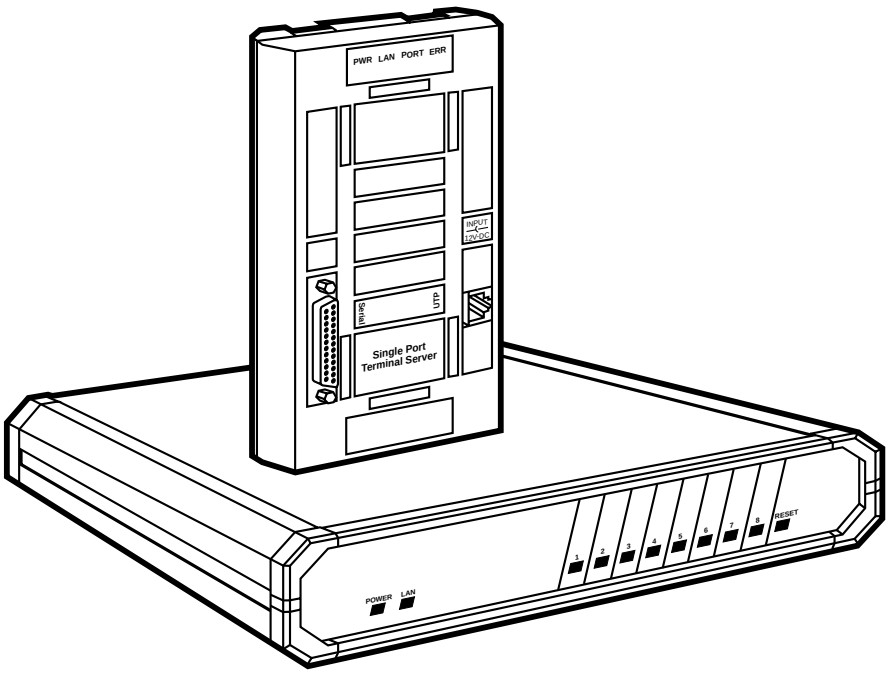
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

FEBRUARY 1998

LE2101A-BT-R2
LE2101AE-BT-R2
LE2101A-T-R2
LE2101AE-T-R2
LE2104A-AUI-R2
LE2104A-BNC-R2
LE2104A-TP-R2
LE2204A-AUI-R2
LE2204A-BNC-R2
LE2204A-TP-R2
LE2508A-AUI-R2
LE2508A-BNC-R2
LE2508A-TP-R2
LE2608A-AUI-R2
LE2608A-BNC-R2
LE2608A-TP-R2

Terminal Servers



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

NORMAS OFICIALES MEXICANAS (NOM)

ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El parato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equio eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

CONTENTS

1. Specifications

Protocol — *LE2101A-R2, LE2101AE-R2*: LAN: TCP/IP; *LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2*: LAN: TCP/IP, LAT; Serial ports: None, PPP, SLIP

Indicators — *LE2101A-R2, LE2101AE-R2*: (1) Power LED, (1) LAN, (1) Port, (1) ERR (Error); *LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2*: (1) Power LED, For each port: (1) LAN and (1) Activity

Connectors — *LE2101A-T-R2, LE2101AE-T-R2*: (1) DB25, (1) RJ-45, *LE2101A-BT-R2, LE2101AE-BT-R2*: (1) DB25, (1) RJ-45, (1) BNC); All multiport models: (1) IEC 320, (1) DB25 female (parallel); AUI multiport models: (1) DB15 female and (4) or (8) RJ-45; BNC multiport models: (1) BNC and (4) or (8) RJ-45; TP multiport models: (1) RJ-45 10BASE-T and (4) or (8) RJ-45 serial

Speed — Ethernet: 10 Mbps; Serial: up to 115 Kbps

Operating Temperature — 32° to 122°F (0° to 50°C)

Humidity — 0% to 90% noncondensing

Power — *LE2101A-R2*: Input: 120 VAC/60 Hz, Output: 12 VDC, 800 mA, 9.6 VA, *LE2101AE-R2*: Input: 220 VAC/50 Hz, Output: 12 VDC, 800 mA, 9.6 VA; *LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2*: 100-230 VAC, autosensing

Size — *LE2101A-R2, LE2101AE-R2*: 1.5"H x 4.5"W x 7.5"D (3.8 x 11.4 x 19 cm); *LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2*: 1.7"H x 8.5"W x 11.7"D (4.3 x 21.6 x 29.7 cm)

Weight — *LE2101A-R2, LE2101AE-R2*: 1 lb. (0.5 kg); *LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2*: 4.7 lb. (2.1 kg)

2. Overview

The Terminal Servers make possible Ethernet connections to computer equipment that was not designed to be networked. Serial devices such as personal computers, printers, terminals, and modems are supported by the Terminal Servers and the Ethernet concurrently. The Terminal Servers can be configured to provide services from network nodes as well as to access services from the network's nodes.

2.1 Terminal Server

The TCP/IP standard network protocol is supported by the single-port Terminal Servers (LE2101A-R2). The Telnet™ and LAT™ standard network protocols are supported by the multiport Terminal Servers (LE2104A-R2, LE2204A-R2, LE2508A-R2, LE2608A-R2). The Telnet protocol, provided on most UNIX® systems, allows initiation of a session to create a terminal connection to a network host supported by the Telnet.

Domain Name Servers can be used on the Terminal Servers to enable a network name Terminal Server to convert text node names into numeric IP addresses. A local host table displays IP address resolution, which permits the use of a host name instead of an IP address, thereby simplifying the use of the Telnet protocol.

Digital Equipment Corporation™ LAT (Local Area Transport) protocol is supported on almost all DEC™ operating systems for terminal connections on local networks.

Multiple sessions, including LAT and TCP/IP combinations, can be executed by any port on the multiport Terminal Servers to connect with any host. Turning on a device may immediately establish communication between the user and a host. The user can alternate between displays to view sessions running simultaneously.

In addition, the Terminal Server can be accessed from the LAN side and will provide an outgoing connection to serial devices (dial out). This facility, known as Reverse LAT, Telnet Server/Telnet Listener, or Reverse Telnet, allows the host system connected to the LAN to access the Terminal Server, and furthermore, any device connected to one of its serial or parallel ports (such as a printer).

2.2 Remote Access Server

The Remote Access facility of the Terminal Server allows remote TCP/IP stations connected via modems to the PSTN (Public Switched Telephone Network) to access a LAN-based TCP/IP network. This dialup method of connection uses either SLIP (Serial Line IP) or PPP (Point-to-Point Protocol) to allow the remote station (for example, a PC or a UNIX workstation) to become a native member of the central network to which the Terminal Server is connected.

In order to protect the central network from unauthorized access, the RADIUS (Remote Authentication Dial-In User Service) protocol is implemented by the Terminal Server. RADIUS provides central user-authentication and accounting services and supports the PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) sub-protocols of PPP.

2.3 Available Models

The following models are available:

- Single-Port Terminal Server (10BASE-T) (part number LE2101A-T-R2)
- Single-Port Terminal Server (10BASE-T/BNC) (part number LE2101A-BT-R2)
- Terminal Server/4 TCP/IP (AUI) (part number LE2104A-AUI-R2)
- Terminal Server/4 TCP/IP (BNC) (part number LE2104A-BNC-R2)
- Terminal Server/4 TCP/IP (TP) (part number LE2104A-TP-R2)
- Terminal Server/4 TCP/LAT (AUI) (part number LE2204A-AUI-R2)
- Terminal Server/4 TCP/LAT (BNC) (part number LE2204A-BNC-R2)
- Terminal Server/4 TCP/LAT (TP) (part number LE2204A-TP-R2)
- Terminal Server/8 TCP/IP (AUI) (part number LE2508A-AUI-R2)
- Terminal Server/8 TCP/IP (BNC) (part number LE2508A-BNC-R2)
- Terminal Server/8 TCP/IP (TP) (part number LE2508A-TP-R2)
- Terminal Server/8 TCP/LAT (AUI) (part number LE2608A-AUI-R2)
- Terminal Server/8 TCP/LAT (BNC) (part number LE2608A-BNC-R2)
- Terminal Server/8 TCP/LAT (TP) (part number LE2608A-TP-R2)

2.4 Terms

The following are brief descriptions of the network components occurring in this manual.

A *session* is a logical connection to a service, such as a terminal connected to a host through the Terminal Server.

A *service* is a device that can establish a network connection, such as a host that terminals can connect to. The Terminal Servers also offer services of attached printers and modems.

A *node* is an intelligent device (e.g., a host, an Ethernet workstation, or a Terminal Server) with a direct connection to the Ethernet network and an Ethernet address. Devices connected to a Terminal Server serial port are excluded by this category.

A *host* is a computer attached to the network. A "host" is generally an interactive computer that enables users to log in.

Local Mode is when the user issues commands directly to the Terminal Server. In local mode, all of the commands in the Command Reference of this User's Manual are available.

Service Mode is where the user interacts with connected services and/or hosts. All the user input in service mode goes to the connected services and/or hosts, and not the Terminal Server.

2.5 Features of the Terminal Servers

- Easy To Use—Command-line editing, recall and completion are all supported by the Terminal Server's local mode.
- Easy Configuration—The Terminal Server's powerful command interface is easy for users as well as system managers to operate. Software upgrades are simple, since the Terminal Server's operating code is immediately downloaded upon power on.
- Small Size—The small case of the Terminal Server is conveniently sized for the office environment. The Terminal Server runs without a fan and does not make any noise.
- Multiple Session Support—Multiple LAT and Telnet sessions can run simultaneously, with each session connected to any host and using any supported protocol. The user can alternate between displays of up to eight multiple sessions supported on each connected terminal.
- Connectivity—Terminals are directly connected to the network by the Terminal Server. Direct connectivity simplifies terminal cabling, saves physical ports on the host, and enables the terminal to be available for multiple hosts.
- Load Balancing—The load-balancing feature enables a Terminal Server to connect to the most unoccupied node when a LAT service is provided by more than one node. CPU utilization is thereby balanced and improves response times to the user.
- UNIX Compatibility—Telnet is supported by almost all UNIX systems. The Terminal Servers offer support for Domain Name Servers and a local host table that contains IP addresses of frequently used hosts.
- DEC Compatibility—The Terminal Servers are fully compatible with most DEC operating systems since it supports LAT and NCP™.
- Telnet to LAT Gateway—A user in a Telnet session is able to communicate with LAT services. A user in a LAT session is able to communicate with Telnet services.
- Host-Initiated Transfers—Hosts can share modems and printers when a Terminal Server is configured to provide its attached devices as services to other nodes. Jobs can be queued concurrently to Terminal Servers services by TCP/IP and LAT hosts.

- Remote Console Support—DEC NCP and TSM facilities can be used to configure Terminal Servers from a remote location. Simple configuration of the Terminal Servers by UNIX managers is provided by the Telnet Terminal Server features of the IP network.

- SNMP—The Simple Network Management Protocol is supported by the Terminal Servers to enable network managers to have an overall view of the network load, error conditions, and problematic sites.

- Security—The Terminal Servers can be set up to limit user access to services by using group codes. The Terminal Server can be configured for automatic logout of a session when a device is turned off or upon port disconnection. Ports can be restricted to give a limited view of the network and be prevented from issuing privileged commands. Password protection is available for privileges, ports, services, and remote access. Ports may be locked by users and unlocked with pre-designated passwords.

- Diagnostics—During power-on, diagnostics are executed and can run interactively to troubleshoot difficulties with network and serial lines.

- SLIP and PPP—SLIP or PPP can be used to access the TCP/IP Internet LAN by IP hosts connected to the Terminal Server's serial ports.

3. Installation

This chapter explains how to install the Terminal Server. With correct planning and a suitable choice of interfaces and cabling, installation will be relatively simple and trouble-free.

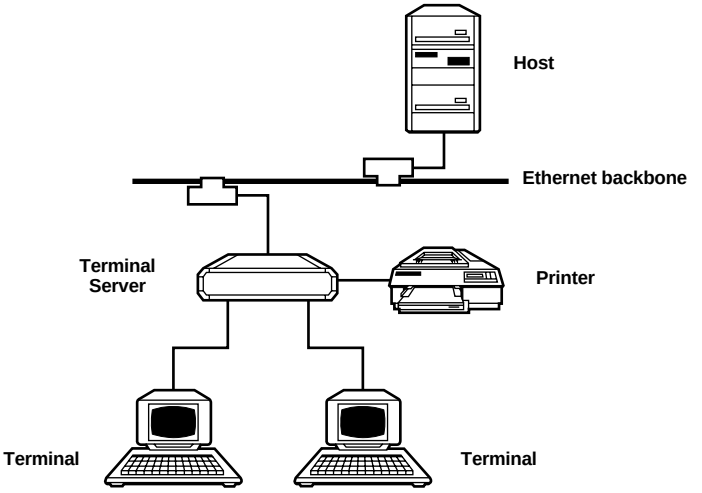


Figure 3-1. A Typical Terminal Server Layout.

The typical configuration shown in **Figure 3-1** shows the Terminal Server functioning as a primary interface between the local user (at a terminal, for example) and the network. Even if the installation is far more complex, the principles of initial hardware server and individual port configuration remain the same.

Take care when connecting Terminal Servers to the Ethernet network. You may need certain adapters and/or cables to connect all the individual components of the Terminal Server subsystem (such as terminals, printers, and modems). All the relevant information is provided in this manual.

Follow these three steps to setup the Terminal Server:

1. Physically setup the Terminal Server.
2. Configure the Terminal Server for first-time use.
3. Define individual ports.

3.1 Indicators of the Terminal Server

Table 3-1 describes the front and back panels, switches/buttons, and LED indicators for each Terminal Server model.

Table 3-1. Terminal Server Indicators.

Model	Buttons/Switches	Power	LEDs[2]
LE2101A-R2	Power jack	External 115-VAC power supply[1]	PWR, LAN, PORT, and ERROR
LE2101AE-R2	Power jack	External 230-VAC power supply	PWR, LAN, PORT, and ERROR
LE2104A-R2, LE2204A-R2	Power socket and Switch, Reset Button	110-220 VAC, 50-60 Hz	PWR, LAN, and 4x port
LE2508A-R2, LE2608A-R2	Power socket and Switch, Reset Button	110-220 VAC, 50-60 Hz	PWR, LAN, and 8x port

NOTES

[1]AC/DC, unregulated adapter with TUV, UL, or CSA approval.
Input: 220 VAC/50 Hz or 120 VAC/60 Hz
Output: 12 VDC, 800 mA, 9.6 VA
Cord: 5.5*2.1mm barrel, center negative

[2]PWR—indicates that the unit is receiving power.
LAN—indicates network (LAN) activity.
PORT—indicates that the indicated port is already in use.
ERR—indicates that the power-on diagnostics check has detected an error.

Table 3-2. Power-On Diagnostic Indication.

Code	Description
9	Base RAM test
8	N/A
7	N/A
6	N/A
5	N/A
4	TIMER test
3	LAN (Ethernet) test
2	NVRAM test
0	Power-On test completed. (If this flashes more than twice, NVRAM has been restored to default.)

Table 3-3. Loader Indication.

Code	Description
L	The base unit has entered the software-download state. A loader prompt is displayed on the terminal where the INIT UPDATE command was executed.
L (flashing)	A new software module is currently being downloaded into the base unit.
P	Final phase of software downloading—updating the FLASH memory.
—	FLASH EPROM clearing (one segment moving every few seconds).

Table 3-4. Hardware Fault Indication.

Code	Description
H	The base unit Front End Processor (FEP) is not responding.
d	Inconsistency in DPRAM protocol version. Turns to L and prompts the LOADER.
r	Rebooting the Terminal Server (warm boot).
h	High-rise FEP not responding.
j	Jumper is set to Restore Factory defaults.
b	Hardware problem in base FEP.
F	Software error caused a processor fault.

3.2 The Installation Process

3.2.1 Unpacking the Terminal Server

Your package should contain the following items:

- Terminal Server
- This user manual

If anything is missing or damaged, contact Black Box at 724-746-5500.

3.2.2 Selecting a Location

Before installing the Terminal Server, verify that the chosen site meets the following requirements:

- Select a clean location that is away from a heat source, such as direct sunlight. Make sure the location is not near equipment that emits electromagnetic interference (EMI) such as electric motors.
- Make sure that proper power outlets and network points are accessible.
- Allow for at least 4 inches (10 cm) clearance above and to all sides of the unit for cable connections. Place the Terminal Server on a secure flat surface.
- The ambient operating temperature for the Terminal Server is 32 to 122 °F (0 to 50 °C), at a relative humidity of up to 90%, noncondensing.

3.3.3 Connecting the Terminal Server to the LAN Network

Connect the Terminal Server to the Ethernet network using the appropriate networking procedures and cables for your configuration of the Terminal Server port (RJ-45/UTP, BNC, or AUI) and site network (hub, transceiver).

NOTE

The LE2101A-BT-R2 and LE2101AE-BT-R2 automatically sense the network topology (UTP or BNC). For this to function correctly, connect to the network by plugging in the power before switching on the Terminal Server.

3.3.4 Connecting Serial Devices to the Terminal Server

You may connect any RS-232/RS-423 device to any of the serial ports of the Terminal Server. This section describes the following procedures: connecting DCE and DTE devices, pin layouts of the RJ-45 connector, and RJ-45 to DB25 or DB9 conversions.

Connecting DCE and DTE Devices

Two types of RS-232 devices can be connected to the Terminal Server serial ports:

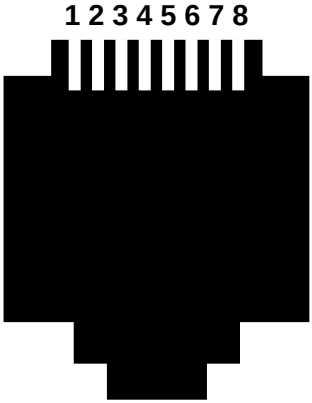
- DTE (Data Terminal Equipment) Devices—These are directly-attached devices, such as terminals and computers, that provide data in the form of digital signals at its output.
- DCE (Data Circuit Terminating Equipment) Devices—These are devices that provide the functions required to establish, maintain, and terminate connections and also provide the signal conversions required for communication between a data terminal equipment and the telephone line or data circuit. Modems connected to the serial port of the Terminal Server in order to overcome the RS-232 50-ft distance limit are considered to be DCE devices.

The Terminal Server serial ports act as individual DTEs. A simple and direct pin-to-pin cable is required if such a serial port is to be connected to a modem (similarly for any other DTE-to-DCE connection).

However, if terminals are connected directly to one another (in a DTE-to-DTE configuration, since both the terminal device and the Terminal Server port are DTEs), a special cable must be used. This cable, known as a "cross cable" or "null modem cable," includes crossed-connections between specific RS-232 pins so that each DTE will recognize the other as a DCE.

The RJ-45 Serial Port

All the Terminal Servers have RJ-45 connectors, which operate as RS-232 (or RS-423) interfaces. **Figure 3-2** describes the pin layout used in the RJ-45 ports.



1: Clear To Send (CTS) - input
2: Data Terminal Ready (DTR) - output
3: Transmit (TX+)
4: Transmit Return (TX-)
5: Receive Return (RX-)
6: Receive (RX+)
7: Data Set Ready (DSR) - input
8: Request To Send (RTS) - output

Figure 3-2. RJ-45 Serial Port Pinout.

RJ-45 to DB25/DB9 (DTE) Conversion

Table 3-5 describes the cable wiring required for connecting a DTE device (such as a terminal) with a RS-232 (DB9/25) port, to the Terminal Server's RJ-45 serial port.

Table 3-5. RJ-45 to DB25 (DTE) Conversion.

RJ-45 Pin	RJ-45 Signal Name	DB25 pin	RS-232	DB9 pin
1*	Clear to Send (CTS)	4	RTS	7
2*	Data Terminal Ready (DTR)	6	DSR	6
3	Transmit (TX+)	3	RCV	2
4	Transmit Return (TX-)	7	GND	5
5	Receive Return (RX-)	7	GND	5
6	Receive (RX+)	2	XMT	3
7*	Data Set Ready (DSR)	20	DTR	4
8*	Request to Send (RTS)	5	CTS	8

RJ-45 to DB25/DB9 (DCE) Conversion

The following table describes the cable wiring required for connecting a DCE device with an RS-232, DB25 port (such as a modem) to a Terminal Server's RJ-45 serial port.

Table 3-6. RJ-45 to DB25/DB9 (DCE) Conversion.

RJ-45 Pin	RJ-45 Signal Name	DB25 pin	RS-232	DB9 pin
1*	Clear to Send (CTS)	5	CTS	8
2*	Data Terminal Ready (DTR)	20	DTR	4
3	Transmit (TX+)	2	XMT	3
4	Transmit Return (TX-)	7	GND	5
5	Receive Return (RX-)	7	GND	5
6	Receive (RX+)	3	RCV	2
7*	Data Set Ready (DSR)	6	DSR	6
8*	Request to Send (RTS)	4	RTS	7

The pins marked with an asterisk (*) are required only for modem-control or for flow-control, so you may ignore these pins when connecting a terminal.

For applications requiring DTR handshaking or for printers that use pin 11 for Printer Busy Signals, connect RJ-45 pin 1 (CTS) to DB25 pin 20 (for DTR) or pin 11 (Printer Busy), respectively.

The RJ-45 adapter does not support chassis ground but does supply signal ground to both pin 4 and pin 5. The reason for this is that on many DB25 devices, pin 1 is left unconnected. In other cases, signal ground and chassis ground are not electrically equivalent and connecting one to the other with a cross-cable can potentially damage *both* devices. The Transmit Return (pin 4) and Receive Return (pin 5) pins must be connected to signal ground (pin 7 on the DB25) when connecting an RJ-45 connector to an RS-232 connector.

The RS-232 and RS-423 standards specify a maximum length of cable that may be used to connect devices. For example, the RS-232 specification for 9600 baud connections limits the cable length to 50 feet. In practice, the 50-foot limit is often exceeded and this may cause noise that may also lead to interference and unpredictable results. When cabling directly from a Terminal Server to an RS-423 terminal, use twisted pair cabling for maximum noise immunity. Using long flat cables may result in noise problems.

3.3 Power On Procedure and Diagnostics

3.3.1 Single-Port Terminal Server

Once the unit is powered, the power LED turns ON and the device goes through initial "Power On" diagnostic tests. During these tests, which last for approximately three seconds, all the unit LEDs should alternate ON and then OFF. If a hardware failure is detected during any test, one or more of the LEDs will flash at a constant rate. If this happens, call for technical support. The PWR LED always remains ON when connected to power.

3.3.2 4- and 8-Port Terminal Servers

Immediately after the Terminal Server is powered on, it executes a "Power On" diagnostic procedure and all of the LEDs on the front panel will flash. All the LEDs light sequentially from left to right for approximately five seconds. After the last LED has gone out, only the Power LED should remain on. The entire diagnostic procedure lasts for approximately ten seconds. Normal operation of the Terminal Server can commence once these diagnostics complete successfully.\

If a diagnostic test reveals a fatal error, then all of the LEDs will light for a few seconds. An error code will be indicated by leaving some of the port LEDs ON. The display will then alternate between having all the LEDs on and the error-code display. In the unlikely event of failure, contact technical support for further assistance. If the diagnostic test reveals a non-fatal error (such as the failure of a particular port), the Terminal Server will continue to operate.

3.4 Restoring Factory Defaults

In rare cases where access to the Terminal Server is not possible and the suspected cause may be incorrect configuration settings, or when you forget the privileged password, you need to be able to restore the device to factory defaults. A direct consequence of this step is that all configuration changes made to the Terminal Server in the past will be lost (including the Internet address which will default to 0.0.0.0) and the privileged password will be restored to *system*.

The following sections describe the procedure to restore factory defaults in all the different Terminal Server models.

3.4.1 Single-Port Terminal Server

1. Turn the power OFF by unplugging the terminal server power cable.
2. Remove the lid of the unit by pressing the four tabs.
3. Place the factory default jumper (JP2), located in the corner nearest the PWR LED, on pins 1 and 2.
4. Plug in the power cord.
5. Wait until all the PORT and LAN LEDs flash (for a few seconds) and unplug the power cord.
6. Return the factory defaults jumper (JP2) to pins 2 and 3.
7. Replace the lid and plug in the power cable. Factory defaults have now been restored.

3.4.2 4- and 8-Port Terminal Servers

1. Turn the power off and unplug the terminal server power cable.
2. Remove the upper lid by unscrewing the fastener at the back end of the case.
3. Remove the printer-control printed circuit. This is the raised small printed circuit to which a gray ribbon cable is connected. Unscrew its mounting screw and carefully lift and disconnect the small board from its socket connector.
4. Plug in the power cord and switch the power back on.

WARNING

Do not touch the power supply area. You might be shocked!

5. Wait until the LEDs display an error pattern (a sequence in which all the LEDs light for a few seconds and finally display an error code).
6. Switch the power off, unplug the power cord, and replace the lid. Switch on the unit by plugging in the power cord. Factory defaults have now been restored.

4. Configuration Guide

4.1 Introduction

This chapter explains how your system administrator can configure the Terminal Server. Each section describes the required configuration for a particular application of the Terminal Server. You only need to configure the Terminal Server once, since it remembers the configuration setup when it is powered off.

Carefully read through the general description issues and then refer to the section that is best suited for your needs.

The description for each task in the following sections will contain:

- A general description of the major Terminal Server feature involved in the task.
- A relevant example showing the required sequence of commands needed to implement the feature. In each particular example, the most common scenario is simulated.
- A thorough explanation of each statement in the example.

For more detailed information about the Terminal Server commands, refer to **Chapters 6, 7,** and **8**.

Table 4-1. Quick Look-Up Table.

Environment	Task	Section	Page
TCP/IP	Basic setup of the TCP/IP network interface of the Terminal Server	Configuring IP parameters	
TCP/IP for Terminal Server mode	Connecting a display terminal	Configuring terminal ports	
	Connecting a printer to the parallel port	Adding TCP/IP printers	
	Using BOOTP	Using the BOOTP protocol	
TCP/IP for Remote Access mode	Connecting remote stations with SLIP	Configuring SLIP Ports	
	Connecting remote stations with PPP	Configuring PPP Ports	
Security	Using RADIUS for authentication	Implementing RADIUS authentication	
	Using the RADIUS accounting facility	Accounting using RADIUS	
Management	Using an SNMP agent	Configuring the SNMP agent	
LAT	Basic configuration of LAT services of the Terminal Server	Configuring LAT services	
	Connecting a display terminal	Configuring LAT services	
	Connecting a printer	LAT printers	

4.2 Access to Management Commands

After the successful installation of the Terminal Server, the next step is the correct configuration of the unit so it can function as either a Terminal or Remote Access Server. The system administrator should connect to the system to configure the device. Please refer to the following sections for more information.

When the Server is configured for the first time, it should be accessed by a terminal connected to one of the serial ports of the server. Later, after an IP address is initially defined for the server, basic configurations which need to be entered or modified can be implemented remotely by the system administrator who can now also access the server using Telnet or LAT sessions. Once accessed, either from a directly-connected terminal or from the network, the same command language is used for configuration and operation of the server.

4.2.1 Using Privileged Mode

Many of the Terminal Server configuration commands require that the user be in a special mode, known as *privileged mode*, which is equivalent to becoming a superuser. This mode is initialized with the SET PRIV command which prompts the user to enter a password. This protects the Terminal Server from being configured by any unauthorized persons. Commands that require privileged mode are disallowed for ordinary (not superusers) users and any attempts to enter them results in a security violation error message. The factory default password is system (in lower case). Once in privileged mode, the system administrator can change this password to one of his own choosing. The following example shows how an administrator, joe, changes the password from the default *system* to *peace*.

```
Terminal Server  SW V4.1.3, HW V1.0

Enter username> joe
Local> SET PRIVILEGED
Password> system
Local> CHANGE SERVER PRIVILEGED PASSWORD
Password> peace
Verification> peace
Local>
```

Figure 4-1. Changing the System Password.

NOTES

The opening banner that appears when logging into the Server displays valuable information about the model type and current software version.

When passwords are entered, they are not echoed on the display. You need to verify the new choice once before it is accepted.

CAUTION

There is no way for the administrator to recall the privileged password if its is forgotten. Keep a record of the password in a safe place. If the password is forgotten, the administrator will have to restore the factory default settings (see Chapter 3), which will discard all the configuration changes made to the Terminal Server since initialization.

4.2.2 Using the Online Help

You can display brief descriptions of all Terminal Server commands and characteristics available for the security level of your port by typing HELP at the Terminal Server local prompt. The Terminal Server also offers limited tutorial help that describes various end-user tasks. There are two online help facilities:

- The HELP command—Provides an on-screen description of the chosen command. **Figure 4-2** shows an example.

```
Local>HELP SET PORT SPEED

PORTS SPEED (INPUT/OUTPUT) (nonprivileged)

This nonprivileged option establishes the port speed in
bits per second (bps). Valid speeds include: 75, 110,
134,150, 3000, 600, 1200, 1800, 2000, 2400, 4800, 9600,
19200,38400, 57600, and 115200. The default port speed
is 9600.

The speed of each direction can be specified
independently.

INPUT SPEED specifies the speed from the device to the
Terminal Server. OUTPUT SPEED specifies the speed from
the Terminal Server to the device.

Restriction

*A port that is active in the AUTOBAUD process cannot
accept SPEED modifications.

Local>
```

Figure 4-2. The Help Command.

- Automatic Command Completion (ACC)—While entering commands and not sure of the next allowed command keyword, one can enter a question mark ? in its place. The Terminal Server will respond immediately with all the possible parameters available from that particular point on. Note that non-privileged and privileged users will see different listings when using the ACC facility because of their different respective security levels.

  After listing the possible parameters, the Terminal Server will automatically display a new prompt line with the initial command already in place and with the cursor at the end of the preceding chosen keyword. The Terminal Server now waits for the additional parameters to be entered—which can include a further question mark.

  Figure 4-3 shows the logical sequence of events in finding out from the online help how to change the Terminal Server's Internet address.

```
Local> SET ?
     INTernet     POrts        SERVEr       SNMP
     SYstem       TELnet       BOotp        AUTHentication
     ACCounting

Local> SET INT ?
     ADdress      SUBnet       MASk         GATeway
     HOSt         NAme         NAMEServer

Local> SET INT ad ?
     NONe         ip_address

Local> SET INT AD 111.222.222.111
```

Figure 4-3. Changing the Internet Address.

ACC presents possible keywords as a combination of CAPITAL and small letters. It is enough to enter just that portion of the command seen in capital letters for it to be recognized by the Terminal Server. Therefore, INTERNET can be abbreviated to INT and PORTS to PO.

If the whole parameter is in small letters (such as ip_address in the previous example), then it should be entered as an equivalent value (such as 111.222.222.111).

4.2.3 Command Line Editing/Special Keys

Several special keys may be used to facilitate the command entry process. These keys can be used from any ANSI-compliant terminal. **Table 4-2** displays these keys and their functions.

Table 4-2. Special Keys Functions.

Key	Function
Left and right arrow keys	Moves the cursor along the current command line to enable changes to be made.
Up and down arrow keys	Scrolls through previous commands entered by the user. Each arrow-up press will regress to a previously entered command line. Similarly, an arrow-down will progress to a more recently entered command line (dependent on terminal program).
<Backspace> or <Delete>	Deletes the one character to the left of the cursor.
<Ctrl/U>	Deletes the current command line.
<Ctrl/Z>	Operates like a <Ctrl/U> except when entered in response to a password or verification prompt. It stops the password-entering process (either the password itself or the verification) and returns the Terminal Server to local mode. If it is used in response to a username prompt, it causes the defined port name to be used for the specific username. NOTE: <Ctrl/Z) does not unlock a locked terminal (refer to the LOCK command).
<Enter>	Executes the current command line.

4.2.4 Naming Conventions for Terminal Server and for LAT Services

Some commands require you to enter a name, whether it is that of the Terminal Server itself or a node, port, or service. All variable names must consist of a string of between 1 and 16 characters and cannot be abbreviated. The allowable characters are from A to Z, 0 to 9, $, - (hyphen), _ (underscore), and the . (period). The Terminal Server is not case-sensitive.

Terminal Server names must be unique to a local area network (LAN) and port names must be unique within the Terminal Server itself. LAT service names must be unique for each service on the LAN, but one service may be offered by multiple service nodes.

These naming conventions do not apply to user names, Terminal Server names or service identification messages.

4.2.5 Command Requirements and Restrictions

You can enter the Terminal Server commands in either uppercase or lowercase characters, or a combination of both since the Terminal Server is not case-sensitive. The words in a command line must be separated by one or more spaces.

Command lines can contain up to 132 characters. You can continue a command line onto a second terminal display line provided you do not press the <Return> key at the end of the first display line. In local mode, there is no such type-ahead facility.

You can interrupt current local mode output by pressing the <Break> key or by entering your local switch character (discussed later). When a command fails to execute, you get an error message. If you make an error in a command line, the Terminal Server rejects the entire command line. If you get an error message, check the command syntax and re-enter all or part of the command as required. When a command has executed successfully, the Terminal Server will display the local mode prompt.

4.2.6 Management Command Language

Commands may be entered in the Terminal Server in Local Mode. The local mode is easily identified by the local prompt and cursor, Local>, which appears once a connection is established with the server from either a directly-connected terminal (in which case the operator needs to press the <Enter> key twice) or via some form of remote network access (using either Telnet or LAT). This mode allows the administrator to enter commands. Each command line begins with a verb that instructs the server to perform a specific operation. The two major categories of commands are:

- Management Command—Used to configure the Terminal Server. These are implemented mainly by the system administrator. However, some limited management commands are also available to an ordinary user. Here, the relevant commands will affect the user's own port only.
- User Commands—Used to operate the Terminal Server by ordinary end-users.

Management Commands

Management commands are used to configure and verify the Terminal Server setup. The three groups of commands are shown in **Table 4-3**.

Table 4-3. Management Commands.

Group	Commands
(I) To add settings	SET, DEFINE, or CHANGE
(II) To remove settings	CLEAR or PURGE
(III) To verify settings	SHOW or LIST

Each command group affects either the Permanent Data Base (PDB) or the Operational Data Base (ODB) setup of the Terminal Server.The PDB resides in non-volatile memory so its contents are saved even without external power connected to the Terminal Server. The ODB, however, resides in regular RAM (Random Access Memory) which means that any changes made to the ODB will be lost if the Terminal Server is disconnected from its power source or is reinitialized in any other way.

When the Terminal Server is switched on, the contents of the PDB are copies to the ODB. In fact, parameters associated with the serial and parallel ports of the Terminal Server are copied from the PDB to the ODB each time that port is accessed or disconnected.

Table 4-4 shows the confines of each management command: (A √ indicates that the specified database is influenced by the relevant command while an X means that it is not influenced).

Table 4-4. Management Commands.

Operation	Command	PDB	ODB
Configure Options	DEFINE	√	X
	SET	X	√
	CHANGE	√	√
View Configuration*	SHOW	X	√
	LIST	√	X
Remote Configuration Options	CLEAR	X	√
	PURGE	√	X

NOTE

Use the LIST command to view changes implemented by the DEFINE command and use SHOW to view changes made by the SET command.

4.2 Configuring Terminal Server Parameters

The initial setup of the IP environment in the Terminal Server involves several key steps:

- Defining IP and/or LAT parameters—This involves the configuration of the basic IP and/or LAT parameters of the Server's network port. For IP use, the IP address, subnet mask, gateway, DNS server need to be defined. For LAT, the Terminal Server is ready immediately.
- Defining server wide characteristics—This involves Password enable, authentication, Inactivity, ID-String, Broadcast.
- Defining port characteristics—This involves setting the access, speed, flow control, signals, messages, Break, and a password.
- Defining session characteristics—This includes definition of the default protocol, dedication, session-limits, auto-connect. For Telnet sessions specifically, there is the definition of: CR translation, binary translation, special characters, and for LAT sessions there are settings of groups, queues, and services.

4.3.1 Basic IP Setup

The following example illustrates the basic IP setup of the Terminal Server:

```
1. Local> CHANGE INTERNET ADDRESS 111.122.133.144
2. Local> CHANGE INTERNET MASK 255.255.255.0
3. Local> CHANGE INTERNET GATEWAY 111.122.133.155
NETWORK ANY
```

Figure 4-4. Basic IP Setup of a Terminal Server.

Step 1: Defines the IP Address

Statement 1 defines the IP address of the Terminal Server.
(In this example, 111.122.133.144).

Step 2: Defines the Subnet Mask Information

Statement 2 defines the subnet mask information. If your configuration does not use subnets, you will not need to define the mask value as the Terminal Server will define the correct mask value according to the class of IP address.

Subnets divide one network into multiple smaller ones. This specifies that this will not be a regular Class C address (up to 254 hosts) but rather that the network ID portion will be extended by the first 3 bits of the fourth byte.

Step 3: Defines the IP Router (gateway)

Statement 3 defines the IP router (gateway) that will be used for transmitting frames to stations outside the local network and builds the Routing Table of the Terminal Server. The router IP address, in this example, is defined as 111.122.133.155. The ANY parameter specifies that IP frames to any network will be transferred through this router.

You may add more entries to the Routing Table, specifying distinct networks and hosts. Refer to **Chapters 6, 7,** and **8** for more information.

Step 4: Verify the IP Setup

The basic IP settings can be verified by using the commands: SHOW INTERNET, SHOW INTERNET GATEWAY.

Note that if DEFINE is used as the verb in a configuration command, that specific configuration will be available only after re-initializing the Terminal Server. For this purpose, you would use the INIT DELAY 0 command.

Figure 4-5 shows a sample output of the SHOW commands (SHOW may be abbreviated as SH).

```
Local> SH INTERNET
Internet Address:  111.122.133.144
Subnet Mask:  255.255.255.0

Local> SH INTERNET GATEWAY
Gateway:  111.122.133.155 Network:  255.255.255.0
```

Figure 4-5. SHOW Commands.

4.3.2 Domain Name System (DNS) Server Setup

The Terminal Server may access a DNS (Domain Name Server) in order to translate IP host names into IP addresses. This allows users to refer to hosts by their names rather than by their addresses, while avoiding the need to update the Host Table in each and every Terminal Server. For example:

```
1. Local> DEFINE INTERNET NAME RESOLUTION DOMAIN machine.test.com
2. Local> DEFINE INTERNET NAMESERVER sample ADDRESS 222.223.224.225
```

Figure 4-6. DNS Server Setup.

Step 1: Defines the Domain Name

Statement 1 defines the *domain name* in which the Terminal Server is operating. This allows users to specify the default relative host name (when referring to an address within the defined domain) and to omit the domain name from each specific request.

Step 2: Defines the DNS Address

Statement 2 defines the specific IP address of the remote DNS server itself (222.223.224.225 in the abov e example). It also specifies the DNS server name to be *sample* (largely for display purposes). The Terminal Server can hold 20 addresses in its built-in Host Table. If this table contains data, the Terminal Server will first search it for name resolution before querying the DNS server.

```
LOCAL> DEFINE INTERNET HOST machine2 ADDRESS 111.132.132.111
```

Step 3: Verify the DNS Setup

Use the Show Internet Name Resolution command. The following shows the output of these commands:

```
Local> SHOW INTERNET NAME RESOLUTION
Domain Name: MACHINE.TEST.COM

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

Nameservers:
222.223.224.225      SAMPLE.MACHINE.TEST.COM
Local>
```

Figure 4-8. Show Internet Name Resolution Command.

4.3.3 Using the Bootp Protocol

Setting the Terminal Server IP parameters can be done based on its specific hardware address (Ethernet MAC address). It is the BOOTP server that provides the hardware-to-IP address resolution. With BOOTP, the network manager can assign all the network IP addresses using only one file on the BOOTP server. This also allows him to update the default router and DNS server on all the devices from one centralized location. The BOOTP server can run on any UNIX-based machine or PC running a suitable BOOTP application.

On Power-On (or reset), the Terminal Server can search for a BOOTP server on the local network and request a valid IP address for itself, for its gateway and for its DNS server. These addresses will then be used and can also be saved in non-volatile memory if required.

The following is an example of configuring the Terminal Server to use BOOTP:

```
1. Local> DEFINE BOOTP ALWAYS
2. Local> DEFINE BOOTP SAVE
3. Local> DEFINE BOOTP VENDOR NONE
```

Figure 4-9. Configuring the Server to use BOOTP.

Step 1: Defining when to use BOOTP

Statement 1 is used to configure the Terminal Server to make use of BOOTP features every time it is powered on or reset. The Terminal Server will broadcast a request onto the local network and if an online BOOTP server responds with IP values, they will become the settings for the Terminal Server.

Step 2: Defining the Save Option

The IP parameters received from the BOOTP server are implemented with immediate effect. These values will also be saved in non-volatile memory. Statement 2 saves these values. Statement 3 specifies which BOOTP extensions, if any, are to be used. See **Chapters 6, 7,** and **8** for more details.

4.4 Configuring Serial Ports

One can connect display terminals, printers, serial IP stations, and other devices with asynchronous ports to any of the Terminal Server's serial ports. Each class of device requires a slightly different serial port configuration. Please refer to the next sections for the correct setting for each application of a serial port.

A common use for Terminal Server ports is for connecting local terminals. There is an autobaud feature that attempts to configure a port with the correct baud rate by analyzing the first two <Enter> key presses made by the user before logging in. For devices that do not log in, such as printers, or for low rates less than 1200 baud, this autobaud aid does not work. Ports required to offer services should also have this feature disabled. Refer to the SET PORT n AUTOBAUD command.

Multiple Characteristics in a Single Command Line: You may enter multiple options in a single command line, restricted only by the 132 character limit. For example, if you wish to set port 3 on the Terminal Server for not receiving broadcast messages, even parity, and a port speed of 19200, you would type the following command line at the local prompt:

```
Local> SET PORT 3 BROADCAST DISABLED PARITY EVEN SPEED 19200
```

The SET PORT BROADCAST enables/disables messages from other users. Another notable option used often for asynchronous ports include SET PORT LOSS AUTHENTICATION which is used in low-speed connections to notify the user in case of data loss.

4.4.1 Port Naming Convention

Table 4-5 shows the names by which the PORT command refers to the serial and parallel ports of the Terminal Servers.

Table 4-5. Port Naming Convention.

Model	Port Type	Name	LAT Name
Single-Port Terminal Server	Serial	1	N/A
4-Port Terminal Server	Serial	1-4	PORT_1-PORT_4
4-Port Terminal Server	Parallel	PRINTER	PRINTER_1
8-Port Terminal Server	Serial	1-8	PORT_1-PORT_16
8-Port Terminal Server	Parallel	PRINTER	PRINTER_1

4.4.2 Specifying a Port List

When specifying a port-list in a Terminal Server command, you can refer either to a single port or to a range of ports (lowest-to-highest or vice-versa). The parallel port is designated a name PRINTER. When setting port characteristics with one or more options, the port-list can have embedded spaces.

```
1 Local> DEFINE PORT 2 AUTOBAUD DISABLED SPEED 19200
2 Local> DEFINE PORT 2 CHARACTER 8 PARITY NONE STOP 1
3 Local> DEFINE PORT 2 FLOW CONTROL XON
```

Figure 4-10. Different Port List Methods.

In the example shown in **Figure 4-10**, statement 1 refers to ports 1, 2, and 3—as well as the parallel port (of a 4- or 8-Port Terminal Server).

4.5 Configuring Terminal Ports

The most common device used with the Terminal Server is the display terminal. This section describes the serial port and other settings necessary to configure the Terminal Server for connection of display terminals. Terminals may be connected to the Terminal Server using one of two methods:

- Directly-Attached Terminal—The terminal is connected with a cross-cable (or "null-modem cable") to the serial port of the Terminal Server. The Terminal Server supports either RS-232 or RS-423 standard automatically (there is no need to configure for either). Verify that all cables in use are within the maximum length specified by these standards.
- Modem-Attached Terminal—The terminal is connected via modem and therefore, avoids the distance limitations mentioned above. The modem may be asynchronous, leased-line, or any dialup modem. The modem near the server port should be connected with a straight DCE cable to the serial port of the Terminal Server.

4.5.1 Physical Characteristics—Directly-Attached Terminals

The following examples show some common commands one can use when configuring terminal ports. Although all of the examples refer to port 2, one can configure more than one port in each command.

Figure 4-11 shows how to define the physical characteristics of the serial port.

```
1. Local> DEFINE PORT 2 AUTOBAUD DISABLED SPEED 19200
2. Local> DEFINE PORT 2 CHARACTER 8 PARITY NONE STOP 1
3. Local> DEFINE PORT 2 FLOW CONTROL XON
```

Figure 4-11. Configuring a Port for a Directly-Attached Terminal.

Step 1: Define the Port Speed

Statement 1 prevents the Terminal Server from sensing the speed used by the specified port automatically. Rather, it specifies a forced baud rate.

NOTE

The port characteristics must match the settings of the terminal in order for communications to work. Setting a baud rate of 19200 on the port and using a terminal with a set baud rate of 9600 will not work.

One can also set different speeds for input (terminal-to-Terminal Server) and for output (Terminal Server-to-terminal). This is done by entering DEFINE PORT INPUT SPEED xxxx, and DEFINE PORT OUTPUT SPEED yyyy.

Step 2: Define the Port Async Parameters

Statement 2 specifies the character size, parity setting, and number of stop bits. This example shows the most common scenario sometimes referred to in literature as 8-N-1 (8 bits per character, No parity, and 1 stop bit).

Step 3: Define the Port Flow Control

Statement 3 dictates that the port will use XON/XOFF flow control—also known as software flow control. This is the most common case for directly-attached terminals. If this statement is entered, the attached terminal must also be set to use the same flow control mechanism. You may also use other methods of flow control. Other relevant configuration commands that may apply here are DEFINE PORT FLOW CONTROL and DEFINE PORT LOSS NOTIFICATION.

4.5.2 Physical Characteristics—Modem-Attached Terminals

The example in **Figure 4-12** shows how to define the physical characteristics of the serial port with a modem connection to a terminal.

```
1 Local> DEFINE PORT 3 AUTOBAUD DISABLED SPEED 19200
2 Local> DEFINE PORT 3 CHARACTER 8 PARITY NONE STOP 1
3 Local> DEFINE PORT 3 FLOW CONTROL CTS
4 Local> DEFINE PORT 3 SIGNAL CHECK ENABLED
5 Local> DEFINE PORT 3 SIGNAL CONTROL ENABLED
```

Figure 4-12. Configuring a Port for a Modem-Attached Terminal.

Step 1: Define the Port Characteristics

In statement 1, a fixed speed of 19200 baud is defined and in 2, the port is defined as 8-N-1.

Step 2: Define the Port Flow Control

In statement 3, the recommended flow control mechanism for modem-attached terminals—CTS/RTS—is implemented.

NOTE

CTS/RTS is a flow control between the Terminal Server and the attached modem. The modem itself must be configured to use the same flow control mechanism.

Step 3: Define the Modem Control Options

Statements 4 and 5 define the ability of the Terminal Server to work with the RS-232 (or RS-423) signal lines (DTR and DSR signals). This feature allows the host to log out a session if the modem disconnects and also to force the modem to disconnect if the host itself ends a session. Enabling Signal Check on a specific port will cause the Terminal Server to wait for an active DSR signal before starting any data reception and to log out the port if the DSR signal is inactive.

Enabling Signal Control will configure the Terminal Server to activate DTR during an active session and to deactivate it when the port is logged out.

4.5.3 Operational Characteristics

In addition to the physical characteristics defined in the previous section, various operational characteristics may be defined for the ports.

Figure 4-13 shows examples that show several options that can be selected for a terminal.

```
1 Local> DEFINE PORT 1 DEDICATED 111.112.113.114

2 Local> DEFINE PORT 1 PREFERRED 111.112.113.114

3 Local> DEFINE PORT 1 SESSION LIMIT 3

4 Local> DEFINE PORT 1 INACTIVITY LOGOUT ENABLED

5 Local> DEFINE PORT 1 TELNET CLIENT TERMTYPE vt220
```

Figure 4-13. Operational Port Options.

1. Defining the Port as Dedicated

Statement 1 defines the port as a *dedicated port* which means that it prevents users from logging on to any other server than that specified (111.112.113.114). By default, using a dedicated setting on a port makes that port AUTOC ONNECT, disable BREAK, and allows a single session.

2. Defining the Port as Preferred

Statement 2 specifies a preferred host on the specified port. This is useful when you need to allow the user to connect to any host, not necessarily from the start, but with simplified access to a particular host. In **Figure 4-13**, the user would only need to enter CONNECT with no further parameters, or even just C, and the port would automatically Telnet to the preferred host 111.112.113.114.

If neither the DEDICATED nor the PREFERRED characteristics is predefined, the user will have to enter the full Telnet command and host name or address as part of the CONNECT command.

3. Defining the Maximum Number of Concurrent Sessions

Statement 3 limits the number of concurrent sessions permitted from the port, in this example to three. It allows the user to open up to three sessions, and to switch back and forth among them. The default is four sessions, but users on DEDICATED ports are automatically set to a limit of one.

4. Defining an Inactivity Log-out Period

Statement 4 enables the inactivity logout facility. This automatically logs off the user after a set period of idle time (set by the DEFINE SERVER INACTIVITY TIMER command).

5. Defining the Type of Terminal Connected to the Port

Statement 5 defines the type of terminal connected to the port. This information (vt220 in the example, which stands for the DEC VT220 display terminal) is used during the opening stage of the Telnet session to advise the host as to the type of terminal in use. Most UNIX applications will use this information in order to determine the appropriate data stream for communication with the terminal. The Terminal Server itself does not use this information when communicating with the attached device nor does it verify the validity of the name entered so any character string may be used. This setting is optional. The default is ANSI.

Other configuration commands that may apply here are:

- DEFINE PORT BREAK LOCAL/DISABLED/REMOTE—this defines the handling of a BREAK signal sent from the terminal to the Terminal Server. There are three possibilities:

a. LOCAL specifies that the BREAK signal will be used to switch the user to local mode. This is the default definition.

b. DISABLED specifies that the BREAK signal is to be ignored.

c. REMOTE causes the BREAK signal to be translated into a special Telnet command that is sent to the host (TELNET BREAK) without affecting the Terminal Server.

- DEFINE PORT BROADCAST ENABLED/DISABLED—This allows/disallows the port to display messages from any other ports. Messages are sent using the BROADCAST command. (Default: ENABLED)

- DEFINE PORT LOCK ENABLED/DISABLED—This allows/disallows a user to lock his terminal (Default: ENABLED)

- DEFINE PORT PASSWORD ENABLED/DISABLED—This determines if the *global server password* is required to log in to the specified port. This password is set by the DEF SERVER LOGIN PASSWORD command and applies to all the ports. If enabled, initial connection to a protected port will display a single # and you have three chances to enter the password. (Default: DISABLED and set to "access.")

NOTE

This command should not be confused with PORT AUTHENTICATION, which is used with RADIUS to fully authenticate specific users and passwords.

- DEFINE PORT SECURITY ENABLED/DISABLED—This forces the port into a secure status where only several non-privileged commands are permitted. (Default: DISABLED—meaning that the port is not secured.)

- DEFINE PORT TELNET CLIENT—These parameters control the behavior and options of the Telnet session initiated by the terminal connected to the port. The default conditions are generally appropriate. Reasons for change may include a need to prevent a special character from being interrupted by the Terminal Server and to allow it to be sent to the application. For further information, refer to **Chapters 6, 7,** and **8**.

- DEFINE PORT USERNAME user_name—This associates a permanent username to the port, eliminating the prompt-request usually displayed on login. This parameter is overridden if the port login needs to be authenticated by RADIUS.

- DEFINE PORT VERIFICATION ENABLED/DISABLED—This defines if the Terminal Server will send messages to the attached device regarding the connection, disconnection, or switching of sessions. (Default: ENABLED)

4.5.4 Using Special Characters

Certain specially-defined characters that are sent from a terminal attached to a port are acknowledged by the Terminal Server as commands and, therefore, are not forwarded to the user's session. Occasionally, a specific application will require that one or more of these characters should nevertheless be forwarded since they have special meaning that can not be altered. In such a case, these characters must be disabled or changed in the Terminal Server.

Table 4-6 lists functions of the Terminal Server that are set, by default, to use specific characters. It shows the functions, the default keys that are assigned to them and the commands that alter them.

NOTES

Some functions are defaulted to NONE.

The ^ refers to the Control-key that should be pressed together with the subsequent letter.

Table 4-6. Special Characters Functions.

Function	Default Key	Command
Resume connection with previous session	NONE	PORT BACKWARDS SWITCH
Resume connection with next session on the session list	NONE	PORT FORWARD SWITCH
Switch to local mode	NONE	PORT LOCAL SWITCH
Send TELNET Abort Output (AO) request	^O	PORT TELNET CLIENT AO
Send TELNET Are-you-there (AYT) request	^T	PORT TELNET CLIENT AYT
Send TELNET Break (BRK) request	NONE	PORT TELNET CLIENT BRK
Send TELNET End of Record (EOR) request	^Y	PORT TELNET CLIENT EOR
Send TELNET Interrupt Process (IP) request	^Y	PORT TELNET CLIENT IP
Send TELNET Synch (Synch) request	^X	PORT TELNET SYNCH

4.5.5 Logical Characteristics—LAT

The following example shows several logical options that are unique to the LAT environment. You can add them to a terminal definition.

```
1 Local> DEFINE PORT 1 DEFAULT PROTOCOL LAT
2 Local> DEFINE PORT 1 AUTHORIZED GROUPS ALL ENABLED
3 Local> DEFINE PORT 1 DEDICATED r11at
```

Figure 4-14. Configuring Terminal—Logical Port Setup for LAT

Step 1: Define LAT as the Default Protocol

Statement 1 indicates that the primary use of the port will be for LAT sessions (the default is Telnet). The Terminal Server will assume that all user requests are for LAT services unless TELNET will be specifically indicated in the user's command.

Step 2: Define Authorized LAT Group for the Port

Statement 2 permits all LAT service groups to be available to this port. If this command is omitted, only group 0 will be authorized. The user may later use the PORT GROUPS command to restrict the authorized groups further and to associate himself with only part of the groups. For example, when he uses the SHOW SERVICES command, he will see only a partial listing of available services, those that belong to his group. Statement 3 specifies that on this DEDICATED port, the user is prevented from logging on to any host on the network other than that specified.

Other configuration commands that may be used for LAT terminals are:

- DEFINE PORT LIMITED VIEW—This prevents the terminal user from listing the LAT nodes and LAT services. (Default: DISABLED)
- DEFINE PORT NAME—This specifies a unique port name to the port. Refer to the previous section for the list of default names.
- DEFINE REMOTE PORT MODIFICATION—This allows or prevents a LAT service to change port characteristics. (Default: DISABLED)

4.6 Accessing the Terminal Server from Remote/Network (Reverse-Telnet)

One can Telnet to the Terminal Server as well as to each of its specific ports, including its parallel port, without needing separate IP numbers for each. This allows you to share asynchronous devices such as modems and parallel devices such as printers.

The Terminal Server is pre-configured with a Telnet listener function on TCP port 23. Once a Telnet session is initiated to the Terminal Server on this TCP port from any Telnet client, the user sees the same interface as if he was accessing the server from a terminal connected directly to one of its serial ports. This is useful for accessing the Terminal Server from a Telnet client for management purposes.

The Telnet listener function is also associated with a TCP port in order to differentiate between the serial ports of the Terminal Server, (bearing in mind that the Terminal Server owns only one IP address and that several printers may be connected at once). Therefore, there may be several Telnet listeners defined on one specific Terminal Server, each listening on its own TCP port and directing the information received by the session to a specific serial or parallel port.

The Reverse Telnet (or Telnet Listener) service of the Terminal Server may be used for many common applications:

- Connecting printers to the Terminal Server in a TCP/IP environment—Terminal Server ports that are connected to printers are configured as a Telnet listener. Hosts that need to print on these printers will use the Telnet protocol to communicate with the Terminal Server.

- Communicating with serial devices from LAN stations—A Telnet listener can also be configured to connect a Telnet client through the Terminal Server to a specific serial (RS-232) device such as a modem.

  In a specific case, the connecting Telnet client could be that of another Terminal Server. In this case, its serial device connects and starts a Telnet session on its behalf with a similar device. This is referred to as a back-to-back application, and allows the transfer of serial traffic over TCP/IP backbones.

Figure 4-15 shows a typical configuration of a Telnet listener. Port 1 is used in this example, but any port could be used, including the parallel port, which is referred to as PRINTER.

```
1 Local> DEFINE PORT 1 ACCESS REMOTE AUTOBAUD DISABLE SPEED 9600
1 Local> DEFINE TELNET LISTENER 2001 PORTS 1 ENABLED
1 Local> DEFINE TELNET LISTENER 2001 CONNECTIONS ENABLED

2 Local> DEFINE PORT 1 TELNET SERVER NEWLINE TO TERMINAL <LF>
2 Local> DEFINE PORT 1 TELNET SERVER NEWLINE FROM TERMINAL<CRLF>

3 Local> DEFINE PORT 1 TELNET SERVER BREAK NONE
3 Local> DEFINE PORT 1 TELNET SERVER AO NONE
3 Local> DEFINE PORT 1 TELNET SERVER AYT NONE
3 Local> DEFINE PORT 1 TELNET SERVER IP NONE
```

Figure 4-15. Telnet-Listener—Possible Configuration Options.

1. Define the Port and set Telnet Listener

Statements 1 define the port as a REMOTE port and sets the baud rate to 9600. You can also define a local port or a dynamic port to be a Telnet listener. This access parameter only determines who can login and from which end of the connection. The access itself is allowed regardless of the Telnet Listener itself.

The AUTOBAUD mechanism cannot be used as the port would not be able to receive the <Enter> keystroke required for automatic line-speed regulation. The baud rate set here should be the same as that used by the serial device connected to the port.

The Telnet listener function is also defined. The Telnet listener will wait for incoming connection requests on TCP port 2001 and will redirect any received data to the physical serial port 1 and vice-versa. Use a TCP port that can be easily associated with the serial port used. The physical port number and the TCP Port number are not actually dependent on one another. TCP port 2001 is bound to physical port 1 above only for convenience. We could have used TCP port 2007 for physical port 16.

NOTE

More than one serial port can be configured using this command (a rotary facility). If more than one port is defined and a session is started, the server will direct the data to the first available port among those defined. Each subsequent connection to the same port will be associated with the next available port until all ports assigned to this listener are in use.

Statements 2 designate a single or double character sequence which is translated to a new line when received by the Terminal Server from the terminal, or which is sent from the Terminal Server to the user terminal after receiving a new line character sequence from the remote host.

2. Define the Telnet Server

Statements 3 specify that the Telnet server function used with this port will disregard the following special Telnet signals: AO (*abort output*), AYT (*Are you there*), BRK (*Break*), and IP (*Interrupt Process*). These are relevant to binary communication and not always required. The BRK option is an important one to point out because it specifies whether a local break request initiated by the remote user is interpreted into a break at the Terminal Server port or echoed through as a special character.

3. Verify the Configuration

The following steps need to be carried out in order to verify the configuration of a Telnet listener:

1. Verify the configuration with the SHOW TELNET LISTENER command as shown in **Figure 4-16**.

```
Local> SHOW TELNET LISTENER 2001
Listener TCP-port: 2001
Identification:
Ports: 1
Connections:  Enabled
Local>
```

Figure 4-16. Show Telnet Listener Command.

2. Connect the asynchronous device to the serial on which the listener function has been defined (port 1 in the above example).

3. From any Telnet client that can reach the Terminal Server, open a Telnet session with the Terminal Server. A typical command would be: telnet *CS_IP_address TCP_PORT*, where `CS_IP_address` is the IP address of the Terminal Server and `TCP_PORT` is the TCP port defined in the Telnet Listener command.

4. After the connection is established, any data from the attached device is transmitted to the network and back.

5. The same is applicable for the parallel printer port but it is uni-directional.

4.7 Configure LAT Services (Reverse LAT)

A LAT service may be defined in the Terminal Server to allow other LAT hosts to create a session with the Terminal Server. The following applications may necessitate reverse LAT services:

- Accessing the Terminal Server from another LAT node for management purposes–A LAT service may be defined to allow access to the Terminal Server itself. When a LAT session from any LAT node to the Terminal Server is started, the same user interface is presented to the operator as if he was accessing the server from a terminal connected directly to one of its serial ports.

- Connecting printers to the Terminal Server in a LAT environment—Terminal Server ports that are connected to printers should be configured as a LAT service. Hosts that need to print will then start a LAT session with the Terminal Server. Any combination of service names together with the port they serve may be defined. More than one service name can be defined and this name can then be used to access more than one port.

- Communicating with serial devices from a LAT node—A LAT service can be configured to connect other LAT nodes to any serial (RS-232) device. In particular, the connecting LAT node can be another Terminal Server that connects with a serial device and starts the LAT session on behalf of these devices.

The following examples show:

- Definition of a LAT service for accessing the Terminal Server.
- Definition of a LAT service for connecting a printer.

4.7.1 Define LAT Service for an Access Port

```
1 Local> DEFINE PORT 1 ACCESS REMOTE

2 Local> DEFINE SERVICE justaname CONNECTIONS ENABLED
3 Local> DEFINE SERVICE justaname PORTS ACCESS
```

Figure 4-17. A LAT Service Accessible Port.

1. Definition of a Port

Statement 1 defines port 1 with the ACCESS REMOTE characteristic, allowing it to be accessed from the LAN.

2. Definition of the LAT Service

Statement 1 and 2 define a new LAT service called *justaname* and enable it. Moreover, statement 3 defines it as an *access* service, which means that a user initiating a session to this service will be communicating with the Terminal Server itself, rather than a serial port (as in **Figure 4-18**).

4.7.2 Defining a LAT Service for a Serial Port

```
3 Local> DEFINE SERVICE justaname PORTS 1 ENABLED
```

Figure 4-18. LAT Service for a Serial Port.

If Statement 3 from the previous example is replaced by the one above, associate it with serial port 1.

Other configuration commands that may apply here are:

- DEFINE SERVICE PASSWORD—This assigns a password to a LAT service. The LAT node that would access that service must submit this password.
- DEFINE SERVICE QUEUE ENABLED/DISABLED—This indicates the use of the LAT queue facility. When this option is enabled, any request for a LAT session to the service will be queued and attended to on a FIFO (First-In, First-Out) basis.

4.8 Configuring Printer Ports

4.8.1 Adding TCP/IP Printers

The process of configuring a printer in a TCP/IP environment involves two key steps:

- Definition of a *Telnet listener* function to the port where the printer is connected.
- Defining the printer in the host printing system by having it use either Telnet or the compatible **prtcp** program as the printing program.

A Telnet listener is defined in the Terminal Server and a printer is defined in the UNIX system. The UNIX printer is directed to use a script and the script is executed with a Telnet command. When a print job is sent by UNIX, a Telnet session is established and the data is sent to the Terminal Server. The Terminal Server, based on the TCP port used in the session, will pass the data either to the serial or to the parallel port defined in the Telnet-Listener command. UNIX may use either the original Telnet program or the **prtcp** program. The same parameters are used in either.

Host Definition

Copy the downloaded PRTCP.C source and MAKEFILE executable files to your UNIX system and compile using the given MAKEFILE. You may have to change the library file you link with to fit your Operating System. Then, follow the relevant instructions for your UNIX to complete the procedure.

Sun Os

Perform the following steps for each printer:

1. Edit the /etc/printcap file to include a queue named CSqueue (for example):

   ```
   CSqueue|CSqueue:\
   :lp=/dev/null:sd=/usr/spool:of=/etc/CSprint
   ```

2. Create the /etc/CSprint shell script:

   ```
   #!/bin/csh -f
   telnet 130.34.28.10 2007
   ```

   You can now use the following standard command for printing:

   ```
   LPR -PCSqueue file_name
   ```

   Where `CSqueue` is the queue defined in step 1, and `file_name` is the file to be printed.

IBM AIX

Follow these steps for each printer:

1. Define a printer device:

   ```
   cp/dev/null/dev/printer_name
   chmode 666/dev/printer_name
   ```

2. Define the printer to the AIX system:

   ```
   smit mkvirptr
   ```

3. Choose 1 on the menu shown to determine where the printer will be attached.

4. Specify the device defined in the previous step (printer_name).

5. When defining the queue name, choose a name other than the printer name.

6. Answer any other questions relevant to the printer attached.

7. Create a script file with the following script:

```
#!/bin/sh
/usr/lib/lpd/piobe $*|telnet IP_address_of_Passaport TCP_port
```

This will be the "back-end shell script" for the printer. It uses the piobe program (standard AIX printing program) and pipes the results to a Telnet program that drives the information to the Terminal Server.

If prtcp is used, replace the Telnet program in the above script with prtcp. Note that in this case, you must start the STREAMS environment of the AIX, by executing the *strload* command. Refer to the AIX documentation regarding *PSE* (Portable STREAMS Environment) for more information on the STREAMS environment. The prtcp program uses the TLI system services provided by PSE.

8. Make the script executable:

```
chmod +x backend_file_name
```

9. Define the script the AIX system by:

```
smit chquedev
```

10. Choose the printer and queue defined earlier and edit the "backend program path name" to contain the script created in step 7.

11. Use the lp -d *printer_name* command to print.

HP/UX

1. Define a printer using the program **sam**, specifying */dev/null* as the printer device, or use the following command:

```
/usr/lib/lpshut
/usr/lib/lpadmin -pprinter_name -v/dev/null -minterface_script_file
/usr/lib/lpsched
```

Replace `printer_name` with a name of your choice.

The above command will also create a script file at /usr/spool/interface/printer_name.

2. Replace the script by the following script:

```
cat $6 | telnet IP_address_of_Passaport TCP_port
```

3. If prtcp is used, replace the Telnet program in the above script by prtcp.

4. The script will pipe the printed data through the Telnet command to the IP address of the Terminal Server and to the TCP port defined in the Telnet listener command at the Terminal Server.

5. Restart the **lpsched** process by executing *lpshut* and *lpsched* so that the new definition will be used.

6. Use the *accept* and *enable* commands (both with the printer name as a parameter) to make the printer available.

7. The printer is now ready to print.

SCO

1. Define a printer using the **sysadmsh** program, specifying */dev/null* as the printer device, or use the following command:

```
/usr/lib/lpadmin -p printer_name -v /dev/n
```

Replace printer_name by a name of your choice.

2. The following command will create a script file at

```
/usr/spool/lp/admins/lp/interfaces/printer_name
```

3. Replace the script by the following script:

```
cat $6 | telnet IP_address_of_Passaport TCP_port
```

4. If prtcp is used, replace the Telnet program in the above script by prtcp.

5. The script will pipe the printed data through the Telnet command to the IP address of the Terminal Server and to the TCP port defined in the Telnet listener command at the Terminal Server.

6. Restrat the **lpsched** process (by executing *lpshut* and *lpsched*)so that the new definition will be used.

7. Use the *accept* and *enable* commands (both with the printer name as a parameter) to make the printer available.

8. The printer is now ready to print.

4.8.2 LAT PRINTERS

The process of configuring a printer in a LAT environment involves two steps:

- Definition of a LAT Service function on the port where the printer is connected (refer to Defining LAT Services)
- Definition of the printer in the host printing system

VMS

The following describes the VMS procedure needed in order to define a Terminal Server port as a printer.

```
$ RUN SYS$SYSTEM:LATCP
LCP> CREATE PORT port_name/APPLICATION
LCP> SET PORT port_name/NODE=node_name/SERV=serv_name
LCP> EXIT
$ SET DEVICE/SPOOL=(queue_name, SYS$SYSDEVICE) port_name
```

Figure 4-19. VMS Procedure.

In this example:

- *serv_name* is the name of the LAT service defined on the Terminal Server for the printer
- *node_name* is the node name of the Terminal Server. The Terminal Server does not have a default name but this may be changed by using the DEFINE SERVER NAME command (see Advanced LAT Definitions).
- *queue_name* is the name of the VMS queue created and initiated by this procedure
- *port_name* is of LATxxxx

4.9 Advanced LAT Definitions

The Terminal Server does not require any special definitons in order to work in a LAT environment. LAT, being both dynamic and specifically designed for terminal server environments, is very easy to operate and use. However,

several configuration commands are available in order to enhance control over LAT functionality.

The following list shows some of these commands. A complete list can be found in **Chapters 6, 7,** and **8**.

- DEFINE SERVER NAME—This allows you to change the Terminal Server default name which is CS_xxxxxxxxxxxx, where the 12 xs are the hexadecimal representation of the Terminal Server Ethernet MAC address. This value may be changed to facilitate the definition of the server in other systems (such as when defining printers for VMS hosts).

- DEFINE SERVER CIRCUIT TIME nnn—This defines the time interval between consecutive messages sent by the Terminal Server to the LAT services. The range allowed is between thirty to two hundred milliseconds. The default is 80 milliseconds.

- DEFINE SERVER KEEPALIVE TIMER nnn—This defines the interval between consecutive messages sent for maintaining a LAT session—when there is no data to transmit. The allowed range is 10 to 180 seconds. The default is 20 seconds. Modifying this value may effect the amount of traffic on the local network.

4.10 Advanced Telnet Definitions

The Terminal Server has a group of commands relating to a specific port as a TELNET CLIENT and another for a port as a TELNET SERVER. It is important to distinguish between the two:

- The SET PORT TELNET CLIENT commands change the Telnet client characteristics for the specified port as these commands relate to new Telnet connections established from the specified port.

- The SET PORT TELNET SERVER commands change the Telnet server characteristics for the specified port as these commands relate to new Telnet connections established to the specified port.

A TCP/IP host can translate data transferred during Telnet in several ways and some of the Telnet protocol parameters can be changed using the Telnet Option Negotiation procedure in order to facilitate this.

4.11 Configuring SLIP Ports

The Terminal Server can be used to connect SLIP devices to an IP network. The SLIP (Serial Link Internet Protocol) protocol is a simple implementation of the IP protocol over Asynchronous links. The SLIP device can be a PC, workstation, router, or any other device connected through a serial port to the Terminal Server.

Any SLIP device must be assigned a unique IP address which must be part of the same subnet to which the Terminal Server is connected.

The following example shows a sample configuration of a port which will be used for a SLIP connection.

```
1 Local> DEFINE PORT 2 AUTOBAUD DISABLED SPEED 19200
2 Local> DEFINE PORT 2 DEDICATED SLIP
3 Local> DEFINE PORT 2 SLIP ENABLED
4 Local> DEFINE PORT 2 FLOW DISABLED
5 Local> DEFINE PORT 2 SLIP HOST 111.122.133.144
6 Local> DEFINE PORT 2 USERNAME "SLIP 2"
```

Figure 4-20. Configuring a Port for a SLIP Connection.

Step 1: Define the Port Characteristics

Command 1 defines a fixed speed (of 19200 baud) unlike for directly-attached terminals.

Step 2: Define port as Dedicated SLIP and Enable it

Statement 2 specifies that the port will be attached automatically as a SLIP host when the user logs on to the Terminal Server. DEDICATED prevents the user from using the port as a terminal port and negates the need for any character-mode communication—except the user name and password (if needed). This simplifies the script required to connect the SLIP device to the Terminal Server.

Statement 3 enables the port to work in SLIP mode. To enter SLIP mode, the user issues a "CONNECT SLIP" command or uses the Dedicate definition as in statement 2. After starting the SLIP mode, the Terminal Server will expect only SLIP frames from the attached device.

Step 3: Define the Port Flow Control

We recommend that you disable flow control for directly-attached devices with SLIP connections, such as when a modem is used. Command 2 disables the flow control that is implemented by the SLIP itself. Note that the XON/XOFF mechanism must not be used for SLIP connections.

Step 3: Define the SLIP Port Address

Statement 5 configures the IP address of the port. The IP address can be configured on the port in one of three different methods:

- Configuration by using the Terminal Server command language (as in the example above)
- Configuration by a RADIUS server
- Configuration learned during the session, using the first SLIP frame coming from the device

Step 4: Define the Port User Name

Statement 6 defines a permanent user name to the port eliminating the request-prompt usually displayed when the user logs in. This setting is overridden if the port log-in is to be authenticated by a RADIUS server.

USING COMPRESSED SLIP

Compressed SLIP is an improvement on the regular SLIP protocol. Since IP is a protocol used on a network with many devices and SLIP is a protocol used between only two devices, the IP header contains a lot of data that is now redundant. This data causes a waste of bandwidth when traveling over slow links—a loss that can be countered. The Van-Jacobson Compression method, when supported by both the Terminal Server and the attached device, can save this TCP overhead. The CSLIP protocol can manage up to 16 concurrent TCP/IP sessions.

The following example shows how to add CSLIP capability to a pre-defined SLIP port.

```
1 Local> DEFINE PORT 3 SLIP COMPRESSION ENABLED
2 Local> DEFINE PORT 3 SLIP COMPRESSION AUTOCOMPRESS
3 Local> DEFINE PORT 3 SLIP COMPRESSION STATES 16
```

Figure 4-21. Configuration of a CSLIP Port.

Step 1: Define the Port Characteristics

Statements 1 and 2 set the post-SLIP mode as CSLIP. When using command 1 to implement TCP/IP through the port, the remote node connected to the port must also support the CSLIP protocol. With command 2, the Terminal Server checks the first IP packets received from the node and uses the CSLIP only if initiated by it.

Step 2: Define the Port CSLIP States

Statement 3 defines the maximum number of CSLIP states to be used on the port. The Van-Jacobson compression method uses a STATE data-structure for each concurrent TCP connection. This parameter can limit the number of states. Valid values are between one and sixteen. The default is 16 states.

4.12 Configuring PPP Ports

The Terminal Server can be used to connect devices to the IP network using PPP (Point-to-Point Protocol). The IP-over-PPP protocol uses the standard PPP Link Control Protocol (LCP) to determine the data-link connection and

the IP Control Protocol (IPCP) to establish and configure the network-layer protocol. The PPP device can be a PC, workstation, router or any other device connected through a serial port to the Terminal Server. (For detailed information on both LCP and IPCP, refer to RFC1331 and RFC1332—both available on the Internet.)

Any PPP device must be assigned a unique IP address. This IP address must be a part of the same subnet to which the Terminal Server is connected.

The following example shows how to define the characteristics of a port for PPP connection.

```
1 Local> DEFINE PORT 1 AUTOB DISABLED SPEED 19200
2 Local> DEFINE PORT 1 DEDICATED PPP
3 Local> DEFINE PORT 1 PPP ENABLED
4 Local> DEFINE PORT 1 FLOW DISABLED BREAK DISABLED
4 Local> DEFINE PORT 1 SIGNAL_CONTROL ENABLED SIGNAL_CHECK ENABLED
5 Local> DEFINE PORT 1 PPP IPCP HOST 111.112.113.114
6 Local> DEFINE PORT 1 USERNAME “PPP 1”
```

Figure 4-22. PPP Port Configuration.

Step 1: Define the Port Characteristics

Command 1 defines a fixed speed (of 19200 baud) unlike for directly-attached terminals. Note that AUTOBAUD cannot be performed on PPP frames.

Step 2: Define Port as Dedicated PPP and Enable it

Statement 2 specifies that the port will be attached automatically as a PPP host when the user logs on to the Terminal Server. DEDICATED prevents the user from using the port as a terminal port and negates the need for any character-mode communication—except the user name and password (if needed). This simplifies the script required to connect the PPP device to the Terminal Server.

Statement 3 enables the port to work in PPP mode. To enter PPP mode, the user issues a "CONNECT PPP" command or uses the Dedicated definition as in statement 2. After starting the PPP mode, the Terminal Server will expect only PPP frames from the attached device.

Step 3: Define the Port Flow Control

We recommend that you disable flow control for directly-attached devices with PPP connections, such as when a modem is used. Command 4 disables the flow control that is implemented in any case by the PPP itself.

Step 4: Define the Port IPCP Address

Statement 5 configures the IP address of the port. The IP address can be configured in one of three different methods:

- Configuration using the Terminal Server command language (as in this example)
- Configuration by a RADIUS server
- Learning during IPCP negotiation with the connected device

Step 5: Define the port user name

Statement 6 defines a permanent username to the port eliminating the request-prompt usually displayed when the user logs in. This setting is overridden if the port log-in is to be authenticated by a RADIUS server.

4.12.1 Using Advanced PPP Parameters

The following example shows some additional and more advanced settings available for a PPP defined port. In this example, the same Terminal Server as in the previous example is configured for a modem connection, but also has additional settings to restart the LCP protocol if the connection restarts and

to compress PPP fields. It also forces the node to use a pre-configured IP address on the port.

```
1 Local> DEFINE PORT 1 CHARACTER 8 PARITY EVEN STOP 1

2 Local> DEFINE PORT 1 PPP IPCP COMPRESSION ENABLED
3 Local> DEFINE PORT 1 PPP IPCP COMPRESSION STATES 8
4 Local> DEFINE PORT 1 PPP IPCP ADDRESS ENABLED

5 Local> DEFINE PORT 1 PPP LCP ACFC ENABLED
6 Local> DEFINE PORT 1 PPP LCP PFC ENABLED
7 Local> DEFINE PORT 1 PPP LCP MAP 000A0000
```

Figure 4-23. Advanced Settings for a PPP Defined Port.

1: Definition of Port Communication Parameters

Statement 1 defines the general communication parameters dealing with bits per character, parity and stop bits.

2: PPP IPCP Compression Settings

Statements 2 through 4 specify the IPCP settings. This includes the use of Van-Jacobson compression (2) where the IPCP enables the nodes to negotiate the use of this compression method to reduce the overhead of the TCP/IP headers. Statement 3 specifies the number of TCP connections that the Terminal Server can decompress from the peer at any given time while 4 specifies that the Terminal Server should attempt to negotiate the IP address for both ends of the link. If the negotiation is rejected, the IP layer will fail to open.

3: PPP LCP Compression Settings

Command 5 deals with PPP Address and Control Field Compression and affects the HDLC frames at the Link Layer. These frames include address and control bytes that are obsolete on a PPP link. 5 causes the Terminal Server to negotiate for the omission of these fields during the establishment of a LCP connection.

For PPP links that are used only to connect two stations and that use a single Data-Link Protocol (IP in the Terminal Server case), Protocol Field Compression can reduce the overhead on the PPP frames. Command 6 enables the compression of the PPP Protocol Field.

Statement 6 says that the Terminal Server should invoke PPP Link Control Protocol (LCP) frames after the port is logged on. In this example, the LCP Configuration request starts after the modem is connected and DSR is active.

Statement 7 deals with changing the default Async-Control-Character-Map (ACCM) and causes the Terminal Server to perform byte-stuffing on the bytes representing XON/XOFF. This command prevents the Terminal Server from sending through any character that could be wrongly translated by the modem as flow control characters.

For passive PPP devices as control devices that need to be reconnected after any loss of connection, you should use the DEF PORT n PPP UP PASSIVE DISABLE command.

4.12.2 Verifying PPP Port Configuration and Status

The Terminal Server PPP configuration and status can be verified using the SHOW PORT PPP commands.

A PPP connection starts with the LCP layer establishing the Data Link layer.

The following example displays the port's LCP configuration.

```
Local> SHOW PORT 1 LCP CHARACTERISTICS
Port 1:  PPP 1          Server: CS_0020d207090

LCP Characteristics:
LCP:                    Enabled
Passive Open:           Enabled
Restart Timer:          3 seconds
Max Configure:          10 transmissions
Max Terminate:          2 transmissions
Max Failure:            10 transmissions

LCP Options:            Local:
MRU:                    1500
Character Map:          FFFFFFFF
Authentication:         None
Link Quality:           Disabled
Magic Number:           Disabled
PF Compress:            Disabled
ACF Compress:           Disabled
FCS Size:               16 Bit
```

Figure 4-24. LCP Configuration for a Port.

To find out the current state of a link, you can check the LCP status:

```
Local> SHOW PORT 1 LCP STATUS

Port 1:  PPP 1                Server: CS_0020d2070790

LCP Status:

State:                  Opened
Authentication:         None

LCP Options:            Local:

MRU:                    1500
Character Map:          FFFFFFFF
Authentication:         None
Link Quality:           Disabled
Magic Number:           Disabled
PF Compress:            Disabled
ACF Compress:           Disabled
FCS Size:               16 Bit
```

Figure 4-25. Checking the LCP Status.

The negotiation of IPCP starts after the Link Layer is established and the LCP state is OPENED. The following example asking to verify the IPCP configuration displays an IPCP valid configuration.

```
Local> SHOW PORT 1 ICPC CHARACTERISTICS
Port 1:  PPP 1          Server: CS_0020d2070790

IPCP Characteristics:

IPCP:                   Enabled
Passive Open:           Disabled
Restart Timer:          3 seconds
Max Configure:          10 transmissions
Max Terminate:          2 transmissions
Max Failure:            10 transmissions

IPCP Options:           Local:
Negotiate Address:      Enabled
Remote IP Address:      111.112.113.114
Compress Header:        Disabled
Compress States:        16
```

Figure 4-26. Verifying the IPCP Configuration.

To find out the current state of the IPCP layer, check the IPCP status as follows:

```
Local> SHOW PORT 1 IPCP STATUS
Port 1:  PPP 1          Server: CS_0020d2070790

IPCP Status:

State:                  Opened
Since Open:             0 02:12:08

IPCP Options:           Local:

Negotiate Address:      Enabled
IP Address:             111.112.113.114
Compress Header:        Disabled
Compress States:        0
```

Figure 4-27. Checking the IPCP Status.

4.13 Configuring Security Options

4.13.1 User Security Levels

Three levels of security are available for Terminal Server ports:

- Privileged status—The user at a privileged port has access to the entire Terminal Server command set including commands that manage the Terminal Server, its ports, its sessions, and its services.

  Any user who knows the privileged password can set a port's status to privileged with the SET PRIVILEGED command. For security reasons, a Terminal Server usually has only one privileged user—the person managing the Terminal Server.

- Non-privileged status—Non-privileged status is the default for all interactive ports. Users at a non-privileged port cannot access commands that change the state of the Terminal Server or other ports, but they can use all commands required for connecting to LAT services and Internet hosts from an interactive port.

  Non-privileged users can also modify certain port characteristics and display information about the Terminal Server, its port, and service nodes.

- Secure status—Secure status restricts the commands that are available on a port to a subset of the non-privileged commands. This subset includes commands that are required for connecting to Telnet services and Internet hosts from that particular port. Secure users have access to only limited display information and cannot use the broadcast feature that is available to non-privileged users. Also, secure users cannot use CHANGE and DEFINE commands (only the SET keyword is valid).

  All commands that you can enter from a secure port are identified in **Chapters 6, 7,** and **8**, by the designation "secure." To view all secure commands, issue the SET PORT SECURITY ENABLED command and then access the Terminal Server online help. The commands listed will be those available to secure users.

4.13.2 Conventions for Specifying Passwords

Unless otherwise stated, all passwords consist of between one and sixteen ASCII characters. When specifying passwords in Terminal Server commands, either enclose the password in quotation marks and include it in the command line, or enter the command without the password and let the Terminal Server prompt you for it. You can omit the password value and be prompted for it only in the case where the password characteristic is the only characteristic in the command line. Note that passwords are case sensitive, for example, "SYSTEM" and "system" are different.

The Terminal Server does not echo a password that is entered in response to a password prompt. When you specify a new password, the Terminal Server displays a verification prompt and waits for you to re-enter the password (which again is not echoed). If both entries match, the password is approved and the local mode prompt is displayed. If the password is rejected, the Terminal Server returns to the local mode prompt. You can press <Ctrl/Z> at any time to interrupt password processing and return to the local mode prompt.

You can change the Terminal Server characteristics LOGIN PASSWORD and PRIVILEGED PASSWORD, but you cannot clear them; you can change or clear the service characteristic PASSWORD and the Terminal Server characteristic ACCESS PASSWORD.

To clear a service password, specify quotation marks with nothing in between them (" ") in place of the password in the command line.

The privileged mode of the Terminal Server is password protected. Please refer to *Using Privileged Mode* for further information.

4.13.3 Using a General Password

A general password may be defined for the Terminal Server and both enabled or disabled per port. If a serial port is defined with the PASSWORD characteristic, then each log-in operation to this port will prompt the user (with a #) to enter a valid general password. Once the password is entered and verified, the user will then see the usual Terminal Server startup screen.

The following example shows how to protect port 1 with a general password.

```
1 Local> DEFINE SERVER LOGIN PASSWORD secret
Password>secret (not echoed)
Verification> secret (not echoed)
2 Local> DEFINE PORT 1 PASSWORD ENABLED
```

Figure 4-28. Protecting Port 1 with a General Password.

Statement 1 sets the server log-in password as "secret." This is a global password and each port defined with the PASSWORD characteristic (as in statement 2) will use the *same* password.

When a user connects to port 1 and tries to log in, he will be prompted to enter the correct server password (with a # prompt).

4.14 Authentication—Using RADIUS

RADIUS (Remote Authentication Dial In User Service) is a system of distributed accounting and security that both secures remote access to networks and network services against unauthorized access and monitors the accounting activity of sessions. RADIUS security includes two pieces: an authentication server and client protocols. The server is installed on a central computer at the customer's site. The client side is implemented in the Terminal Servers.

RADIUS is designed to simplify the security process by separating security technology from communications technology. All user authentication and network service access information is located on the authentication, or RADIUS, server. This information is contained in a variety of formats suitable to the customer's requirements. RADIUS in its generic form will authenticate users against a UNIX password file, Network Information Service (NIS), as well as a separately maintained RADIUS database.

Terminal Servers working with modems operate as RADIUS clients. The RADIUS client sends authentication requests to the RADIUS server which responds accordingly.

The protocol defines two entities:

- RADIUS Client—a device that needs authentication services. The Terminal Server, for example, functions as a RADIUS client.
- RADIUS Server—a device that receives authentication requests from RADIUS clients and responds either with Accept (authentication validated) or Reject (authentication failed). The RADIUS server is usually implemented on UNIX workstations and is downloadable as free public domain for most UNIX and also for Windows NT operating systems.

The RADIUS clients communicate with the RADIUS server using UDP. Many separate RADIUS clients may use the services of a single RADIUS server, even when the server is connected to a different network. The fact that the RADIUS server can be centralized allows the system administrator to define the users and password data bases in one place only and to avoid having to define every user individually in every distinct Terminal Server.

How it Works: User Authentication with RADIUS

RADIUS authenticates users through a series of communications between the client and the server. Once a user is authenticated, the client provides that use with access to the appropriate network services.

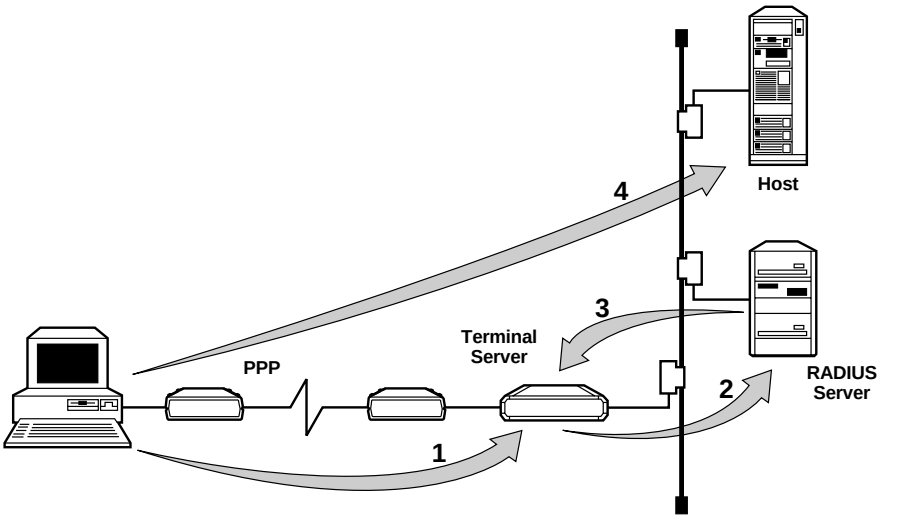


Figure 4-29. User Authentication.

A typical description of such a process involves the following:

- Using a modem, the user dials-in to a modem connected to the Terminal Server. Once the modem connection is completed, the Terminal Server prompts the user for a name and password.

- The Terminal Server creates a data packet from this information called the authentication request. This packet includes information identifying the specific access server sending the authentication request, the port that is being used for the modem connection, and the user name and password. For protection from eavesdropping hackers, the Terminal Server, acting as a RADIUS client, encrypts the password before it is sent on its journey to the RADIUS server.

- The Authentication Request is sent over the network from the RADIUS client to the RADIUS server. This communication can be done over a local or wide-area network, allowing network managers to locate RADIUS clients remotely from the RADIUS server. If the RADIUS server cannot be reached, the RADIUS client can route the request to an alternate server.

- When an Authentication Request is received, the Authentication Server validates the request and decrypts the data packet to access the user name and password information. This information is passed on to the appropriate security system being supported (either UNIX password files or Kerberos, a commercially available security system or even a custom developed security system).

- If the user name and password are correct, the server sends an Authentication Acknowledgement that includes information on the user's network system and service requirements. For example, the RADIUS server will tell the access server that a user needs TCP/IP using PPP (Point-to-Point Protocol) or that the user needs SLIP (Serial Line Internet Protocol) to connect to the network. The acknowledgement can even contain filtering information to limit a user's access to specific resources on the network.

- If at any point in this log-in process conditions are not met, the RADIUS server sends an Authentication Reject to the access server and the user is denied access to the network.

- To ensure that requests are not responded to by unauthorized hackers on the network, the RADIUS server sends an authentication key, or signature, identifying itself to the Terminal Server. Once this information is received by the Terminal Server, it enables the necessary configuration to deliver the right network services to the user.

4.14.1 Implementing RADIUS Authentication

The Terminal Server must be configured with the parameter of at least one (primary) RADIUS server in order to use the RADIUS authentication. The following example configures the Terminal Server to use RADIUS:

```
1 Local> DEFINE AUTHENTICATION PRIMARY ADDRESS 133.144.155.166
  Local> DEFINE AUTHENTICATION ALTERNATE ADDRESS 133.144.155.177
  Local> DEFINE AUTHENTICATION RETRIES 3
2 Local> DEFINE AUTHENTICATION PRIMARY SECRET my-secret
3 Local> DEFINE PORT 1 AUTHENTICATION ENABLED
4 Local> DEFINE AUTHENTICATION ENABLED
```

Figure 4-30. Setting Up RADIUS Authentication.

1: Primary and Alternate RADIUS Authentication Server Configuration

The Terminal Server must be configured with a valid RADIUS server IP address and a shared secret. Statements 1 define the Internet addresses of two valid RADIUS servers, primary and alternate, at least one of which must be accessible for authentication of users. The third command line specifies that the Terminal Server should retry sending an authentication request three times to the primary RADIUS server. After this, it either turns to an alternate RADIUS server (if defined) or rejects the login request.

Statement 2 defines the shared secret that is known to both the RADIUS client (in this case, the Terminal Server) and the RADIUS server. The secret should be entered into the RADIUS "clients" database file in the following format:

```
133.144.155.166  my-secret
```

2: Enabling RADIUS Authentication

Statement 3 enables RADIUS authentication on PORT number 1. If AUTHENTICATION is enabled globally, as with statement 4, the port can only be logged in to by a user with a valid user name and password. A valid user name is a user name that has an entry in the RADIUS server "users" file in the following format:

```
andy Password= "abcdef"
     User-Service-Type = Login-User,
     Login-Host = 111.222.111.222,
     Login-Service = Telnet
```

Figure 4-31. Enabling RADIUS Authentication.

In this example, the user name is "andy" and the password is "abcdef." The user would be connected automatically via Telnet to the specified address of 111.222.111.222).

4.14.2 USING PAP AND CHAP

Authorization protocols are not mandatory on a PPP link, but they are important because they provide a certain level of security on the serial connection.

A port used for PPP connection commonly requires user authentication to eliminate unwanted waste of resources. In addition to the user name and password normally used to log in to the Terminal Server, a port can be configured further to also authenticate the user using one of the standard PPP authentication protocols.

The two authentication protocols that may be employed on a PPP link are:

- PAP—Password Authentication Protocol is used to authenticate user on the same principle as the standard login. The client authenticates itself to the server by sending a user name (and optionally a password) to the server. The server then compares it with its hidden database. The Terminal Server checks the data in its RADIUS server database (see Authentication—Using Radius).

- CHAP—Challenge-Handshake Authentication Protocol is used to authenticate users using challenge-response schemes, thereby preventing the unwanted capture of user name and password. The server sends a randomly generated challenge string to the client, along with its hostname. The client uses the hostname to look up an appropriate key, combines this with the challenge and encrypts it with a special algorithm. The resulting string is returned to the server along with the client hostname.

The server then performs the same computation, as the client, on the challenge string. The server only permits the client to connect if the results are identical.

An additional security feature of CHAP is that the client authentication is not only required at the initial connect time, but the server also sends challenge strings to the client at regular intervals to detect if the client has been replaced by an imposter. The following example shows how to add PAP capability to an already defined PPP port.

```
1 Local> DEFINE PORT 5 PPP LCP AUTHENTICATION PAP
2 Local> DEFINE PORT 5 AUTHENTICATION ENABLE
```

Figure 4-32. PPP with Authentication.

Statement 1 configures the port to use PPP PAP protocol. The node must send a valid user name and password using the PPP PAP protocol.

4.15 Accounting Using RADIUS

Accounting of the Terminal Server is available only when using the RADIUS protocol. The accounting data is recorded on a RADIUS accounting server.

IMPLEMENTING RADIUS ACCOUNTING

The following example configures the Terminal Server to register accounting information:

```
1 Local> DEFINE ACCOUNTING PRIMARY ADDRESS 110.111.112.113
  Local> DEFINE ACCOUNTING ALTERNATE ADDRESS 111.112.113.114
2 Local> DEFINE ACCOUNTING PRIMARY SECRET acc-secret
3 Local> DEFINE ACCOUNTING ENABLED
```

Figure 4-33. Accounting with RADIUS.

1: Primary and Alternate RADIUS Accounting Server configuration

This setup is the same as for RADIUS authentication servers discussed in the previous example. However, the accounting server does not necessarily have to be the same physical server as that used for authentication.

2: Enabling RADIUS Accounting

Statement 3 enables RADIUS accounting on all the ports. There would not be much sense in enabling accounting without authentication as users could then enter using any user name they choose.

The accounting log accumulated on the server file (one for each RADIUS client) will look like this:

```
Mon Jul 8 09:13;10 1996
      User-Name = "andy"
```

```
      Client-Id=111.122.133.144
      Client-Port-Id=3
      Acct-Status-Type=Start
      Acct-Session-Id="IP (111.122.133.144)-Session (004)"

Mon Jul 8 09:17:12 1996
      User-Name="andy"
      Client-Id=111.122.133.144
      Client-Port-Id=3
      Acct-Status-Type=Stop
      Acct-Session-Id="IP (111.122.133.144)-Session (004)"

Mon Jul 8 09:18;35 1996
      User-Name="john"
      Client-Id=111.122.133.144
      Client-Port-Id=6
      Acct-Status-Type=Start
      Acct-Session-Id="IP (111.122.133.144)-Session (004)"

Mon Jul 8 09:25:55 1996
      User-Name="john"
      Client-Id=111.122.133.144
      Client-Port-Id=6
      Acct-Status-Type=Stop
      Acct-Session-Id="IP (111.122.133.144)-Session (004)"
```

Figure 4-34. Accounting Log.

4.16 Configuring the SNMP Agent

The Terminal Server can be managed through the network using SNMP (Simple Network Management Protocol). This management can be carried out by using any NMS (Network Management Station). The SNMP lets one

acquire and initialize the configuration of the Terminal Server, check the different interface counters and also to get TRAPs on several Terminal Server special events.

The following example shows how to configure a Terminal Server to work with an NMS station.

```
1 Local> DEF SNMP COMMUNITY "PASSaMGMT" ADDRESS 112.114.116.118
2 Local> DEF SNMP COMMUNITY "PASSaMGMT" GET ENABLED
3 Local> DEF SNMP COMMUNITY "PASSaMGMT" TRAP ENABLED
4 Local> DEF SNMP AUTHENTICATION FAILURE ENABLED
5 Local> DEF SNMP ENABLED
```

Figure 4-35. SNMP Agent Settings.

1: Define an SNMP Community

A community name must be assigned to a specific SNMP management station to permit it to control the Terminal Server. Statement 1 assigns the community name PASSa MGMT to this IP address. The community name must be configured into the management station and is verified by the protocol on every request.

2: Assign Capabilities for a Given Community

Statement 2 configures the Terminal Server to answer any SNMP GET requests from those stations using this community. Statement 3 configures the Terminal Server to send a TRAP on special events to the station configured in Statement 1.

3: Authentication Failure Alerts

The SNMP community serves as a password for SNMP management stations and the Terminal Server. If a management station sends an unauthorized request, it can cause an SNMP Alert. Statement 4 causes the Terminal Server

to send TRAPs on these events to all stations configured as in statement 1.

4: Enabling SNMP

Statement 5 configures the Terminal Server to support SNMP frames. If SNMP is disabled, no TRAPs are sent and all SNMP requests are ignored.

SUPPORTED MANAGEMENT INFORMATION BASES (MIBS)

The Terminal Server supports the standard MIBs for IP interface, Character stream devices, RS-232 interface and Parallel interface, as listed below. The management station must include these MIBs in order to be able to access the Terminal Server parameters. These MIBs can be accessed using MIB browser or any management application.

Table 4-7. MIBs Supported by the Terminal Server.

MIB	Description
RFC 1213	Management Information Base (MIB II) for Internet Protocol suite management.
RFC 1316	Definitions of Managed Objects for Character Stream Devices, the Character MIB.
RFC 1317	Definitions of Managed Objects for RS-232-like hardware devices, the RS-232-like MIB. The draft version dated March 19, 1991 is also supported for backwards compatibility.
RFC 1318	Definitions of Managed Objects for parallel hardware devices.

5. User Commands and Applications

This chapter covers the basic operations that a non-privileged user may need when using the Terminal Server. The interaction between the user and the

Terminal Server is important to comprehend and a correct grasp of these concepts will allow trouble-free and effortless operations.

Certain control characters allow the user to circulate between sessions and to control each one in turn. These include controls for breaking out of sessions, terminating sessions, and switching between active sessions.

5.1 Terminal Sessions

Starting a Session

The CONNECT command is used to connect to remote hosts. For LAT services, issue the CONNECT *service_name* command. For Telnet hosts, the equivalent would be CONNECT TELNET *host_name*, or even TELNET *host_name*. An explicit IP number can be substituted for the *host_name* and an explicit port number can also be added. For example, to connect to port 2005 of host 111.122.133.144.

```
Local>TELNET 111.122.133.144.2005
```

Navigation Between Sessions

The <break> key switches the user back to *local* mode while keeping any current sessions alive in the background.

Once in local mode, you can use the FORWARDS and BACKWARDS commands to step through active sessions. Specific keys can be assigned as shortcuts to these commands. The first session initiated by the user is at the start of the session list. The SHOW SESSIONS command displays a list of the open sessions. FORWARDS brings the most recent session forward. The list is cyclic. Note that up to 4 active sessions can be maintained by each port of the Terminal Server.

NOTE

Do not assign the <break>, <forwards>, and <backwards> keys to common keys that are used in normal terminal operations to prevent them from being unintentionally activated.

RESUME <x>, issued from the local prompt, switches the user back to the specified session. One can either resume back to the default current session from which one issued the break command, or to another specified session x, from the list of active sessions.

Ending Sessions

DISCONNECT or CLOSE can be used in a similar way to terminate a current, specific, or even all the sessions.

Opening SLIP Sessions

Presuming the port has been configured correctly for SLIP, one can use the following to initiate a PPP session:

```
Local> CONNECT PPP
```

NOTE

PPP cannot be enabled on ports with MULTISESSIONS ENABLED.

5.2 Examples of Common Applications

Example 1: Dedicated—User/Port

In this scenario, a user needs to be connected to a dedicated port on a specific server with minimal user interface. A dedicated connection as set up below will connect the user directly to the specified server as soon as the user

logs into port 3 with two <Enter> key-presses.

```
Local> DEFINE PORT 3 USERNAME "ALEX"
Local> DEFINE PORT 3 DEFAULT PROTOCOL TELNET
Local> DEFINE PORT 3 TELNET CLIENT TERMTYPE VT100
Local> DEFINE PORT 3 DEDICATED 111.123.143.111
Local> DEFINE PORT 3 VERIFICATION DISABLE
```

Figure 5-1. Setting Up a Dedicated Port.

Example 2: Telnet-Listener—Accessing a Modem from a Remote Location

In this scenario, a user wishes to connect a modem to one port of the Terminal Server, and to allow it to be accessed from the network for dialout. As for any other device connected to a port that needs to be accessed from remote, you will use the reverse-Telnet or Telnet-Listener method.

Here, the modem is to be connected to port 5 at 9600 baud.

```
Local> DEFINE PORT 5 AUTOBAUD DISABLE SPEED 9600
Local> DEFINE PORT 5 ACCESS REMOTE
Local> DEFINE PORT 5 TELNET LISTENER 2005 PORT 5 ENABLED
Local> DEFINE PORT 5 TELNET LISTENER 2005 CONNECTIONS ENABLED
Local> DEFINE PORT 5 TELNET SERVER NEW FROM TERMINAL <LF>*
Local> LOGOUT PORT 5
Local> INIT DELAY 0
```

Figure 5-2. Sharing a Dialout Modem.

*This command suppresses the extra line echoes in the modem response.

Then, you Telnet to xxxx.xxxx.xxxx.xxxx 2005 (ip_address of the Terminal Server, port 5) and connect directly to the modem and issued standard AT modem commands.

Example 3: Back-to-Back—Serial to Serial Communication Over an IP Backbone

In this scenario, a site wishes to connect an asynchronous serial device to a

LAN (either local or remote) using a Terminal Server. On the one site, the operator has a terminal connected via another Terminal Server to a LAN. Both LANs are connected to each other via a pair of routers and a WAN.

At the local site, the user sets up a dedicated Telnet as follows:

```
Local> DEFINE INTERNET ADDRESS ip_address
Local> DEFINE INTERNET MASK net_mask
Local> DEFINE INTERNET GATEWAY ip_address
Local> DEFINE PORT n AUTOBAUD DISABLE SPEED speed
Local> DEFINE PORT n USERNAME user_name
Local> DEFINE PORT n DEDICATED ip_address PORT 200n
Local> DEFINE PORT n TELNET CLIENT NEW LINE TO TERMINAL <CR>
Local> DEFINE PORT n TELNET CLIENT{ip}{ayt}{synch}{ao}{brk}NONE*
Local> INIT DELAY 0
```

Figure 4-3. Local Site Telnet Setup.

*Each in a separate command line.

At the remote site, the user sets up a Telnet-Listener.

```
Local> DEFINE INTERNET ADDRESS ip_address
Local> DEFINE INTERNET MASK net_mask
Local> DEFINE INTERNET GATEWAY ip_address
Local> DEFINE TELNET LISTENER 200n PORT n ENABLED
Local> DEFINE TELNET LISTENER 200n CONNECTIONS ENABLED
```

```
Local> DEFINE PORT n AUTOBAUD DISABLE SPEED speed
Local> DEFINE PORT n ACCESS REMOTE
Local> DEFINE PORT n TELNET server NEW LINE TO TERMINAL <CR>
Local> DEFINE PORT n TELNET server {ip}{ayt}{eor}{ao}{nop}NONE*
Local> INIT DELAY 0
```

Figure 5-4. Remote Site Telnet Setup.

*Each in a separate command line.

In this last scenario, a user might wish to connect a card-reader with its centralized controller. Rather than using traditional modems, one will transport the asynchronous data between the units using TCP/IP over a WAN using the Terminal Server. A back-to-back connection would establish a permanent virtual circuit so that any asynchronous data from the one unit will be encapsulated in a TCP/IP packet and delivered to the other. In this example, a session is opened between the card-reader and its controller and any keystroke or data entered into the card-reader is transmitted to its controller over TCP/IP.

Example 4: Remote Access with PPP and Windows 95

In this scenario, a user wishes to use a PC running Windows 95 to establish a dedicated PPP link via a modem. In earlier versions of Windows, the dialup was achieved by using third party Winsock applications (such as Trumpet) and a script. In Windows 95, the TCP/IP stack is internal.

This operating system supports PPP through its dialup networking configuration, with a default PAP authentication scheme. Although Windows 95 includes support for dialup networking, allowing computers to connect to remote hosts, there is no provision for scripting.

To add scripting capabilities to Windows 95 dialup networking form the CD version of Windows 95, use the included DScript utility. To install DScript, use the double-click on Add/Remove Programs in Control Panel, click the Windows Setup tab, click Have Disk button, and install from the ADMIN\APPTOOLS\DSCRIPT directory on the CD.

A sample script to connect to the Terminal Server is as follows:

```
proc main
      delay 1
      transmit “^M”
      delay 1
      transmit “^M”
      wait for “name>”
      transmit $USERID
      transmit “^M”
      wait for “Local>”
      transmit “c ppp^M”
endproc
```

As a RADIUS client, the 8-Port Terminal Server can use either PAP or CHAP for password verification. However, the Terminal Server does not include its own database. In order for PAP or CHAP to work, you need a software version of 4.0 or above on the Terminal Server, with authentication both enabled and configured.

A manual solution for using RADIUS with the Terminal Server is to add a terminal window to the Dialup Networking configuration. This is achieved in the following manner:

- Open Dialup Networking from the Control Panel and if necessary, double click on Make New Connection and fill in the relevant details when prompted.
- Right click on the new connection icon you have just created and choose Properties.
- Click on the Configure button and choose the Options tab.
- Make sure the box that brings up a terminal window after dialing is checked.

In this case, once the connection is established, a terminal window will open on the screen. You then press <Enter> a couple of times and receive the Local> prompt from the Terminal Server. Then you can log in with the standard user-name and password. If the port was specified on the Terminal Server to be dedicated for PPP, a PPP session will immediately begin. If not,

the user must initialize it manually by typing:

```
Local> Connect PPP
```

Additional Note for Dedicated PPP:

- A dedicated PPP port will transmit negotiation requests upon sensing a change in the modem's DSR signal. This DSR assertion may often cause the modem to disconnect as it receives data from the RS-232C while it is still in negotiation. To overcome this problem, you can monitor the DCD line instead, which is asserted only after negotiation is complete. This means incorporating a change on the modem end of the RS-232C cable—moving the wire from pin 6 to pin 8.

- Modem settings are also important to establishing reliable PPP sessions. Typically, the following settings should be adhered to:

  AT&F0&D2&S1E0Q1\n2S0=1

6. Command Descriptions

This chapter describes the Terminal Server commands that are not explained in one of the following command categories: SET/DEFINE/CHANGE (**Chapter 7**), SHOW/LIST (**Chapter 8**), or CLEAR/PURGE (**Chapter 9**).

BACKWARDS (secure)

BACKWARDS

This command (available to all users) resumes the session preceding your current session in the list produced by the SHOW SESSIONS command. Your preceding session is the one with the next lower number to your current session. If your current session is 1, your preceding session is the one at the end of the SHOW SESSIONS display.

BROADCAST (nonprivileged)

BROADCAST {PORT *port-list* } {"*message-text*"}
{ALL } { *message-text*}

This nonprivileged command sends a message to other Terminal Server ports.

PORT *port-list*

Indicates one or more ports to receive your message.

ALL

This privileged parameter indicates that the message is sent to all ports on the Terminal Server.

message-text

This is the text of the message. Uppercase letters are used to broadcast the message from the Terminal Server unless it is enclosed in quotation marks. You cannot embed quoted text within the message. The maximum number of characters is 115, depending on space available on the command line.

Any of the following conditions will prevent your message from being transmitted:

- The port characteristic BROADCAST is set to DISABLED on the port, displaying a warning message.

- PASSALL or PASTHRU mode is currently set as an active Telnet session on the port. For further reference, see the SET SESSION Telnet command.
- The port is locked or logged out.
- Output flow control from the Terminal Server to the port is turned off.

Restriction:

- Nonprivileged users must specify a single target port. Only privileged users can specify ALL or a port-list to transmit a message to multiple ports.

Example

Local> BROADCAST ALL “Shutting down in 5 minutes”

This command sends the string “Shutting down in 5 minutes” to all ports.

CLOSE PORT (secure)

See the DISCONNECT/CLOSE PORT command (**page 109**) for information on CLOSE and CLOSE PORT.

CONNECT (secure)

```
                [ip-address      ]
CONNECT         [host-name       ]
                [service name    ]
```

This secured command requests a connection using the default protocol set for this port (refer to DEFINE PORT DEFAULT PROTOCOL). The destination part is not required—if missing, the preferred destination will be used (refer to DEFINE PORT PREFERRED).

ip-address

The internet address of a host. The address must be specified in dot-notation (for example, 191.34.75.4).

host-name

The ip domain name of a host. The name may be absolute (e.g., don.sales.radlinx.com) or relative (e.g., sales.radlinx).

service-name

Specifies the Telnet service on a Terminal Server to which you want to connect. If the service is offered by multiple service nodes, the Terminal Server connects to the node with the highest service rating.

In order to use a specific protocol (other than the default), choose one of the specific connect requests listed below.

CONNECT LAT (secure , 4- and 8-Port models only)

```
CONNECT {LAT    } service-name     {NODE node-name}
        {SERVICE}          {PORT                  }
{DESTINATION port-name    }
{PORT                     }
```

This secure command requests a connection to the LAT service. For more information, refer to the CONNECT ANY, CONNECT PORT, and CONNECT Telnet commands.

service-name

Specifies the Telnet service on a Terminal Server to which you want to connect. The default specification is your preferred service if it has been defined. In the event that the service is offered by multiple service nodes, the Terminal Server connects to the node with the highest service rating.

NODE *node-name*

Indicates a particular service node to which you want to connect. The default node is the highest-rated node that offers the service.

DESTINATION *port-name*

Specifies a particular Terminal Server port to which you want to connect. The default port you are connected to is the first available port offering the service. If DESTINATION is specified without specifying NODE, users are connected to the specified port on the local Terminal Server node, assuming the service is offered.

PORT

This command connects you with the port's preferred service.

Examples

```
Local> CONNECT
Local> CONNECT ADMIN
Local> CONNECT METDATA NODE DATAserver DESTINATION
PORT_6
```

If a preferred service is defined, the first command connects the port to its preferred service; the second command connects the port to the service ADMIN; and the last command connects the port to the service METDATA at PORT 6 on the Terminal Server DATAserver.

CONNECT ANY (secure)

CONNECT {ANY}{*host-name*}

This command determines whether a specified host is using the Telnet or LAT protocol. First the Terminal Server checks the Telnet protocol. If that fails, the Terminal Server then checks the LAT protocol. The Terminal Server establishes a connection to that host when a protocol is found. This command is available to all users.

The keyword ANY can be omitted from the command line if ANY is already set as the default protocol for the port. The host-name may be omitted from the command line if the host-name has been set as a preferred service.

host-name

Indicates the name of the LAT service or the Telnet host to which you want to connect.

Restriction:

- This command cannot be used if AUTOCONNECT is ENABLED on the port.

Example

```
Local> CONNECT ANY JUMBO
```

This command checks the host JUMBO to determine whether the Telnet protocol or the LAT protocol is used and then connects to the host JUMBO.

CONNECT PPP (secure)

CONNECT [PPP]

This secure command specifies that a PPP session will be started on the port. You must specify PPP in the command line if PPP is not the default protocol.

Restrictions:

- The port must have PPP enabled.
- Only one SLIP or PPP session per port is allowed at any given time.
- During a PPP session, all switch characters are passed on as data.

Example

```
Local> CONNECT PPP
```

This command starts a PPP session on the current port.

CONNECT SLIP (secure)

CONNECT [SLIP]

This command, which is available to all users, specifies that a SLIP session will be started on the port. If SLIP is not the default protocol, you must specify SLIP in the command line.

NOTE

If a HOST ADDRESS has not been set prior to entering the CONNECT SLIP command, the access server will determine the address from the first internet packet received on the port.

Restrictions:

- The port must have SLIP enabled.
- Only one SLIP or PPP session per port is allowed at any given time.
- During a SLIP session, all switch characters are passed on as data.

Example

```
Local> CONNECT SLIP
```

This command starts a SLIP session on the current port.

CONNECT TELNET/OPEN/TELNET (secure)

{CONNECT} {*ip-address* }
{OPEN }{TELNET}{*host-name* }[[PORT] *tcp-port*]
{Telnet }

This command requests a connection to the specified target which may be an internet address or an internet host name. The Terminal Server checks the protocol enabled on the requested port prior to connection. This command is available to all users.

This command works the same way as OPEN/Telnet.

Either of the following methods may be used to make connections:

- Specify the host either by *host-name* or *ip-addr*, and specify the *tcp-port*.
- Specify only the host either by *host-name* or *ip-addr*. The default *tcp-port* 23 is assumed.

CONNECT, OPEN, or Telnet

Indicates that only Telnet will be used to attempt the connection. The port's default protocol will be used by the Terminal Server if Telnet is missing from the command line. Telnet is the factory-set default protocol.

Telnet

TELNET must be specified if TELNET is not the port's default protocol.

ip-address

The internet address of a host. The address must be specified in dot-notation (for example, 191.34.75.4).

host-name

The ip domain name of a host. The name may be absolute (e.g., don.sales.radlinx.com.) or relative (e.g., sales.radlinx).

[PORT] tcp-port

The TCP port number on an internet host. For example, the Telnet server "well known port" is 23 decimal. The default on a Telnet connection request where the TCP port number is not specified is port 23.

Example

```
Local> CONNECT Telnet BART 2001
```

This command connects your port to Telnet host BART at TCP port number 2001.

DISCONNECT/CLOSE (secure)

{DISCONNECT}{ALL }
{CLOSE }{SESSION *session-number* }

This command (available to all users) terminates all interactive sessions or a specific session. For more information, refer to the DISCONNECT/CLOSE PORT command (**page 109**).

ALL

Terminates all sessions on a port.

SESSION *session-number*

Closes a particular session. The default session is the current session.

Examples

```
Local> CLOSE SESSION 1
```

This command disconnect session 1.

```
Local> DISCONNECT ALL
```

This command *disconnects all* sessions on the port.

DISCONNECT/CLOSE PORT (privileged)

{DISCONNECT}PORT *port-number*
{CLOSE }

This privileged command is used to terminate a session to a dedicated service on another port. The LOGOUT PORT command may be used to disconnect sessions of interactive users.

port-number

Specifies the port you want to disconnect.

Example

```
Local> DISCONNECT PORT 3
```

This command terminates the sessions on PORT 3.

FORWARDS (secure)

FORWARDS

This command connects you to the session that follows your current session in the session list. The sessions list can be displayed with the SHOW SESSIONS command. The FORWARDS command allows you to continue the session with the next higher session number than your current session. In the event that your current session has the highest session number, FORWARDS connects you to the session with the lowest session number. This command is available to all users.

HELP (secure)

HELP [*topic* [*subtopic*]]

This command displays conventional on-line HELP for the Terminal Server. **Section 4.2.2** provides an overview of the most common form of on-line help.

Different Help displays are available for privileged, nonprivileged, limited view or secure users. For example, if you enter HELP at a nonprivileged port, only those commands and characteristics that can be specified by a nonprivileged user are displayed.

topic [*subtopic*]

Indicates a command keyword and possible options for obtaining on-line help information.

Example

```
Local> HELP DEFINE PORT ACCESS
```

This command initiates on-line help documentation for defining the port characteristic ACCESS in the permanent database.

INITIALIZE (Privileged)

```
                          [DELAY minutes      ]
INITIALIZE [SERVER] [UPDATE FLASHROM]
                          [DIAGNOSE           ]
                          [DISABLE            ]
```

This privileged command reinitializes the Terminal Server. By default, the Terminal Server will be reinitialized about 1 minute after this command is processed. You can also specify no delay, or you can specify a longer delay in order to perform an orderly shutdown. You can execute a diagnostic test on the server, too, but only qualified service personnel should work with the diagnostics.

DELAY *minutes*

Specifies number of minutes to delay the initialization procedure . The default delay is one minute. The user may specify from a minimum of 0 to a maximum of 1440 minutes.

UPDATE FLASHROM

This command option initiates a software update process and requires the FLASH product option. The update process always executes on physical port 1 of the Terminal Server where it expects a software file to be uploaded in ASCII format (e.g., from a PC equipped with PROCMM communication software or equivalent).

After this command is entered, the Terminal Server displays:

```
Loader>
```

The user must then enter the LOAD command and initiate the ASCII mode file transfer on the PC side (in PROCOMM—PageUp key and choosing the ASCII mode with the *filename*) and supply the name of the file to upload.

The update process takes about 10 minutes (depending on the port speed). After a successful load, the Terminal Server comes up with the new software version. In case of error, an appropriate error message will be displayed.

DIAGNOSE

Displays the diagnostics-system main menu, through which extensive testing of the Terminal Server can be performed. Since this option may inadvertently damage the Terminal Server, it should be used only by qualified service personnel.

Example

```
Local> INITIALIZE DELAY 5
```

This command specifies initialization of the Terminal Server after 5 minutes have elapsed.

Restrictions:

- The INITIALIZE UPDATE command requires the FLASH product option.
- The INITIALIZE UPDATE command always executes on physical port #1 of the Terminal Server.

INITIALIZE CANCEL (privileged)

INITIALIZE [server] CANCEL

This privileged command discontinues a previous INITIALIZE command if the initialization process has not begun.

LOCK (secure)

LOCK

This command (available to all users) prevents unauthorized use of your terminal in your absence.

When the Terminal Server characteristic LOCK and the SET PORT characteristic LOCK are ENABLED, the Terminal Server responds to a LOCK command by prompting for a lock password.

You can specify a password ranging from 1 to 16 characters. The Terminal Server prompts you to enter the password twice. The password does not display on your terminal. The Terminal Server displays an unlock password prompt (Unlock Password>) when both password entries are equivalent. Your terminal remains locked until you enter the password again, returning you to local mode.

Example

```
Local> LOCK

Lock Password> MINE (not displayed)

Verification> MINE (not displayed)

Local Port 6 locked

Unlock Password> MINE (not displayed)

Local>
```

If a user forgets the unlock password, a privileged user must LOGOUT the port before it can be logged in and used again.

LOGOUT (Secure)

```
                [ALL                ]
LOGOUT[PORT [port-list              ]
                [port-number        ]
```

This command logs out a port on the Terminal Server and terminates any sessions associated with the port. The port characteristics in the port's operational database are reset to the values defined in the permanent database when you log out a port.

When using the Telnet to LAT gateway feature, your session is assigned a virtual port number of the form V##. Use this virtual port number to log out.

The LOGOUT command drops outgoing modem signals when a port has signal control enabled.

PORT

Causes a full logout from your own port.

ALL

This privileged option logs out all ports other than the port where the command is entered.

port-list

This privileged option specifies the port(s) you want to log out. The default is your own port; however, if your port is not indicated in the list it will not be logged out.

Examples

```
Local> LOGOUT

Local> LOGOUT PORT 2

Local> LOGOUT PORT V06
```

The first command logs out the port where the command is entered and terminates all sessions on that port. The second command logs out of port 2 and disconnects all sessions. The third session logs out Telnet to LAT gateway session V06.

OPEN/TELNET (secure)

For information on this command, refer to the CONNECT Telnet/OPEN/Telnet command (**page 107**).

PING/TEST INTERNET (nonprivileged)

{PING }{*host-name* }
{TEST INTERNET}{*inet-address*}

This nonprivileged command tests end-to-end communication between the Terminal Server and the specified target over an internet-protocol network. The target can be an internet domain name or an internet address.

PING tests for the availability of the target by establishing a PING session on the port. The timer begins when the user receives a "Pinging..." message. The ping session continues until the user presses any key, or terminates the session with the DISCONNECT/CLOSE SESSION command. The ping session continues up to 100 times.

NOTE

If the BREAK key or local switch was pressed during a PING session, the PING does not stop. The user may RESUME the PING session or has to DISCONNECT it.

PING or TEST INTERNET

This command indicates that an Internet Control Message Protocol (ICMP) Request is sent to the specified target. The target returns an ICMP Reply message after receiving the message.

host-name

Specifies the absolute domain name (such as tom.xyz.dec.com) or the relative domain name (tom) of a host.

ip-address

The IP address of a host. The address must be specified in dot-notation (nnn.nnn.nnn.nnn).

Restriction

- There can be only one PING/TEST INTERNET session per port.

Example

```
Local> PING 136.3.41.20
```

This command tests internet connectivity to the IP address 136.3.41.20.

REMOVE QUEUE (Privileged , 4- and 8-Port models only)

```
                    {ALL                    }
                    {ENTRY entry-number }
REMOVE QUEUE {NODE node-name            }
                    {SERVICE service-name   }
```

This privileged command removes queued LAT connection request (for remote access to Terminal Server ports) from the Terminal Server queue.

Removing an entry from the Terminal Server queue causes the Terminal Server to send a message to the service node that requested the remote access that the queued entry was deleted by a Terminal Server user.

ALL

Indicates that all entries in the queue are removed.

ENTRY *entry-number*

Specifies a particular entry by number.

NODE *node-name*

Specifies all entries initiated from the specified node.

SERVICE *service-name*

Specifies all entries initiated from the specified service node.

Example

```
Local> REMOVE QUEUE ENTRY 2
```

This command removes entry 2 from the Terminal Server queue.

RESTORE DEFAULTS (privileged)

RESTORE DEFAULTS

Restores factory defaults.

RESUME (secure)

RESUME [SESSION *session-number*]

Resumes an interactive session from local mode. This command is available to all users.

SESSION *session-number*

Specifies the session to be resumed. Your current session is resumed by the Terminal Server when this parameter is omitted.

Examples

```
Local> RESUME

Local> RESUME SESSION 8
```

The first command resumes your current session. The second command resumes session 8 in your session list.

SEND TELNET (secure)

```
                {AO                 }
                {AYT                }
                {BREAK (BRK)        }
                {EOR                }
Send Telnet     {IP                 }
                {NOP                }
                {REQUEST STATUS     }
                {RESUME OUTPUT      }
                {SYNCH          }
```

This command (available to all users) calls up the corresponding Telnet function on the current Telnet session.

AO (Abort Output)

Aborts any output en route to the user's terminal.

AYT (Are-You-There)

Requests a response from the remote Telnet implementation. Then the remote host sends back a message that it is currently in operation.

BREAK (BRK)

The BREAK or BRK command sends a Telnet Break command to the remote host. This command indicates that the Break key or the Attention key was pressed; however, different remote hosts may interpret this differently.

EOR (End-of-Record)

Sends a Telnet End-of-Record command to the remote host indicating the end of the current input record.

IP (Interrupt Process)

Sends a Telnet command to the remote host to interrupt or abort the remote process.

NOP (No-Operation)

Sends a Telnet No-Operation command to the remote host.

REQUEST STATUS

Requests that the peer Telnet implementation respond with the current status of all Telnet options for this session.

RESUME OUTPUT

Resumes a session after an Abort Output signal has been sent and the port hangs.

Restrictions:

- The session must be resumed to see an AYT response.
- The session must be resumed to view a REQUEST STATUS response.
- The SEND TELNET RESUME OUTPUT command can be used only after sending an Abort Output signal. The Abort Output signal may have been sent either by entering a SEND Telnet AO command or by typing the keyboard character defined as AO.

SYNCH

Drops all input currently en route to the remote process. This includes input queued both by the local Terminal Server and the remote host.

Example

```
Local> SEND Telnet AO
```

This command invokes the Abort Output (AO) function on the current Telnet session.

TEST INTERNET

For information on this command, refer to the PING command

TEST LOOP (Privileged)

TEST LOOP *ethernet-address*

This privileged command tests the connectivity between your Terminal Server and another Ethernet node on the network.

ethernet-address

Specifies the Ethernet address of the target node. An Ethernet address is a string of 12 hexadecimal digits in the form nn-nn-nn-nn-nn-nn.

TEST PORT (Secure)

TEST [PORT *port-number*] [COUNT {n }] [WIDTH *n*]...
{NONE}]

...[LOOPBACK{EXTERNAL}]
{INTERNAL}]

Tests a port on the Terminal Server. The Terminal Server sends a stream of characters to the specified port. Problems with the terminal or with the connection of the port to the Terminal Server are seen as irregularities in the rotating ASCII pattern.

PORT port-number

A privileged parameter that specifies the port to be tested (default: your own port).

COUNT *n*

Indicates the number of test lines to be sent, ranging from 1 to 65535. The default value is 23 lines. Specify NONE to produce a continuous display, then press any key to terminate the display.
WIDTH *n*

Specifies the number of characters per line (range: 1 to 132; default: 72).

LOOPBACK

A privileged parameter that specifies that test data is looped back from an EXTERNAL port loopback connector or from the INTERNAL port hardware (default: no loopback).

Restriction:

- You must set AUTOBAUD DISABLED to the tested port.
- Only privileged users can test a port other than their own.
- You cannot specify LOOPBACK when testing your own port.
- You cannot terminate a test from the port you are testing.
- You cannot specify LOOPBACK on port printer.
- Test on the printer port will not end if a parallel device is not connected.

TEST SERVICE (Privileged , 4- and 8-Port models only)

TEST SERVICE *service-name* [NODE *node-name*] [DESTINATION *port-name*] [COUNT{*n* } {NONE}]

This privileged command tests the end-to-end Terminal Servers over the LAT network. The test is performed between the Terminal Server and a service node. A report of the test results is displayed by the Terminal Server when completed.

service-name

Indicates the name of the service to be tested.

NODE *node-name*

Specifies the service node to be tested. The default node is the highest rated node that supports the specified service.

DESTINATION *port-name*

Specifies which port offering the service is to be tested.

COUNT *n*

Specifies the number of test buffers to be sent (default: 1). To invoke a continuous test enter COUNTNONE. To discontinue the test press the Break key or enter a local switch character.

ZERO COUNTERS (Privileged)

```
                    [ALL                                ]
                    [INTERNET[NAME RESOLUTION           ]
ZERO [COUNTERS]     [NODE node-name                     ]
                    [PORT [ALL     ][SLIP   ]           ]
                    [SNMP  [port-list ][PPP    ]        ]
```

This privileged command resets counters for the Terminal Server . Entering this command without parameters zeroes only the Terminal Server counters.

This command does not zero the uptime counter in displays. This counter is reset only after an initialization or after turning on the power of the Terminal Server.

ALL

Zeroes all counters except port.

INTERNET

Clears the internet counters corresponding to the specified entity.

NAME RESOLUTION

Indicates that only internet domain-name-system internet counters are to be cleared.

NODE *node-name*

Zeroes counters for data exchanges between the Terminal Server and the specified service node.

ALL

Specifies all Terminal Server ports.

port-list

Zeroes error counters and status counters for the specified port(s).

SLIP

Clears the SLIP counters for the specified port.

SNMP

Clears all SNMP error and access counters.

Examples

```
Local> ZERO INTERNET
```

Clears the Terminal Server internet counters.

```
Local> ZERO PORT 5 SLIP
```

Clears the SLIP-specific counters for port 5.

```
Local> ZERO SNMP COUNTERS
```

Clears the SNMP access and error counters.

7. SET/DEFINE/CHANGE Commands

This chapter describes the SET, DEFINE, and CHANGE commands.

SET commands change characteristics and options stored in the Terminal Server's operational database.

DEFINE commands change characteristics stored in the Terminal Server's permanent database.

CHANGE commands change characteristics stored in the Terminal Servers permanent and operational databases.

You can use the CHANGE command anywhere you can use the DEFINE and SET commands. If an error is produced by either the DEFINE or SET command, the CHANGE command will not modify either database.

ACCOUNTING (privileged)

```
{SET       }
{DEFINE    }ACCOUNTING{ENABLED  }
{CHANGE    }          {DISABLED }
```

This privileged command designates the use of the RADIUS ACCOUNTING protocol. The RADIUS (Remote Authorization Dial In User Service) can be used to record the Terminal Server login and logout events on an accounting server.

During the ACCOUNTING process, the user's username, port ID, and IP address (for IP sessions) are sent to a RADIUS accounting server. The server will record the information into a file. A primary server is tried first. If no acknowledgement is received (after a timeout and several retries, both can be configured) an alternate server is tried. The addresses of the primary and alternate ACCOUNTING server are configured using the DEFINE ACCOUNTING ADDRESS command.

When the Terminal Server is communicating with an ACCOUNTING server, the MD5 algorithm is used to encrypt information and verify responses from the ACCOUNTING server. The MD5 algorithm requires that a secret (password) will be shared at both sides communicating with each other—the Terminal Server and the ACCOUNTING server in this case. The secret is set using the DEFINE ACCOUNTING SECRET command (see below). Please note that this is not the user's password, but a general password used to secure the ACCOUNTING process itself. The secret is not displayed in SHOW ACCOUNTING. The only way to verify its value is to re-enter the command.

ENABLED

Use the RADIUS protocol to record login and logout events.

DISABLED

Do not use the RADIUS accounting protocol. This is the default.

ACCOUNTING ADDRESS (privileged)

{SET }
{DEFINE }ACCOUNTING{PRIMARY }ADDRESS *ip-address*
{CHANGE } {ALTERNATE }

This privileged command specifies the addresses of the primary and alternate RADIUS accounting servers. Once an accounting event occurs, the Terminal Server will send an accounting request to the primary accounting server. If it does not get an acknowledgement, it will retry it again. The timeout value and the retries count can be configured with the ACCOUNTING TIMEOUT and ACCOUNTING RETRIES commands. Once the retries has reached the limit, the Terminal Server will try to access the alternate server and repeat the process again.

PRIMARY

This parameter specifies that the address is configured for the PRIMARY ACCOUNTING server.

ALTERNATE

This parameter specifies that the address is configured for the ALTERNATE ACCOUNTING server.
ip-address

The Internet (IP) address of the accounting server.

ACCOUNTING RETRIES (privileged)

{SET }
{DEFINE }ACCOUNTING RETRIES *count*
{CHANGE }

This privileged command specifies the number of times the Terminal Server will retry to send a message to the accounting server. Once this count is reached, the Terminal Server will either try to use the alternate server, or will reject the user login request.

count

This parameter specifies the number of retries. The allowed range is 2 - 10. The default is 5.

ACCOUNTING SECRET

{SET }
{DEFINE }ACCOUNTING{PRIMARY }SECRET *secret*
{CHANGE } {ALTERNATE }

This privileged command specifies the secret password that is used by the Terminal Server when communicating with the RADIUS ACCOUNTING server. This secret should be configured both in the Terminal Server and in the RADIUS server.

PRIMARY

This parameter specifies that the secret is configured for the primary ACCOUNTING server.

ALTERNATE

This parameter specifies that the secret is configured for the alternate ACCOUNTING server.

secret

The secret used with the specified ACCOUNTING server. 1-16 case sensitive characters.

ACCOUNTING TIMEOUT(privileged)

{SET }
{DEFINE }ACCOUNTING TIMEOUT *seconds*
{CHANGE }

This privileged command specifies the timeout value, inseconds, after which the Terminal Server will re-send an ACCOUNTING request to the ACCOUNTING server.

seconds

This parameter specifies that the number of seconds after which the Terminal Server will re-send its request to the ACCOUNTING server. The allowed range is 2-60. The default is 2.

AUTHENTICATION

{SET }
{DEFINE }AUTHENTICATION{ENABLED }
{CHANGE } {DISABLED }

This privileged command designates the use of the RADIUS authentication protocol. The RADIUS (Remote Authorization Dial In User Service) protocol can be used to authenticate users trying to login to the Terminal Server.

During the authentication process, the user's username and password are sent for verification to a RADIUS server. A primary server is tried first. If no answer is received (after a timeout and several retries, both can be configured) an alternate server is tried. Once a positive answer is received, the user login request is granted, and the user may access the Terminal Server's services. If a negative response is received (or no response at all) the user request is rejected and the user is disconnected. The addresses of the primary and alternate authentication server are configured using the DEFINE AUTHENTICATION ADDRESS command.

When the Terminal Server is communicating with an authentication server, the MD5 algorithm is used to encrypt passwords and verify responses from the authentication server. The MD5 algorithm requires that a secret (password) will be shared at both sides communicating with each other—the Terminal Server and the authentication server in this case. The secret is set using the DEFINE AUTHENTICATION SECRET command (see below). Please note that this is not the user's password, but a general password used to secure the authentication process itself. The secret is not displayed in SHOW AUTHENTICATION. The only way to verify its value is to re-enter the command.

The username and password are either requested by the a prompt (for users accessing the server in terminal mode), or by using PPP PAP or CHAP protocols. Please note that each port should be defined with PORT AUTHENTICATION ENABLED in order for the authentication process to take place.

ENABLED

Use the RADIUS protocol to authenticate users for each port configured with PORT AUTHENTICATION ENABLED.

DISABLED

Do not use the RADIUS protocol to authenticate users. This is the default.

AUTHENTICATION ADDRESS (privileged)

{SET }
{DEFINE }AUTHENTICATION{PRIMARY }ADDRESS *ip-address*
{CHANGE} {ALTERNATE}

This privileged command specifies the addresses of the primary and alternate RADIUS authentication servers. During the verification of the user's name and password, the Terminal Server will send an authentication request to the primary authentication server. If it does not get a response, it will retry it again. The timeout value and the retries count can be configured with the AUTHENTICATION TIMEOUT and AUTHENTICATION RETRIES commands. Once the retries has reached the limit, the Terminal Server will try to access the alternate server and repeat the process again.

PRIMARY

This parameter specifies that the address is configured for the primary authentication server.

ALTERNATE

This parameter specifies that the address is configured for the alternate authentication server.

ip-address

The Internet (IP) address of the authentication server.

AUTHENTICATION RETRIES (privileged)

{SET }
{DEFINE }AUTHENTICATION RETRIES *count*
{CHANGE }

This privileged command specifies the number of times the Terminal Server will retry to send a message to the authentication server. Once this count is reached, the Terminal Server will either try to use the alternate server (if configured), or will reject the user login request.

count

This parameter specifies the number of retries. The allowed range is 2-10. The default is 5.

AUTHENTICATON SECRET (privileged)

{SET }
{DEFINE }AUTHENTICATION{PRIMARY }SECRET *secret*
{CHANGE } {ALTERNATE }

This privileged command specifies the secret password that is used by the Terminal Server when communicating with the RADIUS authentication server. This secret should be configured both in the Terminal Server and in the RADIUS server.

PRIMARY

This parameter specifies that the secret is configured for the primary authentication server.

ALTERNATE

This parameter specifies that the secret is configured for the alternate authentication server.

secret

The secret used with the specified authentication server. 1-16 case sensitive characters.

AUTHENTICATION TIMEOUT (privileged)

{SET }
{DEFINE }AUTHENTICATION TIMEOUT *seconds*
{CHANGE }

This privileged command specifies the timeout value, in seconds, after which the Terminal Server will re-send an authentication request to the authentication server.

seconds

This parameter specifies the number of seconds after which the Terminal Server will re-send its request to the authentication server. The allowed range is 2-60. The default is 2.

BOOTP (privileged)

```
{SET      }       {DISABLE  }
{DEFINE   }BOOTP{ALWAYS   }{SAVE   }
{CHANGE   }       {ONZERO   }{NOSAVE  }
```

This privileged command designates the use of a BOOTP protocol. The BOOTP protocol can be used to find the Terminal Server's Internet address from a BOOTP server. The BOOTP server contains a data base to associate an Ethernet MAC address with an IP address. Using DHCP or CMU extensions for the BOOTP protocol can supply the IP gateway (router) address as well as the IP netmask. Refer also to SET BOOTP VENDOR command.

DISABLE

Do not use the BOOTP protocol to obtain the Terminal Server's IP address.

ALWAYS

When initialized, always use the BOOTP protocol to obtain the Terminal Server's IP address.

ONZERO

When initialized, if the Terminal Server configured IP address is null, use the BOOTP protocol to obtain the Terminal Server's IP address. This is the default.

SAVE

Save all the parameters received in a BOOTP reply message in the Terminal Server's permanent database and set the current IP parameters to these values.

NOSAVE

Use the parameters received in a BOOTP reply message as the current IP parameters. Do not save them in the Terminal Server's permanent database. This is the default.

BOOTP VENDOR (privileged)

```
{SET     }                {CMU  }
{DEFINE  }BOOTP VENDOR{DHCP}
{CHANGE  }                {NONE}
```

This privileged command specifies BOOTP protocol extensions to be used for the BOOTP request and reply. The extensions enable the Terminal Server to obtain the gateway (default router) and netmask values from the BOOTP server.

CMU

This parameter specifies the use of the CMU (Carnegie Mellon University) extension for the BOOTP protocol. Using this extension, the Terminal Server can obtain the IP address IP mask and default gateway.

DHCP

This parameter specifies the use of the DHCP (RFC 1048 or RFC 1533) extension for the BOOTP protocol. Using this extension, the Terminal Server can obtain the IP address IP mask and default gateway.

NONE

This parameter specifies the use of no extension for the BOOTP protocol. Using this option, the Terminal Server can obtain only its IP address.

INTERNET (privileged)

```
{SET     }          {ADDRESS{ip-address}          }
{DEFINE  } INTERNET {        {NONE     }          }
{CHANGE  }          {[SUBNET]MASK{net-mask}       }
                                 {NONE     }      }
```

This privileged command modifies the Terminal Server internet address and subnet mask.

In order for the Terminal Server to perform in the internet environment the internet address definition must be included in the Terminal Server database.

Depending on the class of the internet address defined, the subnet mask defaults to a Class A, B, or C mask. If the default subnet mask is sufficient, you do not have to specify the subnet mask.

ADDRESS

Specifies the Terminal Server internet address.

ip-address

The internet address must be a valid internet address of the form n.n.n.n, where n is a decimal number ranging from 0 to 255.

NONE

Entering the DEFINE INTERNET ADDRESS NONE command erases the previously defined internet address from the Terminal Server permanent database.

[SUBNET] MASK

Indicates the Terminal Server subnet mask used to partition the host section of an internet address into subnets.

net-mask

The subnet mask must be of the form n.n.n.n where n is a decimal number in the 0 to 255 range. Failure to specify a subnet mask causes the Terminal Server to default to either a Class A, B, or C subnet mask, depending on the current Terminal Server internet address. The default for a Class A subnet mask is 255.0.0.0; for a Class B, 255.255.0.0; and for a Class C, 255.255.255.0. No default subnet mask exists if an internet address has not been defined.

NONE

Deletes a previously defined internet subnet mask.

Restrictions:

- You cannot use the Set or Change option to change the internet address while the internet protocols are running.
- To avoid using the default subnet mask you must configure the subnet mask prior to configuring the internet address. Subnet mask may not be equal to 0, nor may subnet mask be identical to the network broadcast address.
- You cannot use the NONE characteristic with the SET INTERNET ADDRESS or CHANGE INTERNET ADDRESS command.

Example

```
Local> DEFINE INTERNET ADDRESS 192.114.34.158
```

This command enters the internet address 192.114.34.158 into the permanent databases.

INTERNET GATEWAY (privileged)

{SET }
{DEFINE }INTERNET GATEWAY *ip-address...*
{CHANGE }

HOST[ADDRESS] *ip-address*
...[NETWORK{*net-address*[[SUBNET]MASK submask]}]

This privileged command enters a gateway into the Terminal Server gateway database.

ip-address

Indicates the internet address of the gateway being defined. This address must be located in the same network as the Terminal Server. It must be a valid internet address in the form n.n.n.n, where n is a decimal number ranging from 0 to 255.

CAUTION

Failure to specify *ip-address* with the NETWORK characteristic sets NETWORK ANY as the default.

HOST [ADDRESS] *ip-address*

Indicates a host that is accessible through the gateway. Use this option to define a gateway to a specific host, rather than to a network.

ANY

This default option specifies that ANY network address can be reached through the defined gateway.

net-address

Specifies a network that is reachable through the gateway. Use this option to define a gateway to a network, rather than to a specific host. The net-address must be a valid network address.

[SUBNET] MASK submask

When used with NETWORK, this command determines the exact SUBNET that the user can reach through the defined GATEWAY. If the SUBNET MASK option is omitted, the subnet mask in the Terminal Server operational database is the default. Do not overlap subnets (similar subnet mask addresses).

Restrictions:

- You cannot define more than 8 gateway entries in the permanent database.
- You must use a separate SET/DEFINE/CHANGE INTERNET GATEWAY command to assign the same ip-address to each network. You may use the SET/DEFINE/CHANGE command with various network addresses for the same gateway (using the same internet address).

Example

```
Local> CHANGE INTERNET GATEWAY 192.114.l.60 NETWORK
127.10.1.0
```

This command enters an internet gateway with an internet address of 192.114.l.60 and a network address of 127.10.1.0 in the Terminal Server operational and permanent databases. Omitting the SUBNET MASK option causes the Terminal Server to use the current internet subnet mask in the Terminal Server operational database (and no subnet mask in the Terminal Server permanent database). All connections to the hosts beginning with address 127.10 will go through the gateway address 195.1.1.60.

INTERNET HOST (privileged)

{SET }
{DEFINE } INTERNET HOST *host-name* ADDRESS *ip-address*
{CHANGE }

This is a privileged command that enters internet hosts into the Terminal Server domain name system (DNS) database local HOSTS table.

host-name

Indicates an internet host name. The name length may range from 1 to 50 characters.

ip-address

Specifies the internet address of the internet host. Valid internet addresses must be of the form n.n.n.n, where n is a decimal number ranging from 0 to 255.

Restriction:

- The DNS HOSTS table can contain up to 20 entries.

Example

```
Local> SET INTERNET HOST COMPUSERVE.COM ADDRESS
198.4.8.1
```

Internet host COMPUSERVE.COM is entered into the Terminal Server DNS operational database by this command.

INTERNET NAME RESOLUTION (privileged)

```
                                    {DOMAIN{domain      }}
                                           {DEFAULT     }}
                                    {LOCAL              }}
{SET    }INTERNET NAME RESOLUTION   {MODE{REMOTE        }}
{DEFINE}                                   {ORDERED     }}
{CHANGE}                            {RETRY LIMIT value  }}
                                    {TIME LIMIT value   }}
```

The parameters associated with the internet domain name system (DNS) function are modified in the Terminal Server database by this privileged command.

domain

Specifies the containing domain name of the Terminal Server. Whenever a relative name is searched for, the DNS first searches for this name. Upon failure DNS concatenates the string specified by this parameter to the name and retries the search.

Relative and absolute domain names

An absolute domain name is denoted by a trailing "." whereas any other form denotes a relative name. For example, Gong.Foo. is an absolute name which will be searched for literally: Chin.Ho.COM is a relative name.

MODE

Specifies the order in which resources will be searched to resolve IP names:

In LOCAL mode, the Terminal Server searches for internet addresses in its own DNS HOSTS table for data entered through previous command(s). In REMOTE mode, the Terminal Server attempts to resolve the name by querying the name server(s) specified by the command(s).

In ORDERED mode, the Terminal Server first queries user entered data from the HOSTS DNS table. If the name is not found in the DNS local HOSTS table, the Terminal Server then queries the name server(s). ORDERED is the default mode.

RETRY LIMIT value

Specifies the maximum number of times DNS will query the same name server. The allowable range is 1-5. The default value is 3.

TIME LIMIT value

Indicates the minimum delay (in seconds) between successive retries of queries to name servers to resolve a DNS name. The allowable range is 1-10. The default value is 4.

Example

```
Local> SET INTERNET NAME RESOLUTION RETRY LIMIT 5
```

This command sets a limit of 5 DNS queries to the same name server.

INTERNET NAMEserver (privileged)

{SET }
{DEFINE } INTERNET NAMEserver [*name*]ADDRESS *ip-address*
{CHANGE }

This privileged command designates DNS name server(s) that will be queried to resolve ip names entered in other commands.

name

Specifies an optional name for the DNS name server. This name is used for descriptive purposes and is not checked for correctness to ensure that this indeed is the true name of the name server whose ip-address is specified in the next parameter.

ip-address

Specifies the IP address of the DNS name server. This parameter determines the name server against which DNS name resolution will be attempted. The address must be a valid IP address of the form n.n.n.n where each n is a decimal number in the range 0-255.

Multiple name servers can be defined by successively repeating this command. The order in which the name servers will be queried is the chronological entry order.

NOTE

The name server(s) referenced by this command must be properly equipped and configured to perform the DNS name service function.

Restrictions:

- Up to 10 name servers can be defined.

Example

```
Local> DEFINE INTERNET NAMEserver aristo.tau.ac.il
ADDRESS 192.213.45.13
```

This command adds a DNS name server whose IP address is 192.213.45.13 to the Terminal Server permanent database.

PORT (secure)

{SET } [ALL] *characteristic* [characteristic(s)]
{DEFINE } PORT [port-list]
{CHANGE }

This command modifies port characteristics. The DEFINE PORT command modifies port characteristics in the permanent database. Modifications do not take effect immediately but are implemented at the next login. This command is available for all users.

The SET PORT command modifies port characteristics in the operational database. These modifications take effect immediately but remain in effect only until port logout. Port characteristics revert to the permanent database values the next time the port is logged in.

To change port characteristics in both the permanent and operational databases use the CHANGE PORT command. This command performs the functions of both the DEFINE PORT and SET PORT commands.

ALL

This is a privileged parameter that indicates that the defined characteristics are applicable to all ports.

port-list

A privileged parameter indicating the port or ports to which to apply the defined characteristics. The default is your own port. See Chapter 6 for further details on specifying port-list.

Restrictions:

- Secure users cannot access the DEFINE PORT or CHANGE PORT commands.
- Secure and nonprivileged users cannot specify all port characteristics. These restrictions are specified with the applicable characteristics.
- Only privileged users can specify port characteristics for ports other than the port being used.

- You cannot modify remote management port characteristics.

Example

```
Local> SET PORT 8 AUTHORIZED 1,2,6-19,25 ENABLED SESSION
LIMIT 3
```

The parameters in this command influence the way port 8 can be used in service mode. When the port is logged out, these settings revert to their original values.

PORT ACCESS (privileged)

```
{SET     }                          {LOCAL   }
{DEFINE  } PORT ACCESS{REMOTE    }
{CHANGE  }                          {DYNAMIC }
                                    {NONE    }
```

This is a privileged option that specifies the type of access the device using the port can accept.

CAUTION

Changes in a port's access become effective on the next port login. You should use the DEFINE or CHANGE command to preserve them after logout.

LOCAL

Allows access to the Terminal Server local mode command set. This is the default.

REMOTE

Grants access to the port device (typically a line printer) by service node applications or to a port device offered as a LAT service or Telnet listener.

DYNAMIC

Enables alternation of the port between remote access and local access.

NONE

Prevents access to the port.

Restrictions:

- You cannot use the SET or CHANGE port-list ACCESS REMOTE or NONE command when any of the ports in the *port-list* are logged in.

- You cannot use the SET or CHANGE *port-list* ACCESS DYNAMIC or LOCAL command if any port in the *port-list* is defined as REMOTE or NONE.

PORT AUTHENTICATION (privileged)

```
{SET          }
{DEFINE       }PORT AUTHentication{ENABLED     }
{CHANGE       }                   {DISABLED    }
```

This privileged command specifies whether the user login request to this port will be authenticated. If this characteristic is enabled, the user will be prompted to enter a username and a password (in terminal mode), or go through PAP/CHAP process in PPP mode. In addition, it overrides the PORT PASSWORD verification.

Only if PORT AUTHENTICATION is set to DISABLE, the PORT PASSWORD option may be used.

ENABLED

Authenticate user login requests for this port—verify the username and password.

DISABLED

Do not authenticate user login on this port. This is the default.

PORT AUTHORIZED GROUPS (privileged , 4- and 8-port models only)

{SET }
{DEFINE} PORT AUTHORIZED [GROUPS]{*group-list* }{ENABLED}
{CHANGE} {ALL }{DISABLED}

This is a privileged command that enables you to authorize groups of LAT service nodes to be available to the port. The default is group 0 ENABLED and all other groups DISABLED. To enable or disable all groups for the port, specify ALL.

group-list

One or more decimal codes ranging in value from 0 to 255, each representing a LAT group code. Multiple codes may be indicated by specifying a range of ascending numbers, by using commas between individual numbers, or a combination of both. For example, the group list 1, 3, 5-8, 14 specifies groups 1, 3, 5, 6, 7, 8, and 14.

ENABLED/DISABLED

ENABLED or DISABLED adds groups or removes groups from the existing list for the port. To set a new list, specify the *group-list* value.

PORT AUTOBAUD (privileged)

{SET }
{DEFINE} PORT AUTOBAUD{ENABLED}
{CHANGE} {DISABLED}

This is a privileged command that determines whether the Terminal Server automatically detects the speed, parity, and character size of the port device during login. This option also sets the Terminal Server port characteristics to correspond with the port device (default: ENABLED). The AUTOBAUD function is effective only when the CHARACTER SIZE and PARITY characteristics of the port device are set to either 8 and NONE or 7 and EVEN.

Disable AUTOBAUD for port set to ACCESS REMOTE or ACCESS DYNAMIC. Enabling AUTOBAUD on ports that have a preferred or dedicated service requires you to press the Return key once more to connect to the service.

CAUTION

Modifications of this characteristic are implemented on the next port login. Use the DEFINE or CHANGE command to preserve these changes after logout.

PORT AUTOCONNECT (nonprivileged)

{SET }
{DEFINE }PORT AUTOCONNECT {ENABLED}
{CHANGE } {DISABLED}

This nonprivileged option indicates if the Terminal Server automatically connects the port to a dedicated or a preferred LAT or Telnet service during port login. It also reconnects the port when a LAT or Telnet connection failure occurs. When AUTOCONNECT is ENABLED, the Terminal Server solicits for the requested LAT or Telnet service and then executes the desired connection. The default condition is DISABLED.

Restriction:

- AUTOCONNECT must be DISABLED when using DEFAULT PROTOCOL ANY.

PORT BACKWARDS SWITCH (secure)

{SET }
{DEFINE } PORT BACKWARDS[SWITCH]{character }
{CHANGE } {NONE }

This option sets a switch character that permits resumption of a previous session in the session list without returning to local mode. You can clear an existing switch by specifying NONE (default). This option is available to all users.

Restriction:

- The DEFINE or CHANGE commands may not be used by secure users with this characteristic.

PORT BREAK (secure)

{SET } {LOCAL }
{DEFINE }PORT BREAK {REMOTE }
{CHANGE } {DISABLED }

This option sets the Break key specifications during a session. This option is available to all users.
LOCAL

Defines a break signal as a local switch character for the Terminal Server and takes the user back to local mode. This is the default.

REMOTE

When this option is used, the Terminal Server transfers the LAT session break signals to the connected session.

DISABLED

Instructs the Terminal Server to ignore break signals until the user returns to local mode.

Restriction:

- The DEFINE or CHANGE commands may not be used by secure users with this characteristic.

PORT BROADCAST (nonprivileged)

```
{SET       }                        {ENABLED   }
{DEFINE    } PORT BROADCAST         {DISABLED  }
```

This is a nonprivileged option that indicates if a port can receive a message sent from another port. The default condition is ENABLED.

PORT CHARACTER SIZE (nonprivileged)

```
{SET       }
{DEFINE    }PORT CHARACTER [SIZE]   {7}
{CHANGE    }                        {8}
```

This nonprivileged option that sets the number of bits interchanged between the port and the Terminal Server. Either 7 or 8 bits is acceptable; 8 is the default.

Restriction:

- When the AUTOBAUD function for a port is enabled, the CHARACTER SIZE cannot be changed.

PORT DEDICATED (privileged)

```
{SET       }
{DEFINE    } PORT DEDICATED...
{CHANGE    }

{service-name[NODE{node-name}][DESTINATION{port-name}4- and 8-Port
                                                              models]}
                    {NONE    }]          {NONE   }          ]}
...{host-name[PORT tcp-port]                                 }
  {NONE                                                            }
```

This privileged option permanently assigns a service to a local terminal port. The default option is no dedicated service. When the value for service-name, NODE, or DESTINATION is NONE, any previous entered value is overridden. Changes to this characteristic are implemented on the next port login. AUTOCONNECT is immediately enabled when a dedicated service is indicated; at port login, the port is automatically connected to the dedicated service.

NOTE

If AUTOCONNECT is enabled and AUTOBAUD is disabled on a port that is DEDICATED, the session is started when the Terminal Server is initialized.

service-name

Specifies the name of the dedicated LAT service.

NODE *node-name*

Indicates a LAT service node from which the dedicated service is available.

DESTINATION

Sets a specific port for connection.

host-name [PORT *tcp-port*]

Specifies the internet host name or address, and an optional Telnet TCP port number.

PPP

Specifies that the local access port is permanently assigned to a single PPP session.

SLIP

Specifies that the local access port is permanently assigned to a single SLIP session.

Restrictions:

- The word Telnet is not valid as a *service-name* or *host-name*.
- If the target port is not currently logged in, you can specify DEDICATED with the SET PORT command. When you have a dedicated service, you cannot enable MULTISESSIONS.

PORT DEFAULT PROTOCOL (privileged)

		{ANY }
		{AUTOLINK }
{SET }		{LAT 4- and 8-Port models only}
{DEFINE }	}PORT DEFAULT [PROTOCOL]	{PPP }
{CHANGE }		{SLIP }
		{Telnet }

This option specifies the default protocol for the port. Telnet is the factory-set default. The default protocol clarifies commands when a protocol option has not been indicated. Setting a protocol option overrides the default protocol. For instance, CONNECT *host-name* requires clarification whereas CONNECT Telnet *host-name* is not ambiguous.

ANY

Defines the default protocol as ANY. The Terminal Server searches for network resources on the TCP/IP network before searching for resources on the LAT network.

LAT

Fixes the LAT protocol as the default if the user has not specified a protocol with the CONNECT command.

PPP

Defines the default protocol as PPP. If you do not specify a protocol with the CONNECT command, the Terminal Server defaults to the PPP protocol.

SLIP

Defines the default protocol as SLIP. If you do not specify a protocol with the CONNECT command, the Terminal Server defaults to the SLIP protocol.

Telnet

Causes the Terminal Server to default to a Telnet protocol when the user fails to specify a protocol with the CONNECT command.

Restrictions:

- The CONNECT and CONNECT PORT commands use the default protocol only. To override the default and set internet connections, use the Telnet and OPEN commands.

- Set the PORT AUTOCONNECT characteristic to DISABLED when the DEFAULT PROTOCOL is set to ANY.
- Only privileged users can use the DEFINE and CHANGE commands; however, all users can use the SET command.

PORT DSRLOGOUT (privileged)

DSRLOGOUT {ENABLED}
{DISABLED}

This is a privileged option that indicates whether a Terminal Server should log out a port that has a disabled attached device. DSRLOGOUT can only be enabled when the port hardware supports DSR signals. When DSR flow control is enabled, DSRLOGOUT must not be specified. DSRLOGOUT is disabled by default.

ENABLED

The Terminal Server will logout a port id. DSR is deasserted.

DISABLED

The Terminal Server will not use the DSR signal status to logout a port. This is the default.

NOTE

When DSR flow control is enabled, DSRLOGOUT must not be specified. DSRLOGOUT is disabled by default.

PORT DTRWAIT (privileged)

{SET }
{DEFINE }PORT DTRWAIT{ENABLED}
{CHANGE } {DISABLED}

This is a privileged option that indicates if the Terminal Server will use the DTR to indicate whether the port is being used by the Terminal Server for ports with ACCESS=REMOTE (e.g., ports with TELNET LISTENER).

These modifications take effect when you log out of the port.

ENABLED

- For ports defined with ACCESS=REMOTE, the Terminal Server asserts DTR when a connection to the port, from the Terminal Server, is requested. This may signal the modem connected to the port to dial a number that is preconfigured to the modem. When the session is terminated, the Terminal Server will deassert the DTR.
- For ports defined with ACCESS=LOCAL, the DTR signal will always be deasserted.

DISABLED

The DTR signal is always asserted by the Terminal Server—for both LOCAL and REMOTE ports. However, if SIGNAL CONTROL is enabled for the port, the DTR will be deasserted for 5 seconds when the port logs out.

NOTE

The DTR may also be used as a flow control signal.

You should only set DTRWAIT ENABLED for ports that have SIGNAL CONTROL ENABLED.

PORT FAILOVER (nonprivileged , 4- and 8-port models only)

```
{SET      }
{DEFINE   }PORT FAILOVER{ENABLED}
{CHANGE   }             {DISABLED}
```

This is a nonprivileged option that indicates that upon disconnection from a LAT service, an automatic attempt will be made to connect to another node that provides the service. The default is ENABLED.

PORT FLOW CONTROL (nonprivileged)

```
{SET      }
{DEFINE   }{INPUT  }PORT FLOW[CONTROL]{ENABLED}
{CHANGE   }{OUTPUT }                  {DISABLED}
```

A nonprivileged option that sets flow-control direction. The default is that flow control is in both directions).

```
{SET      }                    {CTS      }
{DEFINE   }PORT FLOW [CONTROL] {DSR      }
{CHANGE   }                    {XON      }
                               {DISABLED }
```

A nonprivileged option that identifies the flow-control category used by the Terminal Server to control data transmission with the port.

CTS

Specifies Clear-To-Send/Request-To-Send (CTS/RTS) modem signal flow control. This option is exclusively applicable to Terminal Servers that support these signals.

This type of flow control is usually used by null modems. When the Terminal Server detects an input overflow condition it deasserts RTS, thus signaling to the attached device to cease transmitting.

DSR

Indicates DTR/DSR signal flow control. When Terminal Server detects an input overflow condition it deasserts DTR, thus signaling to the attached device to cease transmitting.

XON

Sets Transmit On/Transmit Off (XON/XOFF) flow control. The default flow control is XON.

DISABLED

Specifies no flow control.

PORT FORWARD SWITCH (secure)

```
{SET     }
{DEFINE  }PORT FORWARD [SWITCH]{character}
{CHANGE  }                      {NONE     }
```

A switch character option permits continuation of the next session in your session list without reverting to local mode. NONE (the default) clears an existing switch. This option is available to all users.

Restriction:

- Secure users cannot use the DEFINE or CHANGE command with this characteristic.

PORT GROUPS (nonprivileged , 4- and 8-port models only)

```
{SET     }
{DEFINE  }PORT GROUPS{group-list  }[ENABLED ]
{CHANGE  }           {ALL         }[DISABLED]
```

This is a nonprivileged option that identifies which groups are currently enabled on the port from those authorized for the port (refer to the AUTHORIZED GROUPS command). GROUPS should be utilized to select the port's nodes and services you want displayed.

Logging in to a port enables all authorized groups for that port. Consequently, when port characteristics are reset to their defaults, the default for GROUPS corresponds to the default for AUTHORIZED GROUPS (i.e., group 0 ENABLED and all other groups DISABLED).

To add or remove groups within the authorized list, use the group-list format with ENABLED or DISABLED. To replace the existing list with a new list, specify group-list without either ENABLED or DISABLED. To enable or disable all authorized groups, specify ALL.

group-list

One or more decimal codes representing a LAT group code in the range from 0 to 255. Multiple codes may be indicated by individual numbers separated with commas, by a range of numbers (in ascending order), or a combination of both. For instance, the group list 1, 4, 9-11, 13 specifies groups l, 4, 9, 10, 11, and 14.

Restriction:

- GROUPS can only be specified with the SET PORT command.

PORT INACTIVITY LOGOUT (privileged)

```
{SET              }
{DEFINE           }PORT INACTIVITY [LOGOUT]{ENABLED }
{CHANGE           }                        {DISABLED}
```

This privileged option indicates whether the Terminal Server logs out a port automatically after an inactive period. The Terminal Server automatically logs out the port after the time-out period if ACCESS LOCAL is specified at a port and the local terminal user does not use the port. If a port is set to ACCESS REMOTE and there is no activity for a session, the Terminal Server terminates the session and logs out the port after the time-out period elapses. The Terminal Server characteristic INACTIVITY TIMER should be used to set the time-out period. More details are available in the terminal SERVER INACTIVITY TIMER command. The default is DISABLED.

PORT INTERRUPTS (privileged)

```
{SET              }
{DEFINE           }PORT INTERRUPTS{ENABLED }
{CHANGE           }               {DISABLED}
```

This privileged option determines if the Break key can be accessed by a local user in an attempt to terminate a remote session at an ACCESS DYNAMIC port in order to log in to the Terminal Server (default: DISABLED).

PORT LIMITED VIEW (privileged)

```
{SET          }
{DEFINE       }PORT LIMITED [VIEW]{ENABLED }
{CHANGE       }                   {DISABLED}
```

This is a privileged option that specifies whether a nonprivileged port is prevented from listing LAT nodes, LAT services, or internet databases such as internet host, ARP entries, and gateways. The default is DISABLED.

PORT LOCAL SWITCH (secure)

```
{SET          }
{DEFINE       }PORT LOCAL [SWITCH]{character}
{CHANGE       }                   {NONE     }
```

This option specifies a switch character that can be used for reestablishing local mode from service mode. Although the switch character can be any keyboard character unused characters such as Ctrl/L is recommended. NONE (the default option) clears an existing switch. This option is available to all users.

Restriction:

- The DEFINE or CHANGE command cannot be used with this characteristic for secure users.

PORT LOCK (privileged)

{SET }
{DEFINE }PORT LOCK{ENABLED }
{CHANGE } {DISABLED}

This privileged option indicates if the LOCK command is accessible to a port user. When the LOCK characteristic is ENABLED on a port as well as on the Terminal Server, the port user can specify LOCK to deny access to the terminal where the command is entered. Input is hindered by the LOCK command until a user enters the unlock password at that terminal. DISABLED prevents the use of the LOCK command. The default is ENABLED.

PORT LOSS NOTIFICATION (nonprivileged)

{SET }
{DEFINE }PORT LOSS [NOTIFICATION]{ENABLED }
{CHANGE } {DISABLED}

This nonprivileged option determines whether a beep is sounded upon losing an input character because of data error or overrun. The default is ENABLED.

Restriction:

- LOSS NOTIFICATION is only relevant when PORT ACCESS is LOCAL or DYNAMIC.

PORT NAME (privileged)

{SET }
{DEFINE }PORT NAME *port-name*
{CHANGE }

This privileged option specifies a unique port name on the Terminal Server. Naming conventions and more details are available in Chapter 6.

The default is PORT_n, where n is the port number.

PORT PARITY (nonprivileged)

```
                                        {EVEN    }
{SET     }                              {ODD     }
{DEFINE  }PORT PARITY                   {MARK    }
{CHANGE  }                              {SPACE   }
                                        {NONE    }
```

A nonprivileged option that specifies the port parity as EVEN, ODD, MARK, SPACE, or NONE (default).

Restriction:

- PARITY cannot be changed for a port that is currently in the AUTOBAUD process.

PORT PARITY CHECK (nonprivileged)

```
{SET     }                  {CHECK     }
{DEFINE}PORT PARITY         {NOCHECK   }
{CHANGE}
```

This is a nonprivileged option that specifies whether the Terminal Server will check the parity on data arriving at the port.

CHECK

The Terminal Server will check the parity, according to the setting of DEFINE PORT PARITY. This is the default.

NOCHECK

The Terminal Server will not check the parity.

PORT PASSWORD (privileged)

{SET }
{DEFINE }PORT PASSWORD{ENABLED }
{CHANGE } {DISABLED}

This privileged option determines whether a password is necessary for a user to login to the Terminal Server. Setting the Terminal Server characteristic LOGIN PASSWORD specifies the login password. The default is DISABLED.

CAUTION

The next port login implements changes to this characteristic. You should use the DEFINE or CHANGE command to preserve them after logout.

PORT PPP (privileged)

{SET }
{DEFINE }PORT PPP {ENABLED }
{CHANGE } {DISABLED}

This privileged option specifies that a point-to-point protocol (PPP) session may be started on the specified port. If this option is ENABLED, the PPP session startup prepares for a link startup. The default status is DISABLED. The LCP ENABLE/DISABLE and LCP PASSIVE ENABLE/DISABLE commands determine the LINK startup. PPP and LCP must be ENABLED to bring up a PPP session.

NOTE

If PPP is DISABLED on a port running a PPP session, the session is taken down immediately without notification to the peer.

If PPP is ENABLED on the console port, console messages are not displayed while a PPP is active.

Restrictions:

- On ports with MULTISESSIONS ENABLED you cannot enable PPP. A port whose PPP characteristic is DISABLED prevents a PPP session from starting on it.
- The attached device on the port must support the PPP protocol to establish a link.

PORT PPP IPCP

{SET	}	
{DEFINE	}PORT[PPP]IPCP	{ENABLED }
{CHANGE	}	{DISABLED}

This option controls whether the IPCP negotiation is allowed on the link. Using this option, a manager can "bounce" the link to pick up new locally configured parameters. The PORT PPP IPCP command can be used to debug IPCP setups.

Restrictions:

- The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.
- From a remote port this command can only be entered by a privileged user.

PORT PPP IPCP ADDRESS

{SET	}	
{DEFINE	}PORT[PPP]IPCP ADDRESS	{ENABLED }
{CHANGE	}	{DISABLED}

This option specifies whether the Terminal Server should attempt to negotiate the IP address for both ends of this link. If ENABLED, the Terminal Server always attempts to negotiate using IPCP option #3, ADDRESS, first, as this is the preferred method. If the attached device does not support option #3, the Terminal Server falls back and attempts to negotiate using option #1, ADDRESSES.

The Terminal Server internet IP address is always proposed as the Terminal Server's local address. If the port has an IP address assigned to it, the Terminal Server requires that the attached device use that address. The attached device can inform the Terminal Server of its IP address via negotiation if no address is assigned to the port. If the peer's address is part of the Terminal Server subnet and is not currently held by another port on the Terminal Server, the Terminal Server allows the peer to use this address, otherwise, the peer's proposed address is rejected.

It is possible that the link will come up if these address negotiations fail. However, each peer may have inconsistent knowledge about the system with which it is exchanging IP datagrams.

The Terminal Server assumes that the peer has the address currently set up on the port if the link is open. IP datagrams for that IP address are forwarded. The Terminal Server does not forward IP datagrams if there is no address associated with the port.

Restrictions:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- Only a privileged user can enter this command from a remote port.

PORT PPP IPCP COMPRESSION

{SET	}	
{DEFINE	}PORT[PPP]IPCP COMPRESSION	{ENABLED }
{CHANGE	}	{DISABLED}

This option specifies whether the Terminal Server negotiates the use of a compression protocol. The Van Jacobson Compressed TCP/IP protocol is the only compression protocol supported. If it is used, it must be implemented by each peer in both directions.

The peers may compress the TCP/IP headers when this option is ENABLED. This causes fewer bytes to be sent across the asynchronous line, and increases the line's bandwidth and performance.

Restrictions:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- Only a privileged user can enter this command from a remote port.

PORT PPP IPCP COMPRESSION STATES

{SET }
{DEFINE }PORT[PPP]IPCP COMPRESSION STATES "number"
{CHANGE }
This option specifies the number of TCP connections the Terminal Server can decompress from the peer at any given time. The range of values is 4-16. The default value is 16.

Restrictions:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- Only a privileged user can enter this command from a remote port.

PORT PPP IPCP HOST ADDRESS (nonprivileged)

{SET }
{DEFINE }PORT[PPP]IPCP HOST ADDRESS nn.nn.nn.nn
{CHANGE }

This nonprivileged option associates a host address with the PPP interface, allowing the Terminal Server to know what IP device is directly attached on the other side of the PPP link. The default for this characteristic is address 0.0.0.0 (no address defined). Use the CLEAR/PURGE PORT PPP (or SLIP) HOST ADDRESS command to remove an existing address.

Restrictions:

- The IPCP HOST ADDRESS must be configured manually on both sides of the link if address negotiations are not used.
- A nonprivileged status is required for the DEFINE and CHANGE commands. The SET command has a secure status.
- This command does not support *port-list*. An address can be associated with only one port.
- The host address and the Terminal Server must reside in the same subnetwork.
- The host address cannot use the SET or CHANGE command on a port that already has an IP address.
- Only one IP address is allowed per port. Both SLIP and PPP use the same address, which can be configured by the SLIP or PPP protocol command.

PORT PPP LCP

{SET	}	
{DEFINE	}PORT[PPP]LCP	{ENABLED }
{CHANGE	}	{DISABLED}

This option controls whether the LCP negotiation is allowed on the link. To do this, DISABLE and ENABLE LCP for a running PPP session. The LCP characteristic will generally be ENABLED, so that LCP starts the link normally. Change the characteristic value to force the LCP link to renegotiate using the new, locally configured parameters. This allows connection to the link without having to first bring the link down.

Restriction:

- This command can be entered only by a privileged user from a port other than the one on which the PPP session is running.

PORT PPP LCP ACFC

{SET	}		
{DEFINE	}PORT[PPP]LCP AUTHENTICATION	{PAP	}
{CHANGE	}	{DISABLE	}

This command allows a link to be configured so that the address and control field compression (ACFC) is negotiated.

PPP uses unnumbered HDLC frames to encapsulate each packet it sends. These frames include address and control bytes which serve no useful purpose on a PPP link. ENABLE the ACFC option for the Terminal Server to request that this field be omitted. The address and control field information is sent if the ACFC option is DISABLED. The default is DISABLED.

Restriction:

- The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.

PORT PPP LCP AUTHENTICATION (privileged)

{SET }
{DEFINE }PORT[PPP]LCP ACFC {ENABLED }
{CHANGE } {DISABLED}

This privileged command specifies whether the Terminal Server requires the peer to use the PPP PAP protocol to authenticate itself. The peer must provide the Terminal Server with the LOGIN password if PAP is specified.

Restrictions:

- SET, DEFINE, and CHANGE are all privileged commands.
- The Terminal Server does not authenticate itself to the peer.

PORT PPP LCP MAP

{SET }
{DEFINE }PORT[PPP]LCP MAP"*hex-number*"
{CHANGE }

This command lets the Terminal Server tell the peer which characters require byte-stuffing. Some characters potentially have special meaning to the underlying layers of software or hardware—for example, XON/XOFF. Byte-stuffing lets these characters be encapsulated into a two-byte sequence that allows the original character to pass as data. By default, the low 32 ASCII bytes are byte stuffed, which requires additional overhead and consumes bandwidth on a slow serial line. The fewer characters that require byte-stuffing on a given line, the better the performance. This option provides a means to inform the peer of which specific characters require byte-stuffing.

To identify which characters must be stuffed bits are set in the mask. The bits are ordered left to right, such that the hex character 0x0 would need the mask to have the leftmost bit set, that is, 0x80000000. The default of having all character bytes stuffed would use a mask of 0xFFFFFFFF.

Restriction:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

Example

The mask would be set to 0x000A0000 if only XON and XOFF require byte-stuffing. The following is the syntax for the command:

```
Local>  SET PORT LCP MAP A0000
```

PORT PPP LCP MRU

{SET }
{DEFINE }PORT[PPP]LCP MRU "*number*"
{CHANGE }

This option specifies the size in bytes of the maximum receive units (MRU) that the Terminal Server wants to negotiate for the link. This command tells the peer what the server wants to see as an upper limit to packet size. By setting the MRU size you can tune the link performance. The default value for this option is 1500 bytes and its range is 64 to 1500 bytes. The server accepts packets of up to 1500 bytes regardless of the negotiated setting.

Restriction:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

PORT PPP LCP PASSIVE

{SET }
{DEFINE }PORT[PPP]LCP PASSIVE {ENABLED }
{CHANGE } {DISABLED}

This option controls whether the LCP will actively open the LCP link on connection, or will wait passively for packets from the peer to start the link. The LCP waits for the peer to begin negotiations if LCP PASSIVE is ENABLED. The LCP actively tries to start negotiations as soon as the PPP session is started if LCP PASSIVE is DISABLED.

NOTE

The link will not be negotiated if both the Terminal Server and the attached device use PASSIVE.

Restriction:

- The DEFINE and CHANGE commands require privileged status. The SET command requires a secure status.

PORT PPP LCP PFC

{SET	}	
{DEFINE	}PORT[PPP] LCP PFC	{ENABLED }
{CHANGE	}	{DISABLED}

To identify the type of packet being sent, PPP uses a two-character protocol field. This field may be compressed into a single byte and still uniquely identify the protocol type. This option lets you conserve bandwidth for slow serial lines. PFC is an abbreviation for "protocol-field compression."

Restriction:

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

PORT PPP LCP/IPCP MAXCONFIGURE

{SET	}		
{DEFINE	} PORT [PPP]	{LCP }	MAXCONFIGURE nn
{CHANGE	}	{IPCP}	

This option determine how many times the LCP, IPCP, or ATCP will send a configure request packet to the peer without receiving a configure acknowledgment signal. The LCP/IPCP assumes that the peer cannot respond if the peer failed to send an acknowledgment signal after the assigned number of request packets. The default value for this option is 10.

Restriction

- The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP MAXFAILURE

{SET }
{DEFINE }PORT [PPP] {LCP }MAXFAILURE nn
{CHANGE } {IPCP}

This option determines how many times LCP, IPCP, or ATCP will send a negative acknowledgment message (NAK) for the peer's proposed options before deciding to start rejecting the problem options (the options whose values the LCP/IPCP finds objectionable).

Once LCP/IPCP rejects the problem options, either the link establishment will fail or the options must take on the default value. The default value for this characteristic is 10.

Restriction:

- The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP MAXTERMINATE

{SET }
{DEFINE }PORT [PPP] {LCP }MAXTERMINATE nn
{CHANGE } {IPCP}

This option determines how many times the LCP, IPCP, or ATCP will send a terminate request packet to the peer without receiving a terminate acknowledgment signal. A takedown of the link will result from the failure of the peer to send an acknowledgment signal after the assigned number of request packets. The default number of request packets is 2.

Restriction

- The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP RESTART

{SET }
{DEFINE }PORT [PPP] {LCP }RESTART nn
{CHANGE } {IPCP}

This option determines how many seconds there will be between an LCP, IPCP, or ATCP configure terminate retransmit while LCP/IPCP configuration or link termination is taking place. For example, the LCP will send one configure request packet to the peer and will wait a period of time for a response. If no response is received within the time limit, another configure request will be sent. Setting the LCP/IPCP RESTART option determines how long the wait period is. The default for this option is 3 seconds.

Restriction:

- The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PREFERRED (nonprivileged)

{SET }
{DEFINE }PORT PREFERRED...
{CHANGE }

{service-name (4- and 8-Port models only)}[NODE{*node-name*}] [DESTINATION{*portname*}]
{NONE } [{NONE }]
...{*host-name* }[PORT *tcp-port*]
{NONE }

This nonprivileged option sets a preferred network service when a CONNECT command is specified for the port without a service name. The default is no preferred service.

When a value is indicated for NODE or for DESTINATION, the Terminal Server does not attempt automatic failover for LAT sessions. Specifying NONE as the value for the preferred service-name, NODE, or DESTINATION overrides any prior entry for that field.

service-name

Indicates the LAT service name to which you want to connect.

host-name

Specifies the internet host name or internet host address to which you want to connect.

NODE *node-name*

Sets a particular LAT service node to which you want to connect.

tcp-port

Specifies the optional Telnet/TCP port number.

DESTINATION

Indicates a particular port to which you want to connect.

port-name

To set the port's default protocol to match the protocol (Telnet or LAT) of the preferred service, use the DEFINE PORT command. The default setting connects you to the first available port that offers the service.

Restriction:

- NODE and DESTINATION are valid only when LAT service is specified as the preferred service.

PORT QUEUING (nonprivileged, 4- and 8-port models only)

```
{SET      }
{DEFINE   }PORT QUEUEING{ENABLED }
{CHANGE   }             {DISABLED}
```

This nonprivileged option determines whether queuing of LAT service connection requests is enabled for the port. If QUEUING is disabled after requests have been queued, those requests are retained until the LAT service begins. The default is DISABLED.

PORT REMOTE MODIFICATION (nonprivileged, 4- and 8-port models only)

{SET }
{DEFINE }PORT REMOTE [MODIFICATION]{ENABLED }
{CHANGE } {DISABLED}

This nonprivileged option determines whether a suitable LAT service node can change port characteristics (e.g. SPEED, CHARACTER SIZE, PARITY, and LOSS NOTIFICATION) to correspond to the port characteristics of a remote device on the Terminal Server. The default is DISABLED.

Restriction:

- The port user can modify the physical port characteristics when this characteristic is enabled on a secure port. To prevent this, make sure REMOTE MODIFICATION and SECURITY are not enabled on the same port.

PORT SECURITY (privileged)

{SET }
{DEFINE }PORT SECURITY{ENABLED }
{CHANGE } {DISABLED}

This privileged option indicates if secure status on the port is ENABLED or DISABLED. When ENABLED, the commands available on the port are limited to a subset of nonprivileged commands. When DISABLED, all nonprivileged commands are available to the port. The default is DISABLED.

PORT SESSION LIMIT (privileged)

{SET }
{DEFINE }PORT SESSION LIMIT{*limit* }
{CHANGE } {NONE}

This is a privileged option that restricts the number of permitted sessions ranging from 0 to 8. The maximum number of sessions is allowed on the Terminal Server when NONE is specified. The default value is 4.

PORT SIGNAL CHECK (privileged)

{SET }
{DEFINE } PORT SIGNAL [CHECK] {ENABLED }
{CHANGE } {DISABLED}

This privileged option indicates if the Terminal Server checks for incoming signals on a remote terminal port prior to connection. In the absence of the DSR signal, the Terminal Server rejects an attempted connection, either LOCAL or REMOTE. On Terminal Servers using the RJ-45 jacks, RTS is asserted when the Terminal Server wishes to transmit data on the port. Actual transmission begins when the CTS signal is asserted by the modem. The default is DISABLED.

Restriction:

- SIGNAL CHECK should not be used for a port using CTS flow control, DSR flow control, or SIGNAL CONTROL.

PORT SIGNAL CONTROL (privileged)

{SET }
{DEFINE } PORT SIGNAL CONTROL {ENABLED }
{CHANGE } {DISABLED}

This privileged option determines if modem signals are asserted by the Terminal Server. DISABLED should be specified for ports connected to devices or device cables that do not support modem signals. Modifications of this characteristic take effect on the following port login. The default is DISABLED.

Restriction:

- Only the DEFINE command is valid with SIGNAL CONTROL; the SET/CHANGE command cannot be used.

PORT SLIP (nonprivileged)

```
{SET      }
{DEFINE   }PORT SLIP   {ENABLED }
{CHANGE   }            {DISABLED}
```

This nonprivileged option specifies whether SLIP is enabled for the port (the default is DISABLED). The attached device on the port must support the SLIP protocol to enable SLIP. The SLIP session for the port is disconnected when SLIP is disabled.

port-list

This parameter specifies one or more physical port.

ALL

Specifies all of the physical ports, not including the remote management console.

Restriction:

- You cannot enable SLIP on ports with the MULTISESSIONS command or characteristics enabled.

PORT SLIP COMPRESSION (nonprivileged)

```
{SET (secure)  }
{DEFINE        } PORT SLIP COMPRESSION {ENABLED      }
{CHANGE        }                       {DISABLED     }
                                       {AUTOCOMPRESS }
```

This nonprivileged command determines whether or not the TCP/IP header compression is used on SLIP/CSLIP. The default for this option is COMPRESSION DISABLED. The following are the three states and requirements for COMPRESSION:

ENABLED

Compression must be used on the link.

DISABLED

Compression cannot be used on the link.

AUTOCOMPRESS, SLIP/CSLIP

Initially set to compression disabled; however, if the SLIP receives a compressed packet, compression starts automatically.

Restriction:

- The SET PORT SLIP COMPRESSION command is a secure option.

PORT SLIP COMPRESSION STATES (privileged)

{SET }
{DEFINE } PORT SLIP COMPRESSION STATES
{CHANGE }

This privileged command determines how many compression states are used on the SLIP datalink. The same number of states are used in each direction.

number

The number of COMPRESSION STATES used by the port must be between 3 to 16 states.

Restriction:

- The SET SLIP PORT COMPRESSION command is a secure option.

PORT SLIP HOST ADDRESS (nonprivileged)

{SET }
{DEFINE } PORT SLIP HOST [ADDRESS] host-id
{CHANGE }

This nonprivileged option assigns the internet address of the attached device needed to act as a host in the internet environment. This option allows the Terminal Server to determine which Internet Protocol (IP) packets it should transmit or receive over the asynchronous line between the IP host and the internet network.

Restrictions:

- The host addresses must be unique (a port list is not allowed).
- The Terminal Server internet address and the host address must be in the same subnet.
- If the port already has a SLIP HOST address you cannot use the SET or CHANGE command. Use the DEFINE command with the new address and log out of the port to alter an existing address.
- A port can have only one IP address. Both SLIP and PPP use the same address that can be configured by the SLIP or PPP protocol command (see PORT PPP IPCP HOST ADDRESS command).

PORT SLIP MTU (nonprivileged)

{SET }
{DEFINE } PORT SLIP MTU *mtu-size*
{CHANGE }

This nonprivileged option specifies the Maximum Transmission Unit (MTU) for SLIP packets on the port. The MTU is the largest datagram size (in bytes) that is accepted on the port (range: 64 to 1006; default 1006).

Restriction:

- The MTU cannot be changed with an existing SLIP session on the port.

PORT SPEED (INPUT/OUTPUT) (nonprivileged)

```
{SET      }
{DEFINE   } PORT [INPUT  ] SPEED speed
{CHANGE   }      [OUTPUT]
```

This nonprivileged option specifies the port speed in bits per second (bps). The following are the permissible port-speed values: 75,110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600 (default value), 19200, 38400, 57600, and 115200.

To change the speed from the device to the Terminal Server use the INPUT SPEED command. To change the speed from the Terminal Server to the device use the OUTPUT SPEED command.

Restriction

- Speed cannot be modified for a port currently in the AUTOBAUD process.

PORT STOP BITS (nonprivileged)

```
{SET      }                {1       }
{DEFINE   }PORT STOP [BITS]{2       }
{CHANGE   }                {DYNAMIC }
```

This nonprivileged command notifies the Terminal Server to use 1 or 2 stop bits when to output a character. Set STOP BITS to 2 when the port speed is up to 134 bps. Set STOP BITS to 1 for a port speed above 134 bps. To determine the number of stop bits depending on the output speed of the port, use DYNAMIC. The default is DYNAMIC.

PORT TELNET CLIENT (secure)

```
{SET      }
{DEFINE   } PORT [ALL      ]Telnet CLIENT [characteristics]
{CHANGE   }      [port-list ]
```

This option changes the existing Telnet Client characteristics for the specified ports in the Terminal Server database. This option is available to all users.

The characteristics to be associated with new Telnet connections established from the specified port(s) can be set with this command. The following characteristics can be specified to the PORT Telnet CLIENT command:

```
AO [REQUEST]                    IP [REQUEST]
AYT [REQUEST]                   NEWLINE
BINARY                      PROFILE
```

BREAK (BRK) [REQUEST]
CHARACTER [SIZE]
ECHO
EOR [REQUEST]
INPUT/OUTPUT FLOW CONTROL
QUOTE
SWITCH [CHARACTER]
SYNCH [REQUEST]
TOGGLE ECHO

For a detailed description of each of the Telnet CLIENT characteristics, refer to the SET SESSION Telnet command.

Restriction:

- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

ALL and *port-list* are privileged.

PORT TELNET CLIENT TERMTYPE (secure)

{SET }
{DEFINE }PORT TELNET CLIENT TERMTYPE[*term_type*]
{CHANGE } [ANSI]

This option changes the existing Telnet Client characteristics for the specified ports in the Terminal Server database. This option is available to all users.

term_type

The terminal type to be negotiated when new Telnet connections are established from the specified port(s) can be set with this command. The default is ANSI.

PORT TELNET SERVER (privileged)

{SET }
{DEFINE } PORT [ALL] Telnet SERVER [characteristics]
{CHANGE } [*port-list*]

A privileged option that permits specification of the characteristics to be associated with Telnet connections established to the specified port(s). The Telnet Terminal Server characteristics are the current user-definable port parameters attributed to a Telnet Terminal Server connection. The definitions, syntaxes, and restrictions for the following PORT Telnet Terminal Server characteristics appear in the next five sections.

AYT [INDICATION]
BREAK (BRK) [INDICATION]
CHARACTER [SIZE]
IP [INDICATION]
NEWLINE

PORT TELNET SERVER AYT INDICATION (privileged)

{SET }
{DEFINE } PORT TELNET SERVER AYT [INDICATION]{character}
{CHANGE} {NONE }

AYT (Are-You-There) designates which character will be relayed to the Terminal Server port of the Telnet server connection when an AYT request is transmitted by the remote user. There is no default character.

PORT TELNET SERVER BREAK (BRK) INDICATION (privileged)

{SET } {BRK } {character}
{DEFINE} PORT TELNET SERVER{BREAK}[INDICATION]{NONE }
{CHANGE} {BREAK }

BRK (Break) is a privileged command that specifies a character or BREAK signal for transmission to the Terminal Server port of the Telnet server connection when the remote user requests a Telnet break. Individual letters must be entered to specify the break signal. A break signal sent to the Terminal Server port is the default.

PORT TELNET SERVER CHARACTER SIZE (privileged)

```
{SET       }
{DEFINE    } PORT TELNET SERVER [TRANSMIT] {CHARACTER} [SIZE]{7}
{CHANGE    }                    [RECEIVE ]             {8}
```

This command determines if 7-bit or 8-bit characters should be sent and received on this connection. Transmit characters are sent by the Terminal Server to the host. Receive characters are received by the Terminal Server from the host. The default is 8-bit characters for both transmit and receive.

PORT TELNET SERVER IP INDICATION (privileged)

```
{SET       }
{DEFINE    }PORT TELNET SERVER IP[INDICATION]{character}
{CHANGE    }                                 {NONE     }
```

IP (Interrupt Process) is used to define a character which will be sent to the Telnet server connection's associated Terminal Server port when the remote user generates an IP request. There is no character defined by default.

PORT TELNET SERVER NEWLINE FROM TERMINAL (privileged)

```
{SET      }
{DEFINE}PORT TELNET SERVER NEWLINE FROM TERMINAL   {string   }
{CHANGE}                                           {<CR>    }
                                                   {<CRLF>}
                                                   {NONE    }
                                                   {<LF>    }
```

This characteristic specifies a l- or 2-character sequence that is interpreted as a new line when received from the remote user. <CR> is the default.

PORT TELNET SERVER NEWLINE TO TERMINAL (privileged)

```
{SET       }                                       {string   }
{DEFINE    } PORT TELNET SERVER NEWLINE TO TERMINAL {<CR>    }
{CHANGE    }                                       {<CRLF>}
                                                   {NONE     }
                                                   {<LF>     }
```

This characteristic specifies a 1- or 2-character sequence which is relayed to the remote user after a NEWLINE FROM HOST sequence is received from the local Telnet server Terminal Server port. The default is <CRLF>.

PORT TERMINATION

{SET }
{DEFINE }PORT TERMINATION [STRING]{NONE }
{CHANGE } {string }

This command specifies a string that the Terminal Server sends to the port if a TelNet session is disconnected.

STRING

A string of up to two characters in length can be specified, for example, control D, logout.

PORT USERNAME (nonprivileged)

{SET }
{DEFINE } PORT USERNAME {"username"}
{CHANGE }

This is a nonprivileged command that specifies a username of 1 to 16 ASCII characters (enclosed within quotation marks) to be associated with the port. The default is no USERNAME.

Setting a username with the DEFINE PORT command deletes the USERNAME prompt on the subsequent login. This prompt can be retained by specifying another DEFINE PORT USERNAME command as well as a quoted Null String (" ") for the USERNAME characteristics.

PORT VERIFICATION (secure)

{SET }
{DEFINE } PORT VERIFICATION {ENABLED }
{CHANGE } {DISABLED}

This option determines if informational messages are sent by the Terminal Server upon connection disconnection, or switching of sessions. This command does not affect error and warning messages. This command is available to all users. The default option is ENABLED.

Restriction:

- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PRIVILEGED/NONPRIVILEGED (secure)

SET {PRIVILEGED }
{NONPRIVILEGED}

This secure option enables privileged operations to be executed by the port in use. This command causes the Terminal Server to prompt you for the privileged password. Specify the default password SYSTEM the first time the Terminal Server is used. Then set your own password by specifying the SET server PRIVILEGED PASSWORD command. This prevents unauthorized users from accessing privileged commands.

Entering the SET NONPRIVILEGED command or logging out the port will return the port back to nonprivileged status to prevent unauthorized use. Setting the privileged status effects all terminal sessions.

Example

```
Local> SET PRIVILEGED

Password> SYSTEM (not displayed)

Local> SET server PRIVILEGED PASSWORD

Password>SECRET (not displayed)

Verification> SECRET (not displayed)

Local> SET NONPRIVILEGED
```

This example illustrates entering SYSTEM as the default password at the password prompt. Then the port status is set to privileged and the privileged password is modified to SECRET prior to returning the port to nonprivileged status. On a subsequent trial to enter privileged status on this port the password SECRET must be entered.

SERVER (privileged)

{SET }
{DEFINE }server characteristic [characteristic(s)]
{CHANGE }

These privileged options define Terminal Server characteristics.

Restriction:

Some Terminal Server characteristics using a SET command cannot be modified during an active or queued session. These characteristics are listed in their respective restrictions in this section.

Examples

```
Local> DEFINE server IDENTIFICATION “TECHSALES OFC4”
```

This command specifies a Terminal Server identification.

```
Local> SET server CIRCUIT 60 KEEPALIVE 30
```

This command resets values for the circuit and keepalive timers. These values return to their permanent database values upon reinitialization of the Terminal Server.

SERVER ACCESS PASSWORD (privileged)

{SET }
{DEFINE }SERVER ACCESS PASSWORD password
{CHANGE }

This privileged command designates a password that users accessing the Terminal Server not through a physical port must enter. No password checking is the default.

Valid passwords have 1 to 16 characters. The Terminal Server will not check for a password when a quoted null string (" ") appears in the command line.

When ACCESS PASSWORD is the only characteristic in the command line, the password value may be omitted. Then the Terminal Server prompts for the password; the password should be entered.

SERVER ANNOUNCEMENTS (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER ANNOUNCEMENTS{ENABLED }
{CHANGE } {DISABLED}

This LAT protocol command designates whether LAT multicast messages are sent over the Ethernet by the Terminal Server showing the availability of local services. Announcements are relayed only when local services are specified. The default is ENABLED.

SERVER BROADCAST (privileged)

{SET }
{DEFINE } SERVER BROADCAST {ENABLED }
{CHANGE } {DISABLED}

This privileged option determines whether the BROADCAST is ENABLED or DISABLED for users on port devices. The default is ENABLED.

SERVER CIRCUIT TIMER (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER CIRCUIT [TIMER] *milliseconds*
{CHANGE }

This privileged LAT protocol option defines the interval between messages sent to LAT service nodes from the Terminal Server. The valid range is from 30 to 200 milliseconds with a default of 80 milliseconds.

Restrictions:

- If any LAT sessions are active the SET command cannot be used with this parameter.

SERVER IDENTIFICATION (privileged)

{SET }
{DEFINE } SERVER IDENTIFICATION "*id-string*"
{CHANGE }

The *id-string* value is a string ranging from 1 to 40 ASCII characters. The string must be contained in quotation marks ("id-string"). Entering the command with a quoted null string (" ")deletes an identification string. When a user logs into the Terminal Server, this string is displayed in the welcome banner. The default is no identification string.

Restriction:

- The SET command cannot be used with this parameter during an active LAT session.

SERVER INACTIVITY TIMER (privileged)

{SET }
{DEFINE } SERVER INACTIVITY [TIMER] minutes
{CHANGE }

This privileged option indicates the time-out period (ranging 1 to 120 minutes) for ports having the port characteristic INACTIVITY LOGOUT when ENABLED. The timer specifies the length of time that a local terminal port can be logged in without local user activity. The timer also determines the amount of time that a remote terminal port can be logged in the absence of activity for a session at that port. Active session on the port prevent time-out from occurring. The default is 30 minutes.

SERVER KEEPALIVE TIMER (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER KEEPALIVE [TIMER] *seconds*
{CHANGE }

This is a privileged LAT protocol command that designates the interval between messages for LAT circuits on which no data is being transmitted. The range is from 10 to 180 seconds while the default is 20 seconds.

Restriction

- The SET command cannot be used with this parameter while LAT sessions are active.

SERVER LOCK (privileged)

{SET }
{DEFINE } SERVER LOCK {ENABLED }
{CHANGE } {DISABLED}

This privileged command indicates if the LOCK command can be accessed by interactive port users. The default is ENABLED.

SERVER LOGIN PASSWORD (privileged)

{SET }
{DEFINE } SERVER LOGIN PASSWORD ["*password*"]
{CHANGE }

This is a privileged command that designates a password that interactive users are required to use during Terminal Server login. The port characteristic PASSWORD must be specified as ENABLED to obtain the password prompt at port login.

The password value can be omitted when LOGIN PASSWORD is the only characteristic in the command line. Then the Terminal Server prompts for the password.

ACCESS is the default password and is operative when the Terminal Server is delivered or when the Terminal Server characteristics are reset to their default values.

SERVER MULTICAST TIMER (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER MULTICAST [TIMER] seconds
{CHANGE }

This privileged LAT protocol command designates the time span between service announcement transmissions ranging from 10 to 180 seconds. The default is 30 seconds.

SERVER NAME (privileged)

{SET }
{DEFINE } SERVER NAME *server-name*
{CHANGE }

This privileged command designates a Terminal Server name ranging from l to 16 characters. The default is CS_nnnnnnnnnnnn, where each n is one of the 12 hexadecimal characters in the CS Terminal Server's Ethernet address.

Restriction:

- The SET command cannot be used with this parameter during an active session.

SERVER NODE LIMIT (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER NODE [LIMIT] {limit }
{CHANGE } {NONE}

This privileged LAT protocol command specifies the maximum number of LAT service nodes that the Terminal Server maintains in its node database. The range is 1 to 50 (default: 20). NONE implies no limit except the memory constraints of the Terminal Server.

SERVER NUMBER (privileged)

{SET }
{DEFINE } SERVER NUMBER [n]
{CHANGE }

This privileged command indicates a Terminal Server number ranging from 0 to 32767. The default is 0.

Restriction:

- You cannot use the SET command with this parameter while sessions are active.

SERVER PASSWORD LIMIT (privileged)

{SET }
{DEFINE } SERVER PASSWORD LIMIT limit
{CHANGE }

This is a privileged option that designates the number of times (ranging from 1 to 10) that a user is granted to enter the correct password for a Terminal Server operation that is password protected. The default is 3. **Section 7.5** contains more information on password specification.

SERVER PRIVILEGED PASSWORD (privileged)

{SET }
{DEFINE } SERVER PRIVILEGED PASSWORD ["password"]
{CHANGE }

This privileged option designates the password required by a user to access privileged Terminal Server commands at the port issuing the SET PRIVILEGED command. When PRIVILEGED PASSWORD is the only characteristic in the command line, the password value may be omitted and the Terminal Server prompts for the password.

SYSTEM is the default password and is operative when the Terminal Server is delivered or when the Terminal Server characteristics revert to their defaults.

WARNING

Once you have set the password, you cannot change the password without the old password. Do not lose the password. Make sure that all passwords are recorded in a safe place.

SERVER PROMPT (privileged)

{SET }
{DEFINE } SERVER PROMPT ["prompt-string"]
{CHANGE }

This is a privileged command that designates a unique string of characters for the prompt-string value that you assign to the Terminal Server prompt. The default prompt “Local” is substituted by these characters. The prompt-string value is a string of 1 to 16 ASCII characters surrounded by quotation marks ("prompt-string"). Entering the command with a quoted null string (" ") resets the prompt to the default “Local.”

SERVER QUEUE LIMIT (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER QUEUE [LIMIT] {depth }
{CHANGE } {NONE}

This is a privileged LAT protocol command that sets the maximum number of queued connection requests (ranging from 0 to 200) for remote terminal to Terminal Server ports. This number is called the depth of the queue. The default value is 100. The queue is disabled when ascribed a value of 0. NONE is equal to the maximum number of queued connection requests allowed.

SERVER RESPONDER (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER RESPONDER {ENABLED }
{CHANGE } {DISABLED}

This privileged command enables or disables the RESPONDER characteristic.

RESPONDER

Responder enables or disables the CS Terminal Server’s capability to request information for other nodes.

ENABLED

The Terminal Server may respond to information requests on behalf of other nodes as well as responding to solicit information requests targeted to itself. The Terminal Server acts as an agent for another node only when information about the specified service and node resides in local database, and the requesting node’s access codes correspond to the targeted node’s access codes.

DISABLED

This command causes the Terminal Server to respond exclusively to solicit information datagrams that request local node and service information. DISABLED is the default.

NOTE

If the Terminal Server's RESPONDER characteristic is set or cleared, it can still react to local service/node information when it receives a Solicited Information request targeted to itself.

SERVER RETRANSMIT LIMIT (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVER RETRANSMIT [LIMIT] limit
{CHANGE }

This privileged option sets the number of times a LAT message will be retransmitted to a service node if acknowledgment messages are not received by the Terminal Server. The value ranges from 4 to 120 times. 8 is the default.

Restrictions:

- The SET command cannot be used with this parameter during active LAT sessions.

SERVER SERVICE GROUPS (privileged, 4- and 8-port models only)

{SET }
{DEFINE }SERVER[SERVICE]GROUPS{*group-list*}[ENABLED]
{CHANGE } {ALL }[DISABLED]

This privileged command designates which groups are assigned to all locally defined services and which are enabled for the Terminal Server when it operates as a service node. Acceptable values are 0 for ENABLED (the default) and from 1 to 255 for DISABLED. ENABLED with the group-list format adds groups to the existing list; DISABLED removes them. Failure to indicate the keywords ENABLED or DISABLED with a value for group-list establishes a new list. ALL enables or disables all service groups.

group-list

One or more decimal codes in the 0 to 255 range, each representing a LAT group code. Multiple codes can be set by individual numbers separated by commas, by listing a range of ascending numbers, or a combination of both. For instance, the group list l, 5-10, 13 designates groups l, 5, 6, 7, 8, 9, 10, and 13.

SERVER SESSION LIMIT (privileged)

{SET }
{DEFINE } SERVER SESSION LIMIT {*limit* }
{CHANGE } {NONE }

This privileged option indicates the maximum number of active sessions that the Terminal Server will permit at a time. The range is from 0 to 64 with a default of 64. NONE specifies that the limit is equal to the maximum number of sessions permitted on the Terminal Server.

SERVER TCP RETRANSMIT (privileged)

{SET }
{DEFINE }SERVER TCP RETRANSMIT [LIMIT]{*count*}
{CHANGE }

This option specifies maximum retransmission tries for any TCP session that needs to retransmit an unacknowledged packet.

LIMIT

The keyword LIMIT can be omitted.

count

The value, in 2 minute intervals, of the retransmission timer. The default (and minimum) value is 3, which represents the basic limit of 4 minutes. The maximum value is 255, which represents a limit of 8 hours and 30 minutes (=510 minutes).

NOTE

This is a server-wide parameter that effects all telnet sessions (both ingoing and outgoing to/from the Terminal Server). The Terminal Server will use this value in a "retransmission phase" of a TCP session, and will continue to try retransmission until the limit is reached. Then, it will disconnect the telnet session.

SERVICE (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVICE *service-name* [*characteristic*[*characteristic*(*s*)]]
{CHANGE }

This privileged option designates local LAT services and characteristics.

service-name

This is a privileged command that indicates the name of the LAT service to be designated. The maximum number of LAT services defined at a given time is 64.

Summary of SERVICE Characteristics

All characteristics to the SERVICE command are listed below with their respective syntaxes, descriptions, defaults, and restrictions.

CONNECTIONS
IDENTIFICATION
PASSWORD
PORTS
QUEUE

SERVICE CONNECTIONS (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVICE service-name CONNECTIONS {ENABLED }
{CHANGE } {DISABLED}

This privileged command determines if the Terminal Server will be able to receive new connections to the specified LAT service. The default is ENABLED. This command does not influence active sessions.

SERVICE IDENTIFICATION (privileged, 4- and 8-port models only)

{SET }
{DEFINE }SERVICE *service-name* IDENTIFICATION “id-string”
{CHANGE }

This privileged option offers a brief description of the LAT service for the Terminal Server to relay in multicast messages to announce the service. The default is that no description is transmitted.
The id-string value is a string of 1 to 40 ASCII characters. Specifying the command with a quoted null string (" ") clears an identification string.

SERVICE PASSWORD (privileged, 4- and 8-port models only)

{SET }
{DEFINE } SERVICE *service-name* PASSWORD {“*password*”}
{CHANGE }

This is a privileged option that designates a LAT service terminal password that a user must provide for creating a session with the LAT service. The default is that no password is necessary.

When PASSWORD is the only characteristic in the command line, the password value may be omitted, and then the Terminal Server prompts for the password. If no value is entered for the password and the carriage return is pressed, the password will be erased.
Entering a quoted null string (" ") in the command line clears an existing password.

SERVICE PORTS (privileged, 4- and 8-port models only)

```
{SET      }
{DEFINE   } SERVICE service-name PORTS {port-list}[ENABLED]
{CHANGE   }                            {ALL      }[DISABLED]
```

This is a privileged option that indicates ports that offer the LAT service. Designating port-list with ENABLED adds ports from the existing port list; DISABLED removes them. Substituting a new list for an existing one can be accomplished by designating port-list without keywords ENABLED or DISABLED. The default is ALL DISABLED.

ALL

This command enables or disables use of the Telnet service by all ports.

ACCESS

This command affects the LAT remote access users.

port-list

Indicates the port/s affected by the defined characteristics. The default is your own port.

SERVICE QUEUE (privileged, 4- and 8-port models only)

```
{SET      }
{DEFINE   } SERVICE service-name QUEUE{ENABLED }
{CHANGE   }                           {DISABLED}
```

This is a privileged option that determines if requests are submitted into the Terminal Server connection queue by the Terminal Server for a local LAT service when the service is not available. The default is ENABLED. Existing queue entries remain untouched when queuing is disabled.

SESSION LAT (secure, 4- and 8-port models only)

```
                    {INTERACTIVE }
SET SESSION [LAT]   {PASSTHRU    }
                    {PASSALL     }
```

This is a secure option that designates characteristics for the most recent LAT session you entered in service mode. This command is available to all users.

INTERACTIVE

Enables special switch characters and messages at the Terminal Server port. This is the default.

PASSTHRU

Disables all switch characters and Terminal Server messages at the Terminal Server port during the current session. This option should be used to transfer ASCII files.

PASSALL

Disables all switch characters, Terminal Server messages, and XON/XOFF flow control at the Terminal Server port during the current session. This option should be used to transfer binary files.

Restriction:

- During the current session, all messages broadcast to your port are ignored when you SET SESSION to PASSALL or PASTHRU mode.

Example

```
Local> SET SESSION LAT PASSALL
```

This example disables all switch characters, flow-control characters, and Terminal Server messages at the port during the current LAT session.

SESSION TELNET (secure)

SET SESSION Telnet [CLIENT] {Characteristics}

This secure command changes the Telnet client characteristics for the current Telnet session. This option is available to all users.

SESSION TELNET AO REQUEST (secure)

```
                                {character (DEFAULT:CTRL/O)}
SET SESSION Telnet AO [REQUEST] {<DEL>                      }
                                {NONE                       }
```

The abort output (AO) request specifies a keyboard character which calls up the Telnet Abort Output function. This function aborts output en route to the user's terminal. The default character is Ctrl/O. If <DEL> is to be designated as the keyboard character, enter "<DEL>" (including the angle brackets.

SESSION TELNET AYT REQUEST (secure)

```
                                {character (DEFAULT:CTRL/O)}
SET SESSION Telnet AO [REQUEST] {<DEL>                      }
                                {NONE                       }
```

Are-You-There (AYT) request designates a keyboard character to call up the Telnet AYT function. The remote host then returns a message that it is still up and running. The default character is Ctrl/T. If <DEL> is to be designated as the keyboard character, enter "<DEL>" (including the angle brackets).

SESSION TELNET BINARY (secure)

```
                                  {DISABLED  }
SET SESSION TELNET BINARY {DUPLEX            }
                                  {RECEIVE   }
                                  {TRANSMIT}
```

On this Telnet connection, binary data is transmitted and received by use of binary transmission. Each direction can be enabled or disabled separately. DISABLED in both directions is the default.

SESSION TELNET BREAK (BRK) REQUEST (secure)

```
                                                {character}
SET SESSION TELNET {BRK     } [REQUEST]    {BREAK    }
                   {BREAK}                 {NONE     }
```

The BRK or Break request is a secure command that designates a keyboard character to send the Telnet Break command to the remote host. No default BRK character exists. To define <DEL> as the keyboard character, enter "<DEL>" (including the angle brackets).

SESSION TELNET CHARACTER SIZE (secure)

```
SET SESSION TELNET[TRANSMIT]{CHARACTER}[SIZE]{7}
                 [RECEIVE    ]                {8}
```

This secure command determines if the characters sent and received on this connection are 7-bit or 8-bit. 8-bit is the default in both directions.

SESSION TELNET ECHO (secure)

```
SET SESSION TELNET ECHO {LOCAL  }
                       {REMOTE       }
```

This secure Echo (ECHO) option indicates if this connection's input will be echoed locally by the Terminal Server or remotely by the remote host. The default is REMOTE.

Restriction:

- When ECHO is set to LOCAL, input can be suppressed locally by typing the defined TOGGLE ECHO character or setting the PROFILE characteristic to BINARY. See the TOGGLE ECHO command for more information.

SESSION TELNET IP REQUEST (secure)

```
                                          {character (Default: Ctrl/Y)}
SET SESSION TELNET IP [REQUEST]{<DEL>                 }
                               {NONE                  }
```

The interrupt Process (IP) request designates a keyboard character to call up the Telnet Interrupt Process function. Then the remote host interrupts or aborts the remote process. The default character is Ctrl/Y. To define (DEL) as the keyboard character, enter "<DEL>" (including the angle brackets).

SESSION TELNET NEWLINE FROM TERMINAL (secure)

```
                                                    {string          }
                                                    {<CR>            }
SET SESSION TELNET NEWLINE FROM TERMINAL{<CRLF>     }
                                                    {<LF>            }
                                                    {NONE }
```

This secure command designates a 1- or 2-character sequence which is interpreted as a new line when received by the Terminal Server from the terminal. The default is <CR>. If the keyboard character is to be <CR>, enter "<DEL>" (including the angle brackets)..

SESSION TELNET NEWLINE TO TERMINAL (secure)

```
                                                    {string          }
                                                    {<CR>            }
SET SESSION TELNET NEWLINE TO TERMINAL{<CRLF>       }
                                                    {<LF>            }
                                                    {NONE }
```

This is a secure command that specifies a 1- or 2-character sequence which is sent from the Terminal Server to the user's terminal upon receipt of a new line character sequence from the remote host. The default is <CRLF>. Enter "<CRLF>" (including the angle brackets)..

SESSION TELNET PROFILE (secure)

SET SESSION TELNET PROFILE {CHARACTER}
{BINARY }

This is a secure option that selects a set of characteristics for a Telnet connection. This command can prevent the user from having to set all of the individual characteristics in just the right way to produce a desired behavior on a Telnet connection.

CHARACTER and BINARY are the two predefined sets of characteristics. Character mode is used to immediately forward user data to the remote host character by character. The data is echoed by the remote host. Binary mode is used to transmit binary data over the Telnet connection. CHARACTER is the default.

SESSION TELNET QUOTE (secure)

SET SESSION TELNET QUOTE {character}
{NONE }

This is a secure option that designates a keyboard character that causes the character entered next to be interpreted as ordinary user data. To enter keys that are mapped to Telnet functions (e.g., Ctrl/T to AYT, Ctrl/O to AO, etc.) as ordinary data, use a QUOTE character first. No default QUOTE character exists.

SESSION TELNET SWITCH CHARACTER (secure)

SET SESSION TELNET SWITCH CHARACTER {ENABLED }
{DISABLED}

This is a secure option that indicates the CS Terminal Server's interpretation of switch characters for Telnet sessions on the port. The Terminal Server relates to any switch characters defined on the port when ENABLED. The Terminal Server ignores all switch characters on the port when DISABLED. The default is ENABLED.

SESSION TELNET SYNCH REQUEST (secure)

SET SESSION TELNET SYNCH REQUEST {*character* {Default: CTRL/X)}
{<DEL> }
{NONE }

This is a secure option that specifies a keyboard character that invokes the Telnet Synch function. This function discontinues all input en route to the remote process (i.e., it clears the path to the remote process). The default is Ctrl/X. If <DEL> is to be designated as the keyboard character, enter "<DEL>" (including the angle brackets).

SESSION TELNET TOGGLE ECHO (secure)

SET SESSION TELNET TOGGLE ECHO {*character* (Default: Ctrl/E)}
{NONE }

This is a secure option that designates a keyboard character to enable or suppress echoing on a connection. For example, the user might toggle echo OFF while entering a password. The default character is Ctrl/E.

Restriction:

- The TOGGLE ECHO character functions only when the Terminal Server locally echoes input.

SNMP STATE (privileged)

{SET } {ENABLED }
{DEFINE }SNMP STATE {DISABLED}
{CHANGE }

This is a command for privileged users that configures the Simple Network Management Protocol (SNMP) agent for access from SNMP NETWORK MANAGEMENT STATIONS (NMSes). Community names are used for access verification from NMSes.

ENABLED

The Terminal Server can answer GET, GET NEXT, and SET requests through SNMP in addition to generating authentication traps to these hosts when ENABLED. This is the default.

DISABLED

If SNMP requests are disregarded, traps are not created by the Terminal Server when DISABLED.

SNMP COMMUNITY ADDRESS (privileged)

```
                                    [ADDRESS{ANY    }]
                                            {ip-address}
                                    [GET     {ENABLED  }]
{SET}                                        {DISABLED }
{DEFINE}SNMP COMMUNITY community-name [GETNEXT {ENABLED}]
{CHANGE}                                     {DISABLED}
                                    [SET     {ENABLED  }]
                                             {DISABLED }
                                    [TRAP  {ENABLED    }]
                                             {DISABLED }
```

This privileged specifies the community limitation when accessing the Terminal Server SNMP agent from SNMP NETWORK MANAGEMENT STATIONS (NMSes). Community names are used for access verification from NMSes.

Used this command to add a community name or to designate a community's characteristics in the Terminal Server community database. A default community named public is preset in the community database. The default characteristics of the community database are ADDRESS ANY, TRAP DISABLED, GET ENABLED, GET NEXT ENABLED, and SET DISABLED.

community-name

This is an ASCII string enclosed in double quotes with a maximum of 32 printable characters per community-name. When the number of characters for any one name surpasses the 32-character limit, the name is truncated to 32 characters. Each community-name will be associated with either ADDRESS ANY or with one particular ip-address. ANY is the default.

ADDRESS

ip-address

The internet address of the remote host in the form nnn.nnn.nnn.nnn. When valid, the internet's community name and address are checked prior to obtaining access to the CS Terminal Server's databases. When an invalid internet address is entered, an error message appears. Assigning an ip-address to a community name increases the number of overhead characters (requires from 2 characters to 6 characters to store the information). For more details, refer to the community-name.

ANY

ANY should be designated for instructing the Terminal Server to accept SNMP messages from any ip-address associated with that community. ANY can also be designated to detach the community from a specific ip-address which clears a previously defined ip-address.

NOTE

Before specifying ADDRESS as ANY , disable TRAP.

GET

Permits members of the community to read values from the Terminal Server management information base (MIB) when ENABLED. The default is ENABLED.

GET NEXT

Permits members of the community to sequentially read values from the Terminal Server supported MIBs when ENABLED. The default is ENABLED.

SET

Permits exclusion of the word sequentially from the Terminal Server supported MIBs by members of the community. The default is DISABLED.

TRAP

Specifies the internet address as a location that receives traps when ENABLED. The default is DISABLED.

When SNMP Traps are enabled, traps will be sent in the following events:

- Cold Start—Sent when the Terminal Server is initialized.
- Line Up—Sent when a PORT connection is established.
- Line Down—Sent when a PORT is disconnected.
- Authentication—Sent when an unauthorized Internet host tries to access the Terminal Server or when an Internet host attempts an unauthorized SNMP GET request.

Restrictions:

- The Terminal Server must have an internet address assigned to enable the SNMP agent.
- You may use up to 32 characters for a community name. However, it is recommended to use fewer characters per name so as to allow more community names.

Examples

```
Local> DEFINE SNMP COMMUNITY "SHELLY" ADDRESS
192.114.34.60
```

This example defines a SNMP community name "SHELLY," which can be accessed exclusively by the internet host with a address of 192.114.34.60.

```
Local> SET SNMP COMMUNITY "SHELLY" GET ENABLED
```

This example enables internet hosts with access to the community "SHELLY" to use SNMP GET messages to receive value information from the Terminal Server supported MIBs.

Telnet LISTENER (privileged)

{SET } {CONNECTIONS {ENABLED} }
{DEFINE}Telnet LISTENER *tcp-port*{IDENTIFICATION "*id-string*"}
{CHANGE } {ALL }
{PORTS {ACCESS}[ENABLED] }
{*port-list*}

This is a command for privileged users that designates a Telnet listener or Telnet remote access port on the Terminal Server. The listener may be connected to physical Terminal Server ports or with the remote access virtual port. Connections that defined the TCP port as a destination are available for the Terminal Server.

tcp-port

Specifies the TCP port number that remote users specify in their connect request. The default TCP port number is 2000 + (physical port number).

CONNECTIONS

Determines if the listener is ENABLED or DISABLED for connection reception. The default is DISABLED.

IDENTIFICATION *id-string*

A descriptive text string that is associated with the listener for SHOW displays. The default is no *id-string*.

PORTS

Specifies the Terminal Server physical ports or the remote console virtual port with which a Telnet listener will be associated. The port(s) are dissociated with the listener when DISABLED. The default is DISABLED.

NOTE

The above defaults apply to TCP-ports 2001 and above only. TCP-port 23 has the following defaults:

Connections:	Enabled
Identification:	Remote Access
Ports:	Access

ALL

This command associates the listener with all the Terminal Server ports.

ACCESS

This command designates the Telnet remote access port. Users accessing the Terminal Server through this port can subsequently access Telnet nodes or perform management tasks.

NOTE

The number of concurrent sessions to Telnet remote access ports is limited by the Terminal Server SESSION LIMIT parameter and the number of currently existing sessions.

port-list

This option sets the Terminal Server port number(s). See Chapter 6 for more information on specifying *port-list*.

Restrictions:

- You cannot use SET or CHANGE PORTS until CONNECTIONS is DISABLED.

Telnet listener ports cannot be DISABLED during active sessions. You can only ENABLE connections to a Telnet listener if the listener is associated with an Terminal Server ports, or if the internet address has been specified on the Terminal Server.

ACCESS and physical ports cannot be designated simultaneously for a Telnet listener.

Telnet listeners that have physical port(s) destination, limit the number of concurrent sessions to be equal or less to the number of physical port(s) specifying the same TCP port.

Examples

```
Local> SET Telnet LISTENER 23 ACCESS ENABLED

Local> SET Telnet LISTENER 23 CONNECTIONS ENABLED
```

These commands enable a Telnet listener on tcp port 23 designating it as a remote access port.

```
LOCAL> DEFINE Telnet LISTENER 2001 PORTS 1,2

LOCAL> DEFINE Telnet LISTENER 2001 CONNECTIONS ENABLED
```

These commands enable Telnet listener 2001 on Terminal Server ports 1 and 2. The Terminal Server permanent database is effected by these commands.

8. SHOW/LIST Commands

This chapter describes the SHOW and LIST commands.

The SHOW commands display current status or information about various options from the Terminal Server operational database.

The LIST commands display information about various options from the permanent database.

ACCOUNTING (privileged)

{SHOW}ACCOUNTING
{LIST }

This option displays information about the accounting setting from the internal database. The following information is displayed:

```
Accounting Characteristics:

Status:         Enabled
Primary Server: nnn.nnn.nnn.nnn  Alternate Server: nnn.nnn.nnn.nnn
Timeout:        nn               Retries:                       nn
```

Note that the secret is not shown. The only way to verify its value is to set it again, using the DEFINE ACCOUNTING SECRET command.

AUTHENTICATION (privileged)

{SHOW}AUTHENTICATION
{LIST }

This option displays information about the authentication setting from the Terminal Server's internal database. Presented are the addresses of the primary and alternate authentication servers, the timeout and the retries values.

```
Authentication Characteristics:

Status:         Enabled
Primary Server: nnn.nnn.nnn.nnn  Alternate Server: nnn.nnn.nnn.nnn
Timeout:        nn               Retries:                       nn
```

Note that the secret is not shown. The only way to verify its value is to set it again, using the DEFINE AUTHENTICATION SECRET command.

BOOTP (secure)

{SHOW}BOOTP
{LIST }

This option displays information in the Terminal Server's BOOTP database. This command is available to all users.

INTERNET (secure)

{SHOW }INTERNET [CHARACTERISTICS]
{LIST } [COUNTERS]

This option displays information in the Terminal Server internet database. This command is available to all users.

CHARACTERISTICS

This option displays the current settings of the user-definable parameters of the internet protocol, such as the internet address. This is the default display.

COUNTERS

Displays the existing values of the different counters of the internet protocol.

Restriction:

- COUNTERS does not work with the LIST command.

Examples

```
Local> SHOW INTERNET COUNTERS
```

Existing values of the different counters of the internet protocol in the operational database are shown with this command.

```
Local> SHOW INTERNET CHARACTERISTICS
```

The current settings of the user-definable parameters of the internet protocol in the operational database are shown with this command.

INTERNET ARP ENTRY (secure)

{SHOW }INTERNET ARP ENTRY
{LIST }

This command displays the ARP ENTRIES of the Terminal Server ARP database. This command is available to all users.

Example

```
Local> SHOW INTERNET ARP ENTRY
```

All of the operational database's INTERNET ARP ENTRIES are displayed by this command.

INTERNET GATEWAY (secure)

{SHOW }INTERNET GATEWAY
{LIST }

This command displays the internet gateways known to the Terminal Server in addition to the networks and hosts that are available to the user. This command is available to all users.

Restriction:

- INTERNET GATEWAY cannot be used when PORT LIMITED VIEW CHARACTERISTICS is ENABLED.

Example

```
Local> SHOW INTERNET GATEWAY
```

This command specifies the information available to the user, such as all current gateways in the operational database, their corresponding networks, associated subnet masks, and hosts.

INTERNET HOST (secure)

{SHOW }INTERNET HOST [ALL] [CACHED] [STATUS]

{LIST } [LOCAL] [SUMMARY]
[*domain-name*]

This command displays host entry information derived from the Terminal Server internet domain name system (DNS). This command is available to all users.

ALL

Indicates to display all hosts in the DNS cache. This is the default.

CACHED

Indicates to display only hosts that the Terminal Server has in the DNS cache.

LOCAL

Designates that only those hosts defined locally at the Terminal Server will be shown.

domain-name

Specifies the domain name of a host.

STATUS

Specifies the time-to-live (TTL) numbers for each host shown.

SUMMARY

Displays a one-line summary of information about the host. This is the default.

Restrictions

- CACHED is not valid with the LIST command.

Examples

```
Local> SHOW INTERNET HOST LOCAL
```

This command displays all current hosts defined locally in the Terminal Server operational database.

```
Local> LIST INTERNET HOST ALL
```

This command displays all hosts defined in the Terminal Server permanent database.

INTERNET NAME RESOLUTION (secure)

{SHOW}INTERNET NAME RESOLUTION[CHARACTERISTICS]
{LIST }

This command (available to all users) displays information in the Terminal Server domain name system (DNS) database.

When this command is entered, the Terminal Server displays the name servers (both locally configured and learned cached) that serve the current default domain of the Terminal Server. If you change the value of the default domain, the SHOW INTERNET NAME RESOLUTION command will display different name servers.

CHARACTERISTICS

Displays the current settings of the user-definable parameters associated with the Terminal Server DNS module, including domain name, query time limit, resolution time-out host limit, and name servers. This is the default.

Restriction:

- Secure users cannot execute the LIST command.

Example

```
Local> LIST INTERNET NAME RESOLUTION
```

Existing values of the user-definable parameters in the permanent database of the Terminal Server DNS module are shown using this command.

MEMORY (secure)

SHOW MEMORY

This command displays the current memory state. The command shows all dynamic buffers in the Terminal Server and their status. The Terminal Server has several pools of buffers, each has a different size.

The display consists of several lines, one for each buffer pool. Each line contains 4 numbers:

- The first number, *Size*, shows the pool's buffer size in bytes.
- The second number, *Use*, shows how many buffers of that size are used at the moment.
- The third number, *Max*, shows what was the highest consumption of buffers from the time the Terminal Server was reset (*high water mark*).
- The fourth number, *Fail*, shows how many times a buffer allocation request was failed due to shortage in buffers in this pool. If this happens, the Terminal Server will allocate a buffer from the next pool.

The remaining lines show some statistics about special events related to the buffer management system.

NODES (secure, 4- and 8-Port models)

SHOW NODES [ALL][COUNTERS]

[*node—name*][STATUS]
[SUMMARY]

This command provides details about LAT service nodes known to the Terminal Server. This command is available to all users.

The Terminal Server shows only those nodes that have at least one group currently selected on the port for nonprivileged users (as defined in the GROUPS port characteristic). Privileged users, however, can specify ALL to display all of the nodes in the Terminal Server database or a specified node, whether or not the node(s) are included in the current group selection of the port. Nodes that currently accept connections from Terminal Server ports have Reachable, whereas those that do not have Unreachable status.

ALL

This command shows information for all authorized service nodes with Reachable, Unknown, or Unreachable status currently selected on the port. The default display provides only currently selected nodes that are Reachable or Unknown unless ALL is indicated.

node-name

Specifies a service node for which information is displayed.

COUNTERS

Shows existing counter values for the node(s) indicated.

STATUS

This command provides full information about the specified node(s), such as name, address, identification string, enabled group codes, and services. This is the default display when a node name is specified.

SUMMARY

This command provides a one-line information summary display for the specified node(s), including node name, status, and identification string. This is the default display when no node name has been indicated.

Restriction:

- When the LIMITED VIEW port characteristic is ENABLED, the SHOW NODES command is not available to ports.

Examples

```
Local> SHOW NODES ALL
```

This command produces a one-line summary of information from the operational database about each service node with Reachable, Unreachable, or Unknown status.

PORTS (secure)

```
                                                          [CHARACTERISTICS    ]
{SHOW }PORTS[ACCESS{type}] [COUNTERS          ]
{LIST       }      [ALL       ]      [STATUS              ]
                   [port-list ]      [SUMMARY             ]
```

This command displays information about Terminal Server ports, including the characteristics designated with the SET/DEFINE/CHANGE PORT commands. This command is available to all users.

ACCESS (*type*)

This command indicates that information is shown exclusively for ports with ACCESS set to the type chosen, such as LOCAL, REMOTE, DYNAMIC, or NONE. ACCESS is a port characteristic defined with the SET/DEFINE/CHANGE PORT command.

ALL

Indicates that information for all ports is shown.

port-list

Specifies one or more ports for displaying information. The default is the port currently in use.

CHARACTERISTICS

This command lists characteristics that are defined for the specified port(s). This is the default when no port, one port, or a port-list is indicated.

COUNTERS

Displays current counter values for the specified port(s).

STATUS

Displays current port status for the specified port(s).

SUMMARY

This command shows information for the specified port(s), such as port number, accessibility, status, and local services in a one-line summary. This is the default when ALL or ACCESS is specified.

Restriction:

- Port designations (port-list, ALL, and ACCESS) cannot be accessed by users on secure ports in these commands.

Examples

```
Local> SHOW PORT ACCESS REMOTE SUMMARY
```

This command shows a one-line summary of information for those Terminal Server ports whose ACCESS characteristics are designated as REMOTE.

```
Local> SHOW PORTS ALL
```

Displays the operational database's summary for all the Terminal Server ports.

PORT PPP LCP/IPCP (secure)

```
{SHOW }                                    [CHARACTERISTICS    ]
{MONITOR     }PORT n [PPP] {LCP    }       [COUNTERS           ]
{LIST        }             {IPCP   }       [STATUS             ]
```

These secure commands display information associated with PPP LCP, IPCP, or ATCP ports from the access server database.

CHARACTERISTICS

This command displays current values for port PPP LCP, IPCP, or ATCP characteristics. Characteristics for the specified port, which may include name, identification string, restart timer time, maximum transmissions failure, charter mask, as well as additional characteristics, will be displayed. The information includes the latest values configured by the SET PORT n PPP LCP/IPCP command. To see the values actually being used by the link, use the PPP LCP/IPCP STATUS command.

COUNTERS

The COUNTERS command displays information about all the counters relevant to the LCP or IPCP protocol operation. This command is normally used as a diagnostic aid. You can zero each of these counters using the CONNECT and DISCONNECT commands.

STATUS

The STATUS command display information about the state of the LCP or IPCP implementation in the access server. Because of the nature of PPP negotiations, this can be different than the configured characteristics shown with the SHOW PORT n PPP LCP or IPCP CHARACTERISTICS display. This command displays information in the general link status and the status of each of the LCP or IPCP options.

Restrictions:

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.
- Secure users can only specify their port.

PORT SESSION (secure)

SHOW PORT [ALL]SESSION[ALL][CHARACTERISTICS]
[*port-list*] [*session-id*][STATUS]

This command displays information for the session(s) on the Terminal Server from the operational database. This command can display one session at a time (rather than all sessions as exists in the SHOW SESSIONS command). This command is available to all users.

PORT ALL

Displays sessions for all ports on the Terminal Server.

PORT *port-list*

Displays sessions for the specified port(s). The default displays sessions for the existing port.

SESSION ALL

Displays all sessions for the specified port.

SESSION *session-id*

Identifies the session number of the specified port to be displayed. The current session is the default.

CHARACTERISTICS

Displays the current settings for session characteristics. This is the default.

STATUS

Displays the status of the current session.

Restriction:

- Secure users can display only their own port's sessions. They cannot specify SESSION ALL.

The command displays the status of all the current sessions on port 1 in the following example.

Example

```
Local> SHOW PORT 1 SESSION ALL STATUS

Port 1, session 1, Protocol Ping
(no status information available for PING sessions)

Port 1, session 2, Protocol TELNET

Do-Binary                       Disabled

Will-Binary                     Disabled

Do-Echo                         Disabled

Will-Echo                       Enabled

Do-SGA                          Disabled

Will-SGA                        Enabled

Do-Status                       Enabled

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     UNKNOWN

Port 1, session 3, Protocol Telnet

(no status information available for Telnet sessions)
```

PORT SLIP (privileged)

```
{SHOW    }
{MONITOR }PORT[ALL        ]SLIP [CHARACTERISTICS ]
{LIST    }    [port-list  ]     [COUNTERS        ]
```

These privileged commands display information associated with SLIP ports from the access server database. The characteristics that you assign with the SET/DEFINE/CHANGE PORT SLIP command are included.

ALL

Specifies that information for all ports is displayed.

port-list

Specifies one or more ports for which information is displayed (default: the port you are using).

CHARACTERISTICS

Display current values for port SLIP characteristics. This is the default.

COUNTERS

Displays current counter values for the specified port(s).

Restrictions

- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.
- Secure users can specify only their own port.

Example

```
Local>  SHOW PORTS ALL SLIP
```

This command displays all characteristics of SLIP-specific ports in the operational database.

PORT Telnet (secure)

{SHOW }PORT[ALL] Telnet[CLIENT][CHARACTERISTICS]
{LIST } [*port-list*][SERVER]

This command displays information from the Terminal Server database associated with Telnet ports. This command is available to all users.

ALL

Displays the Telnet database for all Terminal Server ports.

port-list

Indicates the Terminal Server port number(s) for which the Telnet database is to be displayed.

Telnet

Shows the Telnet characteristics of the Terminal Server port database.

CLIENT

Displays Telnet CLIENT characteristics. This is the default.

SERVER

Shows Telnet server characteristics.

CHARACTERISTICS

Displays the current port parameters associated with Telnet.

Restriction:

- The port-list characteristic is available only on privileged ports.

Example

```
Local> SHOW PORT ALL Telnet
```

This command shows the Telnet Client characteristics for all Terminal Server Telnet ports.

QUEUE (nonprivileged, 4- and 8-Port models)

```
                [ALL                          ]
SHOW QUEUE[NODE node-name                     ]
                [PORT port-name               ]
                [SERVICE service-name    ]
```

This nonprivileged command displays information about entries in the LAT Terminal Server queue.

ALL

Displays information for all LAT queue entries on the Terminal Server. The default display selection is ALL

NODE *node-name*

Displays information for all LAT queue entries requested by the specified LAT node.

PORT *port-number*

Shows information for all LAT queue entries that are served by the specified port(s).

SERVICE *service-name*

Displays information for all LAT queue service-name entries for the specified service.

Examples

```
Local> SHOW QUEUE NODE SUPPORT
```

This command displays information for all queue entries from node SUPPORT.

SERVER (nonprivileged)

```
                          [CHARACTERISTICS    ]
{SHOW} SERVER             [COUNTERS           ]
{LIST  }          [STATUS                     ]
                          [SUMMARY            ]
```

This is a nonprivileged command that provides service information about the Terminal Server.

CHARACTERISTICS

This command provides definable characteristics for the Terminal Server. The characteristics include a list of LAT groups offered by the Terminal Server (as specified by the SET/DEFINE/CHANGE server SERVICE GROUPS command). This is the default display type.

COUNTERS

Displays current Ethernet data link protocol and LAT protocol counter values for the Terminal Server.

STATUS

Provides status information for the Terminal Server.

SUMMARY

Shows a summary of information for the Terminal Server, such as name, address, identification string, as well as a summary of all groups currently selected by all ports on the Terminal Server.

Restriction:

- COUNTERS and STATUS are not valid with the LIST command.

Example

```
Local> SHOW SERVER COUNTERS
```

This command displays the Terminal Server counters from the operational database.

SERVICES (secure, 4- and 8-Port models)

```
                              [ALL     ]      [CHARACTERISTICS    ]
{SHOW} SERVICES               [LOCAL]         [STATUS             ]
{LIST  }          [service-name    ][SUMMARY                    ]
```

This command provides information about LAT services available for connection. This command is available to all users.

ALL

Displays information for all LAT services in the database that correspond to your current group codes, regardless of the service's availability. Privileged users refer to all LAT services in the database. ALL is the default selection displayed on SHOW commands. If ALL is omitted in the command, the Terminal Server displays only the available LAT services.

LOCAL

Displays information for all LAT services (whether available or unavailable) offered by the local Terminal Server that match your current group codes. LOCAL is functional only in SHOW commands, because LIST commands display only local node LAT services.

service-name

Displays information for the specified service(s), provided they are included in your current group codes. If you do not specify a service name or LOCAL, the Terminal Server displays all LAT services that match your current group codes.

CHARACTERISTICS

Displays definable characteristics for the specified local services, including name, identification string, and ports. For remote LAT services, only the name and identification string are displayed.

STATUS

Displays information about the specified service(s), including node names and their status, rating, and identification string. This is the default when you specify a service name.

SUMMARY

Displays a one-line summary of information for the specified services, including name, status, and identification. This is the default when you do not specify a service name.

Restrictions:

- The SHOW SERVICES command is not available if the LIMITED VIEW port characteristic is enabled.
- ALL, STATUS, and SUMMARY are not valid for the LIST SERVICES command.

Examples

```
Local> SHOW SERVICES LOCAL
```

This command displays summary for all local services from the operational database.

SESSIONS (secure)

SHOW SESSIONS [ALL]
[*port n*]

This command (available to all users) displays session information from the operational database for one or all ports on the Terminal Server. Unlike the SHOW PORT SESSIONS command that displays session characteristics for one session at a time, this command displays all sessions.

Sessions utilizing the Telnet to LAT or LAT to Telnet gateway feature are virtual sessions and are indicated as V##—for example, V05.

ALL

Displays sessions for all ports on the Terminal Server.

port n

Displays sessions for the specified port. If no port is specified, the command displays sessions for your current port.

Restriction:

- Secure users cannot specify PORT and ALL.

SNMP

{SHOW} SNMP [CHARACTERISTICS]
{LIST } [COUNTERS]
[STATUS]

These commands display SNMP-related information, such as SNMP characteristics, error and access counters, and operational status.

CHARACTERISTICS

Displays current values for SNMP community names and internet addresses. Also displays "enabled" or "disabled" for SNMP characteristics GET, GETNEXT, SET, and TRAP.

COUNTERS

Displays current SNMP error and access counters.

STATUS

Displays whether SNMP is running or not running.

Restrictions:

- SNMP CHARACTERISTICS is a privileged command.
- The LIST command is invalid for SNMP COUNTERS or SNMP STATUS.

Examples

```
Local> SHOW SNMP STATUS
```

This command displays whether the SNMP protocol is running or not running.

```
Local> LIST SNMP CHARACTERISTICS
```

This command displays SNMP community names, internet addresses, and whether SNMP characteristics GET, GETNEXT, SET, and TRAP are enabled or disabled.

SYSTEM CHARACTERISTICS (secure)

{SHOW} SYSTEM [CHARACTERISTICS]
{LIST }

This command (available to all users) displays Terminal Server characteristics such as the system location and the system contact person.

CHARACTERISTICS

Displays (in ASCII format) system information such as the name of the system contact person (system manager) and the system location.

Example

```
Local> SHOW SYSTEM
```

The above command displays system-group characteristics as recorded in the Terminal Server operational database.

Telnet LISTENER (secure)

{SHOW} Telnet LISTENER {ALL }[CHARACTERISTICS]
{LIST }   {*tcp-port* }

This command (available to all users) displays information about Telnet listeners on the Terminal Server.

ALL

Specifies that all Telnet listeners are to be displayed.

tcp-port

Specifies that only information about the Telnet listener associated with the specified TCP port is to be displayed.

CHARACTERISTICS

Specifies that the characteristics of the Telnet listener(s) are to be displayed.

Restriction:

- Telnet listener is not available to ports if the LIMITED VIEW port characteristic is enabled.

Example

```
Local> SHOW Telnet LISTENER 2001
```

This command shows the characteristics of the Telnet listener on TCP port 2001.

USERS (nonprivileged)

SHOW USERS

This nonprivileged command displays information about port users.

9. CLEAR/PURGE Commands

This chapter describes the CLEAR and PURGE commands. Both of these commands are used to delete whatever is specified by the keyword from the Terminal Servers databases.

To remove information from the operational database use the CLEAR command.

To remove information from the permanent database use the PURGE command.

INTERNET GATEWAY (privileged)

```
{CLEAR}INTERNET GATEWAY...
{PURGE}
   {ALL
   {              [HOST [ADDRESS] ip-address                          }
....{ip-address                                                       }
                  [NETWORK{ANY                                        }
                  [          {net-addr[[SUBNET]MASK submask]}]        }
```

Erases existing gateway entries from the Terminal Server database for privileged users.

ALL

Specifies all existing gateway entries in the Terminal Server database.

ip-address

Indicates the local network internet address of the gateway to be erased. You may also use the NETWORK *net-address* and HOST *ip-address* options; otherwise, the default is NETWORK ANY. The specified internet address must be expressed as *n.n.n.n* where n is a decimal number ranging from 0 to 255.

HOST [ADDRESS]

Specifies the gateway entry for traffic from the Terminal Server to the specified host.

net-addr

Specifies the gateway entry for traffic from the Terminal Server to the specified network. This is beneficial when only one leg of a gateway is to be removed.

ANY

Specifies the gateway entry for traffic from the Terminal Server to any network. If you do not specify an option with an ip-address, ANY is the default.

[SUBNET] MASK submask

When combined with NETWORK, this command deletes the entry mapping traffic from the exact subnet to this gateway. The default is the internet subnet mask in the Terminal Server's operational database when the mask option is omitted.

Restrictions:

- Gateway entries with active connections cannot be removed by the CLEAR command. However, the PURGE command does remove gateway entries with active connections since it affects only the permanent database.
- The HOST and NETWORK characteristics are not valid with the ALL characteristic.

Examples

```
Local> CLEAR INTERNET GATEWAY ALL
```

Erases all internet gateway entries from the Terminal Server's operational database.

```
Local> PURGE INTERNET GATEWAY 195.1.1.60 NETWORK
195.1.1.61
```

This command deletes the internet gateway with the above internet address and network address from the Terminal Server's permanent database.

INTERNET HOST (Privileged)

	{ALL	}
{CLEAR} INTERNET HOST	{*domain-name*	}
{PURGE}	{CACHED	}
	{LOCAL	}

This privileged command deletes existing internet hosts from the Terminal Server internet domain name system (DNS) database.

ALL

Indicates that all hosts in the DNS cache will be deleted.

domain-name

Specifies the *domain-name* of a host or a domain to be deleted.

CACHED

Only hosts that the Terminal Server has in its DNS cache will be erased by this command.

LOCAL

Deletes only hosts that have been defined locally at the Terminal Server.

Restriction:

- The CACHED characteristic is not valid with the PURGE command.

Examples

```
Local> CLEAR INTERNET HOST CACHED
```

This command acts on the Terminal Server's operational database to delete all internet hosts from the Terminal Server's DNS cache.

```
Local> PURGE INTERNET HOST ALL
```

This command, acting on the Terminal Server permanent database, deletes all internet hosts from the domain name server.

Local> CLEAR INTERNET HOST FALCON

This command acts on the Terminal Server operational database. It deletes internet host FALCON from the domain name server.

INTERNET NAMEserver (privileged)

{CLEAR}INTERNET NAMEserver{ALL }
{PURGE} {[NAME] *name*[ADDRESS ip-address]}

This privileged command deletes existing internet domain name servers from the Terminal Server domain name system (DNS) database, no longer using them for name resolution.

ALL

Indicates that all domain name servers will be deleted.

NAME *name*

Specifies the name of the domain name server to be deleted.

ADDRESS *ip-address*

Specifies the name of the domain name server to be deleted. This option is useful when there are two or more defined name servers with the same name. The address must be a valid internet address of the form n.n.n.n. where n is a decimal number in the ranging from 0 to 255.

Examples

```
Local > PURGE INTERNET NAMEserver ALL
```

This command deletes all name server entries from the Terminal Server DNS permanent database.

```
Local> CLEAR INTERNET NAMEserver NAME INTEL.COM
```

The name server INTEL.COM is deleted from the Terminal Server DNS operational database by this command.

PORT PPP HOST ADDRESS (nonprivileged)

{CLEAR} PORT [ALL] PPP HOST {SLIP} [ADDRESS]
{PURGE} [*port-list*]

This nonprivileged command deletes an internet address of the port's attached device.

ALL

Specifies all access server ports.

port-list

Specifies one or more ports. Refer to **Section 7.6** for more information on specifying port-list.

NOTE

Only one internet address is associated with each port. PPP and SLIP use the same address. In this command, keywords PPP and SLIP are interchangeable.

Restriction:

- You cannot use the CLEAR command with a PPP address on a port with an existing PPP or SLIP session.

Example

```
Local>  PURGE PORT 5 PPP HOST
```

In this command, the address of the PPP host at port 5 is deleted from the access server's permanent database.

SERVICES (privileged, 4- and 8-Port models only)

{CLEAR} SERVICE [*service-name*]
{PURGE} [LOCAL]

This privileged command purges an entry for one or all local LAT services from the Terminal Server database.

service-name

Indicates the name of a LAT service to be erased. The Terminal Server deletes the locally defined LAT services if a service is not specified

LOCAL

Specifies that all locally defined LAT services will be deleted. LOCAL is the default.

Entering the CLEAR SERVICES command under the following circumstances will cause an error message:

- Sessions are established with the service.
- The Terminal Server queue contains CONNECT requests for the specified service.
- The requested service does not exist.

Example

```
Local> PURGE SERVICE ACCT
```

This command deletes all information for service ACCT from the permanent database so that it is no longer a locally defined service.

SNMP COMMUNITY (privileged)

{CLEAR}SNMP COMMUNITY{ALL }
{PURGE} {"*community-name*" }

This privileged command clears an SNMP community name from the Terminal Server database.

ALL

This command indicates the SNMP communities currently defined in the community database, except for the default community PUBLIC.

community-name

Specifies a community name or a community's characteristics in the Terminal Server community database. The *community name* is an ASCII string enclosed in double quotes. The maximum length is 32 characters. The *community name* is truncated to 32 characters if more than 32 characters are entered. See the SET/DEFINE/CHANGE SNMP COMMUNITY command (**Section 10.119**) for further reference.

Example

Local> PURGE SNMP COMMUNITY “Network Management”

This command clears the SNMP community name “Network Management” from the permanent database.

Telnet LISTENER (privileged)

{CLEAR}Telnet LISTENER{*tcp-port* }
{PURGE} {ALL }

This privileged command resets a predefined Telnet listener in the Terminal Server database back to the factory-set defaults.

An error message appears if the CLEAR Telnet LISTENER command is entered while there are sessions active from the specified listener. Before executing the CLEAR command, log out the ports on which these sessions are fixed.

tcp-port

Specifies the TCP port number of the listener to be reset. The port is reset to Connections: DISABLED and Ports: NONE when the listener specified is in the range from 2001 to 2016. The port is reset to Connections: ENABLED and Ports: ACCESS when the listener specified is 23 (used for Telnet remote access).

ALL

Indicates all Telnet listeners currently defined in the designated database.

Restriction:

- The CLEAR Telnet LISTENER command cannot be used with an active session.

Example

```
Local> CLEAR Telnet LISTENER 2010
```

The Telnet listener mapped to TCP port 2010 is reset to factory-set defaults (Connections: DISABLED and Ports: NONE) by this command.

Appendix A: Upgrading to New Software

The following steps will enable you to upgrade the software version on the Terminal Server to the latest release, when necessary. It does not apply to the Single-Port Terminal Server, which requires factory EPROM changes.

The following hardware is required in order to update the software version successfully:

- IBM PC compatible with a 3.5" 1.44 MB disk drive
- At least 2.5 MB of hard-disk space free
- A terminal program supporting XON/XOFF emulation (such as PCPLUS™, PROCOMM™, or Windows® Terminal)

You can get the new release via a 3.5" diskette containing a single file in a self-extracting compressed format. The file name is saved in the form: ver_id.exe where ver_id is the name of the new version release, for example, CS2_3_0.exe for version 2.3.

Follow these steps to upgrade to the new version:

1. Copy this file to a suitable working directory on the hard drive.
2. Make sure that you are currently in the working directory and type the name of the file and press <Enter>. This will expand the compressed file and creates a new file name of the form: ver_id.hex
3. Stop all users from working on the Terminal Server.

4. Run the terminal program of your choice and set the emulation parameters to reflect the following:

a) In Procomm (v2.x or above):

Select protocol options
Select ASCII protocol options and set:

Baud rate:	9600-115200
Echo locally:	NO
Line pacing:	0
CR translation (upload):	NONE
LF translation (upload):	NONE
Strip 8th bit:	NO

Select terminal options and set:

Duplex:	FULL
Soft flow ctl (XON/XOFF):	ON
CR translation:	CR

b) In Microsoft Windows Terminal:

Select the Setting Communication option and set:

Baud rate:	9600-115200
Data bits:	8
Stop bits:	1
Parity:	NONE
Flow control:	XON/XOFF
Connector:	(your choice)
Parity check:	NO
Carrier detect:	NO

5. Physically connect the serial port of the PC to port 1 on the 4- and 8-port Terminal Server. Using the terminal program set above, log into the port by pressing the <Enter> key twice. (Best performance will be achieved at 38400 baud.)

6. Enter the following commands (shown in **bold** characters):

   Local> set priv
   Password> system (or your specific *privileged* password if it has been changed)

   Radlinx TS booting in Console Mode
   Loader Ver 1.0

   loader> LOAD
   send file

   The Terminal Server is now ready to receive the file from the PC.

7. Initiate the ASCII mode file transfer on the PC to upload the file ver_id.hex to the Terminal Server. The following ASCII file transfer parameters, Character pacing, Line pacing, and Pace character, should all be set to zero.

a) In Procomm (v2.x or above):

   Press <PgUp> and then <A> (to indicate ASCII transfer)
   Type the file name ver_id.hex and press <Enter>

b) In Microsoft Windows Terminal:

   Select Transfers and choose Send Text File
   Set the Append LF and Strip LF to NO
   Select the correct path to the source file ver_id.hex and click OK

The update procedure takes around fifteen minutes at 38400 baud. After every ten lines of code of the file being transferred, a dot will be displayed and a section programming message will also be displayed after every several lines (on the 4- and 8-Port Terminal Servers only).

After a successful transfer, the following message will appear:

```
Restarting PASSaPORT CS
```

The Terminal Server will start with a new software version notice.

In the unlikely event of an uploading procedure failing for the 4- or 8-Port Terminal Server, configure the terminal emulation to 19200 baud (the loader's initial speed for this mode). Turn the Terminal Server off and then on. The loader header will be displayed and the process can be retried.

For better performance, you can change the loading speed by typing speed <speed> at the "loader>" prompt and changing the terminal emulation baud rate to match it accordingly.

Appendix B: EPROMS

EPROMs are integrated memory circuits used to store the operating software of the Single-Port Terminal Server. This section will prepare you for two procedures, namely physically removing and replacing EPROMs and programming procedures for programming the ICs.

B.1 Installing/Replacing the EPROMs

The following steps will enable you to physically manipulate the EPROMs if necessary:

For the Single-Port Terminal Server:

1. Disconnect the power and all other cables.
2. Remove the lid of the Terminal Server case by pressing in the four tabs.
3. Locate U12 and U13. These are the EPROM integrated circuits.
4. Remove them with a flat screwdriver. Do this gently so you don't damage them physically and pay careful attention to their fragile pins. Take normal precautions against the dangers of electrostatic discharges.
5. Replace them with the newer versions. Make sure that U12 and U13 are not mixed up and that they are inserted carefully with the right orientation.
6. Replace the lid and the cables as before. The unit is now ready for operation.

B.2 Programming the EPROMs

The new EPROM code is made available either on diskette or through an anonymous FTP site located at *ftp.radlinx.rad.co.il*—in the relevant subdirectories relating to the unit. The code is available as an uncompressed ver_id.hex file where ver_id is the version id number of the release.

The following is an example of the EPROM that is supported.

Single-Port Terminal Server: 27C020-12

NOTE

You must set the programmer to use LOW-BYTE/HIGH-BYTE, or split-level, option when programming these EPROMs for use with the Terminal Server. This is because the software is originally stored as 16-bit words and the EPROMs handle only 8 bits at a time.