFINE ACCOUNTING LOGSIZE 512
```

Changing the Accounting Threshold

Use the ACCOUNTING THRESHOLD command to specify the point in the building of a log when the accounting component sends out a threshold notification.Valid values for the ACCOUNTING THRESHOLD variable are:

- NONE: No notification.
- HALF: Notify when each half of the log file is reached.
- QUARTER: Notify when each quarter of the log file is reached.
- EIGHTH: Notify when each eighth of the log file is reached.
- END: Notify when the end of the log file is reached.

Entries are inserted in the log file progressively (with wrapping) and when the specified points in the buffer are reached, notifications are sent. These notifications are in the form of SNMP traps.

Example: Changing the Accounting Threshold

The following example shows the use of the DEFINE ACCOUNTING THRESHOLD command:

```
Local> DEFINE ACCOUNTING THRESHOLD EIGHTH
```

Changing the Accounting Console

Use the DEFINE ACCOUNTING CONSOLE command to display accounting events on the server console. If ENABLED, the accounting component displays accounting events on the server console port as they occur. Be sure to set the server console port to the desired value (CHANGE SERVER CONSOLE n).

Example: Changing the Accounting Console

The following example shows the use of the DEFINE ACCOUNTING CONSOLE command:

```
Local> DEFINE ACCOUNTING CONSOLE ENABLED
```

Displaying Accounting Characteristics

Use the SHOW ACCOUNTING CHARACTERISTICS command to display the current values of the accounting variables.

Example: Displaying Accounting Characteristics

The following example shows the display that appears when you use the SHOW ACCOUNTING CHARACTERISTICS command:

```
Local> SHOW ACCOUNTING CHARACTERISTICS
Accounting Characteristics:
Threshold:              None      Log Size:              128K
Console Logging:        Disabled
```

Displaying the Accounting Log

Use the SHOW ACCOUNTING LOG command to view the log.

Example: Displaying the Accounting Log

```
Local> SHOW ACCOUNTING LOG
Accounting Log:
Event: Login                                        Time: 026:10:33
Port: 3                                Access: Local
Username: smith

Event: Privilege Password Fail                     Time: 0 26:12:13
Port: 3
Username: smith

Event: User Privilege Level Modified               Time: 0 26:12:44
Port: 3
Username: smith

Event: Session Connect Attempt                     Time: 0 26:15:04
Port: 3 Sessid: 1 Protocol: LAT Access: Local
Username: smith
Peer: CLUSTER1

Event: Session Disconnect                          Time: 0 26:15:50
Port: 3 Sessid: 1 Protocol: LAT
Reason: NORMAL TX: 345 bytes RX: 216 bytes
Username: smith

Event: Login Password Modified                     Time: 0 27:13:51
Port: 3 Username: smith

Event: SNMP Community Modified                     Time: 0 27:14:14
Port: 3 Username: smith

Event: Logout                                      Time: 0 27:15:06
Port: 3 Tx: 1285 bytes Rx: 526 bytes
Username: smith
```

Using the Accounting Console Logging Feature

Description

When console logging is enabled, the accounting component displays the accounting events on the server console as they occur. This can be useful for viewing events on a console terminal or printer. It is also possible to view (and log to a file) the console events remotely. If you place a loopback connector on the access server console port and associate a LAT service or Telnet listener with this port, you can connect to the port and view the console messages remotely.

LAT Remote View of the Accounting Log

The following example shows the commands necessary to remotely view the accounting log messages with a LAT service and loopback connector on port 16 of the access server:

```
Local> CHANGE PORT 16 ACCESS REMOTE
Local> CHANGE PORT 16 AUTOBAUD DISABLED SPEED 57600
Local> CHANGE SERVICE ACCTREMOTE PORT 16 CONNECTION ENABLED
Local> CHANGE SERVER CONSOLE 16
Local> CHANGE SERVER SERVICE GROUP 255
```

From a remote OpenVMS system, type:

```
$ MCT LATCP SET NODE/GROUP=(ENABLE=255)
$ SET HOST/LAT/AUTOCONNECT/LOG=ACCT.LOG ACCTREMOTE
```

This causes the accounting events to be displayed on the remote screen and logged to the file ACCT.LOG.

Example: Telnet Remote View of the Accounting Log

The following example shows the commands necessary to remotely view the accounting log via Telnet with a loopback connector on port 16:

```
Local> CHANGE PORT 16 ACCESS REMOTE
Local> CHANGE TELNET LISTENER 2001 PORT 16
Local> CHANGE TELNET LISTENER 2001 CONNECTION ENABLE
Local> CHANGE SERVER CONSOLE 16
Local> CHANGE PORT 16 AUTOBAUD DISABLED SPEED 57600
```

From a remote UNIX system, the command is (replace x.x.x.x with your server's IP address):

```
# TELNET x.x.x.x 2001
```

This will cause the accounting events to be displayed on the remote screen. To log the events to a file, type the following command (replace x.x.x.x with your server's IP address):

TELNET x.x.x.x 2001 > ACCT.LOG

Appendix A

Cable and Adapter Recommendations

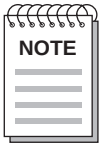
Cable and Adapter Hardware

Cable and Adapter Table

The following table lists the cable and adapter hardware you need to connect devices to specific access server models:

To Connect This Device:	**To This Access Server Model:**	
	90M or 90TL (8 Port) **900TM (32 Port)** **700 (16 Port)** **316 (16 Port)**	**700 (8 Port)**
	Use This Cable and Adapter Hardware:	
Terminal / printer with MMJ port	BN24H-xx cable	H8575-A adapter and BC16E-xx cable
Terminal / printer with DB25 male port	H8575-A adapte and BN24H-xx cable	BC17D-xx (10-wire) cable or BC22D-xx (6-wire) cable
Terminal / printer with DB9 male port	H8575-B adapter and BN24H-xx cable	H8575-A adapter and H8571-J adapter and BC16E-xx cable
PC communication interface with DB9 male port	H8585-AA adapter and BN25G-xx cable	H8575-A adapter and H8571-J adapter and BC16E-xx cable

To Connect This Device:	To This Access Server Model:	
Modems using RI-DCD-DSRS-DTR signals (typically <9600 baud) with DB25 female port	H8585-AB adapter and BN25G-xx cable	BC22E-xx (10-wire) cable or BC22F-xx (25-wire) cable
Modem using CTS-DSR-RTS-DTR signals (typically =>9600 baud) with DB25 female port	H8585-AC adapter andBN25G-xx cable	BC22E-xx (10-wire) cable or BC22F-xx (25-wire) cable
Host computer systems with DB25 male ports (reverse-LAT configuration)	-	BC22R-xx cable



The -xx denotes the length of the cable in meters.

Reference

Refer to the Site Preparation Guide or User's Guide shipped with your access server hardware for further information.

Glossary

access server
A generic name for a family of access servers supported by Cabletron Network Access Software.

access server configuration database
A load host database that contains the DECnet characteristics and the access server type, the load file name, and the dump file name for each access server.

access server image
A file in the access server directory on the load host that contains executable code.

Address Resolution Protocol
See ARP.

American National Standards Institute
See ANSI.

ANSI
American National Standards Institute. This organization compiles and publishes computer industry standards.

ARP
Address Resolution Protocol. The Internet protocol that enables a host or a gateway to dynamically map, or translate, an Internet address into the correct physical hardware address so as to send a packet to a target computer on the same physical network.

American Standard Code for Information Interchange
See ASCII.

AppleTalk
An Apple Computer, Inc., trademark for their network protocol suite.

ASCII
American Standard Code for Information Interchange. A set of 8-bit binary numbers representing the alphabet, punctuation, numerals, and other special symbols used in text representation and communications protocols.

asynchronous
Pertaining to a communication method in which each event occurs with no relation to a timing signal.

atomics
Refers to nontabular objects in a group of objects in a MIB.

authentication
Utilizes Kerberos to verify a user's identity by validating a Kerberos user name and password on a remote Kerberos host (KDC).

authentication trap
An SNMP trap message that is sent to each community with TRAPS enabled whenever an unauthorized Internet host tries to access the access server, or when an Internet host uses an unauthorized SNMP GET or GETNEXT message.

autobaud
The process by which the access server automatically determines the line speed and other characteristics of a terminal attached to one of its ports.

autoconnect
A feature whereby the access server automatically attempts to reconnect a port to a network resource in the following situations: the port becomes disconnected from a resource, the user enters a CONNECT command and the specified resource is unavailable, or the user logs in to a port that has a preferred service defined.

automatic failover
See failover.

bootptab file
This is the file that BOOTP uses to store information necessary to downline load software. The bootptab file is normally shown as /etc/bootptab.

BOOTP
Internet Bootstrap Protocol. This Internet protocol is used to configure the communications software on a load host.

BOOTP/TFTP Server
This is a load host that uses the BOOTP and TFTP Internet protocols to configure the load host and downline load the software.

broadcast
A access server port characteristic that allows one port to send a single message to one or more ports simultaneously.

CCR
Console Carrier Request. An ULTRIX host function that allows connections to the access server remote console port.

Clear To Send
See CTS.

circuit timer
LAT. The LAT protocol timer that determines the minimum interval at which a access server transmits virtual circuit messages.

client-server
Internet. The model of interaction in a distributed system in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the program satisfying the request is called the server.

command line recall and edit
A feature that allows the user to recall and edit previously entered commands.

community name
A character string that is used as a password that the Internet host must know in order to access the access server through SNMP.

connection queue
LAT. The queue on a access server that stores connection requests for a printer or a service.

Console Carrier Request
See CCR.

console port
Any access server port assigned to receive the access server 900 series of messages and to which an interactive device can be connected.

CRC
Cyclic Redundancy Check. An error detection scheme in which a receiver checks each block of data for errors.

CTS
Clear To Send. A signal sent from the port device to the access server to indicate that the port device is ready to receive data.

Cyclic Redundancy Check
See CRC.

datagram
See IP datagram.

Data Set Ready
See DSR.

Data Terminal Ready
See Data Terminal Ready.

data transparency
During a session, the access server normally intercepts and interprets switch characters and flow control characters. Users can enable data transparency, causing these characters to become transparent to the access server. The access server will not intercept them while they are being exchanged in the user's current session, such as during a file transfer or during a block-mode transfer (where the terminal sends a screen of data to the host application).

DECnet
The DIGITAL networking software that uses the DIGITAL Network Architecture (DNA) on both local area networks (LANs) and wide area networks (WANs).

DECnet node address
A unique numeric identification required for each DECnet node, assigned by the network manager. The address is in the form aa.nnnn, where aa is an optional area number (from 2 to 63), and nnnn is the node address (from 1 to 1023).

DECnet node name
A unique 1- to 6-character alphanumeric identification (including at least one alphabetic character) required for each DECnet node assigned by the network manager.

dedicated service
A network resource to which a port is permanently assigned and to which the port is always connected at login, thus emulating a hardwired connection.

dequeue
To remove the first entry in a queue and to attempt the function for which the entry was queued.

DNS
Domain Name System. An Internet naming system that maps, or translates, domain names to addresses. See domain names.

domain names
Internet. The domain name consists of a sequence of subnames separated by a period.

The individual sections of the name might represent sites, groups, or computers, but the domain system simply calls each section a label.

For example, the domain name super.dec.com, contains three labels: super, dec, and com. Any suffix of labels in a domain name is called a domain. Thus, the lowest level domain is super.dec.com, an abbreviation for the computer named super. The second level domain is dec.com (for Digital Equipment Corporation); and the top level domain is com (for commercial institution). As the example shows, domain names are written with the most local label first and the topmost domain last.

Domain Name System
See DNS.

downline loading
The process of sending the access server image from a load host to a access server.

DSR
Data Set Ready. A control signal that is used to inform whether or not a communications device is ready to transmit and receive data.

DSVCONFIG
The configuration procedure used on a load host to configure the load host's node database.

DTR
Data Terminal Ready. A control signal that is used to inform whether or not a data terminal is ready to transmit and receive data.

dump file
A file containing a copy of the access server memory. The load host creates this file when it receives an upline dump from the access server. The file is stored on the load host in the access server directory.

Ethernet
A type of local area network based on carrier-sense multiple-access / collision detection (CSMA / CD).

event logging
This is a process of recording significant occurrences on the network.

failover
LAT. A failure-recovery function provided by LAT software. Failover occurs when a user's current LAT session is disrupted by the failure of the service node. Failover attempts to connect the user to the same service on an alternative service

node. Failover is attempted only if the service is offered by two or more service nodes (as with a VAXcluster service).

flow control
The set of rules used by a communications protocol to ensure that access server ports and port devices do not lose data during data transfers. Flow control prevents the sending network node (or transmitting process) from sending more data than the receiving node (or receiving process) can handle.

gateway
See Internet gateway.

group codes
LAT. Group codes are integers ranging from 0 to 255. They are assigned to LAT services, access servers, and access server ports.

heartbeat
A signal generated by certain Ethernet transceivers. The signal verifies that the collision detection circuitry is operational.

host
A multiuser computer.

host-initiated request
LAT. A connection request from a computer asking a access server to initiate a session.

The session connects an applications device such as a printer on a access server port to an application such as a print queue on the computer.

ICMP
Internet Control Message Protocol. A protocol that is the part of the Internet Protocol that gateways and hosts use to communicate control and error information. If for any reason a gateway cannot forward or deliver a datagram, or if the gateway detects unusual conditions that may affect the host, the gateway uses this protocol to communicate with the host so that the host can take corrective action.

ID
This is an abbreviation for identification.

image
See access server image.

initialization
The process of running the access server diagnostic self-test program and, optionally, downline loading the access server with the access server image.

Installation Verification Procedure
See IVP.

Internet
Internet (written in all lowercase letters) is a collection of packet switching networks that use TCP/IP protocols and are interconnected by gateways. Software enables the networks to function logically as a single, large, virtual network.

3. Internet (written with the first letter capitalized) refers specifically to a collection of networks and gateways, including the ARPANET, MILNET, and NSFnet, that use the TCP/IP protocol suite and function as a single, cooperative virtual network.

Internet address
The 32-bit address assigned to computers that participate on an Internet using the TCP/IP protocols.

Internet Bootstrap Protocol
See BOOTP.

Internet Control Message Protocol
See ICMP.

Internet gateway
A computer that connects two or more networks and passes packets between them. In Internet, computers called gateways provide all interconnections among physical networks. Gateways route packets based on the destination network, not on the destination host.

Internet host
A resource on the TCP/IP network.

Internet name server
An Internet server program that performs name-to-address translation, or mapping, from domain names to Internet addresses. It enables users to assign common names that are easy to remember to computers and then address the computers by name, rather than Internet addresses. When the server program operates on a dedicated computer, the computer itself is usually called a name server. See also local name server and root name server.

Internet Protocol
See TCP / IP.

IP
Internet Protocol. See TCP / IP.

IP datagram
Internet. A basic unit of information transferred over the Internet.

IVP
Installation Verification Procedure. This procedure verifies that the access server software was successfully installed on a OpenVMS load host.

KDC
Key Distribution Center. A Kerberos host that serves to validate a user's identity with a Kerberos user name and password.

keepalive timer
LAT. Because access servers are responsible for monitoring its balanced virtual circuits, each access server maintains a keepalive timer. This timer determines the length of time that a balanced circuit remains inactive.

Kerberos
An authentication service that enhances security in an open network. It was developed as part of Project Athena at Massachusetts Institute of Technology. Project Athena is a software development project that facilitates communication among file servers and workstations in a distributed network environment.

Key Distribution Center
See KDC.

keyword
A word in a command string that further defines the command.

LAN
local area network. A network in which communications are limited to a moderately sized geographic area such as an office building or a campus.

LAT
local area transport. DIGITAL name for the Ethernet protocol used by the DECserver for terminal connections.

LAT architecture
A layered networking model that identifies LAT communications functions, assigns specific functions to distinct layers, and specifies general rules for communication between LAT nodes.

LAT Control Program
A control program that provides a command interface that allows system and network managers to set up and manage an operating system as a LAT service.

LAT network
All the computer systems, or nodes, on a LAN that support the LAT protocol constitute a LAT network.

LAT node
A computer on a LAN that contains LAT software. There are two types of LAT nodes; nodes that access services and nodes that offer services; some nodes perform both functions.

LAT protocol
An integral part of the LAT architectural model that consists of rules that specify the actual format and sequence of the messages used for communication between LAT nodes.

LAT service
A resource on the LAT network.

learned data
Data entered into a access server database by DNS. Contrast with local data.

load host
A computer on the same LAN as the access server that is used to downline load the access server image to the access server. A load host can also receive upline dumps of access server memory.

load host database
A database that contains information about access servers and that allows the load host to perform downline load and upline dump operations. This database contains three databases on the load host: the DECnet operational database, the DECnet permanent database, and the access server configuration database (that is, DSVCONFIG.DAT).

local area network
See LAN.

local data
Data entered into a access server database by a user. Contrast with learned data.

local name server
A name server that is authorized for the domain where the access server is located.

local service
Network resource offered by your access server.

loopback test
A access server asynchronous port test during which data is looped to the module. There are two types of loopback tests: internal and external. The external loopback test requires a loopback connector.

Maintenance Operation Protocol
See MOP.

Management Information Base
See MIB.

Maximum Transmission Unit
See MTU.

MIB
Management Information Base. A listing of variables that can be accessed by SNMP.

MOP
Maintenance Operation Protocol. A maintenance protocol specified in the DIGITAL Network Architecture (DNA) that is used to implement the Remote Console Facility and to perform downline loads, upline dumps, and loopback tests.

MTU
Maximum Transmission Unit. This specifies the IP datagram size in bytes.

multicast
A process whereby a message sent to one address can be transmitted to a number of nodes affiliated with that address. See also broadcast.

multicast timer
A LAT service characteristic that determines the time interval between each multicast message.

multihomed host
An IP host that has more than one IP address.

name resolution
Internet. Refers to the process of translating a name into a corresponding Internet address. The Internet domain name system provides a mechanism for naming computers in which programs use remote name servers to resolve computer names into Internet addresses for those computers.

name server
See Internet name server.

NCP
Network Control Program. The DECnet command interface used to configure, control, monitor, and test DECnet networks.

network access server
See access server.

Network Control Program
See NCP.

Network Management Station
See NMS.

network resource
A device (such as a computer or printer) or software application on a network that performs certain functions and can be accessed by devices, such as access servers and computers.

NMS
Network Management Station. Host computer system with software which allows manager to monitor and control networked devices (including access servers) from one location. Typically refers to system which uses SNMP to communicate but may use other protocols.

node
A network system consisting of a computer system and associated network software.

nonprivileged status
The default status for all interactive access server ports. Users at nonprivileged ports can use a subset of the privileged command set to: change some local port characteristics; display information about the access server, its ports, and service nodes; and execute commands required to connect to services. However, nonprivileged users cannot access commands that change the state of the access server or other ports.

Nonvolatile Random Access Memory
See NVRAM.

NVRAM
Nonvolatile Random Access Memory. This is a RAM that retains its memory upon power loss.

ODL Font Protocol
On-Demand Loading Font Protocol. A protocol that enables Asian terminals connected to the access server to use the LAT protocol to access Japanese and Chinese OpenVMS systems on the LAN.

On-Demand Loading Font Protocol
See ODL Font Protocol.

OpenVMS
An operating system for DIGITAL VAX computers.

operational database
The access server database that contains the values that determine the current operating characteristics of the access server. The values are not preserved through initializations, power losses, and port logouts. Contrast with permanent database.

packet
The basic Ethernet network message unit transmitted by the data link layer, which is made up of a preamble and a data stream.

permanent database
The access server database that contains the values that define the permanent operating characteristics of the access server. These values are preserved through initializations, power losses, and port logouts. Contrast with operational database.

port
A physical access point on the access server to which a device can connect.

preferred service
A predefined network resource to which the access server attempts to connect a specific port whenever a user at that port enters a CONNECT command without a service name.

print spooler
A program that enables many users to share the printing devices of a system, such as a access server.

privileged status
A port status that can only be set by a user that knows the access server privileged password. Users at privileged ports can execute all communications server commands.

qualifier
A parameter in a command string that modifies the command.

queuing
LAT. The process of putting LAT connection requests for a busy printer or service on a waiting list (queue). Requests are dequeued and processed in the order in which they were entered into the queue-first-in / first-out (FIFO).

RAM
Random Access Memory. This is a read and write memory integrated circuit (IC).

Random Access Memory
See RAM.

RCF
Remote Console Facility. A OpenVMS host function that allows connections to the access server remote console port.

realm
An administrative domain within Kerberos in which users are registered and within which they can be authenticated by passwords.

release notes
A text file that can include any of the following: special instructions for installation, information specific to the current release of the product, and any information omitted from the printed documentation. Release notes can be read on line or printed.

Remote Console Facility
See RCF.

remote console port
A logical port with fixed port characteristics values used by the access server software when communicating using the MOP or Telnet protocol. Users can enter most of the access server commands at the remote console port.

remote print queue
A queue on a service node. The queue holds connection requests made from the service node requesting use of a printer (remote printer) on a access server. See host-initiated request.

Request To Send
See RTS.

retransmit limit
The number of times a LAT virtual circuit message is retransmitted to a service node without an acknowledgment message.

root name server
A name server that is at the top level in a domain.

RTS
Request To Send. A signal sent by the access server to the port device to indicate that the access server is ready to exchange control signals or data.

secure port
A port set up so that the port user only has access to a limited subset of the nonprivileged user command set.

secure status
A restrictive status that can be imposed on a port to limit the execution of commands on that port to a subset of the nonprivileged command set.

server
A hardware and/or software device which provides many users with access to a system.

service
A network resource offered by a LAT or Internet host.

service circuit-ID
A load host characteristic that identifies which load host Ethernet controller is used to access a specific access server for maintenance functions.

service node
A LAT node that provides a service on the LAN. The access server can be a service node.

service rating
A value assigned to a network resource by the service node to indicate its relative capability to accept new sessions. The rating is scaled from 0 to 255, where 255 is the greatest capacity. Access servers use this rating to choose a service node when a user attempts to connect to a service that is offered by multiple service nodes.

service session
A session between a network resource and a terminal session on a session management terminal.

session
A two-way network communications path between a network resource and either a access server user, a multiuser computer user, or an application program.

session management
A facility provided by some access servers that uses TD/SMP to communicate with a access server device so that the device can process simultaneous, independent, multiple terminal sessions. On the device, the data exchange of multiple sessions can be processed simultaneously regardless of which session is current.

Simple Network Management Protocol
See SNMP.

SLIP
Serial Line Internet Protocol. This protocol uses a simple framing technique to transmit IP datagrams over serial lines.

SLIP host
An Internet host that uses SLIP as its data link.

SNMP
Simple Network Management Protocol. An Internet protocol that is used to manage systems from one or more Internet hosts.

subnet addressing
An addressing technique that allows a site to share a single Internet network address among multiple logical networks, as long as all the hosts and gateways on those networks cooperate. It is a form of hierarchical routing in which the top level of the routing hierarchy, the core gateway system, uses the network portion of the Internet address (when routing packets) to identify the local gateway. The next level, the local gateway, uses part of the host portion of the Internet address to identify the subnet and route packets to it. And finally, the lowest level, the specific host computer, uses the remainder of the host portion of the address to identify and accept packets addressed to it.

subnet identifier
This is the part of the network address that is unique to the subnet. It can be determined by logically ANDing the Internet address with the subnet mask.

subnet mask
A 32-bit quantity that enables gateways and host computers to know which bits in the Internet address correspond to their subnet address and which correspond to their host addresses.

switch characters
Characters interpreted by the access server that cause the access server to switch between sessions or between local and service modes.

synchronous
Pertaining to a communication method in which each event occurs in relation to a timing signal.

TCP/IP
Transport Control Protocol / Internet Protocol. A suite of Internetworking communication protocols of which TCP and IP are the two most fundamental.

TCP port
This is a protocol port number used by TCP / IP. For access servers, this number is mapped to a physical access server port number.

TD/SMP
Terminal Device / Session Management Protocol. An asynchronous, coded syntax used by the access server and a terminal to manage independent multiple terminal sessions simultaneously over a single physical circuit. See session management.

Telnet
Internet. The Internet standard protocol for remote terminal connection service.

Telnet client
See client-server.

Telnet listener
A service that allows resources to be accessible to a TCP / IP network. The service is provided over Telnet, hence the service is commonly referred to as a Telnet listener.

Typically, printers connect to access server ports associated with a listener. However, personal computers and host computers can also connect to such ports and through them access the TCP / IP network.

Telnet server
See client-server.

Terminal Device/Session Management Protocol
See TD / SMP.

Terminal Server Manager
See TSM.

terminal session
A single session on a access server port that is operating under session management control.

Time To Live
See TTL.

TFTP
Trivial File Transfer Protocol. For access servers, this Internet protocol is used to downline load software from a load host to the access server.

transceiver
Hardware equipment that provides an electrical connection to a network cable for a network node.

Transport Control Protocol/Internet Protocol
See TCP/IP.

TRAP message
An SNMP message sent by the agent (in this case, the access server) to one or more designated Internet hosts.

TSM
Terminal Server Manager. Software that runs on a OpenVMS host system. TSM allows a manager to monitor and control multiple access servers from one location.

The access servers must be connected to the same Ethernet LAN as the OpenVMS host system.

TTL
Time To Live. This is a value that shows the time that an Internet host entry in the access server database has left to be refreshed or removed. This value appears in the SHOW INTERNET HOST STATUS display.

upline dumping
The process of sending a copy of the access server memory to a responding load host, usually following a fatal error. The data is dumped into the unique access server dump file in the access server directory.

UDP
User Datagram Protocol. A protocol that is the part of the Internet Protocol that provides datagram service. It distinguishes between multiple destinations on a host, allowing multiple application programs executing on a host to independently exchange (send and receive) datagrams with multiple application programs on another host.

User Datagram Protocol
See UDP.

virtual circuit
A logical communications path between a access server and a service node. A virtual circuit provides a bidirectional, sequential, timer-based, error-free stream of data.

WAN
Wide Area Network. A network composed of computers connected by communications links that cover distances up to many thousands of miles. Contrast with LAN.

Wide Area Network
See WAN.

XON/XOFF characters
These characters are used with a form of in-band flow control and are transmitted as TxD and RxD data.