TABLE OF CONTENTS

Section **Page**

Topic **Page**

Topic **Page**

Topic **Page**

Topic **Page**

Topic **Page**

Topic **Page**

Topic **Page**

The following are the new or changed commands that are available for V5.1. These commands fall into the following major categories:

Topic **Page**

- **Daemon related SERVER Commands**

- **LPD related Commands**

- **Accounting Commands**

- **Nested Menus Commands**

- **Compressed SLIP Command**

- **ULI related commands**

The following are the new or changed commands that are available for V5.2. These commands fall into the following major categories:

Topic **Page**

- **SecurID related Commands**

- **ARAP related Commands**

Preface

About this Manual.

This manual describes the operation and use of a terminal server software communication package, supplied by Xyplex, Inc. It is intended that this manual will be read by terminal server users and network or terminal server managers.

This manual is organized as follows:

Chapter 1 - Introduction
Chapter 2 - Server Commands

Chapter 1 contains a description of the TCP/IP-LAT software package, and covers some basic user operating procedures.

Chapter 2 describes the terminal server user interface. This chapter describes in detail all of the available commands and options in the terminal server command set, as well as the terminal server command line recall and edit feature. You will use the commands and options in the terminal server command set to establish and monitor computer terminal sessions, and to control or alter the characteristics of these sessions. Within this chapter, all commands are given in alphabetical order.

Conventions.

The following are conventions that will be used throughout this manual:

1. **Unless otherwise specified, commands are executed when you press the RETURN key on the keyboard.**

2. **The CTRL key on the keyboard provides alternate functions when used with some keyboard keys. Throughout this manual, notation such as CTRL/T indicates that you press both the CTRL key and the letter T key at same time. The terminal server will echo this control character as ^T.**

3. **There are two types of command options or qualifiers that are identified in the command syntax lists and option descriptions contained in this manual. These are referred to as keywords and variables. Keywords identify the action you are performing, or the type of object on which the action is to be performed. When you enter a com-mand, you must type each keyword (or the abbreviation for the keyword) exactly as it is shown in the syntax list.**

   Variables identify the type of information that you must supply in a command. The actual information that you supply as a substitute for a variable may be a single character, a text message, a number, a CTRL command, etc.

4. **Throughout this manual, the following typographical conventions are used:**

`Monospace Typeface`	**indicates text that can be displayed or typed at a terminal (i.e.,**
`Monospace Typeface`	**displays, user input, messages, prompts, system responses, etc).**
italics	**indicate variables in command syntax descriptions.**

5. **Throughout this manual, the Xyplex Terminal Server user prompt will be shown as:**

   ```
   Xyplex>
   ```

   for secure and non-privileged users, and

   ```
   Xyplex>>
   ```

   for users at privileged ports. This is the default terminal server user interface prompt; the server manager can specify a different prompt, so the prompt in use at your site may be different.

6. **Throughout this manual, user input in response to system prompts and questions will be shown following a prompt, such as the Xyplex prompt (Xyplex) or a password prompt (# or Password). For example:**

   ```
   Xyplex> CONNECT
   ```

   means that the user has typed the command "CONNECT" in response to the Xyplex prompt.

7. **Throughout this manual, no attempt is made to indicate the minimum number of letters that are needed for a given command, however, most commands can be abbreviated. For example, the SHOW command can be abbreviated to:**

   SH

   The letters "ow" are optional.

8. Throughout this manual, the syntax choices that you can type as part of a command (for example, command options) are indicated by the use of right and left square brackets ("[" and "]", respectively) and by vertical alignment. Unless otherwise indicated, you do not type the brackets. For example, the command syntax shown as:

INITIALIZE [SERVER] [DELAY] [*delay-time*]
[CANCEL]

indicates that "SERVER" is an optional keyword, and that "DELAY delay-time" or "CANCEL" are choices for the INITIALIZE command. To use this command, you could type any of the following:

INITIALIZE SERVER DELAY 5
INITIALIZE DELAY
INITIALIZE CANCEL

or abbreviate these to:

INI S D 5
INI D
INI C

9. Sometimes, an option will apply within another option. This is indicated by the use of square brackets within brackets. For example, the notation:

[*domain-name*[:*telnet-port-number*]]

indicates that you can optionally supply the variable *telnet-port-number* when you specify a *domain-name*. Similarly, the command syntax:

[[SERVICE] *service-name*]

indicates that you can optionally supply the keyword SERVICE with the variable *service-name*, or the variable can be used by itself.

10 Throughout this manual, the following default user prompts will be shown:

VMS	**$**
UNIX/ULTRIX	**%**
DOS	**C:**

A different prompt may be in use at your site.

If you have questions about this product...

At your convenience, please forward these to Xyplex at the following addresses:

Internet Mail: **support@xyplex.com**

United States Mail: **Xyplex, Inc.**
295 Foster Street
Littleton, MA 01460

Attn: Manager, Customer Support

If you have comments about this guide...

To help us in our effort to improve the quality, usefulness, and technical accuracy of the product documentation you receive, Xyplex is interested in any comments or suggestions that you have about this guide, or any technical corrections that you believe should be made. At your convenience, please forward these to Xyplex at the following addresses:

Internet Mail: **documentation@xyplex.com**

United States Mail: **Xyplex, Inc.**
295 Foster Street
Littleton, MA 01460

Attn: Manager, Technical Documentation

Software Upgrade Information

For information on software upgrades contact your local representative, or call Xyplex directly at:

In the United States: **(800) 338-5316**
In Europe: **+44 81 759-1633**
In Asia: **+65 336-0431**

Chapter 1

Introduction

Overview

The software package, supplied by Xyplex, Inc., is called TCP/IP-LAT software. This software operates on Xyplex Terminal Servers and Printer Servers. Terminal servers permit you to connect devices, such as terminals, printers, and modems, to a host computer or node, so that user sessions can be established. Xyplex terminal servers are connected via an Ethernet network. Printer servers permit you to connect printers to the network.

Some of the key features and capabilities of the TCP/IP-LAT software are:

- **Support for LAT protocol. The TCP/IP-LAT software includes a LAT-compatible protocol that makes it directly compatible with DECserver terminal servers and most Digital Equipment Corporation operating systems that support LAT. The Xyplex LAT implementation is the only one directly licensed by Digital Equipment Corporation.**
- **Support for TCP/IP protocol. The TCP/IP-LAT software provides optional support for TCP/IP Telnet protocol. This allows a Xyplex terminal server to connect terminals to other nodes that are running TCP/IP Telnet protocols, such as computers running the UNIX operating system.**

  Xyplex has implemented the following protocols from the Internet protocol suite:

Protocol	Function
Address Resolution Protocol (ARP)	Map 32-bit Internet addresses to 48-bit Ethernet/IEEE 802.3 addresses
Internet Protocol (IP)/Internet Control Message Protocol (ICMP)	Route packets through an Internet network
Transmission Control Protocol (TCP)	End-to-end reliable transmission
Network Terminal Protocol (Telnet)	Network terminal access
User Datagram Protocol (UDP)	Datagram transport and host-initiated queued connection request registration
Berkeley Internet Name Domain Protocol (BIND)	Uses Domain name servers to map user-specified domain-names to Internet addresses.
Serial Line Interface Protocol (SLIP) and Point-to-point Protocol (PPP)	End-to-end Internet connections over a serial line.
Simple Network Management Protocol (SNMP)	The terminal server stores information defined in RFC 1066, Management Information Base, and makes it available on request from an SNMP agent.

Boot Protocol/Trivial File Transfer Protocol (BOOTP/TFTP)	**Transfer load images and parameter files to Xyplex servers.**
Reverse Address Resolution Protocol (RARP)	**Map 48-bit Ethernet/IEEE 802.3 addresses to 32-bit Internet addresses to assist server loading.**

Key TCP features offered by TCP/IP-LAT software include:

1. **the terminal end of a terminal-to-host or terminal-to-terminal Telnet session operating over an Ethernet/IEEE 802.3 Local Area Network.**

2. **user enabling/disabling of special keys to transmit Telnet Interrupt, Erase previous character, Erase line, Abort output, Are you there?, Synchronize, and Attention messages.**

3. **local and remote echo.**

4. **ability to distinguish Internet addresses that can be reached directly from those that must be reached via an Internet gateway.**

5. **local name to Internet address mapping.**

6. **Telnet connections to any TCP port at any Internet address.**

7. **addressing of individual physical ports on a terminal server.**

8. **use of Domain name servers to help resolve domain-names .**

9. **session type changes automatically when negotiating in and out of Telnet binary mode. When the user has finished using the Telnet binary mode and the session successfully negotiates out of binary mode, the terminal server software automatically changes the session type to INTERACTIVE.**

10. **compliance with RFC 1122, Requirements for Internet Hosts - Communication Layers, and RFC 1123, Requirements for Internet Hosts - Application and Support Layers. TCP/IP-LAT software complies with RFCs 1122 and 1123.**

11. **internet-level routing. The TCP/IP-LAT software provides the capability to allow the terminal server manager to specify, in either the permanent or operational database, a gateway to be used to reach a specific destination (this is called "static routing"). Alternatively, the software can also allow the gateways themselves to determine how to reach the desired destination ("dynamic routing"). In this case, the route used is stored in the operational database.**

12. **support for rotary connections. Multiple ports on multiple terminal servers can share the same domain name. When a user attempts to connect to the domain, the user is connected to a port on a server that is associated with that name.**

13. **A system manager can restrict inbound and outbound connection requests on an Internet. A system manager can restrict specific terminal server ports from accessing an Internet address and also restrict access to ports on the terminal server.**

14. A user can run Internet protocols over a serial line. The interface is provided using the Serial Line Internet Protocol (SLIP) and and Point-to-point Protocol (PPP). Applications include:

    - Connecting a remote terminal or PC that supports SLIP/PPP to a node on the local network, via the terminal server. Once connected to the local network, a remote user can perform operations such as file transfers.

    - Connecting a host directly to a serial port.

    - Connecting two networks via server serial ports (connection functions as a simple gateway).

    - End-to-end routing. An end-to-end connection can be made by connecting into a host, such as a terminal server, on one port, and connecting to another host via another SLIP or PPP port. This allows a user to connect anywhere on the Internet.

15. support for remote network management is provided in two ways:

    - Simple Network Management Protocol (SNMP) support. The TCP/IP-LAT software implements the entire standard MIB as appropriate to a system that is not a gateway. The TCP/IP-LAT software agent accepts the GetRequest, GetNextRequest, and the SetRequest functions. The TCP/IP-LAT software implements private MIB objects, but does not implement any experimental MIB objects. The TCP/IP-LAT software implement some SNMP traps.

    - Telnet access to a terminal server's remote console port

16. support for UUCP connections. UUCP connections through a server are enabled by setting a PORT DEFAULT SESSION MODE characteristic to TRANSPARENT.

17. support for RLOGIN.

18. support for full duplex printer daemon. The TCP/IP-LAT distribution media includes a C source code file for a full duplex (bi-directional) printer daemon that supports PostScript® printers.

19. support for Kerberos user verification. Kerberos is a network authentication service developed at the Massachusetts Institute of Technology. It provides a central authority that mediates between clients requesting services and service providers that require client verification.

    Note

    Kerberos encrypts data to Department of Defense Data Encryption Standards (DES). Export of this software from the United States of America is assumed to require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

    Kerberos requires compatible host software running at the TCP/IP host that is the Kerberos master. Although Xyplex, Inc. can supply this software, Xyplex, Inc. does not support this software. Contact Xyplex Customer Support to obtain information about acquiring this software.

20. support for limited Domain Name serving.

- **Novell NetWare® Support. This allows printers connected to the unit to be shared by personal computers and file servers which are on a Novell NetWare local area network (LAN) and who use the Novell RPRINTER utility. At Novell print servers, you configure the printer server to the NetWare software as you would any standard remote printer.**

- **Friendly user interface. The TCP/IP-LAT software uses a simple, yet powerful, command structure that gives users and system managers quick access to all terminal server features, and helps users to "get up to speed" quickly. Key user interface features include:**

  1. **Extensive On-line Help facilities. The user interface provides help for all terminal server commands and command options.**

  2. **Command-Line Recall and Editing. The user interface "remembers" each user's most recently issued commands. The user can then recall, edit, and re-issue the command by using keyboard arrow keys and control keys.**

  3. **Displays. The terminal server provides displays which show the setting for all parameters, as well as statistics about port and terminal server operations. These statistics include network traffic and error counts that can be continuously monitored to make trouble analysis easier.**

  4. **Support for Multiple Sessions. Users can establish one or more sessions with any host computers on the network and quickly switch among these sessions, by typing a switch character.**

  5. **User-Defineable Line Editing Commands. Users can specify the control characters (or no character) to perform various line editing functions.**

6. **Simple Menu Interface. A system manager can develop a custom menu with up to 20 selections and specify the terminal server ports that will generate the menu. When logged onto these ports, nonprivileged users can only perform operations by choosing menu items. (A privileged user can use a different port, where the menu is not enabled, to disable the menu at a port.)**

7. **UNIX "Aliases." Aliases are UNIX-like commands that provide the same function as a Xyplex command. They are designed to give the TCP/IP-LAT software more of a UNIX "look-and-feel".**

8. **Copying port characteristics. The software supports a DEFINE PORT FROM PORT command that copies the permanent characteristics of one port, except the PORT NAME characteristic, to one or more other ports on the same unit.**

9. **Network Commands Scripts. The software allows a port to be configured so that a script file containing commands can be downloaded from a host on the network, and executed at the port. Similar scripts can be required for dial-back ports.**

- **Support for Xremote/Xwindows connections. Units running TCP/IP-LAT software can connect Xwindows terminals to hosts and run multiple windows on a single terminal.**

- **Support for Standard Terminal Server Management Tools. Standard DEC LAT software management tools can be used to manage the operation of the TCP/IP-LAT software. These tools include: the DSVCONFIG utility, the DECnet Network Control Program (NCP), the DECserver Terminal Server Manager (TSM) utility, and the LAT Control Program (LATCP).**

- **Support for Xyplex Server Management Tools. Units running TCP/IP-LAT software can be managed by Xyplex ControlPoint™ network management software.**

- **Security Features. The TCP/IP-LAT software provides means by which the terminal server manager can restrict user access to the terminal server and/or to nodes available to the terminal server via Ethernet connection. The *Software Management Guide* describes these security/access restriction features in more detail.**

- **Support for flow control and modem control signals. For applications which require control of data flow, the TCP/IP-LAT software supports hardware and software handshaking mechanisms. Units which support the Xyplex eight-wire cabling scheme can use concurrent hardware flow control and modem control. Refer to the hardware documentation supplied with your Xyplex unit for more information.**

- **Xyplex Hardware Products Supported. TCP/IP-LAT Software supports the following Xyplex MAXserver and Network 9000 hardware products:**

> **Note**
>
> **Refer to the *Software Kit Information* for a list of TCP/IP-LAT software features that are available on each of the following hardware options.**

  - **the Network 9000 Terminal Server 720 and associated I/O modules. These modules are options for use in the Network 9000 Intra-Networking hub. Various I/O modules are available, and provide either six-wire or eight-wire cabling methods.**

  - **the MAXserver 1600 Sixteen Port Terminal Server, MAXserver 1620 Twenty Port Terminal Server, and MAXserver 1640 Forty Port Terminal Server. These are standalone terminal servers, which provide ports with modem control signals, using the Xyplex eight-wire cabling method. These unit also provides data storage via one memory card. These unit,s and associated software, provides a means of down-loading load images to to other units, storing parameter files, and configuring and managing these units, without a host in the network.**

  - **the MAXserver 800 Eight Port Terminal Server is a standalone terminal server, which provide ports with modem control signals, using the Xyplex eight-wire cabling method.**

  - **the MX-TSERV-J8, MX-TSRVM-J8, andMX-2210 Eight Port Terminal Server cards. These cards are options for use in the MAXserver 5500, 5000, and 4500 model Communication Servers. These cards provide 8 ports, and are useful in applications which require modem control signals. These units use the Xyplex six-wire cabling scheme.**

  - **the MX-TSRVL-J16 Sixteen Port LAT Terminal Server card, MX-TSERV-J16 and MX-2120 Sixteen Port TCP/IP-LAT Terminal Server card. These cards are options for use in the MAXserver 5500, 5000, and 4500 model Communication Servers. These cards provide 16 ports, and are useful in applications which do not require modem control signals. The MX-TSRVL-J16 card supports Xyplex LAT software. These units use the Xyplex three-wire cabling scheme.**

  - **The MX-NPC-P1 Network Printer Card. This card provides shared printer support for a parallel printer, and is available as an option for use in MAXserver 5500, 5000, and 4500 model Communication Servers. This card provides connection to either a Centronics or Dataproducts style parallel port.**

  - **the MX-MAX1800-E Sixteen Port Terminal Server. This is a standalone terminal server, which provides 16 ports with modem control signals. The unit also provides data storage via one floppy disk drive that uses high-density "microfloppy" diskettes (1.44 megabyte, 8.9 cm/3.5 inch). The MAXserver 1800 unit, and associated software, provides a means of down-loading Xyplex LAT or TCP/IP-LAT images to Xyplex MAXserver 1000 Series Products, storing dump files, and configuring and managing these units, without a VAX/VMS host in the network. These units use the Xyplex six-wire cabling scheme.**

  - **the MX-MAX1500-E Sixteen Port Terminal Server. This is a standalone terminal server, which provides 16 ports with modem control signals. These units use the Xyplex six-wire cabling scheme.**

- **the MX-MAX1100-E and MX-MAX1100T Sixteen Port Terminal Server. This is a standalone terminal server, which provides 16 ports with modem control signals. The MAXserver 1100 is a single protocol unit (i.e., supports Xyplex LAT or TCP/IP software), and can be upgraded to a dual protocol unit (i.e., support TCP/IP-LAT software). These units use the Xyplex six-wire cabling scheme.**

- **the MAXserver 1400, 1400A, and 1450 Printer Servers. These are standalone unitx, which provides shared printer support for four devices. This unit provides connections for up to two parallel printers, and up to two serial devices. MAXserver 1400A and 1450 Printer Servers support printing from LAT and TCP/IP hosts, and Novell Netware devices.**

- **the MX-MAN-F2 MAXserver Manager Card. This card is available as an option for use in MAXserver 5500, 5000, and 4500 model Communication Servers. This card, and associated software, provides a means of down-loading Xyplex LAT or TCP/IP-LAT images to Xyplex servers, storing their parameters and dump files, and configuring and managing these servers, without a VAX/VMS host in the network.**

  The MX-MAN-F2 card requires two adjacent MAXserver slots. The card provides data storage via two floppy disk drives that use high-density "microfloppy" diskettes (1.44 megabyte, 8.9 cm/3.5 inch). The MX-MAN-F2 card also provides two ports. One port is a parallel port to which you can connect a parallel printer or other device which supports a Centronics-style parallel interface. A printer connected to this port is used to log management events and messages. The Centronics-style I/O Connector Card supports connections to most Centronics and IBM PC compatible parallel printers. The second port is a serial port to which you can connect a terminal, serial printer, personal computer, or another serial device. The serial port is used to manage the software running at the MAXserver Manager Card (MAXMAN), or to log events.

Chapter 2

Server Command Set

Introduction to the SERVER User Interface

The TCP/IP-LAT software includes a user interface which provides the means by which you:

- **establish, monitor, and control SERVER sessions,**
- **control communications between the SERVER and devices (such as terminals, modems, etc) as well as between the SERVER and service nodes,**
- **control and monitor the availability of services which are offered at SERVER ports,**
- **use security features of the TCP/IP-LAT software, and**
- **recover when problems occur.**

The TCP/IP-LAT user interface provides access to these functions through a series of commands, which are listed in the section titled Available Commands, later in this chapter. This chapter describes in detail each of these commands, and the options available with the command, in separate sections. The commands are listed in alphabetical order, within this chapter. Before reviewing the information in the chapter, you may wish to review the section titled Conventions in the preface of this manual to understand the notation used within this chapter.

Entering SERVER Commands

The user interface provides access to TCP/IP-LAT software features through commands and CTRL characters. Users will enter most commands from the local command prompt. Some SERVER CTRL commands can be issued from within a session. Other CTRL commands only apply at the local command prompt. You must press the RETURN key to execute a command which you have typed (except for CTRL commands which the SERVER executes immediately).

The maximum length of a command line is 132 characters. You can type a command which exceeds the width of the terminal screen as long as you do not press the RETURN key until the command is complete. For most of the commands listed in Table 2-1, you can specify multiple keywords or variables with a single command. When you specify a single command that applies to more than one characteristic, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces.

When a user issues a command which affects more than one port, or which contains multiple characteristics in the same command, the software will first verify that all requested actions are valid before the actions are performed. If any individual action would result in the display of an error message, none of the requested actions are performed.

Table 2-1 describes the available functions that you can enable which allow you to switch among SERVER sessions or to return to the local command mode, as well as the choices for what action the SERVER will take when you press the BREAK key. Some functions are available within LAT or Telnet sessions, as well as from the local command mode. Table 2-2 describes functions that users can enable which are used to manage Telnet sessions. All you need to do to enable any of these features is to use the appropriate DEFINE PORT or SET PORT command to specify which character performs the function. Normally, you will specify an unused CTRL command, or a character such as the backward apostrophe character (`). You can also specify a Compose character, on terminals that support this feature, as a session switching, line editing, or Telnet command character. Refer to the sections which describe the DEFINE/SET PORT commands for more information.

When defining line editing characters, session switching characters, or Telnet command characters, you can specify the caret symbol (^) followed by a letter as a substitute for typing a CTRL character in the SET/DEFINE command. The user will still issue the command with the corresponding CTRL command. For example, the user can type either of the following commands to establish CTRL/B as the forward switch character for the port:

```
Xyplex> SET PORT FORWARD SWITCH ^B
```

or

```
Xyplex> SET PORT FORWARD SWITCH CTRL/B
```

In either case, when the user issues a CTRL/B command, the port will switch to the next session. This feature is particularly useful in TSM scripts.

Note

You cannot define any line editing character, session switching character, or Telnet command to be CTRL/I, CTRL/J, or CTRL/M.

Table 2-1. User-Definable Command Characters.

Command	Description
Backward switch character	The character that causes the SERVER to exit from the current session and return to the previous session.
BREAK	The SERVER can be set up to perform one of the following actions when you press this key: return to the SERVER local command mode (the default), ignore the BREAK key, or send the break to the connection partner (e.g., the service node or Telnet node). While in a Telnet remote session, when a user issues the BREAK command when the PORT BREAK characteristic is set to REMOTE, the SERVER port will pass a BREAK to the host or device to which it is connected.
Forward switch character	A character that causes the SERVER to exit from the current session and go to the next session.
Local switch character	The character that causes the SERVER to exit from the current session and go to the local command prompt.

Note

You can define a terminal answerback message to include either forward or backward switch character, as well as additional characters (for example, a CTRL/W command to refresh the screen in the new session). Then, when you issue the answerback message, the SERVER will switch sessions and pass the additional characters to the new session.

The guide *Using the TCP/IP-LAT Terminal SERVER* describes the command line recall and editing feature. Beginning with the sections which describes the BACKWARDS command, the remainder of this guide describes each command that is available within the SERVER user interface (The section titled Available Commands provides a summary of these). Within each of the command description sections, you will find the material presented in the following order: Description, Privileges, Syntax, Options, Output (where applicable), and Examples.

Table 2-2. User-Definable Telnet Command Characters.

Command	Description
Telnet abort output character	A character that the user can type, when in a Telnet session, to terminate further display of output from a program without aborting or terminating the program itself.
Telnet attention character	A character that the user can type, when in a Telnet session, to cause the host to return to the operating system command prompt. While in a Telnet remote session, when a user issues the TELNET ATTENTION command, or a BREAK command when the PORT BREAK characteristic is set to REMOTE, the remote SERVER port will pass a BREAK to the host or device to which it is connected.
Telnet erase character	A character that the user can type, when in a Telnet session, to delete the character immediately to the left of the cursor.
Telnet erase line character	A character that the user can type, when in a Telnet session, to delete all data to the left of the cursor in the current line of input.
Telnet interrupt character	A character that the user can type, when in a Telnet session, to suspend, interrupt, or abort a user process.
Telnet query character	A character that the user can type, when in a Telnet session, which requests that the node provide an indication that it is still up and running.
Telnet synchronize character	A character that the user can type, when in a Telnet session, to gain control of a "run-away" process.

Common Variables

Table 2-3 defines variables which are used frequently in command descriptions throughout this chapter. These variables are listed here to avoid repetition.

Table 2-3. Common Variables.

Variable Name	Description
node-name	Specifies the name of a node (computer, terminal SERVER, etc) in a LAT network, at which a service is offered. LAT *node-names* are distinct from DECnet *node-names*; however, Xyplex recommends that you set the LAT *node-name* for a SERVER to be the same as the DECnet node-name. For a LAT *node-name* you can specify a name which consists of 1 to 16 ASCII characters, including the letters A through Z, the numbers 0 through 9, and the dollar sign ($), period (.), hyphen (-), and underscore (_) characters. (DECnet *node-names*; are limited to 6 characters.) Lower-case letters in the *node-name* are always translated by the software to upper-case letters. Do not enclose *node-names* in quotation marks (").
port-name	Specifies the name for a port. The port-name can be between 1 and 16 ASCII characters in length. (Note that the SERVER will convert any lower-case letters to upper case.) Do not enclose the port-name in quotation mark characters ("). The port-name must be unique within each SERVER. The default value for this variable is in the form: PORT_*port-number*, where *port-number* is the number of the physical SERVER port.
port-number	The number assigned to the port connector of the SERVER hardware unit to which a device is attached. Valid values for a *port-number* are one or two-digit numbers in the range of 0 to n, where n represents the number of physical ports tat the unit contains. (For example, on a40-port terminal SERVER the physical *port-numbers* are in the range of 1 to 40.) The Remote Console port *port-number* is always port 0.
port-list	A list of one or more *port-numbers*. You can specify multiple ports in a *port-list* by specifying individual *port-numbers* separated by commas, by specifying a range of *port-numbers* separated by a hyphen, or a combination of both (do not include spaces). For example, the *port-list*: 1,3-5,8 refers to the individual ports: 1, 3, 4, 5, and 8.
service-name	The name of a service which is available on the network. Specify a name which consists of 1 to 16 ASCII characters, including the letters A through Z, the numbers 0 through 9, and the dollar sign ($), period (.), hyphen (-), and underscore (_) characters. Lower-case letters in the *service-name* are always translated to upper-case letters. Do not enclose *service-names* in quotation marks (").

Table 2-3 (continued). Common Variables.

Variable Name	Description
INTERNET Variables	
domain-name	**This common variable only applies to INTERNET communications. A *domain-name* identifies an addressable network object, such as a host or SERVER. A *domain-name* maps to an *INTERNET-address* (i.e., the SERVER converts the *domain-name* to an *INTERNET-address* when it communicates over the network). The network object represented by a *domain-name* runs INTERNET protocols. You can think of a *domain-name* as a logical name for an *INTERNET-address*.** **Use the following syntax rules to specify a fully-qualified *domain-name*: the name can consist of up to 50 ASCII characters, including the letters A through Z (lower-case letters are treated as upper-case letters), the numbers 0 through 9, the underscore (_) and hyphen (-) characters. Separate each segment within a *domain-name* specification with a period. Each segment in the *domain-name* can be up to 50 ASCII characters in length. The left-most segment identifies the individual network object. The remaining segments identify the domain where the object is located. Do not enclose *domain-names* in quotation marks ("). Examples of a *domain-name* are NIC.DDN.MIL or XYPLEX.COM.** **A fully qualified *domain-name* must contain at least one period. If a user types a name in a Telnet command that does not contain at least one period, the software appends the default *domain-suffix* to obtain a fully qualified *domain-name*. (Specify the default *domain-suffix* using the DEFINE/SET SERVER INTERNET DEFAULT DOMAIN SUFFIX command.)**
INTERNET-address	**This common variable only applies to Telnet sessions. An *INTERNET-address* identifies a network addressable object, such as a host or SERVER. The network object runs INTERNET protocols. An *INTERNET-address* consists of four numbers separated by periods (.). Valid values for each of the four numbers are whole numbers in the range of 1 through 254 (the numbers 0 and 255 are permitted in some circumstances). An example of an *INTERNET-address* is: 128.10.2.30.**

Table 2-3 (continued). Common Variables.

Variable Name	Description
telnet-port-number	This common variable only applies to Telnet sessions. A *telnet-port-number* is a protocol identifier. Valid values for the *telnet-port-number* are whole numbers in the range of 1 through 32767. Values between 1 through 255 represent "well-known" protocols. The default value is 23. A value other than 23 must represent a Telnet-compatible protocol. Always use a colon (:) to separate the *telnet-port-number* from a *domain-name* or *INTERNET-address*. A *telnet-port-number* can also be used as the address of a specific port on a Xyplex SERVER, when in a Telnet session. To specify the default address for a port, use the formula: *telnet-port-number* = [2000 + (100 x *n*)] where *n* is the physical port number. (Note that, for a Telnet session, the address of a physical port can be specified using the PORT TELNET REMOTE characteristic.)

Reserved Keywords.

The following is a list of "reserved keywords."

ALL	IDENTIFICATION	NODEPASSWORD	SIGNAL
CHARACTERISTICS	IDENTIFICATION	PORTS	STATUS
CONNECTIONS	SIZE	QUEUE	SUMMARY
CR	INTERACTIVE	SERVICE	TCP WINDOW
FILTERING	LIMITED		TRANSPARENT
	LOCAL		

These keywords, or abbreviations of these keywords (for example, "A" or "AL" in the case of the keyword "ALL"), cannot be used to specify a LAT *service-name*. Similarly, the following keywords, or abbreviations of these keywords, cannot be used to specify a *domain-name*.

ALL	IDENTIFICATION	LIMITED	TCP WINDOW
CR	SIZE	LOCAL	TRANSPARENT
FILTERING	INTERACTIVE	SIGNAL	
	LEARNED		

UNIX Aliases

TCP/IP-LAT software provides several Unix-like commands that give the TCP/IP-LAT software more of a Unix "look-and-feel". These commands are referred to as "Unix aliases." These aliases are commands that provide the same function as a TCP/IP-LAT command. The following is a list of the Xyplex commands and their corresponding Unix aliases.

Xyplex Command	Unix Alias
SHOW PORT [*port-list*] STATUS	**STATUS [*port-list*]**
RESUME *session-number*	**FG *session-number***
HELP	**MAN**
SHOW SESSIONS	**JOBS**
SHOW USERS	**WHO**
TEST INTERNET *host* [RECORDROUTE] [NORECORDROUTE]	**PING *host* [RECORDROUTE] [NORECORDROUTE]**
DISCONNECT [*session*]	**CLOSE or KILL [*session*]**
TELNET CONNECT [*domain-name*] [*INTERNET-address*]	**OPEN [*domain-name*] [*INTERNET-address*]**
LOGOUT [*port-list*]	**QUIT [*port-list*]**

Available Commands

This section lists the command syntax for all commands supported by the TCP/IP-LAT software.

Session Management Commands

(S) BACKWARDS

(S) CONNECT [[SERVICE] *service-name*] [NODE *node-name*] [DESTINATION *port-name*]
[*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(P) CONNECT [PORT *port-number*] *service-name* [NODE *node-name*] [DESTINATION *port-name*]]
[*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(S) DISCONNECT [SESSION [*session-number*]]
[ALL]

(P) DISCONNECT [PORT] [*port-list*]

(S) FORWARDS

(S) LAT CONNECT [[SERVICE] *service-name*] [NODE *node-name*] [DESTINATION *port-name*]

(P) LAT CONNECT [PORT *port-number*] *service-name* [NODE *node-name*]
[DESTINATION *port-name*]

(S) LOCK

(S) LOGOUT [PORT]

(P) LOGOUT PORT [*port-list*]
[ALL]

(S) RESUME [[SESSION] *session-number*]
[*service-name*]

(S) RLOGIN *domain-name* [[USERNAME] "*username*"]
INTERNET-address [[USERNAME] "*username*"]
NONE

(S) TELNET CONNECT [*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(P) TELNET CONNECT [PORT *port-number*] [*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

SERVER Setup and Management Commands

The basic syntax for the DEFINE PORT and SET PORT commands is:

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

The following list summarizes the port characteristics which can be defined:

In the syntax list which follows: port characteristics which can be changed by secure users, non-privileged users, or users at privileged ports are indicated with an (S). Port characteristics which can be changed by non-privileged users, or users at privileged ports, are indicated with (N). Port characteristics which can only be set or changed by privileged users are indicated with a (P). The factory default choice for a characteristic is indicated with an asterisk (*). Characteristics which can only be changed via a DEFINE command are indicated with two asterisks (**).

(P) [ACCESS] [DYNAMIC]
[LOCAL]*
[NONE]
[PRT3270]
[REMOTE]

(P) [AUTHORIZED GROUPS] [*group-list*] [DISABLED]
[ENABLED]
[ALL] [DISABLED]
[ENABLED]

(P) [AUTOBAUD] [DISABLED]
[ENABLED]*

(N) [AUTOCONNECT] [DISABLED]*
[ENABLED]

(P) [AUTODEDICATED] [DISABLED]*
[ENABLED]

(S) [AUTOPROMPT] [DISABLED]
[ENABLED]*

(S) [BACKWARD SWITCH] [*character*]
[NONE]*

(N) [BREAK] [DISABLED]
[LOCAL]*
[REMOTE]

(N) [BROADCAST] [DISABLED]
[ENABLED]*

(N) [CHARACTER SIZE] [7]
[8]*

(N) [CONNECTRESUME] [DISABLED]*
[ENABLED]

(P) [DCD TIMEOUT] [*timer-value*]

(P) [DEDICATED SERVICE]** [*service-name*] [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(P) [DEFAULT SESSION MODE] [INTERACTIVE]*
[PASTHRU]
[PASSALL]
[TRANSPARENT]

(P) [DIALBACK] [DISABLED]*
[ENABLED]
[TIMEOUT *time*]

(P) [DIALUP] [DISABLED]*
[ENABLED]

(P) [DSRLOGOUT] [DISABLED]*
[ENABLED]

(P) [DSRWAIT] [DISABLED]*
[ENABLED]

(P) [DTRWAIT] [DISABLED]*
[ENABLED]
[FORCONNECTION]
[FORRING]

(N) [FLOW CONTROL] [CTS]
[DISABLED]
[DSR]
[ENABLED]
[XON]*

(S) [FORWARD SWITCH] [*character*]
[NONE]*

(P) [FROM PORT]** [*port-number*]

(N) [GROUPS] [*group-list*]
[ALL]
[DISABLED]
[ENABLED]

(P) [IDLE TIMEOUT] [*timer-value*]

(P) [INACTIVITY LOGOUT] [DISABLED]*
[ENABLED]

(N) [INPUT FLOW CONTROL] [DISABLED]
[ENABLED]*

(P) [INTERNET CONNECTIONS] [DISABLED]
[ENABLED]*

(P) [INTERNET SECURITY] [INBOUND] [ALLOW] *INTERNET-address* [MASk *security-mask*]
[ENABLED]
[DENY]
[DISABLED]
[OUTBOUND] [ALLOW] *INTERNET-address* [MASk *security-mask*]
[ENABLED]
[DENY]
[DISABLED]
[DEFAULT] [INBOUND] [ALLOW]
[DENY]
[OUTBOUND] [ALLOW]
[DENY]

(P) [INTERNET SLIP] [ENABLED]
[DISABLED]**
[ADDRESS *port-address*] [REMOTE *remote-address* MASK *network-mask*]

(P) [INTERNET TCP WINDOW SIZE] [*TCP-window-size*]

(P) [INTERRUPTS] [DISABLED]*
[ENABLED]

(P) [KERBEROS] [ENABLED]]
[DISABLED]*

(P) [LAT DEDICATED SERVICE] [*service-name*] [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*

(N) [LAT PREFERRED SERVICE] [*service-name*] [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*

(P) [LIMITED [VIEW]] [ENABLED]
[DISABLED]*

(N) [LINE EDITOR] [ENABLED]
[DISABLED]

[BACKSPACE] [*character*]
[NONE]

[BEGINNING] [*character*]
[NONE]

[CANCEL] [*character*]
[NONE]

[DELETE BEGINNING] [*character*]
[NONE]

[DELETE LINE] [*character*]
[NONE]

[END] [*character*]
[NONE]

[FORWARDS] [*character*]
[NONE]

[INSERT TOGGLE] [*character*]
[NONE]

[NEXT LINE] [*character*]
[NONE]

[PREVIOUS LINE] [*character*]
[NONE]

[QUOTING CHARACTER] [*character*]
[NONE]

[REDISPLAY] [*character*]
[NONE]

(S) [LOCAL SWITCH] [*character*]
[NONE]*

(N) [LOSS NOTIFICATION] [DISABLED]
[ENABLED]*

(P) [MENU] [ENABLED]
[DISABLED]*

(N) [MESSAGE CODES] [DISABLED]
[ENABLED]*

(P) [MODEM CONTROL]** [DISABLED]*
[ENABLED]

(N) [MULTISESSIONS] [ENABLED]
[DISABLED]*

(P) [NAME] [*port-name*]

(N) [NOLOSS] [DISABLED]*
[ENABLED]

(N) [OUTPUT FLOW CONTROL] [DISABLED]
[ENABLED]*

(N) [PARITY] [EVEN]
[MARK]
[NONE]*
[ODD]

(P) [PASSWORD] [DISABLED]*
[ENABLED]

(S) [PAUSE] [DISABLED]*
[ENABLED]

(N) [PREFERRED SERVICE] [*service-name*] [NODE] [*node-name*] [DESTINATION] [*port-name*]

[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [NODE] [*node-name*] [DESTINATION] [*port-name*]
[NONE]*
[NONE]* [DESTINATION] [*port-name*]
[NONE]*
[*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(P) [PRIVILEGED MENU] [DISABLED]*
[ENABLED]

(N) [PROMPT] ["*prompt-string*"]

(P) [QUEUING] [DISABLED]*
[ENABLED]

(S) [RESOLVE SERVICE] [ANY]*
[LAT]
[TELNET]

(P) [REMOTE MODIFICATION] [ENABLED]
[DISABLED]*

(N) [SCRIPT] [*script-name*]

(P) [SCRIPT ECHO] [DISABLED]*
[ENABLED]

(P) SCRIPT LOGIN] [DISABLED]*
[ENABLED]
[REQUIRED]

(P) [SECURITY] [DISABLED]*
[ENABLED]

(P) [SESSION LIMIT] [*session-limit*]
[NONE]

(P) [SIGNAL [CHECK]] [ENABLED]
[DISABLED]*

(N) [SPEED] [*speed*]

(N) [STOP BITS *bit-value*]

(S) [TELNET ABORT OUTPUT] [*character*]
[NONE]*

(S) [TELNET ATTENTION] [*character*]
[NONE]*

(N) [TELNET BINARY SESSION MODE] [INTERACTIVE]
[PASSALL]
[PASTHRU]*

(N) [TELNET CSI ESCAPE] [DISABLED]*
[ENABLED]

(P) [TELNET DEDICATED SERVICE]** [*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(N) [TELNET DEFAULT PORT] [*telnet-port-number*]

(N) [TELNET ECHO MODE] [LOCAL]
[REMOTE]*

(S) [TELNET ERASE CHARACTER] [*character*]
[NONE]*

(S) [TELNET ERASE LINE] [*character*]
[NONE]*

(P) [TELNET EOR REFLECTION] [DISABLED]*
[ENABLED]

(S) [TELNET INTERRUPT] [*character*]
[NONE]*

(S) [TELNET NEWLINE] [NULL]*
[LINEFEED]
[NOTHING]

(S) [TELNET NEWLINE FILTERING] [NONE]*
[LINEFEED]

[CR]
[NULL]

(N) [TELNET OPTION DISPLAY] [DISABLED]*
[ENABLED]

(P) [TELNET PREFERRED SERVICE] [*domain-name*[:*telnet-port-number*]]
[*INTERNET-address*[:*telnet-port-number*]]

(S) [TELNET QUERY] [*character*]
[NONE]*

(P) [TELNET REMOTE] [*telnet-port-number*]

(S) [TELNET SYNCHRONIZE] [*character*]
[NONE]*

(N) [TELNET TERMINALTYPE *terminal-type*]

(N) [TELNET TRANSMIT] [BUFFERED]*
[IMMEDIATE]
[IDLETIME] [*character-times*]

(S) [TYPE] [ANSI]
[HARDCOPY]
[SOFTCOPY]*

(P) [TYPEAHEAD SIZE] [*size*]

(N) [USER KERBEROS PASSWORD]

(N) [USERNAME] [*name*]

(S) [VERIFICATION] [DISABLED]
[ENABLED]*

All DEFINE SERVER and SET SERVER commands require that the user be logged on to a privileged terminal. The basic syntax for the DEFINE SERVER and SET SERVER commands is:

[DEFINE] SERVER [*characteristic(s)*]
[SET]

The following list summarizes the SERVER characteristics which can be defined:

[ACCOUNTING ENTRIES *number*]

[ANNOUNCEMENTS] [DISABLED]
[ENABLED]*

[BROADCAST] [DISABLED]
[ENABLED]*

[CHANGE] [DISABLED]*
[ENABLED]

[CIRCUIT TIMER] [*timer-value*]

[CONSOLE LOGOUT] [DISABLED]*
[ENABLED]

[DATE] [*dd mmm yyyy*]

[DUMP] [DISABLED]
[ENABLED]*

[EVENTLOG] [ENABLED]*
[DISABLED]

[HELP] [ENABLED]*
[DISABLED]

[IDENTIFICATION] [*message-string*]

[IDENTIFICATION SIZE] [*size*]

[INACTIVITY TIMER] [*time*]

[INTERNET ADDRESS] [*INTERNET-address*]

[INTERNET BROADCAST ADDRESS] [*INTERNET-address*]

[INTERNET DEFAULT DOMAIN SUFFIX] [*domain-name-suffix1*|*domain-name-suffix2*|...|*domain-name-suffix8*]

[INTERNET DOMAIN TTL] [*time*]

[INTERNET [PRIMARY] DOMAIN ADDRESS] [*INTERNET-address*]
[SECONDARY]

[INTERNET [PRIMARY] GATEWAY ADDRESS] [*INTERNET-address*]
[SECONDARY]

[INTERNET NAME] [*domain-name*]

[INTERNET ROTARY [*INTERNET-address port-list*]
[*domain-name port-list*]

[INTERNET SECURITY] [ENABLED]*
[DISABLED]

[INTERNET SNMP] [GET CLIENT] [*client-number*] [*INTERNET-address*]
[SET CLIENT] [*client-number*] [*INTERNET-address*]
[TRAP CLIENT] [*client-number*] [*INTERNET-address*]

[GET COMMUNITY] [*community-name*]
[NONE]*
[SET COMMUNITY] [*community-name*]
[NONE]*
[TRAP COMMUNITY] [*community-name*]

[SYSTEM CONTACT] [*contact-name*]

[SYSTEM LOCATION] [*location-name*]

[INTERNET SUBNET MASK] [*INTERNET-address-mask*]
[AUTOCONFIGURE] [DISABLED]
[ENABLED]

[INTERNET TTL] [*ttl-value*]

[KEEPALIVE TIMER] [*timer-value*]

[KERBEROS MASTER *domain-name INTERNET-address*]

[KERBEROS PRIMARY SERVER *domain-name INTERNET-address*]

[KERBEROS QUERY LIMIT *limit*]

[KERBEROS REALM *realm-name*]

[KERBEROS SECONDARY SERVER *domain-name INTERNET-address*]

[KERBEROS SECURITY] [LOGIN]
[NONE]

[LOCK] [DISABLED]
[ENABLED]*

[LOGIN] [PASSWORD] [*password*]
[PROMPT] [*prompt*]

[MAINTENANCE PASSWORD] [*password-number*]

[MENU] [ENABLED]*
[DISABLED]
[*item-number string1*]

Note

After you press the RETURN key, you are prompted to enter a Xyplex command with the prompt:

Enter Xyplex command> *string2*

where *string2* represents a series of TCP/IP-LAT commands.

[MENU CONTINUE PROMPT *prompt-text*]

[MENU PROMPT *prompt-text*]

[MULTICAST TIMER] [*time*]

[MULTISESSIONS] [ENABLED]*
[DISABLED]

[NAME] [*SERVER-name*]

[NODE LIMIT] [*limit*]
[NONE]

[NUMBER] [*SERVER-number*]

[PARAMETER SERVER] [CHECK] [DISABLED]
[ENABLED]*
[PROPRIETARY ENABLED]
[TFTP ENABLED]

[TIMER *timer-value*]

[LIMIT *number*]

[RETRANSMIT] [LIMIT *limit*]
[TIMER *timer-value*]

[PARAMETER VERSION *number*]

[PASSWORD LIMIT] [*limit*]
[NONE]

[PRIVILEGED PASSWORD] [*password*]

[PROTOCOL] [KERBEROS] [DISABLED]*
[ENASBLED]
[LAT] [ENABLED]*
[DISABLED]
[PPP] [DISABLED]*
[ENABLED]
[SNMP] [DISABLED]
[ENABLED]*
[TELNET] [ENABLED]*
[DISABLED]
[TN3270] [ENABLED]
[DISABLED]*
[XPRINTER] [DISABLED]*
[ENABLED]
[XREMOTE] [DISABLED]*
[ENABLED]

[PURGE GROUP] [DISABLED]*
[ENABLED]

[PURGE NODE] [DISABLED]*
[ENABLED]

[QUEUE LIMIT] [*queue-limit*]
[NONE]

[REPORT ERRORS] [ENABLED]
[DISABLED]*

[RETRANSMIT LIMIT] [*limit*]

[RLOGIN] [DISABLED]
[ENABLED]*

[SCRIPT SERVER] [*domain-name:directory-path*]
[*INTERNET-address:directory-path*]

[SERVICE GROUPS] [*group-list*] [DISABLED]
[ENABLED]*
[ALL] [DISABLED]
[ENABLED]*

[SESSION LIMIT] [*limit*]
[NONE]

[SNMP] [DISABLED]
[ENABLED]*

[SOFTWARE] [*filename*]

[TEXTPOOL SIZE] [*value*]

[TIME] [*hh:mm:ss*]

[TN3270] DEVICE "*new-device*" CREATE *existing-device*
PORT *port-number*

DEVICE *device-name* TERMINALTYPE "*termtype*"
TN3270TYPE *model*
KEYMAP *key* "*escape-seq*" "*description*"
SCREENMAP *action* "*escape-seq*"

TRANSLATIONTABLE *new-table* CREATE *existing-table*
TRANSLATIONTABLE *trans-name table offset value*

[TIMEZONE] *time*

[WELCOME] ["*message*"]

All DEFINE SERVICE and SET SERVICE commands require that the user be logged on to a privileged terminal. The basic syntax for the DEFINE SERVICE and SET SERVICE commands is:

[DEFINE] SERVICE [*service-name*] [*characteristic(s)*]
[SET]

The following list summarizes the service characteristics which can be defined:

[CONNECTIONS] [DISABLED]
[ENABLED]*

[IDENTIFICATION] [*identification-string*]

[PASSWORD] [*password*]

[PORTS] [*port-list*] [DISABLED]*
[ENABLED]
[ALL] [DISABLED]*
[ENABLED]

[QUEUE] [DISABLED]
[ENABLED]*

The following are miscellaneous DEFINE/SET commands (required privilege level shown).

(P) DEFINE [DOMAIN *domain-name INTERNET-address*]
SET

(P) DEFINE
SET PARAMETER SERVER *node-name* [ADDRESS *ethernet-address*]
[INTERNET ADDRESS *INTERNET-address*]

(P) SET [NOPRIVILEGED]

(S) SET [PRIVILEGED]

(S) SET SESSION [INTERACTIVE]*
[PASSALL]
[PASTHRU]

Service Management Commands

CLEAR SERVICES [*service-name*]
[LOCAL]

PURGE SERVICES [*service-name*]
[LOCAL]

REMOVE QUEUE [ENTRY *entry-number*]
[NODE *node-name*]
[SERVICE *service-name*]
[ALL]

Information Display Commands

SHOW DESTINATIONS
MONITOR

SHOW
MONITOR DOMAIN [*domain-name*] [ALL]
[LEARNED]
[LOCAL]

LIST DOMAIN [*domain-name*] [ALL]

SHOW
MONITOR NODES [*node-name*] [COUNTERS]
[STATUS]
[SUMMARY]
[ALL] [COUNTERS]
[STATUS]
[SUMMARY]

```
SHOW  PARAMETER SERVERS

MONITOR
LIST

SHOW
LIST
MONITOR   PORTS      [port-list]    [CHARACTERISTICS]
                                    [COUNTERS]
                                    [STATUS]
                                    [SUMMARY]
                                    [ALTERNATE CHARACTERISTICS]
                                    [TELNET CHARACTERISTICS]
                                    [INTERNET SECURITY]    [INBOUND]    [ALLOW]
                                                                        [DENY]
                                                           [OUTBOUND]   [ALLOW]
                                                                        [DENY]
                                                           [INTERNET-address]
                                    [KEYMAP]

                         [ALL]      [CHARACTERISTICS]
                                    [COUNTERS]
                                    [STATUS]
                                    [SUMMARY]
                                    [ALTERNATE CHARACTERISTICS]
                                    [TELNET CHARACTERISTICS]
                                    [INTERNET SECURITY]    [INBOUND]    [ALLOW]
                                                                        [DENY]
                                                           [OUTBOUND]   [ALLOW]
                                                                        [DENY]
                                                           [INTERNET-address]

                         [ACCESS]   [DYNAMIC]    [CHARACTERISTICS]
                                    [LOCAL]      [COUNTERS]
                                    [REMOTE]        [STATUS]
                                    [NONE]       [SUMMARY]
                                                 [ALTERNATE CHARACTERISTICS]
                                                 [TELNET CHARACTERISTICS]
                                                 [INTERNET SECURITY]  [INBOUND]  [ALLOW]
                                                                                 [DENY]
                                                                      [OUTBOUND] [ALLOW]
                                                                                 [DENY]
                                                                      [INTERNET-address]

SHOW
MONITOR QUEUE        [ALL]
                     [ENTRY entry-number]
                     [NODE node-name]
                     [PORT port-number]
                     [SERVICE service-name]
```

SHOW
MONITOR SERVER [ACCOUNTING]
[ALTERNATE STATUS]
[CHARACTERISTICS]
[COUNTERS]
[INTERNET CHARACTERISTICS]
[INTERNET COUNTERS]
[INTERNET ICMP COUNTERS]
[INTERNET SNMP CHARACTERISTICS]
[INTERNET SNMP COUNTERS]
[INTERNET TRANSLATION TABLE]
[KERBEROS]
[MENU]
[SCRIPT SERVER]
[STATUS]
[SUMMARY]
[INTERNET ROTARY]
[INTERNET ROUTES] [ALL]
[*destination*]
[*entry*]
[INTERNET SECURITY]

SHOW SERVER [TN3270]
[TN3270 DEVICE *device-name*]
[TN3270 TRANSLATIONTABLE *trans-name table]*

LIST SERVER [CHARACTERISTICS]
[INTERNET CHARACTERISTICS]
[MENU]
[SUMMARY]
[INTERNET ROTARY]
[INTERNET ROUTES] [ALL]
[*destination*]
[*entry*]
[INTERNET SECURITY]
[INTERNET SNMP CHARACTERISTICS]
[KERBEROS]
[SCRIPT SERVER]
[TN3270]
[TN3270 DEVICE *device-name*]
[TN3270 TRANSLATIONTABLE *trans-name table*]

SHOW SERVICE [*service-name*] [CHARACTERISTICS]
MONITOR [STATUS]
[SUMMARY]
[LOCAL] [CHARACTERISTICS]
[STATUS]
[SUMMARY]
[ALL] [CHARACTERISTICS]
[STATUS]
[SUMMARY]

LIST SERVICE [*service-name*] [CHARACTERISTICS]
[LOCAL] [CHARACTERISTICS]

SHOW
MONITOR SESSION [PORT *port-list*]
[ALL]

SHOW UNIT

SHOW
MONITOR USERS

ZERO COUNTERS [NODE *node-name*]
[PORT *port-list*]
[ALL]

Maintenance Commands

CHECK PARAMETER SERVER

CLEAR PARAMETER SERVER *node-name*

CRASH

INITIALIZE [SERVER] [DELAY] [*delay-time*] [OVERRIDE]
[CANCEL]

PURGE PARAMETER SERVER *node-name*

REMOTe Console [NODe *node-name*] [Maintenance [PASsword] *password*]
[*ethernet-address* [Maintenance [PASsword] *password*]

Test [INTERNET] [*domain-name*] [RECORDROUTE]
[NORECORDROUTE]*
[*INTERNET-address*] [RECORDROUTE]
[NORECORDROUTE]*

[LOOP] [*ethernet-address-t*] [Count *n*] [Width *n*] [Help Full Assistant] [*ethernet-address-h*]
[Help Receive Assistant] [*ethernet-address-h*]
[Help Transmit Assistant] [*ethernet-address-h*]

[Port] [*port-number*] [Count *n*] [Width *n*] [Loopback] [External]
[Internal]

[Service] [*service-name*] [NOde *node-name*] [Count *n*] [Width *n*] [Loopback] [External]
[Internal]

TELnet Console [*INTERNET-address*[:*telnet-port-number*]]
[*domain-name*[:*telnet-port-number*]]

Miscellaneous Commands

BRoadcast [[POrt] *port-list*] [*message*]
[ALL] [*message*]

CLEAR Domain [*domain-name*]
[ALL]
[Entry *entry-number*]
[LEarned]
[LOCal]

CLEAR SERVER INTERNET Route [*entry*]
[ALL]

CLEAR SERVER INTERNET Translation Table [*entry-number*]
[*entry-range*]
[ALL]

CLEAR SERVER MENu *item-number*

CLEAR INTERNET SECURITY *entry*
[ALL]

HELP [INTroduction]
[*topic(s)*]

PURGE DOMAIN [*domain-name*]
[ENTRY *entry-number*]
[ALL]

PURGE SERVER INTERNET ROUTE [*entry*]
[ALL]

PURGE INTERNET SECURITY [*entry]*
[ALL]

PURGE SERVER MENU *item-number*

UNIX Aliases

Xyplex Command	Unix Alias
SHOW PORT [*port-list*] STATUS	**STATUS [*port-list*]**
RESUME *session-number*	**FG *session-number***
HELP	**MAN**
SHOW SESSIONS	**JOBS**
SHOW USERS	**WHO**
TEST INTERNET *host* [RECORDROUTE] [NORECORDROUTE]	**PING *host* [RECORDROUTE] [NORECORDROUTE]**
DISCONNECT [*session*]	**CLOSE or KILL [*session*]**
TELNET CONNECT [*domain-name*] [*INTERNET-address*]	**OPEN [*domain-name*] [*INTERNET-address*]**
LOGOUT [*port-list*]	**QUIT [*port-list*]**

BACKWARDS

Select the next available, lower-numbered session

The BACKWARDS commands connects you from the current session to the next lower-numbered session.

Notes

Use the BACKWARDS command to select the next available, lower-numbered session to which your port or terminal is connected. (The unit assigns a session number for each session to which a port is connected.)

For purposes of the BACKWARDS command, the unit tracks session numbers in a "circular" manner. Therefore, when a port is already connected to the lowest numbered session, typing BACKWARDS connects the port to the highest numbered session. When only one session is active at a port, the BACKWARDS command re-connects the port to that session.

You can use the backward switch character, if one is defined for your port, instead of the BACKWARDS command.

Privileges

Secure.

Syntax

BACKWARDS

Options

None.

Products Supported

All terminal server serial ports, and gateway ports.

Examples

1. **This basic example shows how to use the BACKWARDS command to go from one session to the next lower numbered session. Suppose that there are two sessions running at a port, and the SHOW SESSION display for this port appears as shown in Figure 2-2.**

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 2
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Figure 2-2. Example SHOW SESSION Display.

As can be seen in Figure 2-2, the port is connected to two sessions, numbered 1 and 2. Session 2 is the currently active session. If, from the Xyplex> prompt, you type:

```
Xyplex> BACKWARDS
```

the terminal server will connect the port to session number 1 and display the message:

```
Xyplex -012- FINANCEVAX session 1 resumed
```

Figure 2-3 depicts the SHOW SESSION display after you issue the BACKWARDS command (current session number is changed).

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 1
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Figure 2-3. Example SHOW SESSION Display.

2. This example shows how to use the BACKWARDS command to connect to sessions from among three different sessions. Suppose that there are three sessions running at a port, and the SHOW SESSION display for this port appears as shown in Figure 2-3.

```
Xyplex> SHOW SESSIONS

Port 1:  J. Smith         Service Mode     Current Session 3
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
- Session 4: Connected    Interactive      LASER (LASER)
```

Figure 2-4. Example SHOW SESSION Display.

As can be seen in Figure 2-4, the port is connected to three sessions, numbered 1, 3 and 4. Session 3 is the currently active session. If, from the Xyplex> prompt, you type:

```
Xyplex> BACKWARDS
```

the unit will connect the port to session number 1, which is the next available lower numbered session. If you return to the Xyplex> prompt and again type:

```
Xyplex> BACKWARDS
```

the unit will connect the port to session number 4.

BROADCAST

Send a message to selected server port(s)

Use the BROADCAST command to send a text message to other ports.

Notes

Use the BROADCAST command to send a message to one or more specified ports or to all ports on the local terminal server. A number of conditions apply for the server and for the ports to which messages can be sent.

For the server, the BROADCAST command only works when the SERVER BROADCAST characteristic is set to ENABLED. (Refer to the DEFINE/SET SERVER BROADCAST command.)

For the port, broadcast messages can only be sent to ports which are logged on. The port cannot be locked (via the terminal server LOCK command). The port cannot be connected to a dedicated service. The port cannot be performing a MONITOR command. (You can use the SHOW PORT ALL command to determine if a port is available.)

Privileges:

Privileged users can broadcast a message to multiple ports or to all ports. Non-privileged users can broadcast a message to only one port at a time. The BROADCAST command is not available to secure users.

Syntax:

BROADCAST [[PORT] *port-list*] [*message*]
[ALL] [*message*]

Where	Means
PORT	**The message is to be broadcast only to the port(s) specified by the *port-list*.**
port-list	**The port(s) to which the message will be sent.**
ALL	**The message will be broadcast to all ports on the terminal server.**
message	**The text that will be displayed at the port(s) listed in the *port-list* or all ports. The message can be any length, as long as the entire command does not exceed 132 characters in length. You must enclose the message in quotation marks ("). You can include a bell character (CTRL-G) in the text message.**

Examples:

1. Xyplex>> BROADCAST ALL "PAB's going-away party at 1830 today."

   The user is broadcasting a message about a celebration to all users on the terminal server. This can only be done by a privileged terminal server user. The message will be displayed at all terminals exactly as it was typed. For example, the users at the receiving terminals might see a message such as:

   ```
   Xyplex -501- From port 1, Isaacs
         PAB's going-away party at 1830 today.
   ```

2. Xyplex> BROADCAST PORT 1 "^G Printer jammed, re-spool print job."

   The user is broadcasting a message to a specific user or terminal. Non-privileged users may broadcast a message in this manner. The user at the receiving terminal would hear a "beep" sound and see a message such as:

   ```
   Xyplex -501- From port 8, Mikey
         Printer jammed, re-spool print job.
   ```

CHECK PARAMETER SERVER

Force the server to locate parameter servers immediately.

Notes

Use the CHECK PARAMETER SERVER command to force the server to locate additional, eligible parameter servers (i.e., nodes where terminal server parameters can be stored). During normal operation, the server performs this action periodically to insure that a parameter server is available from which the server can obtain parameter information. (The frequency at which this occurs is defined by the SET PARAMETER SERVER CHECK TIMER characteristic. The maximum number of eligible parameter servers, about which the server retains information, is specified using the SET SERVER PARAMETER SERVER LIMIT characteristic.) The CHECK PARAMETER SERVER command requires that the server perform this search immediately, rather than wait for the check timer period to elapse. Note that, the server attempts to keep up to date the parameters stored at all eligible parameter servers.

The Console LED will flash whenever there are permanent parameters that have not yet been stored by at least one parameter server.

Privileges:

Privileged only.

Syntax:

CHECK PARAMETER SERVER

Example:

```
Xyplex>> CHECK PARAMETER SERVER
```

CLEAR DOMAIN

Remove domain-name entries from the operational database.

Notes

Use the CLEAR DOMAIN command to delete, from the operational database, one or more *domain-name* entries known by the server. The deleted *domain-name(s)* can be re-enabled using a SET DOMAIN command or "learned" from a Domain name server. If the *domain-name* is listed in the permanent database, it will again be made available when the server is re-initialized. (Refer also to the description of the PURGE DOMAIN command.)

If the specified *domain-name* is not a fully qualified *domain-name,* the specified name will be concatenated with the default Internet *domain-name-suffix*. The server will display an error message if you use the CLEAR DOMAIN command when the specified Domain name does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR DOMAIN [*domain-name*]
[ALL]
[ENTRY *entry-number*]
[LOCAL]

Where	Means
domain-name	**This specific *domain-name* which will not be available to server users, until the name is re-enabled with a SET DOMAIN command, supplied by a Domain name server, or the server is re-initialized (for *domain-names* that are contained in the permanent database).**
ALL	**All *domain-names* known to the server will no longer be available to server users, until the *domain-names* are re-enabled with a SET DOMAIN command, supplied by a Domain name server, or the server is re-initialized (for *domain-names* that are contained in the permanent database).**
ENTRY	**Specifies that you will identify, by *entry-number* shown in the SHOW/ MONITOR DOMAIN display, the *domain-name/internet-address* combination that will no longer be available to server users.**

Where	Means
entry-number	**The *domain-name* shown in the "Entry" column of the SHOW/MONITOR DOMAIN display, which represents a *domain-name/internet-address* combination that will no longer be available to server users.** **Note that the number of an entry in the operational database does not need to match the entry number in the permanent database. Therefore, if you want to CLEAR and PURGE a *domain-name*, you should make sure that you have selected the correct entry number.**
LEARNED	**All *domain-names* supplied by a Domain name server will no longer be available to server users, until the *domain-names* are re-enabled with a SET DOMAIN command, learned from a Domain name server, or the server is re-initialized (for *domain-names* that are contained in the permanent database).**
LOCAL	**All *domain-names* that have been locally defined at the server (e.g., *domain-names* specified using a SET DOMAIN command) will no longer be available to server users, until the *domain-name* is re-enabled with a SET DOMAIN command, learned from Domain name server, or the server is re-initialized (for *domain-names* that are contained in the permanent database).**

Examples:

1. `Xyplex> CLEAR DOMAIN FINANCESUN.XYPLEX.COM`

The *domain-name* FINANCESUN.XYPLEX.COM will be unavailable, until the server is re-initialized (for *domain-names* that are listed in the permanent database), the *domain-name* is relearned from a Domain name server, or the *domain-name* is re-enabled with a SET DOMAIN command.

2. `Xyplex>> CLEAR DOMAIN LOCAL`

Make all locally specified *domain-names* (e.g., those specified using a SET DOMAIN command) unavailable, until the server is re-initialized (for *domain-names* that are listed in the permanent database), the *domain-name* is relearned from a Domain name server, or each *domain-name* is individually re-enabled with a SET DOMAIN command.

3. `Xyplex>> CLEAR DOMAIN LEARNED`

Make unavailable all *domain-names* supplied by a Domain name server, until the server is re-initialized (for *domain-names* that are listed in the permanent database), the *domain-name* is relearned from a Domain name server, or each *domain-name* is individually re-enabled with a SET DOMAIN command.

4. `Xyplex>> CLEAR DOMAIN ENTRY 5`

Make unavailable to server users the *internet-address* that is associated with the *domain-name* shown in entry number 5 of the SHOW/MONITOR DOMAIN display.

CLEAR INTERNET SECURITY

Remove internet security entries from the operational database.

Notes

This command enables a system manager to remove one or all entries from the Internet Security table in the operational database. Once cleared, an entry can be respecified using the SET PORT INTERNET SECURITY command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized. (Also refer to the PURGE INTERNET SECURITY command, which is used to remove a security table entry from the permanent database.)

Refer to the *Software Management Guide* for a description of the Internet Security feature.

Examine the output of the SHOW/LIST PORT INTERNET SECURITY command to determine the entry number in the Internet Security table that you want to remove. Note that security entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE a security entry, you should make sure that you have selected the correct entry number.

The server will display an error message if the entry you specify does not exist.

The CLEAR INTERNET SECURITY command clears the security assignment (allow or deny access) for all ports in the *port-list*, for which the assignment was made. To disable Internet Security for a specific port, use the DISABLE option of the SET PORT INTERNET SECURITY command.

Privileges:

Privileged only.

Syntax:

CLEAR INTERNET SECURITY ***entry***
[ALL]

Where	Means
entry	**Corresponds to a number appearing in the Entry field of the SHOW/LIST PORT INTERNET SECURITY display.**
ALL	**Clears all entries in the Internet Security table.**

Example:

```
Xyplex>> CLEAR INTERNET SECURITY 3
```

Remove Entry 3 in the Internet Security table from the operational database.

CLEAR PARAMETER SERVER

Remove parameter server entries from the operational database.

Notes

Use the CLEAR PARAMETER SERVER command to remove temporarily a specific parameter server from the list of available parameter servers which the server will maintain. Typically, you would use this command to remove a parameter server from the list maintained by the server, when the parameter server is no longer available. Because the parameter server is removed from the list of eligible parameter servers, the server will not update the parameter settings that are stored at the parameter server as these settings are changed. You can use the SHOW PARAMETER SERVER command to determine if a particular node is currently a parameter server for the server.

Note that the server may return the removed parameter server back to the list of eligible parameter servers the next time it does a check for eligible parameter servers. (This occurs at the frequency specified by the SET PARAMETER SERVER CHECK characteristic, or when the server manager issues a CHECK PARAMETER SERVER command. Also, whether the deleted parameter server returns to the list of eligible parameter servers maintained by the server is subject to the limit defined by the SET SERVER PARAMETER SERVER LIMIT characteristic.) To remove a parameter server permanently from the list of eligible parameter servers maintained by the server, you must disable the parameter server software that is running at the node, remove the parameter server node from the DECnet network, or shut the node down.

For units which store parameters locally in Non-Volatile Storage (NVS), you cannot CLEAR the local paramter server.

Privileges:

Privileged only.

Syntax:

CLEAR PARAMETER SERVER *node-name*

Where	Means
node-name	**Specifies the name of a node, which is a parameter server where server parameters are stored, which is to be removed from the list of eligible parameter servers for the server.**

Example:

```
Xyplex>> CLEAR PARAMETER SERVER NETWORKVAX
```

CLEAR PORT INTERNET SECURITY

Remove internet security entries from the operational database.

Notes

Use the CLEAR PORT INTERNET SECURITY command to remove Internet security entries for one or more designated port(s) from the operational database.

This command removes all Internet security entries pertaining to the designated port(s) from the Internet Security table in the operational database. Once cleared, an operational database entry can be respecified using the SET PORT INTERNET SECURITY command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized.

Refer to the *Software Management Guide* for a description of the Internet Security feature.

Privileges:

Privileged only.

Syntax:

CLEAR PORT [*port-list*] INTERNET SECURITY
[ALL]

Where	Means
port-list	**One or more terminal server ports.**
ALL	**The command will apply to all ports on the server.**

Example:

```
Xyplex>> CLEAR PORT 4 INTERNET SECURITY
```

Remove all entries in the Internet Security table for port 4 from the operational database.

CLEAR SERVER INTERNET ROTARY

Remove internet rotary entries from the operational database.

Notes

Use the CLEAR SERVER INTERNET ROTARY command to delete, from the operational database, one or more internet rotaries entries known by the server. (A rotary is a group of ports on the server which are assigned the same internet-address.) If the rotary is listed in the permanent database, it will again be made available when the server is re-initialized. (Refer also to the description of the PURGE SERVER INTERNET ROTARY command.)

Examine the SHOW/MONITOR SERVER INTERNET ROTARY display to determine the entry number for a particular rotary in the operational database. Note that when you remove an internet rotary entry from the database, the remaining internet rotary entries in the database are not renumbered. Also, internet rotary entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE a rotary, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER INTERNET ROTARY command when the specified entry does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR SERVER INTERNET ROTARY [*entry*]
[ALL]

Where	Means
entry	**Specifies the entry number of the internet rotary which will not be available to server users, until the rotary is re-enabled with a SET SERVER INTERNET ROTARY command, or the server is re-initialized (for internet rotaries that are contained in the permanent database).**
ALL	**Specifies that all internet rotaries known to the server will no longer be available to server users, until the internet rotaries are re-enabled with a SET SERVER INTERNET ROTARY command, or the server is re-initialized (for internet rotaries that are contained in the permanent database).**

Examples:

1. `Xyplex>> CLEAR SERVER INTERNET ROTARY 1`

Make only internet rotary entry number 1 in the operational database (displayed in the SHOW/MONITOR SERVER INTERNET ROTARY display) unavailable, until the server is re-initialized (for internet rotaries that are listed in the permanent database), or the internet rotary is re-enabled with a SET SERVER INTERNET ROTARY command.

2. `Xyplex>> CLEAR SERVER INTERNET ROTARY ALL`

Make all internet rotaries in the operational database (e.g., those specified using a SET SERVER INTERNET ROTARY command) unavailable, until the server is re-initialized (for internet rotaries that are listed in the permanent database), or each internet rotary is individually re-enabled with a SET SERVER INTERNET ROTARY command.

CLEAR SERVER INTERNET ROUTE

Remove internet route entries from the operational database.

Notes

Use the CLEAR SERVER INTERNET ROUTE command to delete, from the operational database, one or more internet-routes entries known by the server. If the internet-route is listed in the permanent database, it will again be made available when the server is re-initialized. (Refer also to the description of the PURGE SERVER INTERNET ROUTE command.)

Examine the SHOW/MONITOR SERVER INTERNET ROUTE display to determine the entry number for a particular internet route in the operational database. Note that when you remove an internet route entry from the database, the remaining internet route entries in the database are not renumbered. Also, internet-route entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE an internet-route, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER INTERNET ROUTE command when the specified entry does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR SERVER INTERNET ROUTE [*entry*]
[ALL]

Where	Means
entry	**Specifies the entry number of the internet-route which will not be available to server users, until the route is re-enabled with a SET SERVER INTERNET ROUTE command, or the server is re-initialized (for internet-routes that are contained in the permanent database).**
ALL	**Specifies that all internet-routes known to the server will no longer be available to server users, until the internet-routes are re-enabled with a SET SERVER INTERNET ROUTE command, or the server is re-initialized (for internet-routes that are contained in the permanent database).**

Examples:

1. `Xyplex>> CLEAR SERVER INTERNET ROUTE 1`

   Make only internet-route entry number 1 in the operational database (displayed in the SHOW/MONITOR SERVER INTERNET ROUTE display) unavailable, until the server is re-initialized (for internet-routes that are listed in the permanent database), or the internet-route is re-enabled with a SET SERVER INTERNET ROUTE command.

2. `Xyplex>> CLEAR SERVER INTERNET ROUTE ALL`

   Make all internet-routes in the operational database (e.g., those specified using a SET SERVER INTERNET ROUTE command) unavailable, until the server is re-initialized (for internet-routes that are listed in the permanent database), or each internet-route is individually re-enabled with a SET SERVER INTERNET ROUTE command.

CLEAR SERVER INTERNET TRANSLATION TABLE

Remove ARP entries from the operational database.

Notes

In an Ethernet local area network, all packets are addressed to their destinations with an Ethernet address. Therefore, for an Internet network running over an Ethernet network, an Internet addresses must be translated to its corresponding Ethernet address. During the course of normal server operations, the server inquires from other hosts on the network about which Ethernet address corresponds to a given Internet address. As a unit acquires Internet-to-Ethernet address translations, it stores them in a table in the operational database. (This table is usually referred to as the ARP table.) The operational database of a unit that runs TCP/IP-LAT software can store up to 60 of the most recently used Internet-to-Ethernet address translations.

Use the CLEAR SERVER INTERNET TRANSLATION TABLE command to delete, from the operational database, one or more Internet-to-Ethernet address translation entries known by the unit. The translation will again be made available when it is relearned by the unit.

Examine the SHOW/MONITOR SERVER INTERNET TRANSLATION TABLE display to determine the entry number for a particular internet route in the operational database. Note that when you remove an entry from the database, the remaining entries in the database are not renumbered.

The unit displays an error message if you use the CLEAR SERVER INTERNET TRANSLATION TABLE command when the specified entry does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR SERVER INTERNET TRANSLATION TABLE [*entry-number*]
[*entry-range*]
[ALL]

Where	Means
entry-number	**Specifies the entry number, from the SHOW/MONITOR SERVER INTERNET TRANSLATION TABLE display, of the translation which will be removed from the operational database of the unit. The unit can relearn the translation.**
entry-range	**Specifies a list of two or more consecutive *entry-numbers*, from the SHOW/ MONITOR SERVER INTERNET TRANSLATION TABLE display, of the translation which will be removed from the operational database of the unit. The unit can relearn the translations.** **You can specify an *entry-range* by specifying a range of *entry-numbers* separated by a hyphen. For example, the *entry-list* 3-5 refers to the individual entries: 3, 4, and 5.**
ALL	**Specifies that all translations known to the unit will be removed from the operational database of the unit. The unit can relearn the translations.**

Examples:

1. `Xyplex>> CLEAR SERVER INTERNET TRANSLATION TABLE 1`

Remove only translation entry number 1 (displayed in the SHOW/ MONITOR SERVER INTERNET TRANSLATION TABLE display) from the operational database.

2. `Xyplex>> CLEAR SERVER INTERNET TRANSLATION TABLE ALL`

Remove all translations from the operational database

3. `Xyplex>> CLEAR SERVER INTERNET TRANSLATION TABLE 3-5`

Remove only the translation entries numbered 3, 4, and 5 (displayed in the SHOW/ MONITOR SERVER INTERNET TRANSLATION TABLE display) from the operational database.

CLEAR SERVER MENU

Remove menu entries from the operational database.

Notes

This command enables a system manager to remove an item on the server's menu from the operational database. Once cleared, the entry can be respecified using the SET SERVER MENU command. If the entry is present in the permanent database, it will appear in the operational database again when the server is re-initialized. (Also refer to the PURGE SERVER MENU command, which is used to remove a menu item from the permanent database.)

Refer to of the *Software Installation and Management Guide* for a description of the Simple Menu Interface feature.

Examine the output of the SHOW/LIST SERVER MENU command to determine the number of the entry you want to remove.

The server will display an error message if the entry you specify does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR SERVER MENU *item-number*

Where	Means
item-number	**Specifies the item number (1 - 20) within the menu that you want to clear.**

Example:

```
Xyplex>> CLEAR SERVER MENU 3
```

Remove the third item from the server's menu in the operational database.

CLEAR SERVER SCRIPT SERVER

Remove script server entries from the operational database.

Notes

Use the CLEAR SERVER SCRIPT SERVER command to delete, from the operational database, one or more script servers, where the server attempts to locate script files. If the script server is listed in the permanent database, it will again be made available when the server is re-initialized. (Refer also to the description of the PURGE SERVER SCRIPT SERVER command.)

Examine the SHOW/MONITOR SERVER SCRIPT SERVER display to determine the entry number for a particular script server in the operational database. Note that when you remove an script server entry from the database, the remaining script server entries in the database are not renumbered. Also, script server entries in the operational database do not need to match the entries in the permanent database. Therefore, if you want to CLEAR and PURGE an script server, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the CLEAR SERVER SCRIPT SERVER command when the specified entry does not exist.

Privileges:

Privileged only.

Syntax:

CLEAR SERVER SCRIPT SERVER **[*entry*]**
[ALL]

Where	Means
entry	**Specifies the entry number of the script server which will not be available, until the script server is re-specified with a SET SERVER SCRIPT SERVER command, or the server is re-initialized (for script servers that are contained in the permanent database).**
ALL	**Specifies that all script servers known to the server will no longer be available until the script servers are re-enabled with a SET SERVER SCRIPT SERVER command, or the server is re-initialized (for script servers that are contained in the permanent database).**

Examples:

1. `Xyplex>> CLEAR SERVER SCRIPT SERVER 1`

Make only script server entry number 1 in the operational database (displayed in the SHOW/MONITOR SERVER SCRIPT SERVER display) unavailable, until the server is re-initialized (for script servers that are listed in the permanent database), or the script server is re-specified with a SET SERVER SCRIPT SERVER command.

2. `Xyplex>> CLEAR SERVER SCRIPT SERVER ALL`

Make all script servers in the operational database (e.g., those specified using a SET SERVER SCRIPT SERVER command) unavailable, until the server is re-initialized (for script servers that are listed in the permanent database), or each script server is individually re-enabled with a SET SERVER SCRIPT SERVER command.

CLEAR SERVICES

Remove locally-offered LAT services from the operational database.

Notes

Use the CLEAR SERVICES command to delete, from the operational database, an entry for one or all of the LAT services offered locally at the server. The deleted service can be re-enabled using a SET SERVICE command. If the service is listed in the permanent database, the service will again be made available when the server is re-initialized. (Refer also to the description of the PURGE SERVICES command.)

The server will display an error message if you use the CLEAR SERVICES command when sessions are established with the service(s) to be deleted, when there are connection requests in the connection queue for the service(s), or when the specified service does not exist.

Privileges

Privileged only.

Syntax

CLEAR SERVICES [*service-name*]
[LOCAL]

Where	Means
service-name	**The name of the local LAT service (e.g., a service which is offered by the server) which will not be offered by the server, until the service is re-enabled with a SET SERVICE command or the server is re-initialized.**
LOCAL	**All local services (e.g., services which are offered by the server) will no longer be offered by the server, until the service is re-enabled with a SET SERVICE command or the server is re-initialized.**

Examples:

1. `Xyplex>> CLEAR SERVICES LOCAL`

Make all services on the server unavailable, until the next time the server is re-initialized (for services that are listed in the permanent database), or each service is individually re-enabled with a SET SERVICE command.

2. `Xyplex>> CLEAR SERVICES LASER`

Make unavailable the service named LASER, which is on the server, until the next time the server is re-initialized (for services that are listed in the permanent database), or the service is re-enabled with a SET SERVICE command.

CLEAR XPRINTER PORTS

Terminate Novell printing at one or more ports..

Notes

Use the CLEAR XPRINTER PORTS command to disconnect ports temporarily from the Novell print servers to which they are connected.

Privileges **Privileged**

Syntax:

CLEAR XPRINTER PORTS **[*port-list*]**
[ALL]

Where	**Means**
port-list	**Terminate Novell client printing at one or more terminal or Xyplex printer server ports.**
ALL	**Terminate Novell client printing at all ports which offer this service.**

Example

```
Xyplex>> CLEAR XPRINTER PORTS 1,3-5
```

CLEAR XPRINTER PSERVER

Terminate Novell printing by one or more Netware printer servers.

Notes

Use the CLEAR XPRINTER PSERVER command to remove temporarily a Novell printer server from the list of active print servers that the Xyplex unit maintains. Once per minute, an active Novell print server broadcasts a message on to the network to indicate that it is "alive." This means that the Xyplex unit will re-learn the print server until you also unload it from the NetWare file server or print server workstation.

Privileges **Privileged**

Syntax:

CLEAR XPRINTER PSERVER ***printer-serve***

Where	**Means**
port-list	**The name of a Novell NetWare printer server that is serviced by the Xyplex unit.**

Example

```
Xyplex>> CLEAR XPRINTER PSERVER LASER
```

CONNECT

Establish a session between your port and a LAT service or a Telnet destination.

Notes

You will use the CONNECT command to establish a session by creating a virtual connection between your port (terminal) and a LAT service that is offered at a service node, or a Telnet destination. Most users will use the CONNECT command to establish a session between the port they are logged on to and a host. When you use the CONNECT command, without specifying a *service-name*, the terminal server will attempt to establish a session with a LAT preferred service or with the preferred Telnet destination (domain-name or internet-address, and telnet-port-number), when any of these have been defined.

In networks where both LAT services and Telnet destinations exist, the terminal server will establish sessions between the port and the LAT service or Telnet destination based on the setting of the PORT RESOLVE SERVICE characteristic. If this characteristic is set to LAT, the terminal server will interpret all command qualifiers as applicable to LAT services. In this case, the terminal server will attempt to locate the service, specified by the *service-name*, among LAT service nodes. If the characteristic is set to Telnet, the terminal server will interpret all CONNECT command qualifiers as applicable to Telnet destinations. In this case, the terminal server will attempt to connect to a Telnet *domain-name/ internet-address* and *telnet-port-number*. If the characteristic is set to ANY, the terminal server will first attempt to connect to a LAT service, then to a Telnet *domain-name/internet-address* and *telnet-port-number*. (Regardless of the setting of the PORT RESOLVE SERVICE characteristic, you can require the terminal server to interpret CONNECT command qualifiers as applicable to either LAT or Telnet, by using the LAT or TELNET keyword. Refer to the descriptions of the LAT CONNECT and TELNET CONNECT commands).

Connections to a LAT service are also subject to the following conditions:

1. Both the port and the device offering the LAT service must have a matching group code.

2. When a service that is offered at a terminal server port is busy, additional connection requests are entered into a connection queue, if the SET SERVICE QUEUE characteristic is set to ENABLED.

LAT services can be offered at more than one LAT service node or port. The terminal server assumes that all services which have the same *service-name* are equivalent. Therefore, when a service is offered at more than one node or port, the terminal server will connect to the node or port which has the highest rating (the relative ability to support additional connections). CONNECT command options permit you to select the particular service node or port, where the service is offered, to which the terminal server will connect.

Privileges

Secure.

Syntax

CONNECT [[SERVICE] *service-name*] [NODE *node-name*] [DESTINATION *port-name*]
[*domain-name[:telnet-port-number*]]
[*internet-address[:telnet-port-number*]]

Where	Means
SERVICE	**An optional keyword that you can use when you provide a *service-name* to which the port will be connected.**
service-name	**Specifies the name of the LAT service to which the port will be connected.**
NODE	**Specifies that you will provide the name of the service node at which the service, specified by the *service-name*, is offered. You would use this keyword when a service is offered at more than one service node.**
node-name	**Specifies the LAT node which offers the service specified by the *service-name*.**
DESTINATION	**Specifies that you will provide the name of the terminal server port at which the service, specified by the *service-name*, is offered. You would use this keyword when a service is offered at more than one port.**
port-name	**Specifies the port on the terminal server which offers the service specified by the *service-name*.**
domain-name	**Specifies the logical name of the Telnet destination that will be the connection partner in a session with the port which you are logged on to. If the specified *domain-name* is not a fully qualified domain-name, the specified name will be concatenated with the default *Internet domain-name-suffix*.** **Note that the first time the server attempts to connect to any *domain-name* (following initialization), a connection takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.**
internet-address	**Specifies the location on the network of the Telnet destination that will be the connection partner in a session with the port which you are logged on to.**
:telnet-port-number	**Specifies the number of the target Internet protocol or physical port number that is used in the session between the port you are logged on to and the connection partner (i.e., host or terminal server). Note that the colon character (:) is required as syntax to separate the *telnet-port-number* from the *domain-name* or *internet-address*.**

Examples:

```
1.  Xyplex> CONNECT FINANCEVAX
```

Establish a session between this port and the LAT service named FINANCEVAX, or the Telnet destination (such as a host or terminal server) whose *domain-name* is FINANCEVAX. Note that the terminal server will interpret the name FINANCEVAX based on the setting of the PORT RESOLVE SERVICE characteristic. If the server attempts to resolve the name as a Telnet destination, the server can also append the default *domain-suffix* to the partial *domain-name* FINANCEVAX.

```
2.  Xyplex> CONNECT
```

Establish a session between this port and the preferred service that the user has defined for the port. The preferred service can be a LAT service or a Telnet destination. Unless the user defined the preferred service using the LAT or TELNET keyword, the terminal server will interpret the name of the preferred service based on the setting of the PORT RESOLVE SERVICE characteristic.

```
3.  Xyplex> CONNECT FINANCESUN.XYPLEX.COM
```

Establish a session between this port and the Telnet destination whose *domain-name* is FINANCESUN.XYPLEX.COM (This type of command is typical for establishing a Telnet session. The name FINANCESUN.XYPLEX.COM exceeds the 16 character limit for a LAT *service-name*.) Note that the user did not specify a *telnet-port-number*. The terminal server will use the default *telnet-port-number* (specified by the PORT TELNET DEFAULT PORT characteristic).

```
4.  Xyplex> CONNECT 128.10.2.30:23
```

Establish a session between this port and Telnet destination whose *internet-address* is 128.10.2.30. Note that the user specified a *telnet-port-number* (23 in this case).

```
5.  Xyplex> CONNECT FINANCEVAX NODE VAX1
```

Establish a session between the port and the LAT service named FINANCEVAX, which is offered at the node named VAX1.

```
6.  Xyplex> CONNECT LASER NODE MAX5000 DESTINATION PORT_2
```

Establish a session between the port and the LAT service named LASER, which is offered at terminal server port 2 on the node named MAX5000.

CONNECT PORT

Establish sessions between a port, other than the port you are logged on to, and a LAT service or Telnet destination.

Notes

Users at privileged ports can establish sessions between a port, other than the port they are logged on to, and a LAT service or Telnet destination. Use the CONNECT PORT command to establish a session by creating a virtual connection between a terminal server port, called the "target" port, and a LAT service or a Telnet destination, or another port on a terminal server. The target port is usually a port other than the port you are currently logged on to.

To use this command, you must specify the name of a LAT service or Telnet destination. This can be done either by the CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The target port cannot have a session in progress (you can terminate an active session using the DISCONNECT PORT or LOGOUT PORT command).

In networks where both LAT services and Telnet destinations exist, the terminal server will establish sessions between the port and the LAT service or Telnet destination based on the setting of the PORT RESOLVE SERVICE characteristic. If this characteristic is set to LAT, the terminal server will interpret all command qualifiers as applicable to LAT services. In this case, the terminal server will attempt to locate the service, specified by the *service-name*, among LAT service nodes. If the characteristic is set to Telnet, the terminal server will interpret all CONNECT command qualifiers as applicable to Telnet destinations. In this case, the terminal server will attempt to connect to a Telnet *domain-name/internet-address* and *telnet-port-number*. If the characteristic is set to ANY, the terminal server will first attempt to connect to a LAT service, then to a Telnet destination (*domain-name* or *internet-address* and *telnet-port-number*). Regardless of the setting of the PORT RESOLVE SERVICE characteristic, you can require the terminal server to interpret CONNECT command qualifiers as applicable to either LAT or Telnet, by using the LAT or TELNET keyword. Refer to the description of the LAT CONNECT and TELNET CONNECT commands, described in sections 2.14 and 2.25, respectively.

LAT services can be offered at more than one service node or port. The terminal server assumes that all services which have the same *service-name* are equivalent. Therefore, when a service is offered at more than one LAT service node or port, the terminal server will connect to the node or port which has the highest rating (the relative ability to support additional connections). CONNECT PORT command options permit you to select the particular service node or port, where the service is offered, to which the terminal server will connect.

Privileges

Privileged only.

CONNECT PORT

Syntax

CONNECT PORT ***port-number*** **[*service-name*] [NODE *node-name*] [DESTINATION *port-number*]**
[*domain-name[:telnet-port-number*]]
[*internet-address[:telnet-port-number*]]

Where	Means
PORT	**Specifies that you will connect a target port to a LAT service or Telnet *domain-name/internet-address* and *telnet-port-number*.**
port-number	**Specifies the number of the target terminal server port which will be connected to a LAT service or Telnet *domain-name/internet-address* and *telnet-port-number*.**
service-name	**Specifies the LAT service to which the target terminal server port, specified by the *port-number* is connected.**
NODE	**Specifies that you will designate a LAT node which offers the service specified by the *service-name*. You would use this keyword when there are multiple LAT service nodes which offer the service.**
node-name	**Specifies the LAT service node which offers the service specified by the *service-name*.**
DESTINATION	**Specifies that you will designate a terminal server port which offers the service specified by the *service-name*. You would use this keyword when there are multiple terminal server ports which offer the service.**
port-name	**Specifies the terminal server port which offers the service, specified by the *service-name*.**
domain-name	**Specifies the logical name of the Telnet destination that will be the connection partner in a session with the target port. If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*.** **Note that the first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.**
internet-address	**Specifies the location on the network of the Telnet destination that will be the connection partner in a session with the target port.**
:telnet-port-number	**Specifies the number of the target Internet protocol or physical port number that is used in the session between the target port and the connection partner. Note that the colon character (:) is required to separate the *telnet-port-number* from the *domain-name* or *internet-address*.**

Examples

```
1.  Xyplex>> CONNECT PORT 5 LASER
```

Establish a session between the target port (port 5) and the LAT service named LASER, or the Telnet destination whose *domain-name* is LASER. Note that the terminal server will interpret the name LASER based on the setting of the PORT RESOLVE SERVICE characteristic.

```
2.  Xyplex>> CONNECT PORT 5
```

Establish a session between the target port (port 5) and the dedicated or preferred service that the user has defined for the port. The dedicated or preferred service can be a LAT service or a Telnet destination. Unless the user defined the dedicated or preferred service using the LAT or TELNET keyword, the terminal server will interpret the name of the dedicated or preferred service based on the setting of the PORT RESOLVE SERVICE characteristic.

```
3.  Xyplex>> CONNECT PORT 5 FINANCESUN.XYPLEX.COM
```

Establish a session between the target port (port 5) and the Telnet destination whose *domain-name* is FINANCESUN.XYPLEX.COM (This type of command is typical for establishing a Telnet session. The name FINANCESUN.XYPLEX.COM exceeds the 16 character limit for a LAT service-name.) Note that the user did not specify a *telnet-port-number*. The terminal server will use the default *telnet-port-number* (defined by the PORT TELNET DEFAULT PORT characteristic).

```
4.  Xyplex>> CONNECT PORT 5 128.10.2.30:23
```

Establish a session between the target port (port 5) and the Telnet destination whose *internet-address* is 128.10.2.30. Note that the user specified a *telnet-port-number* (23 in this case).

```
5.  Xyplex>> CONNECT PORT 5 LASER NODE MAX5000 DESTINATION PORT_2
```

Establish a session between the target port (port 5) and the LAT service named LASER, which is offered at terminal server port 2 on node MAX5000.

CRASH

Cause the server to perform a crash dump procedure

Notes

Use the CRASH command to require the server to execute a "crash dump" procedure when a problem occurs. During a crash dump procedure, the server sends a copy of the contents of its memory to a "dump file" at the dump serverfor analysis (when the SERVER DUMP characteristic is set to ENABLED) by Xyplex Customer Support personnel, and then the server re-initializes (see the INITIALIZE command). When you use the CRASH command, users will not have access to the server until the server re-initializes (users will have to logon and re-connect).

Privileges

Privileged only.

Syntax

CRASH

Example

```
Xyplex>> CRASH
```

DEFINE Commands/SET Commands

Alter permanent or operational characteristics

You will use the terminal server DEFINE and SET commands to specify or change characteristics for domain-names, ports or terminals, servers, services, and user privilege levels. The DEFINE command changes these characteristics within the permanent database. The SET command changes these characteristics only for the operational database. Therefore, when you use the DEFINE command to specify parameters, the definitions do not take effect immediately, but are stored in the permanent database so they remain in effect whenever the terminal server is re-initialized. When you use the Set command, the permanent characteristics of the terminal server are not altered, and any parameters that have been defined via the SET command are not retained, whenever the terminal server is re-initialized. Changes can be made to take effect both immediately and on a permanent basis when the DEFINE/SET SERVER CHANGE characteristic is set to ENABLED.

DEFINE/SET DOMAIN Commands

Add domain-names to the permanent or operational database

Notes

Use the SET DOMAIN command to add *domain-name* entries to the operational database. Use the DEFINE DOMAIN command to add *domain-name* entries to the permanent database. *Domain-names* that are entered into the databases via a SET/DEFINE DOMAIN command are called locally defined *domain-names*. (Changes can be made to take effect both immediately and on a permanent basis when the DEFINE/SET SERVER CHANGE characteristic is set to ENABLED.)

***Domain-names* that are listed in the permanent database, are entered into the operational database whenever the terminal server is re-initialized. *Domain-names* that are listed in the permanent database remain until they are deleted by a PURGE DOMAIN command.**

In addition to the locally defined *domain-names*, the terminal server can use *domain-names* that it obtains from one or more Domain name servers in the network. These *domain-names* are only entered into the operational database. *Domain-names* that are entered into the databases via a Domain name server are called "learned" *domain-names*.

Each *domain-name* can be assigned up to 16 *internet-addresses* (this is called a rotary group). The operational database can contain a maximum of 100 *domain-name/internet address* combinations. (However, if you are using a Domain Name Server, you should not specify more than 99 *domain-name/internet address* combinations, or the server will not be able to learn any *domain-names*.)

Locally defined *domain-names* remain in the operational database until they are removed via a CLEAR DOMAIN command. The terminal server retains a learned *domain-name* in the operational database until:

- **it is removed via a CLEAR DOMAIN command, or**
- **the expiration of a period of time (time to live) that is assigned by the Domain name server. The TCP/IP-LAT software limits the time to live to the value specified by the SERVER INTERNET DOMAIN TTL characteristic, or**
- **the operational database contains the maximum number of *domain-names*, a user adds a new *domain-name* via a SET DOMAIN command, or the terminal server learns a new *domain-name* from a Domain name server. In this case, the terminal server replaces the oldest learned *domain-name* in the operational database with the new name.**

Refer to the *Software Management Guide* for information about setting up a server to perform domain name serving.

Privileges:

Privileged

Syntax:

[DEFINE] DOMAIN *domain-name internet-address*
[SET]

Where	Means
domain-name	**If the specified *domain-name* is not a fully qualified *domain-name,* the specified name will be concatenated with the default Internet *domain-name-suffix*.**
internet-address	**The internet-address of the *domain-name*.**

Examples:

```
1.  Xyplex>> DEFINE DOMAIN UNIXSUN.COM 192.112.119.210
```

Add the *domain-name* UNIXSUN.COM, with the internet-address 192.112.119.210, to the permanent database. This *domain-name* will remain in the permanent database until it is deleted with a PURGE DOMAIN command. The *domain-name* will become available whenever the terminal server is re-initialized.

```
2.  Xyplex>> SET DOMAIN FINANCESUN 192.112.119.200
```

Add the *domain-name* FINANCESUN, with the *internet-address* 192.112.119.200, to the operational database. This *domain-name* will remain in the operational database, until the terminal server is re-initialized, or it is deleted with a CLEAR DOMAIN command. Since the specified *domain-name* is not a fully qualified *domain-name,* the name will be concatenated with the default Internet *domain-suffix* to make a fully-qualified *domain-name*.

DEFINE/SET PORT - General Information

Alter permanent or operational port characteristics

Notes

The DEFINE PORT and SET PORT commands specify or modify port characteristics. Generally, port characteristics control communication between the server and the devices (e.g., terminals, modems, printers) which are connected to the server. Changes that are made using the SET PORT command take effect immediately. Changes made via the SET PORT command only remain in effect until the port is logged out. Changes that are made using the DEFINE PORT command take effect the next time the port is logged in, or when the server is re-initialized. Changes can be made to take effect both immediately and on a permanent basis when the SERVER CHANGE characteristic is set to ENABLED.

Some port characteristics can only be set by users at privileged ports (there is more information on this in the Syntax section below). Regardless of whether or not a command is available to non-privileged or secure users, only privileged users can specify characteristics for ports other than their own port. Secure users can only issue SET PORT commands.

Syntax:

The basic syntax for the DEFINE PORT and SET PORT commands is:

[DEFINE] PORT [*port-list*] [*characteristic(s)*]
[SET]

[DEFINE] PORT [ALL] [*characteristic(s)*]
[SET]

Where	**Means**
port-list	**One or more terminal server ports.**
ALL	**All ports on the server.**

As shown above, multiple port characteristics can be defined or set with a single command. When you specify more than one port characteristic with one command, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.) You can use the term "TERMINAL" interchangeably in place of the term "PORT."

You will find items which are common variables listed throughout this section. Refer to the section on Common Variables at the beginning of this chapter.

DEFINE/SET PORT ACCESS

Specify the type of access permitted for the device using the port(s)

Notes

Specifies the type of access permitted for the device using the port.

The following table lists the action that the software will take when you issue a SET PORT ACCESS command:

Current Setting	New Setting	Action
Local	None Dynamic or Remote	If port is not logged in, create a passive session.
Remote	Local or None Dynamic	If the port has a passive session, discard the session. If the port has a passive session, discard the session and create a new passive session.
Dynamic	Local or None Remote	If the port has a passive session, discard the session. If the port has a passive session, discard the session and create a new passive session.
None	Local Dynamic or Remote	Create a passive session.

A "passive session" means that the port is available to make a remote connection. For ports whose ACCESS characteristic is set to DYNAMIC, when a user auto-bauds the port, the passive session is discarded and the local connection is created.

If there is an active remote session in progress at a port, when the ACCESS characteristic is SET for that port, when the session is disconnected the value for the ACCESS characteristic will revert to the value defined in the permanent database. This operation is different on a DECserver Terminal Server.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **[ACCESS] [DYNAMIC]**
[LOCAL]*
[NONE]
[PRT3270]
[REMOTE]

Where	Means
Dynamic	**The port is accessible from either the local command mode or remotely by port number or by service name.**
Local	**The port is accessible only by the local command mode. This is the default.**
None	**The port is not accessible from either the local command mode, or remotely by port number or by service name.**
PRT3270	**The port will be the TN3270 print screen client for this server. The port must have a TN3270 device assigned for it, and for each user's port the TN3270 device definition or keymap must include a PRINT key definition. This keyword is only valid when the TN3270 feature is enabled on the server. For more information, refer to the *Software Management Guide*.**
Remote	**The device using the port is accessible only remotely by port number or by service name, when the device at the port is offered as a service. Typically, you would set the ACCESS characteristic to REMOTE when the device using the port is a line printer.**

Example

```
Xyplex>> DEFINE PORT ALL ACCESS DYNAMIC
```

The server manager is setting the ACCESS characteristic for all server ports. Notice that in order for the server manager to do this, the port must be privileged (as evidenced by the Xyplex>> prompt).

DEFINE/SET PORT AUTHORIZED GROUPS

Specify which LAT service groups are available at the port.

Notes

Specifies that you will set or change the groups to which the specified port(s) or all ports are authorized to have access. Each device (service node, terminal server, etc) in a LAT network is assigned one or more group codes (this includes both devices which offer services and those which do not offer services). At periodic intervals, each device that offers a service to the network broadcasts an announcement to indicate that the service is available and which group codes may have access to the service. Thus, the server manager can permit (authorize) or restrict access to services by selecting which group codes are enabled or disabled for various ports. Refer to the *Software Management Guide* for more information about authorized groups.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **[AUTHORIZED GROUPS]** [***group-list***] **[DISABLED] [ENABLED]**

Where Means

group-list **Valid values for *group-lists* are whole numbers in the range of 0 to 255. You can specify multiple groups in a *group-list* by specifying individual group numbers separated by commas, by specifying a range of group-numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the *group-list*: 1,23-25,48 refers to the individual groups: 1, 23, 24, 25, and 48.**

When you specify a *group-list*, without specifying the ENABLED or DISABLED keyword (see below), the specified *group-list* replaces the current list for the port(s). The default authorized groups are 0 ENABLED and 1 throught 255 DISABLED.

Disabled **The authorized groups, listed in the *group-list*, are removed from the list of groups available to the specified port(s) or all ports on the server.**

Enabled **Specifies that authorized groups, listed in the *group-list*, are added to the list of groups available to the specified port(s) or all ports on the server.**

Example

```
Xyplex>> DEFINE PORT 5 AUTHORIZED GROUPS 0-255 ENABLED
```

DEFINE/SET PORT AUTOBAUD

Specify whether or not the port will automatically match device characteristics.

Notes

The PORT AUTOBAUD characteristic specifies whether or not the port will determine the port speed, parity, and character size for the device connected to the port, and automatically set matching server port characteristics. The server uses the ASCII RETURN character to determine the port speed, parity, and character size. Normally, the user must press the RETURN key a few times until the server determines the port speed, parity, and character size, and begins a logon sequence.

The AUTOBAUD characteristic only applies at ports whose ACCESS characteristic is set to LOCAL, and whose CHARACTER SIZE characteristic is set to 8 when the PARITY characteristic is set to NONE, or whose CHARACTER SIZE characteristic is set to 7 when the PARITY characteristic is set to EVEN. (Until software loading has completed, terminal servers do not autobaud when the port is receives 7-bit characters with even parity from the device.)

The supported port speeds are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, and 38400 bits per second (baud). The device connected to the port must be set to one of these speeds. (Ports can not autobaud at port speeds above 38400 bps.

This characteristic does not apply to parallel ports.

For ports whose ACCESS characteristic is set to REMOTE or DYNAMIC and AUTOBAUD characteristic is set to ENABLED, when a remote connection is made from the port, the server will set the speed, character size, and parity to match the values set in the permanent database for that port.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **AUTOBAUD [DISABLED]**
[ENABLED]*

Where	Means
DISABLED	**The port will not determine the port speed, parity, and character size at port login, and the port will not automatically set matching terminal port characteristics. The port will expect that any connecting device will be operate at the settings that are stored in the permanent database.**
ENABLED	**The port will determine port speed, parity, and character size at port login, and the port will automatically set matching terminal port characteristics. This is the default setting for the AUTOBAUD characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 AUTOBAUD ENABLED
```

DEFINE/SET PORT AUTOCONNECT

Specify whether or not the port will automatically connect to a dedicated or a preferred service.

Notes

This characteristic has many uses. First, it specifies whether or not the port will automatically connect to either a dedicated service or a preferred service, when the user logs on to a port. This characteristic is automatically enabled for a port, when a dedicated service is defined for that port. However, this characteristic is not subsequently disabled when the dedicated service is deleted.

Second, this characteristic also specifies whether or not the port should attempt to re-connect a session when a connection failure occurs. Re-connection attempts occur at intervals specified by the SERVER KEEPALIVE TIMER characteristic (between 10 and 180 seconds), with a status message being given for each attempt, for ports which are not configured with a dedicated service (no messages are given for ports which are configured with a dedicated service). Re-connection attempts continue until a connection is made or the user terminates further attempts by entering the local command mode.

Finally, the characteristic is useful for controlling server activity when the port uses modem control signals (for example, a port connected to a dial-up line). To use this capability, the ACCESS characteristic must be set to LOCAL for the port, the MODEM CONTROL characteristic must be set to ENABLED, and the port must have a dedicated service defined for it. When the AUTOCONNECT characteristic is disabled, the server will automatically log out a port and disconnect the call when a session ends. When the AUTOCONNECT characteristic is enabled, the server will not log out the port when a session ends.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **[AUTOCONNECT] [DISABLED]***
[ENABLED]

Where	Means
DISABLED	**The port will not automatically connect to a preferred service when the port is logged on (characteristic is enabled when a dedicated service is defined), nor will it automatically attempt to re-connect a session when a connection failure occurs. This is the default .**
ENABLED	**The port will automatically connect to a dedicated or preferred service when the port is logged on, and it will automatically attempt to re-connect a session when a connection failure occurs.**

Example

```
Xyplex>> DEFINE PORT 5 AUTOCONNECT ENABLED
```

DEFINE/SET PORT AUTODEDICATED

Specify whether or not the unit will automatically log on the port and establish a connection to the dedicated service.

Notes

Specifies whether or not the unit will automatically log on the port and establish a connection to the dedicated service that is defined for the port (via the PORT DEDICATED SERVICE, LAT DEDICATED SERVICE, or TELNET DEDICATED SERVICE characteristics) when the unit is initialized or the port is logged out. (The effect of this characteristic is to bypass the login routine and connect the port directly to the dedicated service. If you log out the port, the unit logs on the port again and re-connects to the dedicated service.) If the PORT AUTOBAUD characteristic is set to ENABLED, the unit waits until the port is autobauded before the connection is made. This characteristic is particularly useful for ports which are connected to devices that are unable to send a character (such as a CR/LF) to initiate a session.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **[AUTODEDICATED] [DISABLED]* [ENABLED]**

Where	Means
DISABLED	**The unit will not automatically log on the port and establish a connection to the dedicated service that is defined for the port when the unit is initialized or the port is logged out This is the default.**
ENABLED	**The unit will automatically log on the port and establish a connection to the dedicated service that is defined for the port when the unit is initialized or the port is logged out.**

Example

```
Xyplex>> DEFINE PORT 5 AUTODEDICATED ENABLED
```

DEFINE/SET PORT AUTOPROMPT

Specify whether or not service node will initiate a login sequence

Notes

Specifies whether or not the port will automatically prompt the service node to initiate a system-specific login sequence (i.e., have the service node run its login routine) when a port connection is made. The service node must support this characteristic. This characteristic only applies to LAT sessions.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **AUTOPROMPT [DISABLED] [ENABLED]***

Where	Means
Disabled	**The server will not prompt the service node to initiate its login sequence. In this case, the user must initiate a login sequence (for example, by pressing the RETURN key).**
Enabled	**The server will prompt the service node to initiate its login sequence. This is the default setting for the AUTOPROMPT characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 AUTOPROMPT ENABLED
```

DEFINE/SET PORT BACKWARD SWITCH

Specify a character that allows a user to return to the previous session.

Notes

Specifies whether or not there will be a character that allows a user to return to the previous (lower-numbered) session, without returning to the local command mode.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **BACKWARD SWITCH [*character*]**
[NONE]*

Where	Means
character	**A keyboard character. Specifies the character that the user will type to return to the previous session. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the FORWARD SWITCH characteristic, the LOCAL SWITCH characteristic, or any Telnet command characters). If you do specify a CTRL character, when the user types the character, it will be displayed as ^<Key> (i.e., if the user types CTRL/B, the terminal will echo the characters: ^B).**
NONE	**There will not be a character that the user can type to return to the previous session (therefore, the user will need to return to the local command mode in order to return to the previous session). This command can be used to remove a previously-defined backward switch character. This is the default setting for the BACKWARD SWITCH characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 BACKWARD SWITCH ^B
```

DEFINE/SET PORT BREAK

Specify how the port will interpret a BREAK.

Notes

Use this command to specify the action that the port will take when the user presses the BREAK key.

If you send a break during a remote console session, from a Xyplex Terminal Server port whose PORT BREAK characteristic is set to REMOTE, you may observe unexpected behavior (for example, bad output). This can occur when you establish a remote console session with a Xyplex Terminal Server, a MAXserver Manager Card (MAXman), or a DECserver Terminal Server.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **BREAK [DISABLED]**
[LOCAL]*
[REMOTE]

Where	Means
Disabled	**The server will ignore the BREAK key.**
Local	**The server will return to the local command mode when the user presses the BREAK key. This is the default setting for the BREAK characteristic.**
Remote	**The server will send the break to the connection partner, when the user presses the BREAK key. (Note, in a Telnet session, if you want to use the BREAK key to generate the Telnet attention character, set the BREAK characteristic to REMOTE.)**

Example

```
Xyplex>> DEFINE PORT 5 BREAK LOCAL
```

DEFINE/SET PORT BROADCAST

Enable or disable the broadcasting of messages at server port(s)

Notes

Use this command to specify whether or not this port will display messages that are broadcast from other ports on this server.

Typically, you would permanently disable the display of messages for ports which are connected to devices such as printers, or temporarily disable the display of messages when you do not want to be disturbed by broadcasted messages.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **BROADCAST [DISABLED]**
[ENABLED]*

Where	Means
Disabled	**Specifies that this port will not display messages that are broadcast from other ports on this server.**
Enabled	**Specifies that this port will display messages that are broadcast from other ports on this server. This is the default.**

Example

```
Xyplex>> DEFINE PORT 5 BROADCAST DISABLED
```

DEFINE/SET PORT CHARACTER SIZE

Specify the number of bits per character for transmitted/received data characters

Notes

Use this command to specify the number of bits per character for data characters that are transmitted/received over the server serial interface (e.g., between the server and the device connected to the port).

This characteristic does not apply to parallel ports.

Privilege Level

Non- privileged.

Syntax

DEFINE/SET PORT ***port-list*** **CHARACTER SIZE [7]**
[8]*

Where	Means
7	**The port serial interface will transmit/receive data characters using a seven bits per character format.**
8	**The port serial interface will transmit/receive data characters using an eight bits per character format. This is the default .**

Example

```
Xyplex>> DEFINE PORT 5 CHARACTER SIZE 7
```

DEFINE/SET PORT CONNECTRESUME

Specify whether a CONNECT command can establish a new session to a destination, or resume an existing session with the destination.

Notes

Use this command to specify the manner in which the port will handle a connection attempt (e.g., a CONNECT command) to a destination, when a session with that destination already exists. Depending on the setting for this characteristic, the CONNECT command can either establish a new session to the destination, or resume an existing session with the destination.

Privilege Level

Non- privileged.

Syntax

DEFINE/SET PORT ***port-list*** **CONNECTRESUME [DISABLED]* [ENABLED]**

Where	Means
Disabled	**The port will allow the CONNECT command to establish a new session to a destination, rather than resume an existing session with the destination. This is the default setting.**
Enabled	**The port will allow the CONNECT command to resume an existing session with the specified destination, rather than establishing a new session to that destination.**

Example

```
Xyplex>> DEFINE PORT 5 CONNECTRESUME ENABLED
```

DEFINE/SET PORT DCD TIMEOUT

Specify the period of time that the DCD signal can be deasserted, before the software will disconnect the port.

Notes

Use this command to set or change the period of time that the DCD signal can be deasserted, before the software will disconnect the port. The value you set does not affect the requirement that the DCD signal be asserted by the device for at least two seconds, before modem control "handshaking" is considered to be established. This characteristic requires that the MODEM CONTROL characteristic is set to ENABLED.

This characteristic does not apply to parallel ports or serial ports which do not support modem control signals.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* DCD TIMEOUT *timer-value*

Where	Means
timer-value	**Specifies the the period of time that the DCD signal can be deasserted, before the software will disconnect the port. The range for this variable is between 0 and 10000 milliseconds (do not specify units), in increments of 100 milliseconds. Setting this value to 0 means that the port will deassert the DTR signal immediately after DCD was deasserted. The default value is 2000 milliseconds (2 seconds).**

Example

```
Xyplex>> DEFINE PORT 5 DCD TIMEOUT 200
```

DEFINE PORT DEDICATED SERVICE

Specify a permanent service assignment for a port.

Notes

Use this command to specify whether or not there will be a service to which the port is permanently assigned, or that there will be a change made to the current permanent service assignment for the port. The effect of this characteristic is to automatically connect the port to a dedicated service, whenever a user logs on to that port.

When a connection is attempted, the server will interpret the variable which follows this keyword as either a LAT *service-name* or as a Telnet destination (*domain-name* or *internet-address*), depending on the setting of the RESOLVE SERVICE characteristic. You can also specify the prefixes LAT or TELNET to require the server to interpret the variable as a LAT *service-name* or a Telnet destination. (Refer to the descriptions of the RESOLVE SERVICE, LAT DEDICATED SERVICE and TELNET DEDICATED SERVICE characteristics for more information.)

You can only use a DEFINE command to specify the PORT DEDICATED SERVICE characteristic

Privilege Level

Privileged.

Syntax

DEFINE PORT *port-list* DEDICATED SERVICE [*service-name*] [NODE] [*node-name*] [DESTINATION] [*port-name*] [NONE]*

[NONE]* [DESTINATION] [*port-name*] [NONE]*

[NONE]* [NODE] [*node-name*] [DESTINATION] [*port-name*] [NONE]*

[NONE]* [DESTINATION] [*port-name*] [NONE]*

[*domain-name*[:*telnet-port-number*]]
[*internet-address*[:*telnet-port-number*]]

Where	Means
service-name	**Specifies the name of a LAT service to which the port is permanently assigned.**
NODE	**Specifies that you will set or change the name of the service node on which the dedicated service is offered. (This keyword only applies to services that are offered on a LAT network.)**
node-name	**Specifies the name of the service node at which the dedicated service is offered.**
DESTINATION	**Specifies that you will set or change the name of the server port at which the dedicated service is offered. (This keyword only applies to services that are offered on a LAT network.)**
port-name	**Specifies the name of the server port at which the service, specified by the *service-name*, is offered.**
NONE	**Specifies that this port, all ports, or the ports listed in the *port-list* will not have a dedicated service, or that you wish to cancel a previously-defined dedicated service, service node, or destination server port setting. This is the default setting for the DEDICATED SERVICE, NODE, and DESTINATION characteristics.**
domain-name	**Specifies the logical name of the Telnet destination to which the port is permanently assigned. If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*.**
internet-address	**Specifies the identity or location on the network of the Telnet destination to which the port is permanently assigned.**
:telnet-port-number	**Specifies the number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port is permanently assigned. Note that the colon character (:) is required to separate the *telnet-port-number* from the *domain-name*.**

Example

```
Xyplex>> DEFINE PORT 5 DEDICATED SERVICE FINANCEVAX
```

DEFINE/SET PORT DEFAULT SESSION MODE

Specify the mode to which all sessions are initially set.

Notes

Use this command to specify the mode to which all sessions are initially set.

After an outbound Telnet session is formed from the server, if the remote partner attempts to negotiate the Telnet binary option, the server will use the value set for the PORT TELNET BINARY SESSION MODE to determine what mode to change to for the session.

When binary option negotiation is initiated from a remote host for an inbound Telnet session, the server will use the setting of the PORT TELNET BINARY SESSION MODE to determine what mode to use for the session.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **DEFAULT SESSION MODE** **[INTERACTIVE]***
[PASTHRU]
[PASSALL]
[TRANSPARENT]

Where	Means
INTERACTIVE	**The server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are enabled, and the server will not negotiate the Telnet binary option. This is the default for the DEFAULT SESSION MODE characteristic.**
PASTHRU	**The server will initially set all sessions so that all switching characters and Telnet command characters are interpreted as data, and the server will negotiate the Telnet binary option. Note that XON/XOFF flow control may still be used in this mode.**
PASSALL	**The server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are disabled, and the server will negotiate the Telnet binary option. Use this mode whenever full data transparency is required, but option negotiations are to be recognized.**
TRANSPARENT	**The server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, and Telnet command characters. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU. Transparent is invalid for LAT sessions for ports whose PORT ACCESS characteristic is REMOTE or DYNAMIC. Use this mode whenever full data transparency is required, but no option negotiations are to be recognized.**

Example

```
Xyplex>> DEFINE PORT 5 DEFAULT SESSION MODE PASSALL
```

DEFINE/SET PORT DIALBACK

Specify whether or not the port requires a dialback script in order to be logged in

Notes

Use this command to specify whether or not the port requires a dialback script in order to be logged in. The dialback script contains commands that cause a modem to dial a designated telephone number. Refer to the *Software Management Guide* for a description of the dialback feature.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **DIALBACK [DISABLED]***
[ENABLED]
[TIMEOUT ***time*****]**

Where	Means
DISABLED	**The port does not require a dialback script in order to be logged in. This is the default.**
ENABLED	**Specifies the the port requires a dialback script in order to be logged in.**
TIMEOUT	**Specifies that you will change the amount of time that the remote modem (the modem being called) has to answer a dialback call.**
time	**Specifies the amount of time that the remote modem (the modem being called) has to answer a dialback call. The range for this variable is between 5 and 60 seconds (do not specify units). The default value is 20.**

Example

```
Xyplex>> DEFINE PORT 5 DIALBACK TIMEOUT 10
```

DEFINE/SET PORT DIALUP

Specify to service nodes whether or not the port is considered to be connected to a dial-up line.

Notes

Use this command to specify to service nodes whether or not the port is considered to be connected to a dial-up line. When a service node receives a connection request, the node may accept or reject the request based on the setting of the DIALUP characteristic.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **DIALUP** **[DISABLED]***
[ENABLED]

Where	Means
Disabled	**The port is not connected to a dial-up line. This is the default setting for the DIALUP characteristic.**
Enabled	**The port is connected to a dial-up line.**

Example

```
Xyplex>> DEFINE PORT 5 DIALUP ENABLED
```

DEFINE/SET PORT DSRLOGOUT

Specify whether or not the server should log out a port when the DCD signal is deasserted

Notes

Use this command to specify whether or not the server should log out a port when the DCD signal is deasserted. The DSRLOGOUT characteristic only applies for ports on which the MODEM CONTROL characteristic is set to DISABLED.

Refer to the chapter on setting up modems in the *Software Management Guide* for more information.

This characteristic does not apply to parallel ports.

Privilege Level Privileged.

Syntax

DEFINE/SET PORT *port-list* DSRLOGOUT [DISABLED]*
[ENABLED]

Where	Means
Disabled	**Do not logout the port when the serial interface DCD signal is lost. This is the default setting for the DSRLOGOUT characteristic.**
Enabled	**Logout the port when the serial interface DCD signal is lost.**

Example

```
Xyplex>> DEFINE PORT 5 DSRLOGOUT ENABLED
```

DEFINE/SET PORT DSRWAIT

Specify whether or not the server should begin the login sequence when the device asserts the DCD signal.

Notes

Use this command to specify whether or not the server should begin the login sequence when the device asserts the DCD signal.

Refer to the chapter on setting up modems in the *Software Management Guide* for more information.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* DSRWAIT [DISABLED]*
[ENABLED]

Where	Means
Disabled	**The server should not begin the login sequence when the device asserts the DCD signal. This is the default.**
Enabled	**The server should begin the login sequence when the device asserts the DCD signal. This characteristic requires that the ACCESS characteristic be set to LOCAL or DYNAMIC and the MODEM CONTROL characteristic be set to ENABLED.**

Example

```
Xyplex>> DEFINE PORT 5 DSRWAIT ENABLED
```

DEFINE/SET PORT DTRWAIT

Specify when the port should assert the DTR signal

Notes

Use this command to specify the conditions in which the server port should assert the DTR modem control signal line. This characteristic requires that the MODEM CONTROL characteristic is set to ENABLED.

Refer to the chapter on setting up modems in the *Software Management Guide* for more information.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* DTRWAIT [DISABLED]*
[ENABLED]
[FORCONNECTION]
[FORRING]

Where	Means
Disabled	**The port will continuously assert the DTR signal. This is the default setting for the DTRwait characteristic.** **For ports for which the PORT ACCESS characteristic is set to REMOTE and the DTRWAIT characteristic is set to DISABLED, the server does not wait for the device to assert the DCD signal before accepting data. If the PORT ACCESS characteristic is set to DYNAMIC with the DTRWAIT characteristic set to DISABLED, assertion of the DCD signal by the device will cause the port to accept local connections only. (In some prior releases, this was an invalid combination of PORT characteristics.)**
Enabled	**The port will assert the DTR signal when a remote connection is made, or when the device connected to the port (e.g., the modem) asserts the RING signal.**
FORCONNECTION	**The port will assert the DTR signal when a connection is made.**
FORRING	**The port will assert the DTR signal when the device connected to the port asserts the RING signal.**

Example

```
Xyplex>> DEFINE PORT 5 DTRWAIT ENABLED
```

DEFINE/SET PORT FLOW CONTROL

Specify the type of flow control used by a port

Notes

Use this command to specify the type of flow control ("handshaking") that is used by the serial interface of the specified port(s). Xyplex units supports two flow control methods: XON/XOFF and DCD/DTR. (DCD/DTR flow control is used to emulate either the RTS/CTS or DTR/DSR flow control method.

Units which use 6 or 8 wire serial port cabling support the use of RTS/CTS or DTR/DSR flow control. Units which use 8 wire serial port cabling support the concurrent use of hardware flow control (RTS/CTS or DTR/DSR flow control) and modem control. Units which use 3 wire cabling do not support the use of hardware flow control. Refer to the *Hardware* documentation or *Getting Started Guide* supplied with your unit for a description of associated cabling issues.

Refer to the description of flow control issues in the *Software Management Guide* for more information.

This characteristic does not apply to parallel ports.

Privilege Level

Non- privileged.

Syntax

DEFINE/SET PORT *port-list* FLOW CONTROL [CTS]
[DISABLED]
[DSR]
[ENABLED]
[XON]*

Where	Means
CTS	**The port(s) will use the DCD and DTR modem control signals to provide flow control. (In this case, the DCD and DTR signals are used to emulate RTS/CTS flow control.)**
DISABLED	**The server will not use any flow control methods for the specified port(s).**
DSR	**The server will use the DCD and DTR modem control signals to provide flow control. (In this case, the DCD and DTR signals are being used to emulate DTR/DSR flow control.)**
ENABLED	**The server will use flow control for the specified port(s).**
XON	**The server will use XON/XOFF flow control for the specified port(s). This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 FLOW CONTROL CTS
```

DEFINE/SET PORT FORWARD SWITCH

Specify a character that allows a user to switch to the next higher-numbered session

Notes

Use this command to specify whether or not there will be a character that allows a user to switch to the next (higher-numbered) session, without returning to the local command mode.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **FORWARD SWITCH** **[*character*] [NONE]***

Where	Means
character	**The keyboard character that the user will type to switch to the next session. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the BACKWARD SWITCH characteristic, the LOCAL SWITCH characteristic, or any Telnet command characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).**
NONE	**There will not be a forwards character, and that the user will need to return to the local command mode in order to switch to the next session. This command can be used to remove a previously-defined forwards character. This is the default setting for the FORWARD SWITCH characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 FORWARD SWITCH ^K
```

DEFINE PORT FROM PORT

Copy permanent port characteristics from one port to another port on the same unit

Notes

Use this command to copy the permanent characteristics of one port, except the PORT NAME characteristic, to one or more other ports on the same unit.

This characteristic can only be used with a DEFINE command.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **FROM PORT** ***port-number***

Where	Means
port-number	**The port whose permanent characteristics, except the PORT NAME characteristic, are to be copied to the ports specified by the *port-list*.**

Example

```
Xyplex>> DEFINE PORT 5
```

SET PORT GROUPS

Specify which LAT services will be included in displays shown at your port,

Notes

Use this command to specify which LAT services, represented by groups, which will be included in server displays shown at your port, the ports listed in the *port-list*, or all ports.

This keyword is only available as a SET command.

The GROUPS characteristic is provided as a convenience which permits users to restrict the number of services shown in various server displays. Rather than seeing a lengthy display, users can limit the services shown to those which they use frequently.

Privilege Level

Non- privileged.

Syntax

SET PORT *port-list* GROUPS	**[*group-list*]**	**[DISABLED]**
		[ENABLED]
	[ALL]	**[DISABLED]**
		[ENABLED]

Where	Means
group-list	**Valid values for *group-lists* are whole numbers in the range of 0 to 255. You can specify multiple groups in a *group-list* by specifying individual group numbers separated by commas, by specifying a range of group-numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the *group-list*: 1,23-25,48 refers to the individual groups: 1, 23, 24, 25, and 48.** **When you specify a *group-list*, without specifying the ENABLED or DISABLED keyword (see below), the specified *group-list* replaces the current list for the port(s). The default authorized groups are 0 ENABLED and 1 throught 255 DISABLED.** **Note that the groups, listed in this *group-list*, must be a subset of the groups to which the port is permitted to have access by the AUTHORIZED GROUPS characteristic.**
ALL	**Specifies that access to all authorized groups will be enabled or disabled. This keyword can be used to cancel the changes to the group list and revert to the list of authorized groups specified by the AUTHORIZED GROUPS characteristic.**
DISABLED	**The services, represented by the groups listed in the group-list, will not be included in server displays shown at your port, the specified ports, or all ports on the server. (However, the port can still connect to these services as long as it is permitted to do so based on the setting of the AUTHORIZED GROUPS characteristic.)**
ENABLED	**The services, represented by the groups listed in the group-list, will be included in server displays shown at your port, the specified port(s), or all ports on the server. (However, the port can only display information about these services as long as it is permitted to do so based on the setting of the AUTHORIZED GROUPS characteristic.)** **Note that the group-list, included when the GROUPS characteristic is ENABLED, must be a subset of the groups to which the port is permitted access based on the setting of the AUTHORIZED GROUPS characteristic. The access to groups permitted by the AUTHORIZED GROUPS characteristic still applies when the user specifies ALL in place of a group-list.**

Example

```
Xyplex>> SET PORT 5 GROUPS 1,23-25,48
```

DEFINE/SET PORT IDLE TIMEOUT

Specify an idle timer to prevent "hung" ports

Notes

Specifies that you will define or change the period of time after which an inactive session (for example, a queued connection request or a session initiated by a user) will be disconnected. For ports which have a connection queue, after the session is disconnected, the port is free to accept the next connection request in the connection queue. Typically, this characteristic is used to prevent a "hung" port (for example, a hung printer).

For ports which do not have a connection queue, after the sessions have been disconnected, the software will also begin the inactivity timer (controlled by the SERVER INACTIVITY TIMER characteristic) at the port. When there have been no sessions at the port, for the period of time specified by the SERVER INACTIVITY TIMER characteristic, the user will be logged off of the server port.

This characteristic is not supported for MX-TSERV-J8 terminal server cards.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* IDLE TIMEOUT *time*

Where	Means
time	**Specifies the length of time after which an inactive session, that was the result of a queued connection request, will be disconnected. The range for this variable is between 0 and 480 minutes (do not specify units). Setting this value to 0 means that the session will not be disconnected for being inactive. The default value is 0**

Example

```
Xyplex>> DEFINE PORT 5 IDLE TIMEOUT 10
```

DEFINE/SET PORT INACTIVITY LOGOUT

Specify whether or not inactive ports are logged out

Notes

Use this command to specify whether or not the server will logout a port after a specified period of inactivity has elapsed. Ports are considered to be inactive while they are in local command mode, do not have any sessions established, and there have been no input, output, or modem signal transitions. The DEFINE/SET SERVER INACTIVITY TIMER command specifies the length of the period of inactivity for this characteristic.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **INACTIVITY LOGOUT** **[DISABLED]*** **[ENABLED]**

Where	Means
Disabled	**The server will not logout a port after a specified period of inactivity has elapsed. This is the default setting for the INACTIVITY LOGOUT characteristic.**
Enabled	**The server will logout a port after a specified period of inactivity has elapsed.**

Example

```
Xyplex>> DEFINE PORT 5 INACTIVITY LOGOUT ENABLED
```

DEFINE/SET PORT INPUT FLOW CONTROL

Specify whether or not flow control is used for data input at the port

Notes

Use this command to specify whether or not flow control will be used for input data communications at the port (i.e., data communication which originates at the device connected to the port and which is received by the server). The flow control method used by the port (e.g., XON/XOFF, DCD/DTR, etc) is specified by the PORT FLOW CONTROL characteristic.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **INPUT FLOW CONTROL [DISABLED] [ENABLED]***

Where	Means
Disabled	**The port will not use flow control for input data communications.**
Enabled	**The port will use flow control for input data communications. This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 INPUT FLOW CONTROL ENABLED
```

DEFINE/SET PORT INTERNET CONNECTIONS

Specify if the port can accept an *internet-address* in order to connect to a TCP/IP destination

Notes

Use this command to specify whether or not the port will be able to accept an *internet-address* in order to connect to a TCP/IP destination, or whether all TCP/IP destinations must be specified using the *domain-name* format. This characteristic applies to all connections made via the CONNECT, TELNET CONNECT, RLOGIN, and TELNET CONSOLE commands.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* INTERNET CONNECTIONS [DISABLED] [ENABLED]*

Where	Means
Disabled	**The port will not be able to accept an *internet-address* in order to connect to a TCP/IP destination. All TCP/IP destinations must be specified using the *domain-name* format.**
Enabled	**The port will be able to accept an *internet-address*, as well as addresses using the *domain-name* format, in order to connect to a TCP/IP destination. This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 INTERNET CONNECTIONS ENABLED
```

DEFINE/SET PORT INTERNET SECURITY

Specify whether connections to or from port(s) are allowed or denied.

Notes

The Internet Security feature enables a system manager to build a table of networks, subnets, and nodes that are either allowed or denied a Telnet connection to specified ports. Also enables a system manager to either restrict specific ports from connecting to an Internet address, or to allow connections.

Refer to the *Software Management Guide* for a description of the Internet Security feature.

When you specify ALL ports for a security table entry, the entry does not apply to port 0 (the console port). To define/set security for Port 0, include the port in a port list (e.g., 0 - 16) or individually specify entries for Port 0.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **INTERNET SECURITY** **[INBOUND ALLOW]** ***internet-address*** **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[INBOUND DENY]*internet-address* **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[OUTBOUND ALLOW] ***internet-address*** **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[OUTBOUND DENY]*internet-address* **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]

SET PORT ***port-list*** **INTERNET SECURITY** **[INBOUND ALLOW]** ***internet-address*** **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[INBOUND DENY]*internet-address* **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[OUTBOUND ALLOW] ***internet-address*** **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]
[OUTBOUND DENY]*internet-address* **[MASk** ***security-mask*****]** **[ENABLED]**
[DISABLED]

DEFINE PORT ***port-list*** **INTERNET SECURITY** **[DEFAULT]** **[INBOUND]** **[ALLOW]***
[DENY]
[OUTBOUND] **[ALLOW]***
[DENY]

Where	Means
INBOUND	**The security table entry pertains to inbound connections (i.e., a connection initiated from the device connected to the port).**
OUTBOUND	**The security table entry pertains to outbound connections (i.e., a connection initiated by another device on the network; for example, a host-initiated connection).**
ALLOW	**The server should allow connections from or to the specified internet address.**
DENY	**The server should not allow connections from or to the specified internet address.**
internet-address	**The internet address to which connections are allowed or denied.**
MASK	**Indicates that a network security mask follows.**
security-mask	**Specifies how much of the internet address to use. If you do not specify a security mask for an Inbound entry, a network-specific mask will be used. If you specify neither ENABLED nor DISABLED for this characteristic, and a matching security entry exists, the *port-list* in the command will overwrite the *port-list* in the existing entry.**
ENABLED	**Add the port(s) to the existing *port-list* if a matching entry already exists in the Internet Security table.**
DISABLED	**Remove the port(s) from the *port-list* if a matching entry exists.**
DEFAULT	**Specifies whether the server default for inbound or outbound connections is to allow or deny connections from or to the specified Internet address.**
INBOUND	**The default pertains to inbound connections (i.e., a connection initiated by another device on the network; for example, a host-initiated connection).**
OUTBOUND	**The default pertains to outbound connections (i.e., a connection initiated from the device connected to the port).**
ALLOW	**The default for inbound or outbound connections is to allow connections from or to the specified Internet address. This is the default for the INTERNET SECURITY DEFAULT characteristic.**
DENY	**The default for inbound or outbound connections is to not allow connections from or to the specified Internet address.**

Examples

1.
```
Xyplex>> DEFINE PORT 1 INTERNET SECURITY OUTBOUND ALLOW 192.12.119.1 MASK 255.255.255.0 ENABLED
```

Allow outbound connections via Port 1 to any Internet address of the form 192.12.119.n.

2.
```
Xyplex>> DEFINE PORT 2 INTERNET SECURITY INBOUND DENY 192.19.112.1 MASK 255.255.0.0 ENABLED
```

Do not allow inbound connections to Port 2 for all Internet addresses of the form 192.19.n.n.

DEFINE/SET PORT INTERNET SLIP

Enable or disable SLIP at a port

Notes

Use this command to enable or disable Serial Line Internet Protocol (SLIP) for specific ports.

Refer to the *Software Management Guide* for a description of the SLIP feature.

This characteristic does not apply to parallel ports.

After a port has been logged on and SLIP has been enabled for the port, SLIP cannot be disabled from the same port (because the port expects all input to be in SLIP packets). To disable SLIP for a port that has been logged on, the port must be logged out from a different port.

You can only SET the INTERNET SLIP characteristic to ENABLED for your own port. To enable SLIP for other ports requires a DEFINE command. To disable SLIP for other ports requires a DEFINE command.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **INTERNET SLIP** **[ENABLED]**
[DISABLED]**
[ADDRESS ***port-address*****] [REMOTE** ***remote-address*** **MASK** ***network-mask*****]**

Where	Means
ENABLED	**Enables SLIP for the specified port or *port-list*.**
DISABLED	**Disables SLIP for the specified port. To use this keyword, you must use a DEFINE command. This is the default setting.**
ADDRESS	**Assign a specific internet-address to port.** **If you enable SLIP without setting the port's internet address, the server will obtain the internet address when it receives its first packet from the remote server. No users on the network will be able to initiate a connection with the remote server until the server receives at least one packet from the remote server.**
port-address	**Specifies the Internet address you are assigning to the server port.**
REMOTE	**Specifies that a remote Internet address follows.**
remote-address	**Specifies the remote Internet address to which the *port-address* corresponds. (When this address is on a different network, you define this correlation in the server's static routing table; e.g., using the DEFINE SERVER INTERNET ROUTE command.)**
MASK	**Specifies that a network mask, corresponding to the *remote-address*, follows.**
network-mask	**Specifies how much of the remote Internet address to use.**

Examples

```
Xyplex>> SET PORT INTERNET SLIP ENABLED
```

Enables SLIP for the port.

```
Xyplex>> DEFINE PORT INTERNET SLIP ADDRESS 192.12.119.72 REMOTE 192.12.130.1 MASK 255.255.255.0
```

Assigns the Internet address 192.12.119.72 to the server port. This port is used for communications via SLIP to Internet addresses of the form 192.12.130.n.

DEFINE/SET PORT INTERNET TCP KEEPALIVE TIMER

Enable or Disable the TCP keepalive timer

Notes

You can specify a TCP keepalive timer, which functions like the LAT keepalive timer. When this feature is enabled, the terminal server periodically transmits a null message to the partner of a session. If the Telnet partner does not respond during the length of time you specify, the terminal server disconnects the session.

You assign the the keepalive timer to one or more ports. The value you set for the PORT INTERNET TCP KEEPALIVE characteristic also specifies the frequency at which the server will attempt to reconnect a session when there is a connection failure, for ports at which the AUTOCONNECT characteristic is set to ENABLED. The value of the TCP keepalive timer appears on the SHOW/LIST PORTS ALTERNATE CHARACTERISTICS display.

As you increase the size of the *timer-value*, you will lengthen the time for other nodes to determine when the server goes down. However, as you decrease the size of this value, you increase the amount of network traffic.

You can not change the value for the PORT INTERNET TCP KEEPALIVE TIMER characteristic while there are any active sessions on the server.

Privilege Level

Privileged

Syntax

DEFINE/SET PORTS *port-list* INTERNET TCP KEEPALIVE TIMER *timer-value*

Where	Means
INTERNET TCP KEEPALIVE TIMER	**Specifies that you will define or change the length of time at which the server will transmit a null message to the Telnet partner, when there is no other traffic originating at the server to the partner. The purpose of sending the null message is to notify circuit partner(s) that the server is still active.**
timer-value	**The number of minutes that the terminal server will wait for a response from the Telnet partner before terminating the session. Valid values are the whole numbers 0 through 30. The default is 0, which specifies no keepalive timer.**

Example

```
Xyplex>> DEFINE PORT 5 INTERNET TCP KEEPALIVE TIMER 20
```

DEFINE/SET PORT INTERNET TCP WINDOW SIZE

Specify the size of the TCP window to be used by a TCP/IP session

Notes

A typical TCP/IP session requires about [1600 + (3 * *TCP_window_size*)] bytes. The window size used for a session is that which is in effect when the session starts. You use this command to specify the size of the TCP window to be used by a TCP/IP session.

If you connect a printer to a serial port, and the printer's performance appears to be slow, you might need to increase the TCP window size for that port.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* INTERNET TCP WINDOW SIZE *tcp-window-size*

Where	Means
tcp-window-size	**Specifies the size of TCP window. Valid values for size are whole numbers between 64 and 8192. The default value is 256. If one uses a window size greater than 256 (the default), one may not have sufficient memory for the usual number of sessions on the device.**

Example

```
Xyplex>> DEFINE PORT 5 INTERNET TCP WINDOW SIZE 512
```

DEFINE/SET PORT INTERRUPTS

Specify whether a local user can interrupt a remote session

Notes

Use this command to specify whether a local user can interrupt a remote session at a port, by entering the local switch (or BREAK) character. When the remote session is interrupted, the port will enter the local command mode. (The remote session can be resumed using the local command mode RESUME command.)

An example of this occurs when a port is connected to a hard-copy terminal, which has been set up to accept print jobs that are initiated from elsewhere on the network. The setting for this characteristic determines whether or not a user can interrupt a session, in this case another user's print job, by typing the local switch character or pressing the BREAK key at the hard-copy terminal.

This characteristic only applies if the DEFINE/SET PORT ACCESS characteristic for the port is set to DYNAMIC.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **INTERRUPTS** **[DISABLED]***
[ENABLED]

Where	Means
Disabled	**Local users cannot interrupt a remote session at the port by entering the local switch character. This is the default setting for the INTERRUPTS characteristic.**
Enabled	**Local users can interrupt a remote session at a port by entering the local switch character.**

Example

```
Xyplex>> DEFINE PORT 5 INTERRUPTS ENABLED
```

DEFINE/SET PORT KERBEROS

Enable or disable Kerberos user verification at a port

Notes

Use this command to specify whether the port is to provide Kerberos user verification as part of the login process.

Port 0 is not included when you specify ALL ports. To enable Kerberos user verification for the console port (Port 0), you must specifically list Port 0 when you issue the DEFINE PORT KERBEROS command.

Refer to the *Software Management Guide* for a description of Kerberos support.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* KERBEROS [ENABLED]
[DISABLED]*

Where	Means
ENABLED	**The port is to provide Kerberos user verification.**
DISABLED	**The port is not to provide Kerberos user verification. This is the default.**

Example

```
Xyplex>> DEFINE PORT 5 KERBEROS ENABLED
```

DEFINE/SET PORT KEYMAP

Assign an individual copy of a Tn3270 keymap to this port

Notes

Indicates that you will assign an individual copy of a Tn3270 keymap to this port and change the escape sequences in the keymap. The terminal server uses the keymap information from the device in the TN3270 DEVICE characteristic for this port. This keyword is only valid with the SET command *and* the SERVER TN3270 PORT KEYMAPS characteristic must be set to ENABLED.

Refer to the *Software Management Guide* for information about TN3270 support.

Privilege Level

Secure

Syntax

DEFINE/SET PORT *port-list* KEYMAP [*key* "*escape-seq*" "*description*"] [NONE]

Where	Means
key	**An IBM 3270 display station function. See the *Software Management Guide* for a list of IBM display station functions to use in this variable.**
"***escape-seq***"	**The byte sequence from the local terminal that the terminal server maps to the IBM display station function in the *key* variable. You can specify the characters in the byte sequence in two ways: enter the hexidecimal values, which you obtain from the *Programmer's Reference manual* for the local terminal, or manually press the keys on the terminal. You can use from 0 to 9 hexidecimal values in this variable, and enclose the variable in quotes.**
"***description***"	**A text description. Describes the keymap escape sequence in different keymap displays. These include SHOW PORT KEYMAP and the display that appears when the user presses the SHOWKEYS status key during TN3270 terminal emulation. You can use from 0 to 9 characters in this variable, and enclose the variable in quotes.**
NONE	**Specifies that this port does not have an individual keymap assigned to it. Use this keyword to remove a previously assigned keymap.**

Example

```
Xyplex>> DEFINE PORT 5 KEYMAP PF1 "01 40 13" "F1"
```

DEFINE PORT LAT DEDICATED SERVICE

Assign a permanent LAT service for a port

Notes

Use this command to assign a LAT service to which the port is permanently assigned, or to change or remove the current permanent service assignment for the port. The effect of this characteristic is to automatically connect the port to the dedicated service, whenever a user logs on to that port.

You can only use a DEFINE command to specify the PORT LAT DEDICATED SERVICE characteristic. Refer to the description of theDEFINE PORT DEDICATED SERVICE command.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **LAT DEDICATED SERVICE [***service-name***] [NODE] [***node-name***] [DESTINATION] [***port-name***] [NONE]***

[NONE]* [DESTINATION] [*port-name***] [NONE]***

[NONE]* [NODE] [*node-name***][DESTINATION] [***port-name***] [NONE]***

[NONE]* [DESTINATION] [*port-name***] [NONE]***

Where	Means
service-name	**Specifies the name of the LAT service to which the port is permanently assigned.**
NODE	**Specifies that you will set or change the name of the node on which the dedicated service is offered.**
node-name	**Specifies the name of the LAT service node at which the dedicated service is offered.**
DESTINATION	**Specifies that you will set or change the name of the server port at which the dedicated service is offered.**
port-name	**Specifies the name of the server port at which the service, specified by the service-name, is offered.**
NONE	**Specifies that this port, all ports, or the ports listed in the port-list will not have a dedicated service, or that you wish to cancel a previously-defined dedicated service, service node, or destination server port. This is the default setting for the DEDICATED SERVICE, NODE, and DESTINATION characteristics.**

Example

```
Xyplex>> DEFINE PORT 5 LAT DEDICATED SERVICE VMSHOST
```

DEFINE/SET PORT LAT PREFERRED SERVICE

Assign a LAT service to which the port will connect whenever a user makes a connect request without specifying a service

Notes

Use this command to assign a LAT service to which the port will connect whenever a user makes a connect request without specifying a service, or to change or remove the current preferred service assignment for the port.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **LAT PREFERRED SERVICE [***service-name***] [NODE] [***node-name***] [DESTINATION] [***port-name***]**
[NONE]*
[NONE]* [DESTINATION] [*port-name***]**
[NONE]*
[NONE]* [NODE] [*node-name***] [DESTINATION] [***port-name***]**
[NONE]*
[NONE]* [DESTINATION] [*port-name***]**
[NONE]*

Where Means

service-name **Specifies the name of the LAT service to which the port whenever a user makes a connect request without specifying a service.**

NODE **Specifies that you will set or change the name of the node on which the preferred service is offered.**

node-name **Specifies the name of the service node at which the preferred service is offered.**

DESTINATION **Specifies that you will set or change the name of the server port at which the preferred service is offered.**

port-name **Specifies the name of the server port at which the service, specified by the *service-name*, is offered.**

NONE **Specifies that this port, all ports, or the ports listed in the *port-list* will not have a preferred service, or that you wish to cancel a previously-defined preferred service, service node, or destination server port. This is the default setting for the PREFERRED SERVICE, NODE, and DESTINATION characteristics.**

Example

```
Xyplex>> DEFINE PORT 5 LAT PREFERRED SERVICE FINANCEVAX
```

DEFINE/SET PORT LIMITED VIEW

Limit access to node and service displays for secure and non-privileged users

Notes

Use this command to enable or disable node and service display restrictions for secure and non-privileged users. Specifically, these users can not view the SHOW/LIST NODES or SERVICES displays.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* LIMITED [VIEW] [ENABLED]
[DISABLED]*

Where	Means
VIEW	**An optional keyword.**
ENABLED	**Specifies that a secure or non-privileged user(s) at the port(s) listed in the *port-list* can not view SHOW/LIST NODES or SERVICES displays.**
DISABLED	**Specifies that a secure or non-privileged user(s) at the port(s) listed in the *port-list* can view SHOW/LIST NODES or SERVICES displays. This is the default for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 LIMITED VIEW ENABLED
```

DEFINE/SET PORT LINE EDITOR

Specify line editing character and enable or disable line editing at a port

Notes

Use this command to define, change, or delete a line editing character, or enable or disable the command line editing feature. The guide *Using the TCP/IP-LAT Terminal Server* contains a description of the command line editing feature.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **LINE EDITOR**

[ENABLED]*
[DISABLED]

[BACKSPACE] **[*character*]**
[NONE]

[BEGINNING] **[*character*]**
[NONE]

[CANCEL] **[*character*]**
[NONE]

[DELETE BEGINNING] **[*character*]**
[NONE]

[DELETE LINE] **[*character*]**
[NONE]

[END] **[*character*]**
[NONE]

[FORWARDS] **[*character*]**
[NONE]

[INSERT TOGGLE] **[*character*]**
[NONE]

[NEXT LINE] **[*character*]**
[NONE]

[PREVIOUS LINE] **[*character*]**
[NONE]

[QUOTING CHARACTER] **[*character*]**
[NONE]

[REDISPLAY] **[*character*]**
[NONE]

Where	Means
DISABLED	The command line editing feature will not be available at the specified port(s).
ENABLED	The command line editing feature will be available at the specified port(s)
BACKSPACE	Define, change, or delete the line editing character that will move the cursor one position to the left. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.
BEGINNING	Define, change, or delete the line editing character that will place the cursor at the beginning of the current command line. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.
CANCEL	Define, change, or delete the line editing character that will cancel an interactive operation (such as changing a password), or delete the current command line.
DELETE BEGINNING	Define, change, or delete the line editing character that will delete everything on the current command line, from the cursor position to the beginning of the line.
DELETE LINE	Define, change, or delete the line editing character that will delete the current command line.
END	Define, change, or delete the line editing character that will place the cursor at the end of the current command line. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.
FORWARD	Define, change, or delete the line editing character that will move the cursor one position to the right. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.
INSERT TOGGLE	Define, change, or delete the line editing character that alternates between the insert character and overstrike character modes of operation. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.
NEXT LINE	Define, change, or delete the line editing character that will recall the next command in the command history.
PREVIOUS LINE	Define, change, or delete the line editing character that will recall the previous command in the command history.
QUOTING CHARACTER	Define, change, or delete the line editing character that will quote the next character.
REDISPLAY	Define, change, or delete the line editing character that will re-display the current command line. The command character you define will be ignored by ports whose PORT TYPE characteristic is set to HARDCOPY.

character **A keyboard character that the user will type to perform the specified line editing function. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the PORT BACKWARD SWITCH or FORWARD SWITCH characteristics, or any Telnet command characters, or line-editor characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).**

NONE **There will not be a character that the user can type to perform the specified line editing function.. This command can be used to remove a previously-defined line editing character.**

Example

```
Xyplex>> DEFINE PORT 5 LINE EDITOR REDISPLAY ^B
```

DEFINE/SET PORT LOCAL SWITCH

Specify a character that allows a user to return to the local command mode

Notes

Use this command to specify whether or not there will be a character that allows a user to return to the local command mode.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged

Syntax

DEFINE/SET PORT ***port-list*** **LOCAL SWITCH** **[*character*]**
[NONE]*

Where	Means
character	**A keyboard character that the user will type to return to the local command mode. It is recommended that you specify an unused CTRL character. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the PORT BACKWARD SWITCH or FORWARD SWITCH characteristics, or any Telnet command characters, or line-editor characters). If you do specify a CTRL character, when you type the character, it will be displayed as ^<Key> (i.e., if you type CTRL/B, the terminal will echo the characters: ^B).**
NONE	**There will not be a character that the user can type to return to the local command mode. This command can be used to remove a previously-defined local switch character. This is the default setting for the LOCAL SWITCH characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 LOCAL SWITCH ^B
```

DEFINE/SET PORT LOSS NOTIFICATION

Specify whether the port should notify the user of lost data

Notes

Use this command to specify whether or not the server sends a Bell character to the device connected to the port, whenever input data (from the device) are lost due to a receive data error or a receive overrun error. (For example, the server will have the terminal beep when the user types a command line that exceeds 132 characters in length.)

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **LOSS NOTIFICATION [DISABLED] [ENABLED]***

Where	Means
DISABLED	**The server will not send a Bell character to the device attached to the port, whenever input data are lost.**
ENABLED	**The server will send a Bell character to the device connected to the port, whenever input data are lost. This is the default.**

Example

```
Xyplex>> DEFINE PORT 5 LOSS NOTIFICATION DISABLED
```

DEFINE/SET PORT MENU

Enable or disable the Simple Menu Interface at a port

Notes

Use this command to enable a simple menu interface at a port. Once you enable the menu for a port, a nonprivileged user at that port can only perform operations by choosing menu items. (A privileged user can disable the port menu from a different port, where the menu is not enabled.)

Refer to the *Software Management Guide* for a description of the Simple Menu Interface feature.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* MENU [ENABLED]
[DISABLED]*

Where	Means
ENABLED	**Enables the menu for the specified port or port-list.**
DISABLED	**Disables the menu for the specified port or *port-list*. This is the default setting for the MENU characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 MENU ENABLED
```

DEFINE/SET PORT MESSAGE CODES

Specify whether or not a message code or message number is displayed as part of an error message

Notes

Use this command to specify whether or not, when status or error messages are displayed, the associated message code or message number is shown, or only the text of the message is shown.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **MESSAGE CODES [DISABLED]**
[ENABLED]*

Where	Means
DISABLED	**Message codes or numbers will not be shown when status or error messages are displayed (i.e., only the message is displayed).**
ENABLED	**Message codes or numbers will be shown when status or error messages are displayed. This is the default setting for the MESSAGE CODES characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 MESSAGE CODES DISABLED
```

DEFINE/SET PORT MODEM CONTROL

Specify whether or not the port uses modem control signals

Notes

Use this command to specify whether or not modem control signals and related PORT characteristics (e.g., DSRWAIT and DTRWAIT) are enabled at the port(s) listed in the *port-list* or all ports.

Units which use 6 or 8 wire serial port cabling support the use modem control signals. Units which use 8 wire serial port cabling support the concurrent use of modem control and hardware flow control (RTS/CTS or DTR/DSR flow control). Units which use 3 wire cabling do not support the use of modem control. Refer to the *Hardware* documentation or *Getting Started Guide* supplied with your unit for a description of associated cabling issues.

Refer to the description about modem control and setting up modems in the *Software Management Guide.*

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* MODEM CONTROL [DISABLED]*
[ENABLED]

Where	Means
DISABLED	**Specifies that modem control signals are not enabled at the port(s) listed in the *port-list* or all ports. This is the default setting for the MODEM CONTROL characteristic. This is typically used in a "data-leads-only" mode. With devices that use data-leads-only mode, only data, and no status signals, are exchanged between the device and the port. Data-leads-only mode is typically used with equipment that support limited EIA interface signals.**
ENABLED	**Specifies that modem control signals are enabled at the port(s) listed in the *port-list* or all ports. Refer to the description about modem control and setting up modems in the *Software Management Guide.***

Example

```
Xyplex>> DEFINE PORT 5 MODEM CONTROL ENABLED
```

DEFINE/SET PORT MULTISESSIONS

Enable or disable the Multisessions feature at a port

Notes

Use this command to specify whether or not the port(s) listed in the *port-list* will support DEC terminals, such as the VT330 and VT420 models, which provide a feature called Dual Session Management. This feature enables users to display and control multiple simultaneous communication sessions. The sessions can be multiplexed (i.e., combined) onto a single serial line to a host.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* MULTISESSIONS [ENABLED]
[DISABLED]*

Where	Means
ENABLED	**The port(s) listed in the *port-list* will support terminals which use Dual Session Management. .**
DISABLED	**The port(s) listed in the *port-list* will not support terminals which use Dual Session Management. This is the default**

Example

```
Xyplex>> DEFINE PORT 5 MULTISESSIONS ENABLED
```

DEFINE/SET PORT NAME

Assign a name to a port

Notes

Whenever a port is logged on, the server assigns the port a name. The default name is in the form: PORT_*port-number*, where *port-number* is the number of the physical server port . For example, the default name for port 1 of a server is PORT_1. You use the DEFINE/SET PORT NAME command to assign a different name to the port.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* NAME *port-name*

Where	Means
port-name	**The new name for the specified port. The port-name can be between 1 and 16 ASCII characters in length. (Note that the server will convert any lower-case letters to upper case.) Do not enclose the port-name in quotation mark characters ("). The *port-name* must be unique within each server. The default value for this variable is in the form: PORT_*port-number*, where *port-number* is the number of the physical server port .**

Example

```
Xyplex>> DEFINE PORT 5 NAME PRINTER-PORT
```

DEFINE/SET PORT NOLOSS

Specify whether or not the port will store data to be passed on to a connection partner while waiting for a session connection to be made

Notes

Use this command to specify whether or not the port will store data in its typeahead buffer while waiting for a session connection to be made and then pass the data to the connection partner after the session connection is made.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* NOLOSS [DISABLED]*
[ENABLED]

Where	Means
DISABLED	**The port will not store data in its typeahead buffer while waiting for a session connection to be made. When the NOLOSS characteristic is set to DISABLED, and the device connected to the port sends a character before the session is established, the port will discard the data. (If the LOSS NOTIFICATION characteristic is set to ENABLED, the port also sends the BELL character to the device.) This is the default setting for the NOLOSS characteristic.**
ENABLED	**The port will store data in its typeahead buffer while waiting for a session connection to be made, and then pass the data to the connection partner after the session connection is made. Typically, you will set the NOLOSS characteristic to ENABLED when the serial port is connected to a device that will begin sending data immediately after it issues a connect command. The maximum amount of data stored is specified by the TYPEAHEAD characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 NOLOSS DISABLED
```

DEFINE/SET PORT OUTPUT FLOW CONTROL

Specify whether or not flow control is used for data output from the port

Notes

Use this command to specify whether or not flow control will be used for output data communications at the port (i.e., data communication which originates at the server and is received by the device connected to the port). The flow control method used by the port (e.g., XON/XOFF, DCD/DTR, etc) is specified by the PORT FLOW CONTROL characteristic.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **OUTPUT FLOW CONTROL** **[DISABLED] [ENABLED]***

Where	Means
Disabled	**The server port will not use flow control for output data communications.**
Enabled	**The server port will use flow control for output data communications. This is the default.**

Example

```
Xyplex>> DEFINE PORT 5 OUTPUT FLOW CONTROL ENABLED
```

DEFINE/SET PORT PARITY

Specify whether or not the port will provide parity bits for error checking

Notes

Specifies whether or not the port will provide a bit (parity bit), with each character, for error checking. The value you set for this characteristic must match the value set at the device attached to the port.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **PARITY** **[EVEN]**
[MARK]
[NONE]*
[ODD]

Where	Means
Even	**The port will ensure that each byte (character) that is transmitted or received contains an even number of 1's, including the parity bit. If the port receives a byte that contains an odd number of 1 bits, it indicates to the server that an error occurred.**
Mark	**The port will always set the parity bit to 1. In this case, the device attached to the port needs to use the parity bit to mark the limit of each frame.**
None	**The port will not include a parity bit for error checking. This is the default value for the PARITY characteristic.**
Odd	**The port will ensure that each byte (character) that is transmitted or received contains an odd number of 1's, including the parity bit. If the port receives a byte that contains an even number of 1 bits, it indicates to the server that an error occurred.**

Example

```
Xyplex>> DEFINE PORT 5 PARITY ODD
```

DEFINE/SET PORT PASSWORD

Specify whether or not a password is required in order to logon the port

Notes

Specifies whether or not the user will be required to supply a password in order to logon to the port(s) listed in the port-list or all ports. If there will be ports for which users are required to supply a password in order to logon, the password is specified by the SET SERVER LOGIN PASSWORD command.

This characteristic can only be changed with a DEFINE command.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **PASSWORD** **[DISABLED]***
[ENABLED]

Where	Means
DISABLED	**Specifies that users will not be required to supply a password in order to logon to the port(s) listed in the port-list or all ports. This is the default setting for the PASSWORD characteristic.**
ENABLED	**Specifies that users will be required to supply a password in order to logon to the port(s) listed in the port-list or all ports.**

Example

```
Xyplex>> DEFINE PORT 5 PASSWORD ENABLED
```

DEFINE/SET PORT PAUSE

Specify whether or not the port will pause at the end of each screenful of information when showing server displays

Notes

Use this command to specify whether the device(s), attached to the port(s) listed in the port-list or all ports, will show server displays one screenful at a time (actually 24 lines at a time) or as a continuous stream of information. If these displays are shown one screenful at a time, the server will pause at the end of each screenful of information, and wait for the user to press a key before it displays the next screenful of information.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged

Syntax

DEFINE/SET PORT ***port-list*** **PAUSE** **[DISABLED]***
[ENABLED]

Where	Means
DISABLED	**The device(s), attached to the port(s) listed in the port-list or all ports, will show server displays as a continuous stream of information, rather than pausing at the end of each screenful of information. This is the default setting for the PAUSE characteristic.**
ENABLED	**The device(s), attached to the port(s) listed in the port-list or all ports, will show server displays one screenful at a time, by pausing to wait for the user to press a key before it displays the next screenful of information.**

Example

```
Xyplex>> DEFINE PORT 5 PAUSE ENABLED
```

DEFINE/SET PORT PPP

Assign a port to exclusive PPP support

The DEFINE/SET PORT PPP commands specify which ports are used for PPP sessions.

Notes

A port which is configured as a PPP port can only be used for PPP sessions; that is to say only PPP packets can be sent or received by the port.

A user at one port cannot use a SET PORT PPP command to enable PPP on another port.

Privilege Level

Non-privileged for your port. Privileged for other ports.

Syntax

DEFINE PORT PPP *port-list* ENABLED|DISABLED
SET PORT PPP ENABLED

Where	Means
ENABLED	**Enable the PPP protocol on one or more terminal server ports.**
DISABLED	**Disable the PPP protocol on one or more terminal server ports. (This is the factory default setting for this option.)**

Example

This command specifies that port 5 will be used for PPP sessions.

```
Xyplex>> define port 5 ppp enabled
```

DEFINE/SET PORT PPP ACTIVE

Specify the how ports will negotiate options when initiating a PPP session

The DEFINE/SET PORT PPP ACTIVE commands specifies the manner by which the port will negotiate PPP options when a PPP session is initiated.

Notes

When a PPP session is initiated, the port and the remote device negotiate the manner in which data are to be transferred during the PPP session. The terminal server port can either initiate the negotiation of PPP options or it can wait until the remote device initiates the negotiation of the options.

When the server port initiates the option negotiations, this is referred to as an "active" start. When the server port waits until the remote device initiates the negotiation of the options, this is referred to as a "passive" start.

A user at one port cannot use a SET PORT PPP ACTIVE command to change the method of option negotiation used at another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP ACTIVE ENABLED|DISABLED
SET PORT PPP ACTIVE ENABLED

Where	Means
ENABLED	**Configure the server port to initiate PPP option negotiations (perform an active start). (This is the factory default setting for this option.)**
DISABLED	**Configure the server port to wait until the remote device initiates the negotiation of the options (perform a passive start).**

Example

This command specifies that port 5 will initiate the option negotiations, at the beginning of a PPP session, rather that wait for the remote device to initiate negotiations.

```
Xyplex>> define port 5 ppp active enabled
```

DEFINE/SET PORT PPP CHARMAP

Specify which ASCII control characters the port will negotiate for use as control characters rather than as data

The DEFINE/SET PORT PPP CHARMAP command specifies which ASCII control characters that the port will propose, during PPP option negotiations, to use as control characters rather than as data.

Notes

During a PPP session, it may be necessary to use some ASCII control characters to control the manner in which data are transferred (for example, for flow control purposes) from one end of the connection to the other. Other control characters may be part of a normal data stream. If these control characters were sent "in the clear" they would confuse devices such as modems, etc. The PPP RFC provides a standard way of "encoding" these characters so that both the port and the remote device can determine when they have received a character that is to be treated as a control character as distinct from using it as data. The method used to encode control characters is to convert them into a two byte token at one end of the link and convert them back at the other end of the link. (The first byte of the token is 7D. The second byte is calculated by adding 20 plus the hexidecimal value of the control character to be encoded. For example, to send an encoded null character, which has the hexidecimal value of 00 the port will send the sequence 7D 20.)

In order to distinguish how one or more control characters are to be interpreted, the port and the remote device negotiate a mutually acceptable"character map." There can be separate character maps for each direction in which data are transmitted.

The PORT PPP CHARMAP characteristic specifies which ASCII control characters that the port will propose, during PPP option negotiations, to use as control characters rather than as data. The specific control characters to be encoded by the port or the remote device are subject to negotiation.

A user at one port cannot use a SET PORT PPP CHARMAP command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP CHARMAP *character-mask*
SET PORT PPP CHARMAP *character-mask*

Where	Means

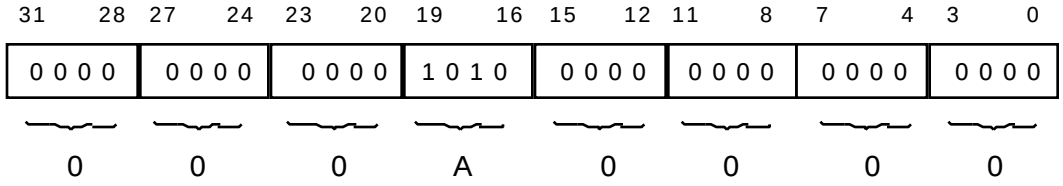
character-mask **The hexidecimal 32-bit value of a control character that the port will propose to use as a control character during a PPP session. Valid values are 00000000 through ffffffff. Commonly used masks include: 00000000 which means that no control characters will be encoded, 000a0000 which means that the XON and XOFF control characters will be encoded, and ffffffff which means that all control characters will be encoded. The default is 000a0000. You can calculate a different mask as follows:**

1. Select the control characters that are to be encoded from the following table:

0		**NUL**	**Null**
1	**^A**	**SOH**	**Start of Heading**
2	**^B**	**STX**	**Start of Text**
3	**^C**	**ETX**	**End of Text**
4	**^D**	**EOT**	**End of Transmission**
5	**^E**	**ENQ**	**Enquiry**
6	**^F**	**ACK**	**Acknowledge**
7	**^G**	**BEL**	**Bell**
8	**^H**	**BS**	**Backspace**
9	**^I**	**HT**	**Horizontal Tab**
10	**^J**	**LF**	**Line Feed**
11	**^K**	**VT**	**Vertical Tab**
12	**^L**	**FF**	**Fprm Feed**
13	**^M**	**CR**	**Carriage Return**
14	**^N**	**SO**	**Shift Out**
15	**^O**	**SI**	**Shift In**
16	**^P**	**DLE**	**Data Link Escape**
17	**^Q**	**DC1**	**Device Control 1 (XON)**
18	**^R**	**DC2**	**Device Control 2**
19	**^S**	**DC3**	**Device Control 3 (XOFF)**
20	**^T**	**DC4**	**Device Control 4**
21	**^U**	**NAK**	**Negative Acknowledge**
22	**^V**	**SYN**	**Synchronous Idle**
23	**^W**	**ETB**	**End of Transmission Block**
24	**^X**	**CAN**	**Cancel**
25	**^Y**	**EM**	**End of Medium**
26	**^Z**	**SUB**	**Substitute**
27		**ESC**	**Escape**
28		**FS**	**File Separator**
29		**GS**	**Group Separator**
30		**RS**	**Record Separator**
31		**US**	**Unit Separator**

2. **The mask consists of eight hexidecimal characters (numbers 0 through 9 and the letters a through f), each of which which represents four of the possible control character options. The bit ordering is from right to left as shown in the figure below. Each group of four bits is then converted to the hexidecimal character used in the mask.**

   The figure shown below depicts the method used to develop the mask 000A0000 (the default mask).



0 = 0000
1 = 0001
2 = 0010
3 = 0011
4 = 0100
5 = 0101
6 = 0110
7 = 0111
8 = 1000
9 = 1001
A = 1010
B = 1011
C = 1100
D = 1101
E = 1110
F = 1111

Example

This command specifies that port 5 will encode all control characters.

```
Xyplex>> define ports 5 ppp charmap ffffffff
```

DEFINE/SET PORT PPP CONFIGURE LIMIT

Specify the number of attempts the port should make to negotiation PPP options.

The DEFINE/SET PORT PPP CONFIGURE LIMIT command determines when a port discontinues attempts to negotiate PPP options.

Notes

The PORT PPP CONFIGURE LIMIT characteristic specifies the maximum number of unanswered PPP option configuration request packets that the port will send, before the software concludes that the remote device is unable to respond. (Refer to the Notes section of the DEFINE/SET PORT PPP RESTART TIMER command for a description of how the PORT PPP CONFIGURE LIMIT command is used during PPP option negotiations.) When the port has sent the number of option configuration request packets specified by the PORT PPP CONFIGURE LIMIT characteristic, it discontinues further attempts to negotiate PPP options and goes into a passive "listening" state.

A user at one port cannot use a SET PORT PPP CONFIGURE LIMIT command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP CONFIGURE LIMIT *limit*
SET PORT PPP CONFIGURE LIMIT *limit*

Where	Means
limit	**The maximum number of unanswered PPP option configuration request packets that the port will send, before discontinuing further attempts to negotiate PPP options and going into a passive "listening" state. Valid values are integers between 2 and 10. The default is 10.**

Example

This command specifies that port 5 will send up to 5 PPP option configuration request packets, before discontinuing further attempts to negotiate PPP options and going into a passive "listening" state.

```
Xyplex>> define ports 5 ppp configure limit 5
```

DEFINE/SET PORT PPP DEFAULTS

Reset PPP port characteristics back to their default values

The DEFINE PORT PPP DEFAULTS command resets the PPP operational characteristics back to their default values.

Notes

This command applies only for the specified port or ports on which PPP is enabled. This command does not affect whether or not PPP is enabled for a given port.

A user at one port cannot use a SET PORT PPP DEFAULTS command to resets the PPP operational characteristics used at another port back to their default values.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP DEFAULTS [ENABLED]
SET PORT PPP DEFAULTS [ENABLED]

Where	Means
ENABLED	**Optional**

Examples

This command specifies that ports 8 through 16 will have the PPP operational characteristics changed back to their default values.

```
Xyplex>> define ports 8-16 ppp defaults enabled
```

DEFINE/SET PORT PPP FAILURE LIMIT

Specify the number of times the port should object to a proposed PPP option, before rejecting negotiation of the option.

The DEFINE/SET PORT PPP FAILURE LIMIT command determines how persistent the port should be in negotiating a given PPP option.

Notes

During PPP option negotiation, the remote device may propose values for options that cannot be accepted by the Xyplex unit. When this occurs, the port will object to (NAK) the option and offer a different value. Sometimes, the remote device will object to that value, and will propose the option again with a different setting). If the option is still unacceptable, the port will again object to (NAK) the option. This continues until the number of times specified by the PORT PPP FAILURE LIMIT characteristic is reached, at which point the port rejects all further attempts at negotiating the option.

A user at one port cannot use a SET PORT PPP FAILURE LIMIT command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP FAILURE LIMIT *limit*
SET PORT PPP FAILURE LIMIT *limit*

Where	Means
limit	**The maximum number of times the port will reject an unsupported option or an unacceptable value for a supported option before the port rejects further negotiation of the option. Valid values are integers between 2 and 10. The default is 3.**

Example

This command specifies that port 5 will reject an unsupported option or an unacceptable value for a supported option up to 5 times before the port rejects further negotiation of the option.

```
Xyplex>> define ports 5 ppp failure limit 5
```

DEFINE/SET PORT PPP IP BROADCASTS

Specify whether or not Internet broadcast packets are forwarded over the PPP link

The DEFINE/SET PORT PPP command determines whether or not a port will transmit Internet broadcast packets over the link or discard broadcast packets received from the remote device.

Notes

Internet broadcast packets are typically packets which contain route or routing information, information to resolve an Internet address or domain name, or requests for such types of information. In some configurations, such as those configurations where only a single node (such as a dial-in PC) is may be useful to eliminate forwarding of these packets in order to improve link efficiency. In configurations where the PPP link is used as a gateway, or when you are running a domain-name resolver program, you will usually want to have these packets be forwarded over the link.

A user at one port cannot use a SET PORT PPP IP BROADCASTS command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP IP BROADCASTS ENABLED|DISABLED
SET PORT PPP IP BROADCASTS ENABLED|DISABLED

Where	Means
ENABLED	**Permit Internet broadcast packets to be transmitted over the PPP link, or allow the port to accept broadcast packets received from the remote device and forward them to the local area network. This is the default.**
DISABLED	**Do not forward Internet broadcast packets over the link to the remote device and discard any broadcast packets received from the remote device.**

Example

This command specifies that port 5 will transmit Internet broadcast packets over the PPP link, and allow the port to accept broadcast packets received from the remote device and forward them to the local area network.

```
Xyplex>> define port 5 ppp ip broadcast enabled
```

DEFINE/SET PORT PPP IP LOCAL ADDRESS

Specify the local Internet address used by the port

The DEFINE/SET PORT PPP LOCAL ADDRESS command determines whether the port will have a user-specified Internet address or if the port will use the Internet address of the terminal server.

Notes

Both the port (the local end of a PPP connection) and the remote device must each have an Internet address assigned to them for the purpose establishing a connection and forwarding data. The Internet address of the port is referred to as a local address. You use the PORT PPP LOCAL ADDRESS characteristic to assign a specific Internet address to a port.

A user at one port cannot use a SET PORT PPP LOCAL ADDRESS command to alter the configuration for another port.

Privilege Level

Privileged.

Syntax

DEFINE PORT *port-list* PPP IP LOCAL ADDRESS *internet-address*
SET PORT PPP IP LOCAL ADDRESS *internet-address*

Where	Means
internet-address	**A standard Internet address (refer to the section describing common variables). The default is 0.0.0.0 (no Internet address). If no Internet address is assigned to the port, the port will use the Internet address of the terminal server itself as the local address when the PPP connection is established.**

Example

This command specifies that port 5 will have the local Internet address of 140.179.211.5.

```
Xyplex>> define ports 5 ppp ip local address 140.179.211.5
```

This command specifies that port 5 will use the terminal server Internet address as the local Internet address.

```
Xyplex>> define ports 5 ppp ip local address 0.0.0.0
```

DEFINE PORT PPP IP REMOTE ADDRESS

Specify the remote Internet address used by the port

The DEFINE PORT PPP REMOTE ADDRESS command determines whether or not a port is constrained to use a specific remote address.

Notes

Both the port (the local end of a PPP connection) and the remote device must each have an Internet address assigned to them for the purpose establishing a connection and forwarding data. The Internet address of the remote device is referred to as a remote address. Normally, when a remote device wishes to make a connection, during option negotiations it will either state the specific remote address that it wishes to use or it will indicate that it wishes to have a remote address assigned to it by the port.

You use the PORT PPP REMOTE ADDRESS characteristic to specify remote Internet address when the remote device indicates during option negotiations that it wants the terminal server to assign the address, or when you want to dedicate the server port to a device with a specific remote address. (In the latter case, if the remote device supplies a remote address that is different than the one specified by the PORT PPP REMOTE ADDRESS characteristic, then the connection may be made, but any data sent by the remote device will not be acknowledged, so the connection is not a useful one.) If neither the remote device nor the terminal server port can supply a remote address, then the PPP connection cannot be formed. When the port supplies the remote address, because the remote device indicates during option negotiations that it wants the terminal server to assign the remote address, the remote device must accept the address supplied to it or a non-meaningful connection will result.

A user at one port cannot use a SET PORT PPP REMOTE ADDRESS command to alter the configuration for another port.

Privilege Level

Privileged

Syntax

DEFINE PORT *port-list* PPP IP REMOTE ADDRESS *internet-address*
SET PORT PPP IP REMOTE ADDRESS *internet-address*

Where	Means
internet-address	**A standard Internet address (refer to the section describing common variables). The default is 0.0.0.0 (no Internet address). If no Internet address is assigned to the port, the port will be configured to use the Internet address specified by the remote device as the remote address when the PPP connection is established. (If that device does not offer a remote address, no connection can be established.)**

Example

This command specifies that remote device connected to port 5 will have the remote Internet address of 140.179.211.5.

```
Xyplex>> define ports 5 ppp ip remote address 140.179.211.5
```

This command specifies that port 5 will use the remote address specified by the remote device during option negotiation.

```
Xyplex>> define ports 5 ppp ip remote address 0.0.0.0
```

DEFINE/SET PORT PPP IP VJ COMPRESSION

Specify whether the port can negotiate the use of data compression over a PPP link

The DEFINE/SET PORT PPP IP VJ COMPRESSION command specifies whether or not the port will try to negotiate the use of a data compression mechanism over a PPP link.

Notes

Data compression allows for more efficient use of a PPP link, by allowing more data to be transferred over the link. One popular method of data compression used in TCP/IP networks is known as Van Jacobson (VJ) compression. Other compression methods are also available, but are not currently supported by the Xyplex terminal server. The use of the Van Jacobson compression method can result in significant bandwidth savings, which can be important when PPP connections are made over telephone lines or when a PPP link is very heavily used. Van Jacobson compression is very memory intensive, however (see the Notes section for the DEFINE/SET PORT PPP IP VJ COMPRESSION SLOTS command description). The use of Van Jacobson compression is negotiated during PPP options negotiation. Compression can be used in one direction by the link, but not by the other, in both directions or in neither direction.

A user at one port cannot use a SET PORT PPP IP VJ COMPRESSION command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP IP VJ COMPRESSION ENABLED|DISABLED
SET PORT PPP IP VJ COMPRESSION ENABLED|DISABLED

Where	Means
ENABLED	**Allow the port to negotiate the use of Van Jacobson compression. This is the default.**
DISABLED	**Do not allow the port to negotiate the use of Van Jacobson compression.**

Example

This command specifies that port 5 will be allowed to negotiate the use of Van Jacobson compression

```
Xyplex>> define port 5 ppp ip vj compression enabled
```

DEFINE/SET PORT PPP IP VJ COMPRESSION SLOTS

Specify the number of data channels which use data compression that the port can propose after objecting to a value

Notes

A PPP link can have a number of sessions (or slots), using higher-level protocols such as TCP/IP, operating across the link. This can happen, for example, when the PPP link is used in a gateway configuration that supports several users, or in a configuration where a single node (such as a dial-in PC) is connected to the port and the single node has several windows in use. When Van Jacobson compression is in use on the link, PPP usually requires that both sides of the link must specify how many slots will use compression. (This is because the compression mechanism is very memory intensive. If too many slots use compression, the terminal server or the remote device could run out of memory resources to perform other tasks.) PPP also requires that each slot have a unique slot number or address. For a link which supports 16 slots, the slots are numbered 0 through 15.

During PPP option negotiation, the remote device may propose a value for the number of slots that will use compression. If the number of slots proposed is between 3 and 15, the port will accept the proposed number. If the number of slots proposed is more than 16, port will object to (NAK) the option and offer the value specified by the PORT PPP IP VJ COMPRESSION SLOTS characteristic. Sometimes, the remote device will accept that number. Other times, the remote device will object to that value, and will propose the option again with a different number of slots. If the number is still unacceptable, the port will again object to (NAK) the option and again propose the number specified by this characteristic. This continues until the number of times specified by the PORT PPP FAILURE LIMIT characteristic is reached, at which point the port rejects all further attempts at negotiating the option.

A user at one port cannot use a SET PORT PPP IP VJ COMPRESSION SLOTS command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT ***port-list*** **PPP IP VJ COMPRESSION SLOTS** ***number***
SET PORT PPP IP VJ COMPRESSION SLOTS ***number***

Where	Means
number	**The number of slots that can use Van Jacobson data compression over a PPP link that the port will propose during PPP options negotiation, when a value larger than 16 is proposed by the remote device. Valid values are integers between 3 and 15. The default is 15.**

Example

This command specifies that port 5 will be propose the use of 15 slots using Van Jacobson compression, if the port objects to the number of slots proposed by the remote device.

```
Xyplex>> define port 5 ppp ip vj compression slots 15
```

DEFINE/SET PORT PPP PAP ENABLED|DISABLED

Specify whether or not the port requires a password from the remote device to form a PPP connection.

The DEFINE/SET PORT PPP PAP commands determines whether or not the remote device must supply a password in order to establish a PPP connection with the server port.

Notes

Both the port (the local end of a PPP connection) and the remote device can be configured to require that the other end of the connection provides a password prior to establishing a PPP connection and forwarding data. It is also possible to configure a link so that a password is required in either direction, both directions, or no direction. The DEFINE/SET PORT PPP PAP commands only affects whether or not the port will require a password in order to form a connection.

For ports which are configured to require that the remote device supplies a password, the standard login password (specified by the DEFINE/SET SERVER LOGIN PASSWORD command; the factory default password is "ACCESS") is the password that the remote device must supply. If the remote device does not supply this password, the port terminates further connection activities.

A user at one port cannot use a SET PORT PPP PAP command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP PAP ENABLED|DISABLED
SET PORT PPP PAP ENABLED|DISABLED

Where	Means
ENABLED	**The remote device must supply the login password in order to establish a PPP connection with the port.**
DISABLED	**The remote device does not need to supply the login password in order to establish a PPP connection with the port. This is the default.**

Examples

This command specifies that ports 8 through 16 will require that remote devices supply the login password in order to establish a PPP connection.

```
Xyplex>> define ports 8-16 ppp pap enabled
```

DEFINE/SET PORT PPP RESTART TIMER

Specify the time a port should wait to retry PPP option negotiations

Notes

The DEFINE PORT PPP RESTART TIMER command specifies the length of the period of time that the port should wait, after sending a configuration request to the remote device, before sending another configuration request.

When a PPP session is initiated, the port and the remote device negotiate the manner in which data are to be transferred during the PPP session. Each partner on the link sends an initial configuration request packet to the other to start these option negotiations. If, after sending its configuration request packet, the terminal server port has not received a response from the remote device within the time specified by the RESTART TIMER characteristic, the port sends another option configuration request. This continues until the number of retries specified by the PORT CONFIGURE LIMIT characteristic is reached, at which time the port assumes that the remote device is no longer available and goes into a passive "listening" state.

This characteristic applies both to ports which actively start option negotiations as well as ports that wait for the remote device to start the option negotiations.

A user at one port cannot use a SET PORT PPP RESTART TIMER command to alter the configuration for another port.

Privilege Level

Non-privileged

Syntax

DEFINE PORT *port-list* PPP [RESTART] TIMER *time*
SET PORT PPP [RESTART] TIMER *time*

Where	Means
RESTART	**Optional keyword.**
time	**The amount of time the port should wait before sending another option configuration request packet. The value for *time* is 1 to 10 seconds (whole numbers only). The default is 3 seconds.**

Examples

This command specifies that port 5 will wait for 5 seconds after sending a PPP option configuration request packet, before sending another option configuration request packet, if the port has not received a reply from the remote device in response to the previous configuration request packet.

```
Xyplex>> define ports 5 ppp restart timer 5
```

DEFINE/SET PORT PREFERRED SERVICE

Assign a service to which the port will connect whenever a user makes a connect request without specifying a service

Notes

Use this command to specify whether or not there will be a service to which the port will connect whenever a user makes a connect request without specifying a service. It can also be used to make a change to the current preferred service assignment for the port.

When a connection is attempted, the server will interpret the variable which follows this keyword as either a LAT service-name or as a Telnet destination (domain-name or internet-address), depending on the setting of the RESOLVE SERVICE characteristic. You can also specify the prefixes LAT or TELNET to require the server to interpret the variable as a LAT service-name or a Telnet destination. (Refer to the descriptions of the RESOLVE SERVICE, LAT and TELNET PREFERRED SERVICE characteristics for more information.)

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **PREFERRED SERVICE** **[***service-name***] [NODE] [***node-name***] [DESTINATION] [***port-name***] [NONE]***

[NONE]* [DESTINATION] [*port-name***] [NONE]***

[NONE]* [NODE] [*node-name***] [DESTINATION] [***port-name***] [NONE]***

[NONE]* [DESTINATION] [*port-name***] [NONE]***

[*domain-name***[:***telnet-port-number***]]**
[*internet-address***[:***telnet-port-number***]]**

Where	Means
service-name	**The name of a LAT service to which the port is automatically connected, when a user makes a connect request without specifying a service-name.**
NODE	**Indicates that you will set or change the name of the node on which the preferred service is offered. (This keyword only applies to services that are offered on a LAT network.)**
node-name	**The name of the service node at which the preferred service is offered.**
DESTINATION	**Indicates that you will set or change the name of the server port at which the preferred service is offered. (This keyword only applies to services that are offered on a LAT network.)**
port-name	**The name of the server port at which the service, specified by the service-name, is offered.**
NONE	**Indicates that this port, all ports, or the ports listed in the port-list will not have a preferred service, or that you wish to cancel a previously-defined preferred service, service node, or destination server port. This is the default setting for the PREFERRED SERVICE, NODE, and DESTINATION characteristics.**
domain-name	**The logical name of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a domain-name. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.**
internet-address	**The identity or location on the network of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying an internet-address.**
:telnet-port-number	**The number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a Telnet addressable network object.**

Example

```
Xyplex>> DEFINE PORT 5 PREFERRED SERVICE FINANCEVAX

Xyplex>> DEFINE PORT 5 PREFERRED SERVICE FINANCEHOST.XYPLEX.COM

Xyplex>> DEFINE PORT 5 PREFERRED SERVICE 140.179.249.100
```

DEFINE/SET PORT PRIVILEGED MENU

Change the privileges for port which use the Simple Menu Interface

Notes

Use this command to specify which ports, will have the menu feature enabled and which will be privileged when the user logs on. The PORT MENU characteristic must also be ENABLED for the port.

If you enter a SET/DEFINE PORT PRIVILEGED MENU DISABLED command at a port where both the MENU feature and the PRIVILEGED MENU feature are enabled, the server will disable both menu features. You can re-enable the regular menu with the DEFINE/SET PORT MENU ENABLED command.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **PRIVILEGED MENU** **[DISABLED]* [ENABLED]**

Where	Means
DISABLED	**The port(s), for which the menu feature is enabled, will not be privileged when the user logs on. This is the default setting for this characteristic.**
ENABLED	**The port(s) will have the the menu feature enabled and will be privileged when a user logs on.**

Example

```
Xyplex>> DEFINE PORT 5 PRIVILEGED MENU ENABLED
```

DEFINE/SET PORT PROMPT

Specify the prompt that will be displayed at devices connected to server port(s)

Notes

Use this command to change the prompt which is displayed at the devices connected to the server serial port(s).

When a port is defined as secure or non-privileged, the server will append one right-angle bracket character (>) to the prompt text string. When a port is defined as privileged, the server will append two right-angle bracket characters (>>) to the prompt text string.

Privilege Level

Non-privileged for your own port. Privileged for other ports.

Syntax

DEFINE/SET PORT ***port-list*** **PROMPT** ***prompt***

Where	Means
prompt	**The prompt which will be displayed at the devices connected to the server port(s). The text can be between 1 and 20 ASCII characters in length. Always enclose the prompt text string in quotation marks ("). The prompt "Xyplex" is the default setting for the LOCAL PROMPT characteristic.**

Example

```
Xyplex>> SET PORT PROMPT "John"

John>>
```

DEFINE/SET PORT QUEUING

Specify whether or not a connection request queue is in use at a port

Notes

Use this command to specify whether or not the port(s) can place a connection request into a queue (called a connection queue) when the requested service is busy.

For service requests that are in the connection queue, at the time when queuing is disabled at a port, these requests remain in the connection queue until the service becomes available.

This characteristic is used when local services are offered at the port.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **QUEUING [DISABLED]***
[ENABLED]

Where	Means
DISABLED	**The port(s) will not place a connection request into a connection queue, when the requested service is busy. This is the default setting for the QUEUING characteristic.**
ENABLED	**The port(s) can place a connection request into a connection queue, when the requested service is busy.**

Example

```
Xyplex>> DEFINE PORT 5 QUEUING ENABLED
```

DEFINE/SET PORT RESOLVE SERVICE

Specify how the port should interpret ambiguous connection requests

Notes

Use this command to specify whether the server should interpret the variable specified in a user CONNECT, SET PORT PREFERRED SERVICE, or SET PORT DEDICATED SERVICE command as a LAT service-name or as a Telnet destination. (This characteristic does not apply when the keywords LAT or TELNET are used.)

Note that the PORT RESOLVE SERVICE characteristic applies both to connections from and to a port. If you attempt to connect to a target port whose RESOLVE SERVICE characteristic is set to a specific protocol (LAT or Telnet), from a port whose RESOLVE SERVICE characteristic is not set to the same protocol, the server does not allow the connection.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **RESOLVE SERVICE** **[ANY]***
[LAT]
[TELNET]

Where	Means
ANY	**The server should first attempt to interpret the variable, specified in a CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE command, as being a LAT service-name. If the server is unable to connect to a matching LAT service, it will then attempt to connect to a TELNET destination (domain-name or internet-address). This is the default setting for the RESOLVE SERVICE characteristic.**
LAT	**The server should interpret the variable, specified in CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE commands, as being a LAT service-name.**
TELNET	**The server should interpret the variable specified in CONNECT, SET PORT PREFERRED SERVICE or SET PORT DEDICATED SERVICE commands, as being a Telnet destination.**

Example

```
Xyplex>> DEFINE PORT 5 RESOLVE SERVICE ANY
```

DEFINE/SET PORT REMOTE MODIFICATION

Specify whether or not VMS processes to alter port characteristics

Notes

Use this command to specify whether or not a process running at a VMS host can change certain PORT characteristics. The PORT characteristics that can be changed are: CHARACTER SIZE, INPUT SPEED and OUTPUT SPEED, LOSS NOTIFICATION, and DEFAULT SESSION MODE.

Refer to the documentation supplied with your VMS application to determine whether or not this characteristic must be enabled.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* REMOTE MODIFICATION [ENABLED] [DISABLED]*

Where	Means
ENABLED	**Specifies that a process running at a VMS host can change certain PORT characteristics.**
DISABLED	**Specifies that a process running at a VMS host cannot change certain PORT characteristics. This is the default.**

Example

```
Xyplex>> DEFINE PORT 5 REMOVE MODIFICATION ENABLED
```

DEFINE/SET PORT SCRIPT

Download a script file and execute the commands contained in the file

Notes

Use this command to have the port download a script from a script server and perform the commands contained in the script file.

Refer to the guide *Using the TCP/IP-LAT Terminal Server* and the *Software Management Guide* for more information about using scripts.

You can use the SCRIPT command as a substitute for the SET PORT SCRIPT command.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* SCRIPT "*script-name*"

Where	Means
script-name	**The name and directory location of the script file to be executed. (The file and directory location must be specified as a UNIX-style filename. For example, /usr/login). You must enclose the *script-name* in quotation marks ("). The maximum length of the script file name, and directory location is 64 characters. If you do not specify a script file name, the server will try to execute the script file that is normally executed when the user logs on to the port.**

Example

```
Xyplex>> DEFINE PORT 5 "/usr/login"
```

DEFINE/SET PORT SCRIPT ECHO

Specify whether or not script commands are displayed during execution of a script

Notes

Use this command to specify whether or not the port will display the TCP/IP-LAT commands contained in a script file while they are being executed.

Refer to the guide *Using the TCP/IP-LAT Terminal Server* and the *Software Management Guide* for more information about using scripts.

Privilege Level Privileged.

Syntax

DEFINE/SET PORT *port-list* SCRIPT ECHO [DISABLED]* [ENABLED]

Where	Means

DISABLED

The port will not display the TCP/IP-LAT commands contained in a script file while they are being executed. This is the default.

ENABLED

The port will display the TCP/IP-LAT commands contained in a script file while they are being executed.

Example

```
Xyplex>> DEFINE PORT 5 SCRIPT ECHO ENABLED
```

DEFINE PORT SCRIPT LOGIN

Specify whether or not a script is needed or is required for logging on a port

Notes

Specifies whether or not the port(s) can use or will require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence.

Refer to the guide *Using the TCP/IP-LAT Terminal Server* and the *Software Management Guide* for more information about using scripts.

Privilege Level

Privileged.

Syntax

DEFINE PORT *port-list* SCRIPT LOGIN [DISABLED]*
[ENABLED]
[REQUIRED]

Where	Means
DISABLED	**The port(s) do not need to have a login script file downloaded from a script server and then executed, in order to complete the login sequence. This is the default.**
ENABLED	**The port(s) will request that a login script file be downloaded from a script server and then executed, prior to completing the login sequence. The port is logged on, even if the server is unable to locate a script file.**
REQUIRED	**The port(s) require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence. If the server is unable to locate the correct script file, the port is not logged on.**

Example

```
Xyplex>> DEFINE PORT 5 SCRIPT LOGIN REQUIRED
```

DEFINE/SET PORT SECURITY

Enable or disable secure status at a port

Notes

Use this command to specify whether or not the port(s) listed in the port-list or all ports will be set to the Secure privilege level. Ports which are set to Secure status are restricted from having access to some port configuration commands and from using the SHOW command to view information about other user's ports or sessions. Refer to the *Software Management Guide* for more information about port security levels.

This characteristic does not apply to parallel ports.

Privilege Level Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **SECURITY [DISABLED]***
[ENABLED]

Where	Means
DISABLED	**The port(s) listed in the port-list or all ports will not be set to secure status. This is the default setting for the SECURITY characteristic.**
ENABLED	**The port(s) listed in the port-list or all ports will be set to secure status.**

Example

```
Xyplex>> DEFINE PORT 5 SECURITY ENABLED
```

DEFINE/SET PORT SESSION LIMIT

Specify the maximum number of sessions that can simultaneously be running at a port

Notes

Use this command to set or change the maximum number of sessions that can be simultaneously connected to the port(s) specified by the port-list.

Additional sessions can require additional server resources. The number of sessions that are permitted varies, depending on the product and type of port. Refer to the chapter on Managing Server Resources in the *Software Management Guide* for more information.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* SESSION LIMIT [*session-limit*]
[NONE]

Where	Means
session-limit	**The maximum number of sessions that can be simultaneously connected to the port(s) specified by the port-list. The number of sessions that are permitted varies (refer to the *Software Management Guide*), depending on the product and type of port. For most products, valid values are whole numbers in the range of 0 and 16. The default value is 4.**
NONE	**The server port(s) specified by the port-list can be simultaneously connected to as many sessions as memory will permit.**

Example

```
Xyplex>> DEFINE PORT 5 SESSION LIMIT 8
```

DEFINE/SET PORT SIGNAL CHECK

Specify whether or not the port should restrict connections to a service offered at this port, if the DSR signal is deasserted

Notes

Use this command to restrict connections to a service offered at this port, if the DSR signal is deasserted. Also specifies whether or not the server should log out a port when the DCD signal is deasserted. The SIGNAL CHECK characteristic only applies for ports for which the FLOW CONTROL characteristic is set to any value except CTS or DSR.

Refer to the discussion about modem control in the *Software Management Guide* for more information.

This characteristic only applies to serial ports which support modem signals. This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* SIGNAL [CHECK] [ENABLED]
[DISABLED]*

Where	Means
CHECK	**An optional keyword.**
DISABLED	**Allow connections to a service offered at the port when DSR is deasserted. Do not logout appropriately configured ports when the serial interface DCD signal is deasserted. This is the default setting for the SIGNAL CHECK characteristic.**
ENABLED	**Disallow connections to a service offered at the port when DSR is deasserted. Logout appropriately configured ports when the serial interface DCD signal is deasserted.**

Example

```
Xyplex>> DEFINE PORT 5 SIGNAL CHECK ENABLED
```

DEFINE/SET PORT SPEED

Specify the port speed (baud rate)

Notes

Use the DEFINE/SET PORT SPEED command to set or change the port speed (baud rate) for one or more ports to match the speed of the device connected to the port. The server will also use the value set for the PORT SPEED characteristic when negotiating options for TELNET and RLOGIN connections.

Note, split speed operation (i.e., input speed different from output speed) is not supported. Not all servers support speeds above 38,400 bps.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged for your own port. Privileged for other ports.

Syntax

DEFINE/SET PORT ***port-list*** **SPEED** ***speed***

Where	Means
speed	**Specifies the port speed, in bits per second, to which the specified port(s) will be set. Valid speeds are 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 56000, 57600, 64000, 76800, and 115200 (do not specify units).**

Example

```
Xyplex>>DEFINE PORT 5 SPEED 9600
```

DEFINE/SET PORT STOP BITS

Specify the number of stop bits to be used

Notes

Use this command to change the number of stop bits to be used to maintain synchronization of data.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **STOP BITS** ***bit-value***

Where	Means
bit-value	**A whole number which maps to the number of stop bits to be used to maintain synchronization of data. The following table indicates how many stop bits will be used for various settings of the** ***bit-value*****:**

bit-value setting	Stop Bits Used
1	1 stop bit
2	2 stop bits
3	1.5 stop bits
4	Server calculates the number of stop bits to use based on the port speed. This is the default.

Example

```
Xyplex>> DEFINE PORT 5 STOP BITS 3
```

DEFINE/SET PORT TELNET ABORT OUTPUT

Specify .whether or not there is a character which terminates the further display of output during a Telnet session

Notes

Use this command to specify whether or not there will be a character, which the user can type during a Telnet session, which terminates the further display of output (such as a text file, etc) at a terminal. (However, typing this character does not abort or terminate any programs that are running - it merely terminates the display of the output of the program.)

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET ABORT OUTPUT [*character*]**
[NONE]*

Where Means

character **Specifies the character which, when typed by a user during a Telnet session, terminates further display of output at a terminal.**

It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, any line editing commands, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ABORT OUTPUT characteristic (in this case CTRL/O).

NONE **There will not be a character, which the user can type during a Telnet session, which terminates the display of output at a terminal. This is the default TELNET ABORT OUTPUT characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET ABORT OUTPUT ^O
```

DEFINE/SET PORT TELNET ATTENTION

Specify whether or not there will be a character which causes a Telnet host to return to the operating system command prompt

Notes

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, causes the Telnet host to return to the operating system command prompt.

While in a Telnet remote session, when a user issues the TELNET ATTENTION command, the remote server port will pass a BREAK to the host or device to which it is connected.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET ATTENTION** **[*character*]**
[NONE]*

Where	Means
character	**Specifies the character which, when typed by a user in a Telnet session, causes the Telnet host to return to the operating system command prompt.** **It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, line editing command, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ATTENTION characteristic (in this case CTRL/Y).**
NONE	**There will not be a character which, when typed by a user in a Telnet session, causes the Telnet host to return to the operating system command prompt. This is the default setting for the TELNET ATTENTION characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET ATTENTION ^Y
```

DEFINE/SET PORT TELNET BINARY SESSION MODE

Specify whether or not Telnet sessions will negotiate binary mode

Notes

Use this command to specify whether or not Telnet sessions will negotiate binary mode, and for ports that can negotiate binary mode, if they should change their session mode to PASSALL or PASTHRU after they have negotiated binary mode.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET BINARY SESSION MODE [INTERACTIVE] [PASSALL] [PASTHRU]***

Where	Means
INTERACTIVE	**Specifies that when binary negotiation is initiated from a remote host, the port will negotiate "won't binary".**
PASSALL	**The port(s) can negotiate binary mode, but disables all switch characters, Telnet command characters, server messages, and XON/XOFF flow control. In PASSALL mode, all characters are passed to the connection partner as data. This allows data files that contain control character to be transferred without interference from the server. Typically, you would use this mode for binary file transfers (e.g., transferring a program via modem).**
PASTHRU	**The port(s) can negotiate binary mode, but disables all switch characters, Telnet command characters, server messages, but leaves XON/XOFF flow control enabled. Typically, you would use this mode for ASCII file transfers (e.g., printing on a line printer connected to a port). This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET BINARY SESSION MODE PASSALL
```

DEFINE/SET PORT TELNET CSI ESCAPE

Specify how to pass to the connection partner eight-bit escape sequences, received by the port during a Telnet session

Notes

Use this command to specify whether or not eight-bit escape sequences, received by the port during a Telnet session, will be passed to the connection partner unaltered (i.e., as eight-bit sequences), or whether these sequences will be translated into their seven-bit equivalents.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET CSI ESCAPE** **[DISABLED]*** **[ENABLED]**

Where	Means
DISABLED	**Eight-bit escape sequences, received by the port during a Telnet session, will be translated into their seven-bit equivalents before they are passed to the connection partner. This is the default setting.**
ENABLED	**Eight-bit escape sequences, received by the port during a Telnet session, will be passed to the connection partner unaltered.**

Example

```
Xyplex>> DEFINE PORT 5  TELNET CSI ESCAPE ENABLED
```

DEFINE PORT TELNET DEDICATED SERVICE

Specify a permanent Telnet service for a port

Notes

Use this command to specify whether or not there will be a Telnet destination to which the port is permanently assigned, or that there will be a change made to the current permanent service assignment for the port. The effect of this characteristic is to automatically connect the port to a dedicated service, whenever a user logs on to that port.

You can only use a DEFINE command to specify a Telnet dedicated service.

Privilege Level

Privileged.

Syntax

DEFINE PORT ***port-list*** **TELNET DEDICATED SERVICE [*domain-name*[:*telnet-port-number*]]**
[*internet-address*[:*telnet-port-number*]]

Where	Means
domain-name	**The logical name of the Telnet destination to which the port is permanently assigned. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.**
internet-address	**The identity or location on the network of the Telnet destination to which the port is permanently assigned.**
:telnet-port-number	**The number of the target Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port is permanently assigned. Note that the colon character (:) is required to separate the telnet-port-number from the domain-name.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET DEDICATED SERVICE FINANCEHOST.XYPLEX.COM

Xyplex>> DEFINE PORT 5 TELNET DEDICATED SERVICE 140.179.244.100
```

DEFINE/SET PORT TELNET DEFAULT PORT

Assign a default telnet-port-number

Notes

Use this command to assign or change the telnet-port-number (protocol or physical port address) which the port will use for operations where the user does not specify a telnet-port-number. This is used to specify the default "source port" number for outgoing (local access) connections being made from this port to a host. (Compare this with the telnet-remote-port number, which is used as the "destination port" for incoming connections.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET DEFAULT PORT [***telnet-port-number***]**

Where	Means
telnet-port-number	**Specifies the number representing a protocol or physical port address which the port will use for operations where the user does not specify a telnet-port-number. The default value is 23.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET DEFAULT PORT 2300
```

DEFINE/SET PORT TELNET ECHO MODE

Specify how characters typed during a Telnet session will be"echoed"

Notes

Use this command to specify how a connection partner will "echo" (return for display at the screen, or print) characters which are typed at the keyboard of a terminal, during a Telnet session.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET ECHO MODE [LOCAL] [REMOTE]***

Where	Means
LOCAL	**Characters which are typed at the keyboard will be echoed by the server.**
REMOTE	**Characters which are typed at the keyboard will be echoed by the connection partner, if possible (i.e., the server will attempt to negotiate remote echo). This is the default setting for the TELNET ECHO MODE characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET ECHO MODE LOCAL
```

DEFINE/SET PORT TELNET EOR REFLECTION

Specify whether or not the port will reply using an End-of-Record (EOR) message

Notes

Use this command to specify whether or not the server will send an End-of-Record (EOR) message back to the host, when the server detects an EOR message at the end of the data sent by the host.

For some UNIX hosts, it is necessary for the print filter to add an EOR (End of Record) "handshake" to the end of the data in a print job or there is a risk that the connection will be closed before the print job is completed. Using EOR messages, the port and the print filter will not close the connection until the hand-shaking is complete, thus guaranteeing that all data are delivered to the port. To use this feature, you must set the PORT TELNET EOR REFLECTION characteristic to ENABLED for the port to which the printer is connected, and you must compile the print filter using the -eor option. (This is described in the *Software Management Guide*.) You must enable or disable EOR handshaking at both the port and the host or connections may not properly be closed when they should be.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET EOR REFLECTION** **[DISABLED]*** **[ENABLED]**

Where	Means
DISABLED	**The server will not send an EOR message back to the host, when the server detects an EOR message at the end of the data sent by the host. This is the default.**
ENABLED	**The server will send an EOR message back to the host, when the server detects an EOR message at the end of the data sent by the host.** **You must only set this characteristic to ENABLED when EOR messages are being used by both the host and the server.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET EOR REFLECTION ENABLED
```

DEFINE/SET PORT TELNET ERASE CHARACTER

Specify a command for Telnet sessions that deletes the character immediately to the left of the cursor

Notes

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET ERASE CHARACTER** **[*character*]**
[NONE]*

Where	Means
character	**The character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor.** **It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, line editing commands, or other Telnet command characters).**
NONE	**There will not be a character which, when typed by a user in a Telnet session, deletes the character immediately to the left of the cursor. This is the default setting for the TELNET ERASE CHARACTER characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET ERASE CHARACTER ^K
```

DEFINE/SET PORT TELNET ERASE LINE

Specify a command for Telnet sessions that deletes all data in the current line of input

Notes

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET ERASE LINE** **[***character***]**
[NONE]*

Where	Means
character	**Specifies the character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed.** **It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET ERASE LINE characteristic (in this case CTRL/U).**
NONE	**There will not be a character which, when typed by a user in a Telnet session, deletes all data in the current line of input, backwards from the cursor position to a prompt or a carriage-return/line-feed. This is the default setting for the TELNET ERASE LINE characteristic. This can also be used to cancel a previously-defined Erase Line character.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET ERASE LINE ^U
```

DEFINE/SET PORT TELNET INTERRUPT

Specify a character for a Telnet session which interrupts terminates a user process.

Notes

Use this command to specify whether or not there will be a character which, when typed by the user in a Telnet session, suspends, interrupts, aborts, or terminates a user process.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET INTERRUPT** **[*character*]**
[NONE]*

Where Means

character **Specifies the character which, when typed by a user in a Telnet session, suspends, interrupts, aborts, or terminates a user process.**

It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET INTERRUPT characteristic (in this case CTRL/C).

NONE **There will not be a character which, when typed by the user in a Telnet session, suspends, interrupts, aborts, or terminates a user process. This is the default setting for the TELNET INTERRUPT characteristic. This can also be used to cancel a previously-defined interrupt character.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET INTERRUPT ^C
```

DEFINE/SET PORT TELNET NEWLINE

Specify how the port should send new-line (RETURN) sequences

Notes

Use this command to specify the character(s) that the server should transmit to the connection partner in a Telnet session, when the user presses the RETURN key.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET NEWLINE** **[NULL]***
[LINEFEED]
[NOTHING]

Where	Means
NULL	**The server should send a carriage-return and a NULL character to the connection partner in a Telnet session, when the user presses the RETURN key. This is the default.**
LINEFEED	**The server should send a carriage-return and a line-feed character to the connection partner in a Telnet session, when the user presses the RETURN key.**
NOTHING	**The server should only send a carriage-return character to the connection partner in a Telnet session, when the user presses the RETURN key.**

Example

```
Xyplex>> DEFINE PORT 5 NEWLINE LINEFEED
```

DEFINE/SET PORT TELNET NEWLINE FILTERING

Specify how the port should translate new-line sequences

Notes

Use this command to specify whether or not the server should translate Telnet new-line sequences going from the network to the serial devices, and if it is translating these sequences, in what manner it will perform this translation.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET NEWLINE FILTERING [NONE]* [LINEFEED] [CR] [NULL] [STANDARD]**

Where	Means
NONE	**The server should not translate Telnet new-line sequences. This is the default setting for this characteristic.**
CR	**The server should translate Telnet new-line sequences by changing a CR/NULL or CR/LF in the data stream to a CR.** **This setting is recommended for port 0 (console port).**
NULL	**The server should translate Telnet new-line sequences by changing a CR/NULL or CR/LF in the data stream to a CR/NULL.**
LINEFEED	**The server should translate Telnet new-line sequences by changing a CR/NULL or CR/LF in the data stream to a CR/LF.**
STANDARD	**The server should translate Telnet new-line sequences by changing a CR/NULL in the data stream to a CR.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET NEWLINE FILTERING CR
```

DEFINE/SET PORT TELNET OPTION DISPLAY

Specify whether or not the port should display Telnet option negotiations.

Notes

Use this command to specify whether or not the port should display Telnet option negotiations.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* TELNET OPTION DISPLAY [DISABLED]* [ENABLED]

Where	Means
DISABLED	**The port should not display Telnet option negotiations. This is the default setting for the TELNET OPTION DISPLAY characteristic.**
ENABLED.	**The port should display Telnet option negotiations.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET OPTION DISPLAY ENABLED
```

DEFINE/SET PORT TELNET PREFERRED SERVICE

Assign a Telnet service to which the port will connect whenever a user makes a connect request without specifying a service

Notes

Use this command to specify whether or not there will be a Telnet destination to which the port will connect whenever a user makes a connect request without specifying a service or that there will be a change made to the current preferred service assignment for the port.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET PREFERRED SERVICE** **[*domain-name*[:*telnet-port-number*]]**
[*internet-address*[:*telnet-port-number*]]

Where	Means
domain-name	**Specifies the logical name of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a domain-name. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.**
internet-address	**Specifies the identity or location on the network of the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying an internet-address.**
:telnet-port-number	**Specifies the number of the Internet protocol or physical port address which will be used for sessions between the port and the Telnet destination to which the port will be connected, whenever a user makes a connect request without specifying a Telnet destination.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET PREFERRED SERVICE FINANCEHOST.XYPLEX.COM

Xyplex>> DEFINE PORT 5 TELNET PREFERRED SERVICE 140.179.244.100
```

DEFINE/SET PORT TELNET QUERY

Specify a command for Telnet sessions that provides a user with an indication that the system is still up and running

Notes

Use this command to specify whether or not there will be a character which, when typed by a user in Telnet session, provides a user with a visible indication that the system is still up and running. This command is useful when a user feels that a session has been unexpectedly "silent" for a long time (this could be due to an unusually heavy load on the network or connection partner, or because an operation requires an unanticipated amount of time to complete, etc).

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET QUERY** **[*character*]**
[NONE]*

Where	Means
character	**Specifies the character which, when typed by a user in a Telnet session, provides a user with a visible indication that the system is still up and running.** **It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, line-editing command, or any other Telnet command characters). If your network supports both LAT and Telnet sessions, you may minimize user confusion caused by switching among different session types if you specify a VMS equivalent to the TELNET QUERY characteristic (in this case CTRL/T).**
NONE	**There will not be a character which, when typed by a user in a Telnet session, provides a user with a visible indication that the system is still up and running. This is the default setting for the TELNET QUERY characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET QUERY ^T
```

DEFINE/SET PORT TELNET REMOTE

Assign a telnet-port-number offered on the network for one or more physical server ports, so that multiple ports can have the same telnet-port-number

Notes

Use this command to assign or change the telnet-port-number offered on the network for one or more physical server ports. This allows multiple ports to have the same telnet-port-number, so that any of these physical ports are available to service Telnet connection requests, made to a specific telnet-port-number. This is used to specify the default destination port number for incoming (remote access) connections being made to this port from a host.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* TELNET REMOTE [*telnet-port-number*]

Where	Means
telnet-port-number	**The telnet-port-number offered on the network as the address for one or more physical ports. More than one port may have the same remote port number. Assigning the same remote port number to multiple ports allows them to be part of the same logical group (for example, several ports can be part of a bank of dialout ports, each of which have the same address). The default value is [2000 + (100 x *n*)], where *n* is the physical server port number.**

Example

```
Xyplex>> DEFINE PORT 5-8 TELNET REMOTE 2500
```

DEFINE/SET PORT TELNET SYNCHRONIZE

Specify a command for Telnet sessions that allows the user to regain control of a "runaway" process

Notes

Use this command to specify whether or not there will be a character which, when typed by a user in a Telnet session, allows the user to regain control of a "runaway" process.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TELNET SYNCHRONIZE [*character*]**
[NONE]*

Where	Means
character	**The character which, when typed by a user in a Telnet session, allows the user to regain control of a run-away process.** **It is recommended that you specify an unused CTRL character for this characteristic. Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, with the character you set for the BACKWARD SWITCH, FORWARD SWITCH, or the LOCAL SWITCH characteristics, or any other Telnet command characters).**
NONE	**There will not be a character which, when typed by a user in a Telnet session, allows the user to regain control of a run-away process. This is the default setting for the TELNET SYNCHRONIZE characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET SYNCHRONIZE ^K
```

DEFINE/SET PORT TELNET TERMINALTYPE

Assign a terminal type to a port for Telnet or RLOGIN sessions

Notes

Use this command to specify whether or not the port will emulate a particular terminal type during a TELNET or RLOGIN session. The server will use the terminal type you specify during Telnet option negotiations. This terminal type is not used for Tn3270 sessions. Refer to the documentation supplied with your host Telnet implementation for a list of valid Telnet terminal types.

Privilege Level

Syntax

DEFINE/SET PORT *port-list* TELNET TERMINALTYPE "*terminal-type*"

Where	Means
terminal-type	**Specifies the terminal type to be used during a TELNET or RLOGIN session. Valid values are text strings up to 21 characters long. You must enclose the *terminal-type* string in quotation marks (").**

Example

```
Xyplex>> DEFINE PORT 5 TELNET TERMINALTYPE "VT220"
```

DEFINE/SET PORT TELNET TN3270 DEVICE

Assign a Tn3270 device to a port

Notes

Use this command to indicate whether or not the ports you specify will emulate a particular terminal type during a Tn3270 session. If you specify a device name, the terminal server will automatically assign the USENGLSH Tn3270 translation to the ports you specify with this keyword. If you want to assign a different translation table to these ports, use the DEFINE/SET PORT TELNET TN3270 TRANSLATIONTABLE command.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET TN3270 DEVICE [*device-name*] [NONE]***

Where	Means
device-name	**Specifies the type of terminal that the ports will emulate during a Tn3270 session. You can use the name of a device supplied by Xyplex (ANSI, VT100, VT220-7, or VT220-8), or the name of a device table you have created. See the *Software Management Guide* for more information about how to create device tables.**
NONE	**Disable the terminal emulation feature. This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET TN3270 DEVICE ANSI
```

DEFINE/SET PORT TELNET TN3270 PRINTER PORT

Assign TN3270 printer ports for TN3270 users

Notes

The server can support two or more local printers for TN3270 screen printing. This version also allows you to assign ports on the terminal server to specific printers, so that the printing always occurs on ports.

To enable support for screen printing, you assign the ACCESS PRT3270 characteristic to one or more ports. The TN3270 printer ports must have valid device names.

The SHOW/LIST MONITOR PORTS TELNET CHARACTERISTICS display includes the TN3270 printer port assignment, or ANY if you have not specified a port.

The following commands set up normal 80-column printing on a terminal server port:

DEFINE PORT *port-list* ACCESS PRT3270
DEFINE PORT *port-list* TELNET TN3270 DEVICE VT100
DEFINE PORT *port-list* AUTOBAUD DISABLED
DEFINE PORT *port-list* SPEED *baud-rate*
DEFINE PORT *port-list* PARITY *parity*
DEFINE PORT *port-list* CHARACTER SIZE *character-size*
LOGOUT PORT *port-list*

See the *Commands Reference Guide* for more information about these commands.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* TELNET TN3270 PRINTERPORT *port-number* | ANY

Where	Means
port-list	**One or more terminal server ports that you want to assign to a printer port for local TN3270 screen printing.**
ANY	**Use any available port with ACCESS PRT3270 enabled to print the screen.**
port-number	**Any valid port number with ACCESS PRT3270 enabled and a valid TN3270 device name. When you assign a printer port to a port, the terminal server**

Example

```
Xyplex>> DEFINE PORT 3 TELNET TN3270 PRINTER PORT 4
```

DEFINE/SET PORT TELNET TN3270 TRANSLATIONTABLE

Assign a Tn3270 language translation table

Notes

Use this command to assign a Tn3270 language translation table to the ports you specify.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET TN3270 TRANSLATIONTABLE [***trans-name***] [NONE]***

Where	Means
trans-name	**Specifies the name of the Tn3270 translation table that the server will use at these ports during Tn3270 sessions. The default is USENGLSH (American English), which the server automatically assigns to ports when you assign them a Tn3270 device type. You can define your own language translation tables, however. See the *Software Management Guide* for more information about how to create translation tables.**
NONE	**Do not assign a Tn3270 translation table to these ports. If you have assigned a Tn3270 device at these ports, you cannot specify NONE as the translation table. Ports that have Tn3270 devices must also have translation tables.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET TN3270 TRANSLATIONTABLE USENGLSH
```

DEFINE/SET PORT TELNET TN3270 XTDATTRS

Enable or disable Tn3270 extended screen attributes

Notes

Use this command to specify whether or not extended screen attributes will be supported at the ports you specify during a Tn3270 session. These attributes include blink, reverse video, underline, and color.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET TN3270 XTDATTRS [DISABLED*] [ENABLED]**

Where	Means
ENABLED	**The port will support extended attributes at the ports you specify during a Tn3270 session.**
DISABLED	**Do not enable the extended attributes feature. This is the default for this characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TELNET TN3270 XTDATTRS ENABLED
```

DEFINE/SET PORT TELNET TRANSMIT

Specify the time when the server will transmit characters which are typed at a port during a Telnet session

Notes

Use this command to specify the time when the server will transmit characters which are typed at a keyboard during a Telnet session. This characteristic is ignored when the TELNET ECHO MODE characteristic is set to REMOTE.

This characteristic does not apply to parallel ports.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT ***port-list*** **TELNET TRANSMIT** **[BUFFERED]***
[IMMEDIATE]
[IDLETIME] [*character-times*]

Where	Means
BUFFERED	**Specifies that, for a Telnet session, the server will not transmit characters typed at the keyboard until a control character (such as the RETURN key) is typed at the keyboard. This is the default.**
IMMEDIATE	**Specifies that, for a Telnet session, the server will send each character as soon as possible after it is typed at the keyboard.**
IDLETIME	**Specifies that you will define or change the maximum amount of time, specified as a number of characters, that the server will wait before transmitting the data in the typeahead buffer to the connection partner.** **This characteristic allows you to specify when the server will transmit user input from a Telnet or RLOGIN session. The server will wait until the port has been idle for the specified period of time, or until the amount of accumulated data exceeds 80% of the typeahead buffer size.** **This characteristic is useful when the device connected to the port waits until a control character (such as the RETURN key) is typed at the keyboard, before it transmits data in the typeahead buffer (for example, data that the user has typed, or from a modem). This characteristic tells the port to send the data at the specified time, even though the control character has not been typed. This characteristic is recommended for ports whose ACCESS characteristic is set to REMOTE or DYNAMIC. This characteristic is intended to help limit the amount of network traffic, when the device connected to the port does not need remote echoing of data.**

character-times **Specifies the maximum amount of time, specified as a number of characters, that the server will wait before transmitting the data in the typeahead buffer to the connection partner. Valid values are whole numbers in the range of 1 to 255 characters. The default value is 1.**

To determine how much time that the server can wait before it will transmit the data in the typeahead buffer to the connection partner, convert *character-times* into seconds, as follows:

time* = [*character-times* * *bits-per-character*] / *port-speed

For example, for a port which has a port-speed of 2400 baud, 8 bits per character, and a TELNET TRANSMIT IDLETIME value of 255, the server will wait 0.85 seconds to transmit data in the typeahead buffer to the connection partner.

Example

```
Xyplex>> DEFINE PORT 5 TELNET TRANSMIT IDLETIME 1
```

DEFINE/SET PORT TELNET URGENT BREAK

Specify how the the server should transmit Break sequences to Telnet partners

Notes

The Telnet Urgent Break feature determines whether or not a Break sequence is marked "Urgent" when sent to a partner in a Telnet session.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* TELNET URGENT BREAK ENABLED | DISABLED

Where	Means
ENABLED	**Break sequences are marked "Urgent" when sent to a partner in a Telnet session.**
DISABLED	**Break sequences are not marked "Urgent" when sent to a partner in a Telnet session. This is the default**

Example

```
Xyplex >>DEFINE PORT TELNET URGENT BREAK ENABLED
```

DEFINE/SET PORT TYPE

Specify the type of terminal connected to a port

Notes

Specifies that you will define or change the type of terminal which is connected to your port, the port(s) specified in the port-list, or all ports. The terminal type affects the manner in which the attached device produces output, and how the server performs certain device specific functions. For terminals which support emulation of multiple terminal types, the setting for this characteristic should match the actual terminal setting. The setting for the TYPE characteristic only affects the operation of the terminal in local command mode.

This characteristic does not apply to parallel ports.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **TYPE** **[ANSI]**
[HARDCOPY]
[SOFTCOPY]*

Where	Means
ANSI	**The terminal produces output on a video display and supports ANSI escape sequences. Generally, this type of terminal supports the clear screen function and special cursor control functions, but not line drawing (e.g., any VT100, VT200, VT300 or compatible terminal).**
HARDCOPY	**The terminal is a hard-copy (e.g., a printing or non-video display) terminal, or will emulate the operation of a hard-copy terminal. Generally, this means that the attached device produces output on paper. For this type of device, when you delete characters, the deleted characters are echoed between back-slash characters (\).**
SOFTCOPY	**The terminal produces output on a video display but does not support ANSI escape sequences. This type of terminal does echo character deletions when you use the DELETE key, but does not support line drawing, the clear screen function, or special cursor control functions. This is the default setting for the TYPE characteristic.**

Example

```
Xyplex>> DEFINE PORT 5 TYPE HARDCOPY
```

DEFINE/SET PORT TYPEAHEAD SIZE

Specify the number of bytes or characters that can be temporarily stored by the port pending transmission

Notes

Use this command to specify the size of the type-ahead buffer (the number of bytes or characters that can be temporarily stored pending transmission) for sessions at your port, the port(s) specified in the port-list, or all ports.

This characteristic does not apply to parallel ports.

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT *port-list* TYPEAHEAD SIZE *size*

Where	Means
size	**Specifies the number of bytes (characters) that can be stored in the type-ahead buffer for sessions at your port, the port(s) specified in the port-list, or all ports. Valid values for this variable are whole numbers in the range of 80 to 16384. The default setting for the TYPEAHEAD SIZE characteristic is 128. You should be careful to limit this value, as the typeahead buffer uses resources from the servers pool.**

Example

```
Xyplex>> DEFINE PORT 5 TYPEAHEAD SIZE 16384
```

DEFINE/SET PORT USER KERBEROS PASSWORD

Specify a Kerberos password

Notes

Use this command to assign or change a Kerberos password. When you issue the DEFINE PORT USER KERBEROS PASSWORD command, the server prompts you for your current password (old password) and the new password. The server then prompts you to verify the new password by retyping it.

The server queries the Kerberos Master when you change a password. If the Master does not respond, you are asked to try again later.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* USER KERBEROS PASSWORD

Example

```
Xyplex> DEFINE PORT USER KERBEROS PASSWORD

Old password>

New password>

Verification>
```

DEFINE/SET PORT USERNAME

Assign a name to a port

Notes

Use this command to define or change a username to be assigned to a port. When a user logs in to a port that has a username assigned to it, the port bypasses the Username prompt. (Depending on the setting of the PASSWORD characteristic, the port may display a password prompt. If the PASSWORD characteristic is set to DISABLED, the port will display the Xyplex> prompt or connect to a dedicated service.) The username also appears in server displays.

If you manage servers using TSM, do not assign a *username* to port 0, or TSM will not work properly.

Privilege Level

Non-privileged.

Syntax

DEFINE/SET PORT *port-list* USERNAME "*name*"

Where	Means
username	**The name to be assigned to the port. The name can be between 1 to 16 ASCII characters in length. You must enclose the name in quotation marks ("). The server will accept the name exactly as it is specified (including spaces, commas, and upper-case or lower-case letters). To cancel a previously-defined username, specify a null string (e.g., " "). The default setting for the USERNAME characteristic is no username, but the default name for the port is a name in the form PORT_*port-number*, where *port-number* is the number of the physical port or 0 for the console port.**

Example

```
Xyplex>> DEFINE PORT 5 USERNAME "John's port"
```

In this example, the server manager is cancelling all previously defined user names for all ports on the server. Afterwards, the portnames revert to the defaults.

```
Xyplex>> DEFINE PORT ALL USERNAME ""
```

DEFINE/SET PORT VERIFICATION

Specify whether or not informational messages are displayed at the port

Notes

Use this command to specify whether or not the server will display informational messages, at the port(s) listed in the port-list or all ports, whenever a user connects, disconnects, or switches a session.

Privilege Level

Secure

Syntax

DEFINE/SET PORT ***port-list*** **VERIFICATION** **[DISABLED]**
[ENABLED]*

Where	Means
DISABLED	**The server will not display informational messages, at the port(s) listed in the port-list or all ports, whenever a user connects, disconnects, or switches a session.**
ENABLED	**The server will display informational messages, at the port(s) listed in the port-list or all ports, whenever a user connects, disconnects, or switches a session. This is the default setting for the VERIFICATION characteristic.**

Example

```
Xyplex> DEFINE PORT VERIFICATION DISABLED
```

DEFINE PORT XDM HOST

Specify the location and query type for an XDM host

The DEFINE PORT XDM HOST command specifies the domain name or Internet address of an XDM host and the query type for that host.

Notes

The query type specifies the method that the terminal server uses to search for an XDM manager. Three query types are available: SPECIFIC, BROADCAST, and INDIRECT. SPECIFIC and INDIRECT query types search for the domain name or Internet address you specify. The BROADCAST query type searches for the XDM host using the terminal server Internet broadcast address specified in the DEFINE/SET SERVER INTERNET BROADCAST ADDRESS command.

The INDIRECT query type is only compatible with version X11R5 X Windows or higher.

Privilege Level

Privileged

Syntax

DEFINE PORT *port-list* XDM HOST [*domain-name*/*internet-address*/NONE] [QUERY [*type*]]

Where	Means
port-list	**One or more ports that you want to associate with the XDM HOST and QUERY type that you specify.**
domain-name ***internet-address***	**The domain name or Internet address of the host that will be the XDM manager for the ports you specify.**
NONE	**Remove the previously defined domain name or Internet address of an XDM host.**

Where	Means
QUERY	**One of the following query types. If you do not specify a query type, the terminal server uses the BROADCAST query type as the default.**

type	Means
SPECIFIC	**The ports you specify search for the host at the location in the *domain-name* or *internet-address* variable, which is the XDM manager. This is the default query type.**
BROADCAST	**The ports you specify search the network for an XDM manager using the Internet broadcast address.**
INDIRECT	**The ports you specify search for the host at the location in the *domain-name* or *internet-address* variable. This host provides a list of XDM managers on the network.**

Examples

1. This command specifies the Internet address of an XDM host. It assumes the Broadcast query type, which is the default, so the command line does not include a specific query type.

```
Xyplex>> define ports 8-16 xdm host 117.153.89.3

Xyplex>>
```

2. This command specifies an XDM host with a domain name, and the Specific query type.

```
Xyplex>> define port 2 xdm host dev.sun.com query type specific

Xyplex>>
```

3. This command specifies an XDM host with an Internet address and the Indirect query type.

```
Xyplex>>  define ports 5-7 xdm host 123.321.32.23 query type
indirect
```

DEFINE PORT XREMOTE

Assign a port to exclusive Xremote support

The DEFINE PORT XREMOTE command determines whether or not a port searches for the XDM host as soon a user logs on to the port, rather than returning the Xyplex command interface.

Notes

If this characteristic is enabled, the terminal server searches for the XDM host you have defined either with a Specific, Indirect, or Broadcast query type. See the DEFINE PORT XDM HOST command for more information on how to do this.

Privilege Level

Privileged

Syntax

DEFINE PORT *port-list* XREMOTE ENABLED/DISABLED

Where	Means
ENABLED	**Enable the Xremote characteristic at the ports you specify.**
DISABLED	**Disable the Xremote feature at the ports you specify. This is the default value for this characteristic.**

Example

```
XYPLEX>> DEFINE PORT 5 XREMOTE ENABLED
```

DEFINE/SET SERVER - General Information

Alter permanent or operational server characteristics

The DEFINE SERVER and SET SERVER commands specify or modify server characteristics. Generally, server characteristics control communication between the server and the nodes. Changes that are made using the SET SERVER command take effect immediately and are only in effect until the server is re-initialized. Changes made via the DEFINE SERVER command take effect whenever the server is re-initialized. Changes can be made to take effect both immediately and on a permanent basis when the SERVER CHANGE characteristic is set to ENABLED.

Only privileged users can use the DEFINE SERVER or SET SERVER commands.

The basic syntax for the DEFINE SERVER and SET SERVER commands is:

[DEFINE] SERVER [*characteristic(s)*]
[SET]

As shown above, multiple server characteristics can be defined or set with a single command. When you specify more than one server characteristic with one command, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.) A summary of syntax for the server characteristics which can be defined follows.

You will find items which are common variables listed throughout this section. Refer to the section on Common Variables at the beginning of this chapter.

DEFINE SERVER ACCOUNTING ENTRIES

Enable or disable the accounting feature

Notes

When the accounting feature is enabled, the server creates an accounting log. Each log entry contains information about successful and attempted connections made to or from the unit, as well as information about sessions that are disconnected.

Use this command to change the maximum number of accounting entries that the server will record in the accounting log. To enable the accounting feature, you change the number of accounting entries from 0 to any number greater than or equal to 1.

You can view the the contents of the accounting log by viewing the SHOW/MONITOR SERVER ACCOUNTING display. Refer also to the *Software Management Guide* for information about the accounting feature.

Privilege Level

Privileged

Syntax

DEFINE SERVER ACCOUNTING ENTRIES *number*

Where	Means
number	**Specifies the maximum number of accounting entries that the server will record in the accounting log. Valid values are whole numbers between zero (0) and 1000. The default is 0. Changing the number from 0 to any other number has the effect of enabling the accounting feature. Changing the number to 0 has the effect of disabling the accounting feature.**

Example

```
Xyplex>> DEFINE SERVER ACCOUNTING ENTRIES 100
```

Support Issues

Requires a minimum of 1 megabyte of memory

DEFINE|SET SERVER ANNOUNCEMENTS

Enable or disable LAT service announcements

Notes

Announcements are multicast messages, which are sent by the server via the Ethernet network, to other servers. These messages indicate which LAT services are available at the server. Announcements are only multicast when there are local services defined at the server.

Use this command to enable or disable these multicast messages.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER ANNOUNCEMENTS [DISABLED]
[ENABLED]*

Where	Means
DISABLED	**Specifies that the server will not multicast announcements about available services.**
ENABLED	**Specifies that the server will multicast announcements about available services. This is the default setting.**

Example

```
Xyplex>> DEFINE SERVER ANNOUNCEMENTS ENABLED
```

Support Issues

None

DEFINE|SET SERVER BROADCAST

Enable or disable use of the BROADCAST command

Notes

This command specifies whether or not the Broadcast command is available to users at this server. The BROADCAST command allows users at one port to send a message to a user at another port.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER BROADCAST [DISABLED]
[ENABLED]*

Where	Means
DISABLED	**Specifies that the Broadcast command is not available to any users at this server.**
ENABLED	**Specifies that the Broadcast command is available to users at this server. This is the default setting for the BROADCAST characteristic.**

Example

```
Xyplex>> DEFINE SERVER BROADCAST ENABLED
```

Support Issues

None

DEFINE|SET SERVER CHANGE

Specify whether or not a DEFINE command alters both the permanent and operational databases

Notes

Normally, a DEFINE command affects only the permanent database, and a SET command affects only the operational database.

Use this command to specify whether or not the server will update both the permanent and operational database when a DEFINE command is issued. This has the effect of allowing you to perform both a DEFINE and SET operation with only a DEFINE command, and is particularly useful when first setting up a server or when you need to issue a large number of commands.

SNMP Set commands are not affected by the setting for this characteristic.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER CHANGE [DISABLED]*
[ENABLED]

Where	Means
DISABLED	**Specifies that the server will not update both the permanent and operational database when a DEFINE command is issued. This is the default.**
ENABLED	**Specifies that the server will update both the permanent and operational database when a DEFINE command is issued.**

Example

```
Xyplex>> DEFINE SERVER CHANGE ENABLED
```

Support Issues

None

DEFINE|SET SERVER CIRCUIT TIMER

Specify the length of the LAT circuit timer

Notes

The value specified for this option is the frequency with which the server communicates with service nodes when LAT sessions are active. During the specified time period, the server collects all data from active sessions, multiplexes the data, and creates Ethernet packets. At the end of the interval, the server transmits all of these packets to the appropriate service nodes for processing. Thus, the value set for this option affects the response time for the user, as well as network performance, and performance at the service nodes.

By changing the circuit timer value, you can manage the relationship (or trade-off) between user response time and efficient use of network and service node resources. For example, setting a short time interval means that users receive fast response time, but there is more traffic on the network and service nodes must respond more frequently. A longer time interval means that users receive a slower response time, but there is less network traffic and server nodes must respond less frequently. Thus, you may decide to specify a longer time interval when network or service node performance suffers from heavy use, while lightly loaded network and service node resources can support faster user response times.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER CIRCUIT TIMER *timer-value*

Where	Means
timer-value	**Specifies the length of the circuit timer interval, in milli-seconds. The value specified must be a whole number in the range of 30 to 200 milliseconds (do not include units). The default value is 80.**

Example

```
Xyplex>> DEFINE SERVER CIRCUIT TIMER 100
```

Support Issues

None

DEFINE|SET SERVER CONSOLE LOGOUT

Specify whether or not the server immediately disconnects the console port when the user logs out a console session

Notes

Use this command to specify whether or not the server will immediately disconnect a console port session when the user logs out from the console port (port 0). This applies to sessions established via REMOTE CONSOLE and TELNET CONSOLE.

The terminal server does not immediately disconnect a console port session with the CONSOLE LOGOUT feature enabled, if the user established the session through the REMOTE CONSOLE command. The terminal server does disconnect the session after about 10 seconds. The terminal server does immediately disconnect console port sessions established through TELNET CONSOLE, TELNET CONNECT, or CHASSIS CONSOLE if the CONSOLE LOGOUT feature is enabled.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER CONSOLE LOGOUT [DISABLED]* [ENABLED]

Where	Means
DISABLED	**Specifies that the server will not immediately disconnect a console port session when the user logs out from the console port. In this case, the user must disconnect the session using the DISCONNECT command. This is the default.**
ENABLED	**Specifies that the server will immediately disconnect a console port session when the user logs out from the console port.**

Example

```
Xyplex>> DEFINE SERVER CONSOLE LOGOUT ENABLED
```

Support Issues

None

SET SERVER DATE

Specify the date for the server

Notes

Specifies that the date that is maintained by the server will be set or changed.

Note that the load server (the host from which the server obtains software to run) supplies the default date that is maintained by the unit.

Privilege Level

Privileged

Syntax

SET SERVER DATE *dd mmm yyyy*

Where	Means
dd mmm yyyy	**Specifies the new date which will be maintained by the unit. Specify this date using the following format:**

dd **is a one or two digit number which is the day of the month. Valid values for dd are numbers in the range of 1 to 31.**

m m m **are the first three letters of the month (e.g., JAN, FEB, etc).**

yyyy **is the year (e.g., 1993).**

Separate each item in the date with a space.

Example

```
Xyplex>> SET SERVER DATE 11 JUL 1993
```

Support Issues

None

DEFINE|SET SERVER DUMP

Enable or Disable memory dumping when a "fatal" error occurs

Notes

Use this command to specify whether or not the server will perform a "crash dump" of the contents of the server memory, when the server detects a fatal error, before the server re-initializes.

During a crash dump procedure, the server sends a copy of the contents of its memory to a "dump file" at the load host for analysis by Xyplex Customer Support personnel, and the server re-initializes.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER DUMP [DISABLED]
[ENABLED]*

Where	Means
DISABLED	**The server will not perform a memory dump when it detects a fatal error.**
ENABLED	**The server will perform a memory dump when it detects a fatal error. This is the default.**

Example

```
Xyplex>> DEFINE SERVER DUMP ENABLED
```

Support Issues

None

DEFINE SERVER DUMP PROTOCOL

Enable or disable dump protocols

The DEFINE SERVER DUMP PROTOCOL command enables or disables one or all dump protocols. The terminal server uses a dump protocol to send information to a dump server.

Notes

All available dump protocols are enabled by default: XMOP, MOP, BOOTP, and RARP.

Privilege Level

Privileged

Syntax

On MAXserver 1620/1640 Terminal Servers or Network 9000 Terminal Server 720:

DEFINE SERVER DUMP *record* PROTOCOL *protocol* [ENABLED]
[DISABLED]

On MAXserver 800/1600 Terminal Servers or MAXserver 1450 Printer Server:

DEFINE SERVER DUMP PROTOCOL *protocol* [ENABLED]
[DISABLED]

Where	Means
record	**One or more of the following MAXserver 1620/1640 Terminal Servers or Network 9000 Terminal Server 720 initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**
protocol	**One of the following protocols :**

Protocol	Means
XMOP	**Xyplex MOP Protocol**
MOP	**Digital Equipment Corporation Maintenance Operations Protocol**
BOOTP	**Bootstrap protocol**
RARP	**UNIX Reverse Address Resolution Protocol**
ALL	**All protocols (only for MAXserver 1620/1640 Terminal Servers or Network 9000 Terminal Server 720)**

ENABLED **Enable the protocol. You can enable only one protocol in the command line, unless you use the keyword ALL to enable all protocols.**

DISABLED **Disable the protocol. You can specify ALL to disable all protocols.**

Examples

1. This command enables BOOTP as a dump protocol for the primary record.

```
Xyplex>> define server dump protocol bootp enabled
```

2. This command disables MOP as a dump protocol for the secondary record.

```
Xyplex>> define server dump secondary protocol mop disabled
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER EVENTLOG

Enable or Disable a MAXserver 1800/1820 or MAXMAN unit event log.

Notes

Specifies whether or not a MAXserver 1800/1820 or MAXMAN unit will record when certain events occur (for example, when it loads another unit, stores parameters or a dump from a unit, offers load/dump/parameter services, etc).

Refer to the *Software Installation Guide for Xyplex Loader Kits* for more information about the event log.

Privilege Level

Privileged

Syntax

DEFINE SERVER EVENTLOG [ENABLED]*
[DISABLED]

Where	Means
ENABLED	**Specifies that a MAXserver 1800/1820 unit will record when certain events occur. This is the default.**
DISABLED	**Specifies that a MAXserver 1800/1820 unit will not record when certain events occur.**

Example

```
Xyplex>> DEFINE SERVER EVENTLOG ENABLED
```

Support Issues

Supported on MAXserver 1800/1820 and MAXMAN units only.

DEFINE SERVER HELP

Enable or disable HELP messages

Notes

Specifies whether or not users will be able to obtain help information about commands via the HELP facility.

Privilege Level

Privileged

Syntax

DEFINE SERVER HELP [ENABLED]*
[DISABLED]

Where	Means
ENABLED	**Specifies that users will be able to obtain help information about commands via the HELP facility. This is the default.**
DISABLED	**Specifies that users will not be able to obtain help information about commands via the HELP facility.**

Example

```
Xyplex>> DEFINE SERVER HELP DISABLED
```

Support Issues

Some hardware types only offer reduced HELP messages.

DEFINE|SET SERVER IDENTIFICATION

Specify an identification message about the server

Notes

Use this command to specify a message identifying the server to be shown in server displays. You can not set this characteristic when there are any active sessions on the server.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER IDENTIFICATION "*message-string*"

Where	Means
message-string	**A text message. Specifies the text that will be displayed, for identification purposes, in server displays. The identification message can be up to 40 ASCII characters long, and must be enclosed within quotation marks ("). To remove a previously specified identification message, enter a quoted null string (" ") for the IDENTIFICATION option. The default for the IDENTIFICATION characteristic is no identification message.**

Example

```
Xyplex>> DEFINE SERVER IDENTIFICATION ""
```

Support Issues

None

DEFINE|SET SERVER IDENTIFICATION SIZE

Specify the maximum length of LAT node and service identification strings that the server stores

Notes

Use this command to specify the maximum length of LAT node and service identification strings that the server stores in memory. (The server obtains these strings from service broadcasts from other nodes and displays them in SHOW/LIST/MONITOR NODES and SERVICES displays.) By changing the maximum length of LAT node and service identification strings, the user can reduce or eliminate the memory used for these identification strings, thus freeing memory for other uses.

Refer to the chapter describing how you manage server resources in the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER IDENTIFICATION SIZE *size*

Where	Means
size	**Specifies the maximum size (bytes) of LAT node and service identification strings that are saved in server memory. Valid values for size are whole numbers between 0 to 63. Specifying a value of 0 will prevent any node or service identification strings from being saved. The default value is 63.**

Example

```
Xyplex>> DEFINE SERVER SERVER IDENTIFICATION SIZE 20
```

Support Issues

None

DEFINE|SET SERVER INACTIVITY TIMER

Specify the period of time after which certain inactive ports are logged out

Notes

Ports are considered inactive while they are in the Local command mode, do not have any active sessions established, and there is no input, output, or modem transition.

Use this commmand to specify the period of time after which an inactive port, for which the DEFINE/SET PORT INACTIVITY LOGOUT characteristic is ENABLED, will be logged out. The SERVER INACTIVITY TIMER characteristic specifies for an entire server, how long inactive ports will remain logged on before the server will log them out. This characteristic only applies to inactive ports, for which the SET PORT INACTIVITY LOGOUT characteristic is enabled.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INACTIVITY TIMER *time*

Where	Means
time	**Specifies the length of time for which a port can remain inactive, before that port is logged out. The range for this common variable is between 1 and 120 minutes (do not specify minutes). The default value is 30.**

Example

```
Xyplex>> DEFINE SERVER INACTIVITY TIMER 20
```

Support Issues

None

DEFINE|SET SERVER INTERNET ADDRESS

Specify the Internet address for this server

Notes

Use this command to specify the Internet address for this server. You cannot SET this parameter while there are any active Telnet sessions on this server.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET ADDRESS *internet-address*

Where	Means
internet-address	**Specifies the Internet address for this server. The default value is 0.0.0.0 (no internet-address).**

Example

```
Xyplex>> DEFINE SERVER INTERNET ADDRESS 140.179.224.100
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET BROADCAST ADDRESS

Specify the Internet address to be used in Internet Broadcast messages

Notes

Specifies that you will define or change the Internet address of this server that is used in Internet Broadcast messages. You cannot change this parameter while there are active Telnet terminal sessions on this server.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET BROADCAST ADDRESS *internet-address*

Where	Means
internet-address	**Specifies the Internet address of this server that is used in Internet Broadcast messages. The default value for this parameter is 255.255.255.255.**

Example

```
Xyplex>> DEFINE SERVER INTERNET BROADCAST ADDRESS 255.255.255.0
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET DEFAULT DOMAIN SUFFIX

Specify the default domain-name-suffix

Notes

Use this command to specify the default *domain-name-suffix* specification(s). The server uses the value(s) that you specify for the default *domain-name-suffixes* to develop a complete (fully-qualified) *domain-name*, whenever the user specifies an incomplete *domain-name*. (Refer to the section listing Common Variables at the beginning of this chapter for a definition of *domain-names*.)

When only a single default *domain-name-suffix* is specified, and a user specifies a *domain-name* that does not contain a period in a SHOW, LIST, CLEAR, PURGE, SET, or DEFINE SERVER INTERNET DOMAIN command, the software appends the default *domain-name-suffix* to the user-specified name. However, if multiple *domain-name-suffixes* are specified, the software will qualify the given name only with the first default *domain-name-suffix* specified by the INTERNET DEFAULT DOMAIN SUFFIX characteristic. Therefore, you should specify the most frequently used suffix as the first one in the list.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET DEFAULT DOMAIN SUFFIX [*suffix-list*]
[NONE]

where the *suffix-list* syntax is:

[*domain-name-suffix1* | *domain-name-suffix2* | ... | *domain-name-suffix8*]

Where	Means
domain-name-suffix1 **through** ***domain-name-suffix8***	**Specifies the *domain-name* specification, which the server uses in order to develop a complete (fully-qualified) *domain-name,* whenever the user specifies an incomplete *domain-name.* The server appends the suffix to the incomplete *domain-name.* Specify *domain-name-suffixes* beginning with a period character (.). The *domain-name-suffixes* must not end with a period character. Do not enclose the name in quotation marks. Separate each domain-name suffix with the vertical bar character (|), and no spaces. The default value for this characteristic is the null value.** **The maximum total characters of all names together, including vertical bars '|' and periods '.', cannot exceed 115 characters. The entire command line cannot exceed 132 characters. Each *domain-name* is limited to a maximum of 50 characters. One of the suffixes may be "no suffixes" which is specified by a single period. The keyword NONE indicates no suffixes.** **Examples of a valid *domain-name-suffix* list: .|.XYPLEX.COM|.ARPA**

Example

```
Xyplex>> DEFINE SERVER INTERNET DEFAULT DOMAIN SUFFIX .|.COM
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET [PRIMARY|SECONDARY] DOMAIN ADDRESS

Specify the internet addresses for Domain Name Servers that the server can use

Notes

Use this command to specify the internet-address at which a Domain name server is located. (Domain name servers are network objects where the network attempts to resolve a domain-name.) The server can use up to two Domain name servers (primary and secondary) to resolve a domain-name. The server will query all designated Domain servers to resolve a domain-name.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET PRIMARY DOMAIN ADDRESS *internet-address*
DEFINE | SET SERVER INTERNET SECONDARY DOMAIN ADDRESS *internet-address*

Where	Means
internet-address	**Specifies the address of the primary or secondary Domain name server. The default value is 0.0.0.0 (no Domain name server)** **You can specify the value for the INTERNET DOMAIN ADDRESS characteristic to be the same as for the INTERNET BROADCAST ADDRESS characteristic. If you do this, then other servers will respond to Domain name requests for their Internet name by supplying their internet-address.**
PRIMARY	**Specifies that the Domain name server at the internet-address is the primary Domain name server.**
SECONDARY	**Specifies that the Domain name server at the internet-address is the secondary Domain name server.**

Example

```
Xyplex>> DEFINE SERVER INTERNET PRIMARY DOMAIN ADDRESS 140.179.224.100
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET DOMAIN TTL

Specify a maximum time-to-live for all learned domain-names

Notes

When Domain Name Servers respond to a request for a domain-name that is made by the server, the response includes a time-to-live (TTL) value, which indicates for how long the server should consider the domain-name to be valid.

Use this command to specify a maximum time-to-live (TTL) value for all *domain-names* learned by the server (i.e., override the TTL supplied by the Domain Name Server).

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET DOMAIN TTL *time*

Where	Means
time	**Specifies the number of hours (0 - 168) domain names are to be kept. All domain name responses that the server receives are assigned this value. If you enter zero (0), the TTL value found in the domain name response will be used. If you enter a value greater than 168, an error message is displayed.**

Example

```
Xyplex>> DEFINE SERVER INTERNET DOMAIN TTL 24
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET GATEWAY ADDRESS

Specify the internet-address at which an Internet gateway can be located

Notes

Use this command to specify for the server the internet-address at which an Internet gateway can be located. The server can use up to two Internet gateways (primary and secondary) to locate a device on an external network. The server will use the the primary gateway to route a transmission to a remote device, until it determines that the gateway has been unable to route the transmission successfully. Then it will use the the secondary gateway.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET [PRIMARY GATEWAY ADDRESS *internet-address*]
DEFINE | SET SERVER INTERNET [SECONDARY GATEWAY ADDRESS *internet-address*]

Where	Means
internet-address	**Specifies the internet-address at which an Internet primary or secondary gateway can be located. The default value is 0.0.0.0 (no gateway).**
PRIMARY	**Specifies that the Internet gateway at the internet-address is the primary Internet gateway.**
SECONDARY	**Specifies that the Internet gateway at the internet-address is the secondary Internet gateway**

Example

```
Xyplex>> DEFINE SERVER INTERNET PRIMARY GATEWAY ADDRESS 140.179.224.100
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE SERVER INTERNET IP REASSEMBLY

Enable or Disable the reassembly of fragmented TCP/IP packets

The SERVER INTERNET IP REASSEMBLY characteristic controls whether or not server will attempt to reassemble fragmented TCP/IP packets that it receives.

Notes

Sometimes, packets that are forwarded by a gateway or a router become fragmented, between the source and the destination (i.e., the server). Generally, packet fragmentation will not be a problem, but when it is the server can either attempt to reassemble the fragmented packets, or it can simply discard them. Packet fragmentation can cause problems, particularly when using protocols that do not include a resend mechanism (for example, UDP, which does not guarantee that data will be received successfully).

The SERVER INTERNET IP REASSEMBLY characteristic controls which of these choices the server will do. If packet fragmentation is a problem, you can enable this characteristic to allow the server to attempt to reassemble the fragmented packets (there is no guarantee that this operation will be successful). This will, however, require additional server memory resources, because the server must store all the fragments until it can reassemble the complete packet. In this case, you may need to increase the setting for the DEFINE/SET SERVER PACKET BUFFER characteristic. If the server has limited extra memory, or when packet fragmentation is not a frequent problem, it is recommended that you disable the SERVER INTERNET IP REASSEMBLY characteristic.

Privilege Level

Privileged.

Syntax

DEFINE SERVER INTERNET IP REASSEMBLY ENABLED|DISABLED

Where	Means
ENABLED	**The server will attempt to reassemble fragmented TCP/IP packets that it receives.**
DISABLED	**The server will not attempt to reassemble fragmented TCP/IP packets that it receives, and the server will discard the fragments. This is the default.**

Example

```
Xyplex>> DEFINE SERVER INTERNET IP REASSEMBLY ENABLED
```

DEFINE|SET SERVER INTERNET NAME

Assign a domain name for the server

Notes

Use this command to specify the domain-name by which the server is known on the network.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET NAME *domain-name*

Where	Means
domain-name	**The domain-name by which the server is known on the network. The specified domain-name must be a fully qualified domain-name (the specified name will not be concatenated with any default Internet domain-name-suffixes).**

Example

```
Xyplex>> DEFINE SERVER INTERNET NAME SERVER1.XYPLEX.COM
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET ROTARY

Assign an internet-address or domain-name to one or more ports

Notes

The term "rotary" refers to the ability to assign the same internet-address or domain-name to multiple ports that offer the same type of service.

Use this command to create a rotary by assigning an internet address to one or more ports on the same server. Refer to the *Software Management Guide* for information about Configuring Rotary Connections.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET ROTARY [*internet-address port-list*] [*domain-name port-list*]

Where	Means
internet-address	**Specifies the *internet-address* that will be assigned to the port(s) in the *port-list*.**
domain-name	**Specifies the *domain-name* that will be assigned to the port(s) in the *port-list*.**
port-list	**Specifies the port(s) to which the *internet-address* or *domain-name* will be assigned.**

Example

```
Xyplex>> DEFINE SERVER INTERNET ROTARY PRINTER.XYPLEX.COM 2-4
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE/SET SERVER INTERNET ROUTE

Add internet routes to the routing table

Notes

An internet route specifies the preferred gateway on the local network to which the server should route traffic on the way to a particular destination host or network. The server contains a list of internet routes in both the operational and permanent databases. This list is called a routing table.

Refer to the section on Configuring Internet Routes in the *Software Management Guide.*

Use this command to add internet-route entries to the operational or permanent routing table. Internet-routes that are entered into the databases via a DEFINE/SET SERVER INTERNET ROUTE commands are called locally defined internet-routes.

In addition to the locally defined internet-routes, the server can use internet-routes that it obtains from one or more Internet gateways in the network. These internet-routes are only entered into the operational database. Internet-routes that are entered into the databases via a Internet gateway are called "learned" internet-routes. The server retains a learned internet-route in the operational database until one of the following occurs:

- **it is removed via a CLEAR SERVER INTERNET ROUTE command.**
- **the expiration of a period of time (time to live) that is assigned by the Internet gateway. The TCP/IP-LAT software limits the time to live to a maximum of 1 week (168 hours).**
- **the operational database contains the maximum number of internet-routes, a user adds a new internet-route via a SET SERVER INTERNET ROUTE command, or the terminal server learns a new internet-route from an Internet gateway. In this case, the terminal server replaces the oldest learned internet-route in the operational database with the new internet-route.**

Internet-routes that are listed in the permanent database are entered into the operational database whenever the terminal server is re-initialized. Internet-routes that are listed in the permanent database remain until they are deleted by a PURGE SERVER INTERNET ROUTE command.

The operational and permanent databases can contain a maximum of 64 internet-routes. Locally defined internet-routes remain in the operational database until they are removed via a CLEAR SERVER INTERNET ROUTE command.

Privilege Level

Privileged

Syntax

DEFINE/SET SERVER INTERNET ROUTE *internet-address* GATEWAY *gateway-internet-address*] [NETWORK] [MASK *subnet-mask*] [FIXED]

[VARIABLE]

[HOST] [FIXED]

[VARIABLE]

Where	Means
internet-address	**Specifies the address of the destination host or the address from which the terminal server should derive the address of the network on which a host is located. Specify using the standard *internet-address* format.**
GATEWAY	**Specifies that the *gateway-internet-address* which follows is the address of the gateway which will forward network traffic to the destination specified by the *internet-address*.**
gateway-internet-address	**Specifies the *internet-address* of the gateway which will forward network traffic to the destination specified by the *internet-address*. Specify using the standard *internet-address* format. The *gateway-internet-address* must be on the local network.**
NETWORK	**Specifies that the terminal server should use the *internet-address* to determine the destination network. This is the default.**
HOST	**Specifies that the terminal server should interpret the *internet-address* as being the address of a host.**
MASK	**Specifies that you will define the Internet *subnet-mask* for the routing table network entry (i.e., cannot be used in conjunction with the HOST keyword). The purpose of a subnet mask is to identify which portion of an Internet address refers to the remote network.**
subnet-mask	**Specifies which portion of an Internet address refers to the remote network. Specify the *subnet-mask* using the same format as an Internet address, with ones for the network portion. (Note, if you do not specify a *subnet-mask* for an internet route entry, the software will automatically specify the *subnet-mask* based on the *internet-address*.**
FIXED	**Specifies that the terminal server cannot modify this internet route entry based on the information contained in ICMP routing messages that it receives. This is the default.**
VARIABLE	**Specifies that the terminal server can modify this internet route entry based on the information contained in ICMP routing messages that it receives.**

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

Examples

1. `Xyplex>> DEFINE SERVER INTERNET ROUTE 192.12.120.255 GATEWAY 128.6.201.7`

Meaning: Assume that you are on a terminal server which has the internet address 128.6.201.4. Since the NETWORK characteristic is the default, the terminal server uses the *internet-address* to determine that all network traffic to the class C network 192.12.120.0 is routed to the gateway at internet address 128.6.201.7. This internet-route entry is added to the permanent database.

2. `Xyplex>> SET SERVER INTERNET ROUTE 130.12.255.255 GATEWAY 128.6.201.8`

Meaning: Assume that you are on a terminal server which has the internet address 128.6.201.4. In this example, all traffic to the class B network 130.12 is routed to the gateway at internet address 128.6.201.7. This internet-route entry is added to the temporary database.

3. `Xyplex>> SET SERVER INTERNET ROUTE 192.12.120.21 GATEWAY 128.6.201.8 HOST`

Meaning: Assume that you are on a terminal server which has the internet address 128.6.201.4. In this example, all traffic to the host at internet address 192.12.120.21 is routed through the gateway at internet address `128.6.201.8`**. This internet-route entry is added to the temporary database.**

4. `Xyplex>> SET SERVER INTERNET ROUTE 192.16.63.255 GATEWAY 128.6.201.8 MASK 255.255.255.00`

Meaning: Assume that you are on a terminal server which has the internet address 128.6.201.4. In this example, the terminal server will route all traffic to the network address C0.10.3X.XX (a hexadecimal representation of the internet address 192.16.63.255 ANDed with the subnet-mask 255.255.255.00, and where hexadecimal numbers show the network portion of the internet address and the letter X represents the host portion of the internet address) to the gateway at internet address 128.6.201.8. This internet-route entry is added to the temporary database.

DEFINE SERVER INTERNET SECURITY

Enable or Disable the internet security feature

Notes

Use this command to specify whether or not Telnet connections can be either allowed or denied between specified ports on the server and specific internet-addresses. (The PORT INTERNET SECURITY characteristic specified for the individual port whether the connection is allowed or denied. This characteristic merely specifies whether or not the feature is available.)

Refer to the *Software Management Guide.*

DEFINE SERVER only command.

Privilege Level

Privileged

Syntax

DEFINE SERVER INTERNET SECURITY ENABLED|DISABLED

Where	Means
ENABLED	**Specifies that Telnet connections can be either allowed or denied between specified ports on the server and specific internet-addresses (via the PORT INTERNET SECURITY characteristic). This is the default.**
DISABLED	**Specifies that Telnet connections can not be either allowed or denied between specified ports on the server and specific internet-addresses (via the PORT INTERNET SECURITY characteristic).**

Example

```
Xyplex>> DEFINE SERVER INTERNET SECURITY DISABLED
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE|SET SERVER INTERNET SNMP

Specify SNMP client, community, and system contact and location information

Notes

Specifies that you will add an SNMP client or community.

When an SNMP community name has been specified for the unit, any SNMP clients which you specify must belong to the same community as the unit, in order for the clients to be able perform an SNMP set on a unit.

When you have not specified an SNMP Set or Get community name or any SNMP clients for the unit, the unit will accept SNMP set or get commands from any client. No traps are transmitted if there are no SNMP Trap clients.

When an SNMP community name has been specified for the unit, any SNMP clients which you specify must belong to the same community as the unit, in order for the clients to be able perform an SNMP set on a unit.

When you have not specified an SNMP community name or any SNMP clients for the unit, the unit will accept SNMP set commands from any client.

Refer to the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET SNMP [GET CLIENT *client-number internet-address*]
[SET CLIENT *client-number internet-address*]
[TRAP CLIENT *client-number internet-address*]

[GET COMMUNITY]	**[*community-name*]** **[NONE]***
[SET COMMUNITY]	**[*community-name*]** **[NONE]***
[TRAP COMMUNITY]	**[*community-name*]**
[SYSTEM CONTACT]	**[*contact-name*]**
[SYSTEM LOCATION]	**[*location-name*]**

Where	Means
GET CLIENT	**Specifies that you will define or change the SNMP clients (e.g., a Network Operations Center, or NOC) which will be permitted to view information about the unit (i.e., perform an SNMP get).**
SET CLIENT	**Specifies that you will define or change the SNMP clients (e.g., a Network Operations Center, or NOC) which will be permitted to set characteristics (i.e., perform an SNMP set) on the unit.**
TRAP CLIENT	**Specifies that you will define or change the SNMP clients (e.g., a Network Operations Center, or NOC) to which SNMP traps generated by the unit will be sent.**
client-number	**Specifies the number of the SNMP client which will be permitted to set characteristics (i.e., perform an SNMP set) on the unit, to view information about the unit (i.e., perform an SNMP get), or to which SNMP traps generated by the unit will be sent. Valid values are the numbers 1, 2, 3, and 4.**
internet-address	**Specifies the internet-address of an SNMP client which will be permitted to set characteristics (i.e., perform an SNMP set) on the unit, to view information about the unit (i.e., perform an SNMP get), or to which SNMP traps generated by the unit will be sent. The default value is 0.0.0.0. Specify the default value to remove a client.**
GET COMMUNITY	**Specifies that you will define or change the name of the SNMP Get community to which the unit belongs. When a community name has been specified for the unit, only SNMP Get clients (e.g., a Network Operations Center, or NOC) which belong to the same Get community are permitted to view information about the unit (i.e., perform an SNMP get).**
SET COMMUNITY	**Specifies that you will define or change the name of the SNMP Set community to which the unit belongs. When a community name has been specified for the unit, only SNMP Set clients (e.g., a Network Operations Center, or NOC) which belong to the same Set community are permitted to set characteristics (i.e., perform an SNMP set) on the unit.**
TRAP COMMUNITY	**Specifies that you will define or change the name of the SNMP Trap community to which the unit belongs. When a community name has been specified for the unit, only SNMP Trap clients (e.g., a Network Operations Center, or NOC) which belong to the same Trap community will receive SNMP traps which are generated by the unit. The default community name is "public"**
"***community-name***"	**Specifies the name of the SNMP Get, Set, or Trap community to which the unit belongs. Valid values are text strings of up to 32 ASCII characters long. The name is case insensitive. The text string must be enclosed within quotation marks ("). The string "public" is default for the Trap community. To clear the Trap community, use the null string ("").**

None — Specifies that the unit does not verify that SNMP clients belong to the same SNMP Get or Set community as the unit. This is the default for the Get and Set community. This keyword does not apply for the Trap community.

INTERNET SNMP SYSTEM CONTACT — Specifies that you will provide the name of a system contact for the unit. This information is available via an SNMP query (get) but is provided for administrative or informational purposes only.

contact-name — Specifies the name of a system contact for the unit. Valid values are text strings of up to 60 ASCII characters long. The text string must be enclosed within quotation marks ("). To remove a previously specified system contact name, enter a quoted null string (" ") for the INTERNET SNMP SYSTEM CONTACT option. The default value for this characteristic is "" (i.e., the null value).

INTERNET SNMP SYSTEM LOCATION — Specifies that you will provide the location of the unit. This information is available via an SNMP query (get) but is provided for administrative or informational purposes only.

location — Specifies the location of the unit. Valid values are text strings of up to 60 ASCII characters long. The text string must be enclosed within quotation marks ("). To remove a previously specified system location, enter a quoted null string (" ") for the INTERNET SNMP SYSTEM LOCATION option. The default value for this characteristic is "" (i.e., the null value).

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

SNMP is not implemented on the following products: MAXserver 1400 Network Printer Server, MAXserver MX-NPC-P1 card, MX-TSERV-J8 and MX-TSRVL-J8 cards.

DEFINE|SET SERVER INTERNET SUBNET MASK

Specify a subnet mask so the server can identify local and remote networks

Notes

The purpose of a subnet mask is to assist the server to distinguish Internet addresses that can be reached directly from those that must be reached via an IP Gateway. Each device running TCP-IP protocols contains a subnet mask. When a user attempts to form a TCP-IP connection with a destination Internet node, the destination Internet address is logically ANDed with the subnet mask. The unit's own Internet address is also logically ANDed with the subnet mask.

The two results of these operations are compared. If they are equal, then the destination is assumed to be reachable without the assistance of an IP Gateway. If they are not equal, then the unit will attempt to reach the destination via an IP Gateway.

You can configure the server to calculate a subnet-mask automatically. In this case, the server selects a new value for the *internet-subnet-mask* based on the class of network (A, B, or C) of the current *internet-address*. When you allow the server to automatically determine the *internet-subnet-mask* (i.e., set the SERVER INTERNET SUBNET MASK AUTOCONFIGURE characteristic to ENABLED), the server changes the *internet-subnet-mask* for either the permanent or operational database whenever the *internet-address* changes.

Use this command to specify the Internet subnet-mask for the server.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET SUBNET MASK [*internet-address-mask*] [AUTOCONFIGURE] [DISABLED] [ENABLED] *

Where	Means
internet-address-mask	**Where subnet mask is defined using the same format as an Internet address, with ones for the network portion. Default: 255.255.255.0.**
AUTOCONFIGURE	**Specifies whether or not the software will use an *internet-subnet-mask* specified by the server manager, or one that has been determined automatically by the server.ENABLED is the default value.)**
DISABLED	**The software will use an *internet-subnet-mask* specified by the server manager. (The server does not automatically change the *internet-subnet-mask* for either the permanent or operational database whenever the *internet-address* changes.)**
ENABLED	**The software will use an *internet-subnet-mask* that has been determined automatically by the server.**

Example

```
Xyplex>> DEFINE SERVER INTERNET SUBNET MASK AUTOCONFIGURE ENABLED
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE SERVER INTERNET TCP RESEQUENCING

Enable or Disable the storage of packets that are received out of sequence

The DEFINE SERVER INTERNET INTERNET TCP RESEQUENCING command specifies whether or not the server will store packets that it receives from a host that are out of sequence, or wait until the host resends the data again.

Notes

Sometimes, when a host has a large amount of data to transmit to a server, the data will be divided among several smaller packets. Each packet is transmitted in sequence, with a sequence number. Occasionally, a packet will be delayed in transmission, usually by an intermediate destination. This can cause the packet to arrive out of sequence.

When a server receives packets out of sequence, it can either discard the data and not acknowledge receipt of the data, or it can collect the packets and wait until any out of sequence packets are received, before passing on the data in the proper sequence. In the former case, where the server does not acknowledge the data, the host will retransmit all the information again. In the latter case, where the server collects all the data until all the missing information is received, the server must expend additional memory in order to store all the collected data, until the missing pieces are received. If the server has limited extra memory, it is recommended that you disable the SERVER INTERNET TCP RESEQUENCING characteristic. If the server has sufficient memory to spare, or when host resources are a problem, you can enable the SERVER INTERNET TCP RESEQUENCING characteristic. In this case, you may need to increase the setting for the DEFINE/SET SERVER PACKET BUFFER characteristic.

Privilege Level

Privileged.

Syntax

DEFINE SERVER INTERNET TCP RESEQUENCING [ENABLED]
[DISABLED]

Where	Means
ENABLED	**The server will attempt to resequence TCP/IP packets that it receives from the sender out of order, without waiting for the sender to retransmit.**
DISABLED	**The server will not attempt to resequence TCP/IP packets that it receives from the sender out of order. In this case, the server will not acknowledge receipt of the packets, which will cause the sender to retransmit the packets. This is the default.**

Example

```
Xyplex>> DEFINE SERVER INTERNET TCP RESEQUENCING ENABLED
```

DEFINE|SET SERVER INTERNET TTL

Specify the maximum amount of time that an Internet data packet can circulate through the network

Notes

Use this command to specify the maximum amount of time that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live"). When each packet is initially transmitted on the network, its time to live is equal to the *ttl-value* specified in the command. The current time to live for the packet is then decremented by 1 second, for each second that the packet is circulating through the network, or for each Internet gateway that the packet goes through.

Note that the SERVER INTERNET CHARACTERISTICS display includes an "Internet TTL" field, which shows the value that is set for this characteristic.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER INTERNET TTL *ttl-value*

Where	Means
ttl-value	**Specifies the maximum amount of time, in seconds, that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live"). The *ttl-value* is a number between 1 and 255 seconds (do not specify seconds). The default for *ttl-value* is 64.**

Example

```
Xyplex>> DEFINE SERVER INTERNET TTL 100
```

Support Issues

Requires that the Telnet protocol is enabled. Not supported on LAT-only units (refer to the Software Kit Information supplied with your kit for a list of units which support Telnet or are LAT-only units).

DEFINE SERVER IPX PROTOCOL

Setting IPX Protocol Packet Type

The DEFINE SERVER IPX PROTOCOL command specifies whether the terminal server or printer server should expect to use Ethernet or IEEE 802.3 (MAC) type packets when communicating with a Novell printer server.

Notes

IPX is a protocol used by Novell NetWare. Xyplex terminal servers and printer servers can accept two packet types over an IPX Interface: Ethernet-type packets and IEEE 802.3 (MAC) type packets. You can only use one of these types at a time. (Ethernet packets and IEEE 802.3 packets have different formats[1].) By factory default, Xyplex terminal servers or printer servers are configured to use Ethernet-type packets for IPX. You must make sure that the protocol type you set for the server matches the value set at your Novell file server. You must re-initialize the unit after making a change to the IPX packet type selection, for the change to take effect.

On a MAXserver 1450 or 1400A Printer Server, if you use the Setup Dialog, it will prompt you for this information, rather than require you to type in this command.

Privilege Level

Privileged

Syntax

DEFINE SERVER IPX PROTOCOL	**ETHERNET**	**ENABLED**
		DISABLED
	MAC	**ENABLED**
		DISABLED

Where	Means
ETHERNET	**The terminal server or printer server will use Ethernet type packets when communicating with a Novell printer server.**
MAC	**The terminal server or printer server will use IEEE 802.3 (MAC) type packets when communicating with a Novell printer server.**
ENABLED	**Enables use of the specified packet type.**
DISABLED	**Disables use of the specified packet type.**

Example

```
Xyplex>> define server ipx protocol mac enabled
```

Support Issues

Requires Multi-Megabyte Load Image.

---

1 IEEE 802.3 (MAC) packets have a 2-byte LENGTH field, where Ethernet packets have a 2-byte TYPE field.

DEFINE|SET SERVER KEEPALIVE TIMER

Specify the length of the LAT keep-alive timer

Notes

Use this command to specify the length of time at which the server will transmit a null message over a LAT virtual circuit, when there is no other traffic originating at the server. The purpose of sending the null message is to notify circuit partner(s) that the server is still active.

The value you set for the KEEPALIVE TIMER characteristic also specifies the frequency at which the server will attempt to reconnect a session when there is a connection failure, for ports at which the AUTOCONNECT characteristic is set to ENABLED.

You can not change the value for the KEEPALIVE TIMER characteristic via a SET SERVER command while there are any active LAT sessions on the server.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KEEPALIVE TIMER *timer-value*

Where	Means
timer-value	**Specifies the length of time (in seconds) at which the server will transmit a null message over a virtual circuit, when there is no other traffic originating at the server. It also specifies the frequency with which the server will attempt to reconnect a session when there is a connection failure, for ports at which the AUTOCONNECT characteristic is set to ENABLED. Valid values for this variable are whole numbers between 10 and 180 seconds (do not supply units). The default value for the KEEPALIVE variable is 20.**

As you increase the size of the timer-value, you will lengthen the time for other nodes to determine when the server goes down. However, as you decrease the size of this value, you increase the amount of network traffic.

Example

```
Xyplex>> DEFINE SERVER KEEPALIVE TIMER 30
```

Support Issues

None

DEFINE SERVER KERBEROS

Enable or Disable the Kerberos security feature

Notes

Specifies whether or not this server will use Kerberos user authentication. No password is required to enable this feature.

Refer to the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE SERVER KERBEROS [ENABLED]
[DISABLED]*

Where	Means
ENABLED	**Enable Kerberos on this server.**
DISABLED	**Disable Kerberos on this server. This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE SERVER KERBEROS ENABLED
```

Support Issues

None

DEFINE|SET SERVER KERBEROS MASTER

Specify the address of the Kerberos master host

Notes

Specifies the *domain-name* or *internet-address* of the Kerberos Master follow. The Kerberos Master maintains the Kerberos database and provides information to primary or secondary Server hosts within a realm. A primary or secondary Server must query the Master when a user changes a Kerberos password.

Refer to the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KERBEROS MASTER [*domain-name*] [*internet-address*]

Where	Means
domain-name	**Specifies the Domain name of the Kerberos Master host. To remove the Kerberos Master host, use NONE as the *domain-name*.**
internet-address	**Specifies the Internet address of the Kerberos Master host.**

Example

```
Xyplex>> DEFINE SERVER KERBEROS MASTER 140.179.224.100
```

Support Issues

None

DEFINE|SET SERVER KERBEROS PRIMARY|SECONDARY SERVER

Specify the *domain-name* or *internet-address* of the Kerberos verification host

Notes

Use these commands to specify the *domain-name* or *internet-address* of the Kerberos primary or secondary Server host. The primary Server host is the first Server host to be queried for user verification. The server queries the secondary Server host if the primary Server host does not respond.

Refer to the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KERBEROS PRIMARY SERVER [*domain-name*] [*internet-address*]

DEFINE | SET SERVER KERBEROS SECONDARY SERVER [*domain-name*] [*internet-address*]

Where	Means
domain-name	**Specifies the Domain name of the Kerberos primary or secondary Server host. To remove the Kerberos primary or secondary server, use NONE as the *domain-name*.**
internet-address	**Specifies the Internet address of the Kerberos primary Server host.**

Example

```
Xyplex>> DEFINE SERVER KERBEROS PRIMARY SERVER 140.179.224.100
```

Support Issues

None

DEFINE|SET SERVER KERBEROS QUERY LIMIT

Specify the maximum number of Server host queries the server can make when attempting to verify a Kerberos ID

Notes

Enables you to specify the maximum number of Server host queries the server can make when attempting to verify a Kerberos ID. When this limit is reached, the server logs out the port and generates an error message. The limit also specifies the maximum number of Master queries the server can make when attempting to change a user's password.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KERBEROS QUERY LIMIT *limit*

Where	Means
limit	**Specifies the maximum number of queries the server can make when attempting to verify a Kerberos ID or change a password. The default query limit is 3. Valid values are whole numbers in the range of 1 through 16.**

Example

```
Xyplex>> DEFINE SERVER KERBEROS QUERY LIMIT 5
```

Support Issues

None

DEFINE|SET SERVER KERBEROS REALM

Specify the name of the Kerberos realm

Notes

Enables you to specify the name of the Kerberos realm to which the primary and secondary Server hosts are associated.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KERBEROS REALM [*realm-name*]
[NONE]*

Where	Means
realm-name	**Specifies the name of the Kerberos realm to which the Master and Server hosts are associated. Valid values are text strings of up to 40 ASCII characters long.**
NONE	**Specifies that no Kerberos Realm exists for this server. Use this keyword to eliminate a previously defined Kerberos realm name. This is the default setting for this characteristic.**

Example

```
Xyplex>> DEFINE SERVER KERBVEROS REALM MEDICAL-NETWORK
```

Support Issues

NONE

DEFINE|SET SERVER KERBEROS SECURITY

Enable or Disable Kerberos user verification.

Notes

Enables you to specify whether the server is to provide Kerberos user verification.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER KERBEROS SECURITY [LOGIN]
[NONE]*

Where	Means
LOGIN	**Specifies that the server is to provide Kerberos user verification.**
NONE	**Specifies that the server is not to provide Kerberos user verification. This is the default.**

Example

```
Xyplex>> DEFINE SERVER KERBEROS SECURITY LOGIN
```

Support Issues

None

DEFINE SERVER LAT SOLICITS

Specify whether or not a server will issue LAT multicast service requests, when a user requests connection to an unknown service

The DEFINE SERVER LAT SOLICITS command allows you to specify whether or not a server will issue LAT multicast service requests, when a user requests connection to an unknown service.

Notes

LAT servers and hosts normally advertise the services which they make available to other servers, by means of LAT announcements.

Normally, the server will store information locally about these services, so that when a user requests a service, the server knows where to locate that service. When the server does not know the location of a service, it can be configured to issue a LAT multicast message on the network, requesting a service announcement from any devices on the network at which the requested service is available. (This is called a LAT solicit.)

Typically, you will not need to enable LAT solicits, since the server will store information about all available services. If, however, you have restricted the number of services or nodes that the server is permitted to store information about, it may be possible for the server to be missing information about an available service (refer to chapter 8 of the *Software Management Guide* for more information). In this case, you might want to enable LAT solicits. Enabling LAT solicits can result in many LAT multicast messages being issued on the network by the server.

Privilege Level

Privileged.

Syntax

DEFINE SERVER LAT SOLICITS ENABLED|DISABLED

Where	Means
ENABLED	**The server will issue LAT multicast service requests, when a user requests connection to an unknown service.**
DISABLED	**The server will not issue LAT multicast service requests, when a user requests connection to an unknown service.**

Example

```
Xyplex>> DEFINE SERVER LAT SOLICITS ENABLED
```

Support Issues

None

DEFINE SERVER LOAD INTERNET ADDRESS

Specify the Internet address of the terminal server for DTFTP loading

The DEFINE SERVER LOAD INTERNET ADDRESS command specifies the Internet address for DTFTP loading.

Notes

Use this command if DTFTP is enabled for the software load image. You must also specify the Internet address of the load host, and the name of the file that contains the load image. If the terminal server gains access to the load host through a gateway, you must also specify the Internet address of the gateway. Use the DEFINE SERVER LOAD INTERNET commands to specify this information.

The Internet address of the terminal server appears in the Server Status display. When you define the address for DTFTP loading, it appears in the SERVER Loaddump Characteristics display.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOAD [*record*|ALL] INTERNET ADDRESS *internet-address*

Where	Means
[*record*]	**One or more of the following initialization records:**
	PRIMARY **SECONDARY** **TERTIARY** **ALL**
	The PRIMARY initialization record is the default.
internet-address	**The Internet address of the terminal server.**

Example

This example specifies an Internet address for the terminal server.

```
Xyplex>> define server load internet address 150.169.70.133
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER LOAD INTERNET [LOAD] FILE

Specify the software load image filename for DTFTP loading

The DEFINE SERVER LOAD INTERNET [LOAD] FILE command specifies the pathname and name of the file that contains the software load image on the Internet host you specify for DTFTP loading.

Notes

Use this command if DTFTP is enabled for the software load image. You must also specify the Internet address of the terminal server and the Internet address of the load host. If the terminal server gains access to the load host through a gateway, you must also specify the Internet address of the gateway. Use the other DEFINE SERVER LOAD INTERNET commands to specify this information.

When you define the load host Internet address for DTFTP loading, it appears in the Server Loaddump Characteristics display. The Internet address you specify with this command overrides the Internet address you specify with the DEFINE/SET SERVER INTERNET ADDRESS command if they are different.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOAD [*record*|ALL] INTERNET [LOAD] FILE
" /*pathname*/*filename*"

Where	Means
[*record*]	**One or more of the following initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**
" /*pathname*/*filename*"	**The pathname and filename of the file that contains the software load image. Most UNIX implementations are case-sensitive, so be sure to use the appropriate upper- and lower-case letters in the filename, or the host may not recognize it. Enclose the pathname and filename in quotes.**

Example

This example specifies the pathname and file name that contains the software load image.

```
Xyplex>> define server load internet file "/usr2/xpcsrv20.sys"
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER LOAD INTERNET [LOAD] GATEWAY

Specify the Internet address of a gateway for DTFTP loading

The DEFINE SERVER LOAD INTERNET GATEWAY command specifies the Internet address of a gateway on the network for DTFTP software image loading.

Notes

Only terminal servers that use a gateway to gain access to an Internet load host through DTFTP require that you specify a gateway address with this command.

When you define the Internet gateway address for DTFTP loading, it appears in the Server Loaddump Characteristics display.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOAD [*record* | ALL] INTERNET [LOAD] GATEWAY *internet-address*

Where	Means
[*record*]	**One or more of the following initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**
internet-address	**The Internet address of the gateway.**

Example

This example specifies an Internet address for the gateway used by the terminal server to gain access to the load host.

```
Xyplex>> define server load internet gateway 150.122.30.164
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER LOAD INTERNET [LOAD] HOST

Specify the Internet address of the load host for DTFTP loading

The DEFINE SERVER SERVER INTERNET [LOAD] HOST command specifies the Internet address of the host where the software load image resides.

Notes

Use this command if DTFTP is enabled to load the software load image. You must also specify the Internet address of the terminal server and the name of the file on the load host that contains the software load image. If the terminal server reaches the load host through a gateway, you must also specify the Internet address of the gateway. Use the other DEFINE SERVER LOAD INTERNET commands to specify this information.

When you define the Internet address of the load host for DTFTP loading, it appears in the Server Loaddump Characteristics display.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOAD [*record*|ALL] INTERNET [LOAD] HOST *internet-address*

Where	Means
[*record*]	**One or more of the following initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**
internet-address	**The Internet address of the host that contains the software load image.**

Example

This example specifies an internet address for the load host that contains the software load image.

```
Xyplex>> define server load internet host 150.122.30.155
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER LOAD PROTOCOL

Enable or disable load protocols

The DEFINE SERVER LOAD PROTOCOL command specifies one or all load protocols to use when the terminal server searches for a software load image file or a parameter file. You specify whether the protocol applies to the software load image or the parameter file in the command line.

Notes

By default, a MAXserver 1620 or 1640 attempts to obtain the software load image using the CARD protocol and the parameter file using the NVS protocol. If a card is not present, or the NVS protocol is disabled, the terminal server attempts to obtain these files using other protocols in this order: XMOP, MOP, BOOTP, RARP, DTFTP. All of these protocols except DTFTP are enabled by default. If you use the keyword ALL to enable all protocols, you also enable DTFTP.

You cannot use DTFTP to load the parameter file. If you do enable DTFTP, you must specify the Internet address of the load host, the Internet address of the terminal server, and the Internet address of the gateway to the load host, if necessary. Use the DEFINE SERVER LOAD INTERNET commands specify this information.

Privilege level

Privileged

Syntax

DEFINE SERVER LOAD [*record*|ALL] *usage* PROTOCOL *protocol* | ALL [ENABLED | DISABLED]

Where	Means
[*record*]	**One or more of the following initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**
usage	**One of the following keywords, which indicate whether you are specifying a protocol for a software load image or a parameter file:** **IMAGE [LOAD]** **PARAMETERS [LOAD]**

Where **Means**

protocol **One of the following keywords which represent different protocols, or the keyword ALL:**

Protocol	Means
NVS	NonVolatile Storage protocol for the parameter file
CARD	Local memory card protocol for the software load image
XMOP	Xyplex MOP Protocol
MOP	Digital Equipment Corporation Maintenance Operations Protocol
BOOTP	Bootstrap protocol
RARP	UNIX Reverse Address Resolution Protocol
DTFTP	UNIX Directed Trivial File Transfer Protocol (software load image only)
ALL	All protocols (you cannot disable all load protocols)

For loading parameters MAXserver 800, 1450, and 1600 units can use either NVS or remote protocols, but not both types.

ENABLED **Enable the protocol in the initialization records you specify. You can enable only one protocol in the command line, unless you use the keyword ALL to enable all protocols.**

DISABLED **Disable the protocol in the initialization records you specify. You cannot use the keyword ALL to disable all load protocols.**

Examples

1. This example enables DTFTP as a protocol to use for the software load image in the primary initialization record. (Enabling this protocol requires that you specify DTFTP information with the DEFINE SERVER LOAD INTERNET commands.)

```
Xyplex>> define server load primary image protocol dtftp enabled
```

2. This example enables MOP as the protocol to use when loading the parameter file from the primary initialization record.

```
Xyplex>> define server load primary parameters protocol mop enabled
```

3. This example disables the RARP protocol for use when loading the parameter file from the secondary initialization record.

```
Xyplex>> define server load secondary parameters protocol rarp disabled
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720

DEFINE SERVER LOAD SOFTWARE

Specify the CARD/XMOP/MOP file name of the software load image

The DEFINE SERVER LOAD SOFTWARE command specifies the CARD/XMOP/MOP filename that contains the software load image.

Notes

You specify this filename if CARD, XMOP, or MOP is enabled as a load protocol for the software load image, and the load image name is different from the default. The default CARD/MOP/XMOP software load image names for a MAXserver 1620 and 1640 is XPCSRV20.

The CARD/XMOP/MOP load image filename appears in the Server Loaddump Characteristics display.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOAD [*record*|ALL] SOFTWARE *filename*

Where	Means
[*record*]	**One of or more the following initialization records:**

PRIMARY
SECONDARY
TERTIARY
ALL

The PRIMARY initialization record is the default.

filename	**A CARD/XMOP/MOP filename, which can consist of up to 16 characters.**

Example

This example specifies XPCSRV20 as the filename for the secondary initialization record.

```
Xyplex>> define server load secondary software XPCSRV20
```

Support Issues

Supported only on MAXserver 800/1600/1620/1640 Terminal Servers or Network 9000 Terminal Server 720.

DEFINE SERVER LOADDUMP ENABLED | DISABLED

Enable or disable an initialization record

Notes

The DEFINE SERVER LOADDUMP ENABLED | DISABLED command disables or enables an initialization record. MAXserver 1620 and 1640 terminal servers have only the primary initialization record enabled by default. You must enable the other initialization records if you want the terminal server to use them.

All initialization records have default values for the loading and dumping protocols, and the CARD/XMOP/MOP load image filename, whether they are enabled or disabled by default.

You cannot disable all three initialization records. If the primary and secondary initialization records are disabled, for example, you cannot disable the tertiary initialization record. If you attempt to do so, the server generates an error message.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOADDUMP [*record*|ALL] DISABLED | ENABLED

Where	Means
[*record*]	**One or more of the following initialization records:**
	PRIMARY **SECONDARY** **TERTIARY** **ALL**
	The PRIMARY initialization record is the default.
ENABLED	**Enable the initialization records you specify.**
DISABLED	**Disable the initialization records you specify. (You cannot disable all three initialization records.)**

Examples

1. This command disables the primary initialization record. With this record disabled, the terminal server first attempts to load or dump using information in the secondary initialization record.

```
Xyplex>> define server loaddump primary disabled
```

2. This command enables all initialization records.

```
Xyplex>> define server loaddump all enabled
```

DEFINE SERVER LOADDUMP DEFAULT

Reset initialization records to the default settings

Notes

The DEFINE SERVER LOADDUMP DEFAULT command resets the parameters in one or more initialization records to the default settings. Initialization parameters include the status of the initialization record, protocols, the CARD/XMOP/MOP load image filename, and the Internet characteristics for DTFTP loading. You can change this information through the initialization configuration menu, with the commands in this chapter, and through SNMP.

The default settings for the secondary initialization record on a terminal server are the following:

Status:	**Disabled**
Load Image Protocols:	**CARD, XMOP, MOP, BOOTP, RARP**
Dump Protocols:	**XMOP, MOP, BOOTP, RARP**
Parameter Protocols:	**NVS, XMOP, MOP, BOOTP, RARP**
Software filename:	**XPCSRV20**

The secondary and tertiary initialization records on the MAXserver 1620 and 1640 are disabled by default. If you reset one of these initialization records to its default settings with, the command also disables the initialization record. See the DEFINE SERVER LOADDUMP ENABLED | DISABLED command for information about how to enable and disable initialization records.

Privilege Level

Privileged

Syntax

DEFINE SERVER LOADDUMP [*record* | ALL] DEFAULT

Where	Means
[*record*]	**One or more of the following initialization records:**

PRIMARY
SECONDARY
TERTIARY
ALL

The PRIMARY initialization record is the default.

Example

This command resets the secondary initialization record to its default settings. Because the secondary initialization record is disabled by default, this command also disables the initialization record.

```
Xyplex>> define server loaddump secondary default
```

DEFINE|SET SERVER LOCK

Enable or Disable the LOCK command

Notes

Specifies whether or not users with interactive terminals can lock (use the LOCK command) their ports, to prohibit unauthorized use of their terminals while they are absent.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER LOCK [DISABLED]
[ENABLED]*

Where	Means
DISABLED	**Users may not use the LOCK command to prohibit use of their terminals while they are absent.**
ENABLED	**Users may use the LOCK command to prohibit use of their terminals while they are absent. This is the default setting for the LOCK characteristic.**

Example

```
Xyplex>> DEFINE SERVER LOCK DISABLED
```

Support Issues

None

DEFINE|SET SERVER LOGIN PASSWORD

Specify a password that interactive users must type when they log on to a port

Notes

Use this command to specify the password that interactive users must type when they log on to a server port for which the PORT PASSWORD characteristic is set to ENABLED. If you type the password on the DEFINE/SET SERVER LOGIN PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER LOGIN PASSWORD command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters.

You can disable the login password on port 0. However, certain programs, such as TSM, Scriptor, and ControlPoint, require a password. These programs will not function properly if you disable the password on port 0.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER LOGIN PASSWORD ***password***

Where	Means
password	**Specifies the new password that interactive users must type when they log on to a server port. The password can be between 1 and 16 ASCII characters in length. The password "ACCESS" is the default password for the LOGIN PASSWORD characteristic. There is only 1 login password per server.**

Example

```
Xyplex>> DEFINE SERVER LOGIN PASSWORD "ACCESS"
```

Support Issues

None

DEFINE|SET SERVER LOGIN PROMPT

Change the prompt that is displayed to request that users type the login password

Notes

Specifies that you will define or change the prompt that is displayed to users to request that they type the login password.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER LOGIN PROMPT *prompt-string*

Where	**Means**
prompt-string	**Specifies the prompt that is displayed to users to request the login password. The prompt can be between 1 and 8 ASCII characters in length. Enclose the prompt-text in quotation mark characters ("). During login, the server will prepend an ASCII bell character (i.e., the server will cause the terminal to "beep") to the login prompt. The default prompt is "#."**

Example

```
Xyplex>> DEFINE SERVER LOGIN PROMPT "PASSWORD"
```

Support Issues

None

DEFINE|SET SERVER MAINTENANCE PASSWORD

Change the maintenance password

Notes

Use this command to change the password that users must type when they want to use certain commands at the server, such as the REMOTE CONSOLE command and the DECnet NCP TRIGGER or NCP LOAD commands. If you type the password on the DEFINE/SET SERVER MAINTENANCE PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER MAINTENANCE PASSWORD command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters. Refer to the description of the REMOTE CONSOLE command for an example of maintenance password use.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER MAINTENANCE PASSWORD ***password-number***

Where	Means
password-number	**Specifies the new password that users must type in order to use the REMOTE CONSOLE command and the DECnet NCP TRIGGER and NCP LOAD commands at this server. The password is a hexadecimal number in the range of 0 to FFFFFFFFFFFFFFFF (i.e., up to 16 hexadecimal digits long). The default password is 0. You can disable the MAINTENANCE PASSWORD characteristic by specifying the default password. There can be only one maintenance password per server.**

Example

```
Xyplex>> DEFINE SERVER MAINTENANCE PASSWORD "FAE7"
```

Support Issues

None

DEFINE SERVER MENU

Enable or Disable the Simple Menu Interface feature or create a menu for users

Notes

Use this command to specify whether or not a system manager can develop a menu with up to 20 selections for the server, or to add new items to the menu.

Refer to the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE SERVER MENU [ENABLED]*
[DISABLED]
[*item-number string1*]

After you press the RETURN key, you are prompted to enter a Xyplex command with the prompt:

Enter Xyplex command> *string2*

where *string2* represents a series of TCP/IP-LAT commands.

Where	Means
ENABLED	**Specifies that designated ports at this server can be configured to use the menu interface. This is the default.**
DISABLED	**Specifies that designated ports at this server can not be configured to use the menu interface.**
item-number	**Specifies the item number (1 - 20) on the server's menu that you want to add or modify.**
string1	**A variable -- a quoted string containing the text of the menu item to be included. (30 characters maximum).**
string2	**A variable -- the Xyplex command string to be executed when the menu item defined in *string1* is selected. The string can contain multiple commands separated by semicolons (64 characters maximum).**

Example

```
Xyplex>> DEFINE SERVER MENU DISABLED
```

Support Issues

None

DEFINE SERVER MENU CONTINUE PROMPT

Specify the text that prompts the user to press the RETURN key

Notes

Use this command to specify the text that prompts the user to press the keyboard RETURN key in order to continue a menu operation, at ports for which the menu is enabled.

Privilege Level

Privileged

Syntax

DEFINE SERVER MENU CONTINUE PROMPT ***prompt-text***

Where	Means
prompt-text	**A text string. Specifies the text that will be displayed which prompts the user to press the keyboard RETURN key in order to continue a menu operation, at ports for which the menu is enabled. The text string can be up to 50 characters long. Enclose the string in quotation marks ("). The default text string is "press <RETURN> to continue."**

Example

```
Xyplex>> DEFINE SERVER MENU PROMPT "press RETURN to continue."
```

Support Issues

None

DEFINE|SET SERVER MENU PROMPT

Specify the prompt for the user to select a menu entry

Notes

Specifies that you will change the text that prompts the user to select a menu entry for the server to perform, at ports for which the menu is enabled.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER MENU PROMPT "*prompt-text*"

Where	Means
prompt-text	**A text string. Specifies the text that will be displayed which prompts the user to select a menu entry for the server to perform, at ports for which the menu is enabled. The text string can be up to 50 characters long. Enclose the string in quotation marks ("). The default text string is "Enter number of selection or use arrow keys:."**

Example

```
Xyplex>> DEFINE SERVER MENU PROMPT "Select a menu number"
```

Support Issues

None

DEFINE|SET SERVER MULTICAST TIMER

Specify the frequency at which the server issues LAT multicast announcements

Notes

Use this command to specify the frequency with which the server will issue an announcement to notify service nodes and other servers of the availability of LAT services. This characteristic only applies when the ANNOUNCEMENTS characteristic is set to ENABLED, and when there are local services defined (i.e., announcements are not made if there are no local services defined).

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER MULTICAST TIMER *time*

Where	Means
timer-value	**Specifies the time interval at which the server transmits a LAT service announcement. Valid values for this variable are between 10 to 180 seconds (do not supply units). The default value for this variable is 30.** **By changing the multicast timer value, you manage the relationship (or trade-off) between the amount of network traffic and the frequency at which nodes obtain information about locally available services.**

Example

```
Xyplex>> DEFINE SERVER MULTICAST TIMER 20
```

Support Issues

None

DEFINE SERVER MULTISESSIONS

Enable or Disable the Multisessions feature

Notes

Specifies whether or not ports on this unit will support DEC terminals, such as the VT330 and VT420 models, which provide a feature called Dual Session Management. This feature enables users to display and control multiple simultaneous communication sessions. The sessions can be multiplexed (i.e., combined) onto a single serial line to a host

Privilege Level

Privileged

Syntax

DEFINE SERVER MULTISESSIONS **[ENABLED]**
[DISABLED]*

Where	Means
ENABLED	**Specifies that ports on this server will support terminals which use Dual Session Management. .**
DISABLED	**Specifies that ports on this server will not support terminals which use Dual Session Management. This is the default**

Example

```
Xyplex>> DEFINE SERVER MULTISESSIONS DISABLED
```

Support Issues

None.

DEFINE|SET SERVER NAME

Assign a unique name for the server

Notes

Use this command to specify a unique name for the server. This name will be used to identify the server for CONNECT commands made at other servers and for host-initiated connections.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER NAME *server-name*

Where	Means
server-name	**Specifies a unique name for the server. You can specify a name that is between 1 and 16 ASCII characters in length. Do not enclose the server-name in quotation marks. The server will convert all lower-case letters to upper-case letters. The default server-name is a seven-character name in the form X*nnnnnn*, where *nnnnnn* represents the last 6 digits of the server Ethernet address. For servers that operate with a parameter server that is a VAX/VMS node, the default name is the DECnet node name that has been assigned by the system manager of that node.**

Example

```
Xyplex>> DEFINE SERVER NAME X01FE87
```

Support Issues

None.

DEFINE|SET SERVER NODE LIMIT

Specify the maximum number of service nodes about which the server will maintain information.

Notes

Use this command to specify the maximum number of service nodes about which the server will maintain information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER NODE LIMIT [*limit*]
[NONE]

Where	Means
limit	**Specifies the maximum number of service nodes about which the server will maintain information. Valid values for this variable are whole numbers in the range of 1 to 1000. The default value for this variable is 100. You should be careful to limit this value, as the number of nodes that the server maintains information about affects other server resources which rely on the server's memory pool. Refer to chapter on Managing Server Resources in the *Software Management Guide* for more information.**
NONE	**Specifies that the server will maintain information about as many service nodes as memory permits.**

Example

```
Xyplex>> DEFINE SERVER NODE LIMIT NONE
```

Support Issues

None

DEFINE|SET SERVER NUMBER

Specify a number by which the server may be identified from other servers

Notes

Use this command to specify a number by which the server may be identified from other servers. The number you specify is for informational purposes only.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER NUMBER *server-number*

Where	Means
server-number	**Specifies the number which will be assigned to the server to distinguish it from other servers. Valid values for this variable are whole numbers in the range of 0 to 32767. The default value for the NUMBER characteristic is 0.**

Example

```
Xyplex>> DEFINE SERVER NUMBER 355
```

Support Issues

None

DEFINE SERVER PACKET COUNT

Specify the number of packets that the server can buffer

Notes

At initialization time, the server sets aside memory for storing packets of data that are waiting to be passed on to another internal server process, both for incoming and outgoing data. The SERVER PACKET COUNT characteristic, allows you to control the maximum number of incoming and outgoing packets, used by internal server processes, that can be buffered in server memory. This characteristic allows you to increase the server's ability to handle large amounts of incoming data at the expense of reducing the amount of memory that is available for other features. For example, you might increase the number of available packet buffers if the server is configured to have many serial ports continuously receiving or outputting data at high speeds (19,200 bps or greater).

You can determine the current setting of the SERVER PACKET COUNT characteristic by examining the "Packet Buffers" field on the SERVER ALTERNATE STATUS or the "Packet Count" field on the SERVER CHARACTERISTICS display. You should only consider increasing the setting for the SERVER PACKET COUNT characteristic if the "Packet Buffers" field on the SERVER ALTERNATE STATUS display indicates that there have been failures or if you are using PPP or have IP reassembly enabled. The server allocates 1556 bytes of memory for each additional packet buffer.

Refer to the *Software Management Guide* for a more thorough description of managing server memory.

Privilege Level

Privileged.

Syntax

DEFINE SERVER PACKET COUNT *packet-buffers*

Where	Means
packet-buffers	**The maximum number of incoming and outgoing packets. For load images which require at least 2MB of memory to run, valid values are whole numbers in the range of 80 to 1088. For load images which can be used with less memory, valid values are whole numbers in the range of 80 to 160. The default value is 80.**

Example

```
Xyplex>> DEFINE SERVER PACKET COUNT 100
```

Support Issues

Supported on MAXserver 800, 1100, 1120, 1500, 1520, 1600, 1620, 1640, 1800, and 1820 Terminal Servers, the MX-TSRVM-J8, MX-TSERV-J16, MX-2120, and MX-2210 Terminal Server Cards, and Network 9000 Terminal Server 720.

DEFINE|SET SERVER PARAMETER SERVER CHECK

Change the manner in which the server locates or updates eligible parameter servers

Notes

Specifies that you will change the manner in which the server locates or updates eligible parameter servers, whether or not the server will attempt to locate additional eligible parameter servers, and whether or not the server can use TFTP or Xyplex proprietary protocols for parameter serving.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER PARAMETER SERVER CHECK **[DISABLED]**
[ENABLED]*
[PROPRIETARY ENABLED]
[TFTP ENABLED]

Where	Means
DISABLED	**Specifies that the server will not attempt to locate additional eligible parameter servers.**
ENABLED	**Specifies that the server will attempt to locate additional eligible parameter servers. This is the default setting for the SERVER PARAMETER SERVER CHECK characteristic.**
PROPRIETARY ENABLED	**Specifies that the server will use a Xyplex proprietary protocol to locate additional eligible parameter servers. To use only the proprietary protocol for this purpose, disable all parameter server checking (use the DEFINE SERVER PARAMETER SERVER CHECK DISABLED command) then enable checking via proprietary protocol (use the DEFINE SERVER PARAMETER SERVER CHECK PROPRIETARY ENABLED command).**
TFTP ENABLED	**Specifies that the server will use TFTP to locate additional eligible parameter servers. To use only TFTP for this purpose, disable all parameter server checking (use the DEFINE SERVER PARAMETER SERVER CHECK DISABLED command) then enable checking via TFTP (use the DEFINE SERVER PARAMETER SERVER CHECK TFTP ENABLED command).**

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER CHECK TFTP ENABLED
```

Support Issues

None

DEFINE/SET SERVER PARAMETER SERVER PATH

Specify Where Parameter Files Can Be Written for TFTP.

The DEFINE | SET SERVER PARAMETER SERVER PATH command allows you to specify the complete directory pathname to be used when writing parameter files.

Notes

Some TFTP implementations require that a unit supply a complete directory name (a "path") when that unit tries to use TFTP to write a file. This requirement can affect Xyplex units when they attempt to store parameter files at UNIX hosts. This characteristic lets you specify exactly where parameter files will be stored.

Privilege Level

Privileged.

Syntax

DEFINE | SET SERVER PARAMETER SERVER PATH "*directory-path*" *s*

Where	Means
" ***directory-path***"	**Specifies the name of the directory where parameter files can be located. A valid *directory-path* can be a string up to 40 characters long, ending with a forwards slash character (/). Enclose the *directory-path* in double quotation marks (").**

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER PATH "/tftpboot"
```

DEFINE|SET SERVER PARAMETER SERVER TIMER

Change frequency at which the server will attempt to locate or update additional eligible parameter servers

Notes

Use this command to specify the frequency at which the server will attempt to locate additional eligible parameter servers or update parameter information at current parameter servers.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER PARAMETER SERVER TIMER *timer-value*]

Where	Means
timer-value	**Specifies the time interval at which the server attempts to locate additional eligible parameter servers. Valid values are between 1 to 120 minutes (do not specify units). The default is 30.**

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER TIMER 10
```

Support Issues

None

DEFINE|SET SERVER PARAMETER SERVER LIMIT

Specify the maximum number of eligible parameter servers that this server may have

Notes

Use this command to specify the number of eligible parameter servers about which the server will retain information (i.e., the maximum number of eligible parameter servers that this server may have).

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER PARAMETER SERVER LIMIT *number*

Where	Means
number	**Specifies the number of eligible parameter servers about which the server will retain information (i.e., the maximum number of eligible parameter servers that this server may have). Valid values are whole numbers between 1 to 8. The default is 4.**

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER LIMIT 5
```

Support Issues

None

DEFINE|SET SERVER PARAMETER SERVER RETRANSMIT

Change the manner in which the server will attempt to update parameter servers which do not acknowledge an update attempt

Notes

Use this command to change the number of attempts the server will make to update parameter information at a parameter server which does not acknowledge the attempt, and the frequency at which the server will update parameter information at a parameter server which has not acknowledged an update attempt.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER PARAMETER SERVER RETRANSMIT [LIMIT *limit*] [TIMER *timer-value*]

Where	Means
LIMIT	**Specifies that you will change the number of attempts the server will make to update parameter information at a parameter server which does not acknowledge the attempt.**
limit	**Specifies the number of attempts the server will make to update parameter information at a parameter server which does not acknowledge the attempt. Valid values are whole numbers in the range of 1 through 100. The default is 3.**
TIMER	**Specifies that you will change the frequency at which the server will update parameter information at a parameter server which has not acknowledged an update attempt.**
timer-value	**Specifies the time interval at which the server attempts to update parameter information at a parameter server which has not acknowledged an update attempt. Valid values are between 1 and 30 minutes (do not specify units). The default is 5.**

Example

```
Xyplex>> DEFINE SERVER PARAMETER SERVER RETRANSMIT LIMIT 10
```

Support Issues

None

DEFINE|SET SERVER PARAMETER VERSION

Specify the version number of the local permanent parameter file

Notes

Use this command to specify the version number of the local permanent parameter file. This is useful when the local parameter version number becomes "out of synch" with the version stored at a remote parameter server.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER PARAMETER VERSION *number*

Where	**Means**
number	**Specifies the version number of the local permanent parameter file.**

Example

```
Xyplex>> DEFINE SERVER PARAMETER VERSION 235
```

Support Issues

None.

DEFINE|SET SERVER PASSWORD LIMIT

Limit the number of times a user can try to enter a password

Notes

Use this command to specify the maximum number of times which the server will prompt the user to enter the correct privileged password or login before the server logs out the port.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER PASSWORD LIMIT [*limit*]
[NONE]

Where	Means
limit	**Specifies the number of times that the server will prompt the user to enter the correct privileged password. When the limit is reached, the server logs out the port. Valid values for this variable are whole numbers in the range of 0 and 250. The default value is 3.**
NONE	**Specifies that the server will prompt the maximum number of times (250) for the user to enter the correct privileged password, before the server logs out the port.**

Example

```
Xyplex>> DEFINE SERVER PASSWORD LIMIT 3
```

Support Issues

None

DEFINE|SET SERVER PAP REMOTE PASSWORD

Specify the password that the server sends to a remote device that is configured to require a password in order to form a PPP connection.

The DEFINE/SET SERVER PAP REMOTE PASSWORD commands specify the password that the server will send to a remote device which requires a password in order to establish a PPP connection.

Notes

A remote device can be configured to require that the port (the local end of a PPP connection) provides a password prior to establishing a PPP connection and forwarding data. Although it is possible to configure a link so that a password is required in either direction, both directions, or no direction, the DEFINE/SET SERVER PAP REMOTE PASSWORD commands only applies when the remote device requires a password. There is only one PPP PAP remote password for the server. If a remote device requires a password, and none has been specified, the server will send a "blank" password and the connection will not be formed.

Note that the Xyplex PPP implementation does not support the ability to require that PAP authentication be used in both directions to establish a PPP connection. The Xyplex PPP implementation can be configured to require that remote devices must supply the login password in order to establish a PPP connection with the port. Refer to the DEFINE/SET PORT PAP ENABLED/DISABLED command description.

When the remote device requires a password, the server will send its nodename and the password specified by the DEFINE/SET SERVER PAP REMOTE PASSWORD command.

Privilege Level

Privileged.

Syntax

DEFINE SERVER PAP REMOTE PASSWORD "*password*"
SET SERVER PAP REMOTE PASSWORD "*password*"

Where	Means
"password"	**The password that the server will send to a remote device which requires a password in order to establish a PPP connection. The password can be a maximum of 16 characters long. Enclose the *password* in double quotation marks ("). To disable a previously enabled password, use a null string enclosed in double quotation marks (i.e., "").**

Example

```
Xyplex>> DEFINE SERVER PAP REMOTE PASSWORD "gumby"
```

DEFINE/SET SERVER PRIVILEGED PASSWORD

Specify the unit's privileged password.

Notes

Use this command to specify the password that users must type when they want to use privileged server commands. If you type the password on the DEFINE/SET SERVER PRIVILEGED PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER PRIVILEGED PASSWORD command line, the system will prompt you for a password. In this case, do not enclose the password in quotation mark characters.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER PRIVILEGED PASSWORD *password*

Where	Means
password	**Specifies the new password that users must type in order to use privileged server commands. The password can be between 1 and 16 printable ASCII characters in length. The default password is SYSTEM. There can be only one privileged password per server.**

Example

```
Xyplex>> DEFINE SERVER PRIVILEGED PASSWORD "MANANGER"
```

Support Issues

None

DEFINE SERVER PROTOCOL LAT

Enable or Disable the LAT protocol

The DEFINE SERVER PROTOCOL LAT command enables or disables the LAT protocol on the terminal server.

Notes

Refer to the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support LAT.

When LAT is disabled, the memory used by LAT becomes available for use by the terminal server. The LAT protocol cannot be disabled if the TELNET protocol is disabled.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL LAT ENABLED/DISABLED

Where	Means
ENABLED	**Enable the LAT protocol on the terminal server. This is the factory default setting for this protocol for all units except a MAXserver 1100/1120 unit.**
DISABLED	**Disable the LAT protocol on the terminal server.**

Examples

```
Xyplex>> DEFINE SERVER protocol lat disabled

Xyplex>>
```

Support Issues

On a MAXserver 1100/1120 unit, if you specify only one protocol (LAT or TELNET) in a DEFINE SERVER PROTOCOL command, the server will enable that protocol and disable the other, without requiring a password. A Xyplex-supplied password is required to enable LAT and TELNET simultaneously on a MAXserver 1100/1120 unit. Contact your Xyplex sales representative if you do not have a password. LAT is enabled by default for all other unit types and no password is needed to disable LAT.

DEFINE SERVER PROTOCOL PPP

Enable or Disable the PPP protocol

The DEFINE SERVER PROTOCOL PPP command enables or disables the PPP protocol on the terminal server.

Notes

Refer to the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support PPP.

When PPP is disabled, the memory used by PPP becomes available for use by the terminal server.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL PPP ENABLED/DISABLED

Where	Means
ENABLED	**Enable the PPP protocol on the terminal server.**
DISABLED	**Disable PPP protocol on the terminal server. (This is the factory default setting for this protocol.)**

Example

```
Xyplex>> DEFINE SERVER protocol ppp enabled

Xyplex>>
```

Support Issues

PPP does not require a software password. PPP runs only on units that support a Multi-Megabyte load image. The following units, with at least 2 megabytes of memory, can support the PPP protocol:

- **Network 9000 Terminal Server 720**
- **MAXserver 800, 1120,1520, 1600, 1620, 1640 and 1820 Terminal Servers**
- **MAXserver 2120 and 2220 for MAXserver chassis.**

DEFINE SERVER PROTOCOL SNMP

Enable or Disable the SNMP protocol

The DEFINE SERVER PROTOCOL SNMP command enables or disables the SNMP protocol on the terminal server.

Notes

Refer to the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support PPP.

When SNMP is disabled, the memory used by SNMP becomes available for use by the terminal server.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL SNMP ENABLED/DISABLED

Where	Means
ENABLED	**Enable the SNMP protocol on the terminal server.**
DISABLED	**Disable SNMP protocol on the terminal server. This is the factory default.**

Examples

```
Xyplex>> DEFINE SERVER protocol snmp disabled

Xyplex>>
```

Support Issues

No password is needed to enable or disable SNMP.

DEFINE SERVER PROTOCOL TELNET

Enable or Disable the TELNET protocol

The DEFINE SERVER PROTOCOL TELNET command enables or disables the TELNET protocol on the terminal server.

Notes

Refer to the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support TELNET.

The TELNET protocol cannot be disabled if the LAT protocol is disabled. The TELNET protocol must be enabled in order for the TN3270 protocol to be enabled.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL TELNET ENABLED/DISABLED

Where	Means
ENABLED	**Enable the TELNET protocol on the terminal server. This is the factory default setting for this protocol for all units except a MAXserver 1100/1120 unit.**
DISABLED	**Disable the TELNET protocol on the terminal server.**

Examples

```
Xyplex>> DEFINE SERVER protocol telnet disabled

Xyplex>>
```

Support Issues

On a MAXserver 1100/1120 unit, if you specify only one protocol (LAT or TELNET) in a DEFINE SERVER PROTOCOL command, the server will enable that protocol and disable the other, without requiring a password. A Xyplex-supplied password is required to enable LAT and TELNET simultaneously on a MAXserver 1100/1120 unit. Contact your Xyplex sales representative if you do not have a password. TELNET is enabled by default for all other unit types and no password is needed to disable TELNET.

DEFINE SERVER PROTOCOL TN3270

Enable or Disable the TN3270 protocol

The DEFINE SERVER PROTOCOL TN3270 command enables or disables the TN3270 protocol on the terminal server.

Notes

Refer to the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support TN3270.

The TELNET protocol cannot be disabled if the LAT protocol is disabled. The TELNET protocol must be enabled in order for the TN3270 protocol to be enabled.

When TN3270 is disabled, the memory used by TN3270 becomes available for use by the terminal server.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL TN3270 ENABLED/DISABLED

Where	Means
ENABLED	**Enable the TN3270 protocol on the terminal server.**
DISABLED	**Disable the TN3270 protocol on the terminal server. This is the factory default.**

Examples

```
Xyplex>> DEFINE SERVER protocol tn3270 disabled

Xyplex>>
```

Support Issues

TN3270 is a keyed feature and requires a software password. Contact your Xyplex sales representative if you do not have a password.

DEFINE SERVER PROTOCOL XPRINTER

Enable or Disable the XPRINTER protocol

Notes

The DEFINE SERVER PROTOCOL XPRINTER command enables or disabled the XPRINTER protocol on the terminal server. When you enter this command to enable the XPRINTER protocol, the command interface prompts you for a password before it enables the protocol. Contact your Xyplex sales representative if you do not have a password.

See the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support XPRINTER.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL XPRINTER ENABLED/DISABLED

Where	Means
ENABLED	**Enable the XPRINTER protocol on the terminal server.**
DISABLED	**Disable XPRINTER protocol on the terminal server. (This is the factory default setting for this protocol.)**

Example

```
Xyplex>> define server protocol xprinter enabled

XPRINTER password> xxxxxxx
```

(The password does not appear on the screen.)

```
Xyplex>>
```

Support Issues

XPRINTER is available as a standard feature on MAXserver 1450 and 1400A Printer Servers. For other units types, XPRINTER is a keyed feature, and requires a software password and a Multi-Megabyte load image. Contact your Xyplex sales representative if you do not have a password. The following unit types, with at least 2 megabytes of memory, can support the XPRINTER protocol:

- **Network 9000 Terminal Server 720**
- **MAXserver 1600/1620/1640**
- **MAXserver 1120/1520/1820**
- **MAXserver 800**
- **MAXserver 2120, 2220**

DEFINE SERVER PROTOCOL XREMOTE

Enable or Disable the Xremote protocol

The DEFINE SERVER PROTOCOL XREMOTE command enables or disabled the Xremote protocol on the terminal server.

Notes

When you enter this command to enable the Xremote protocol, the command interface prompts you for a password before it enables the protocol. Contact your Xyplex sales representative if you do not have a password.

See the *TCP/IP-LAT Software Management Guide* for more information about configuring the terminal server to support Xremote.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL XREMOTE ENABLED/DISABLED

Where	Means
ENABLED	**Enable the Xremote protocol on the terminal server.**
DISABLED	**Disable Xremote protocol on the terminal server. (This is the factory default setting for this protocol.)**

Example

```
Xyplex>> define server protocol xremote enabled

Xremote password> xxxxxxx
```

(The password does not appear on the screen.)

```
Xyplex>>
```

Support Issues

Xremote is a keyed feature, and requires a software password and a Multi-Megabyte load image. Contact your Xyplex sales representative if you do not have a password. The following platforms, with at least 2 megabytes of memory, can support the Xremote protocol:

- **Network 9000 Terminal Server 720**
- **MAXserver 1600/1620/1640**
- **MAXserver 1120/1520/1820**
- **MAXserver 800**
- **MAXserver 2120, 2220**

DEFINE|SET SERVER PURGE GROUP

Specify whether or not the server should remove LAT nodes of particular groups from the node database

Notes

Use this command to specify whether or not the server should remove LAT reachable nodes from the node database, whenever you change the value(s) for the PORT AUTHORIZED GROUPS or SERVER SERVICE GROUPS characteristic(s). The reachable nodes that are removed, are those associated with LAT service groups that are no longer available for the server or port.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER PURGE GROUP [DISABLED]*
[ENABLED]

Where	Means
DISABLED	**Specifies the server should not remove LAT reachable nodes from the node database, whenever you change the value(s) for the PORT AUTHORIZED GROUPS or SERVER SERVICE GROUPS characteristic(s). This is the default.**
ENABLED	**Specifies the server should remove LAT reachable nodes from the node database, whenever you change the value(s) for the PORT AUTHORIZED GROUPS or SERVER SERVICE GROUPS characteristic(s).**

Example

```
Xyplex>> DEFINE SERVER PURGE GROUP ENABLED
```

Support Issues

None

DEFINE|SET SERVER PURGE NODE

Specify whether or not the server should remove LAT nodes when the node database becomes full

Notes

Use this command to specify whether or not the server should remove LAT reachable nodes from the node database, whenever the limit specified by the SERVER NODE LIMIT charactistic is reached.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER PURGE NODE **[DISABLED]***
[ENABLED]

Where	Means
DISABLED	**Specifies that the server should not remove LAT reachable nodes from the node database, whenever the limit specified by the SERVER NODE LIMIT charactistic is reached. This is the default.**
ENABLED	**Specifies that the server should remove LAT reachable nodes from the node database, whenever the limit specified by the SERVER NODE LIMIT charactistic is reached.**

Example

```
Xyplex>> DEFINE SERVER PURGE NODE ENABLED
```

Support Issues

None

DEFINE|SET SERVER QUEUE LIMIT

Specify the size of the connection queue

Notes

Use this command to specify the maximum number of unsatisfied connection requests in the connection queue (i.e., requests made by ports for connection to a service which is busy).

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER QUEUE LIMIT [*queue-limit*]
[NONE]

Where	Means
limit	**Specifies the maximum number of unsatisfied connection requests in the connection queue. Valid values are whole numbers in the range of 0 to 100. The default value for the QUEUE LIMIT characteristic is 24. You can disable the connection request queue by specifying 0.**
NONE	**Specifies that the server connection queue can contain as many unsatisfied connection requests as memory permits.**

Example

```
Xyplex>> DEFINE SERVER QUEUE LIMIT 0
```

Support Issues

None

DEFINE|SET SERVER REPORT ERRORS

Enable or Disable the reporting of unsupported command errors

Notes

Use this command to specify whether or not the server will display error messages when some invalid or unsupported commands are issued by a user or a TSM script.

The REPORT ERRORS characteristic controls the display of error messages for the following SET/DEFINE PORT commands that are not supported by TCP/IP-LAT software: ALTERNATE SPEED, RING, INPUT SPEED, and OUTPUT SPEED. The REPORT ERRORS characteristic also controls the reporting of error messages when a user attempts to issue a command that is not supported by the parallel port of a network printer server or a modem-control-related command for a port that does not support modem signals.

The REPORT ERRORS characteristic controls the display of error messages for the following SET/DEFINE SERVER commands that are not supported by TCP/IP-LAT software: CONSOLE and HEARTBEAT.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER REPORT ERRORS **[ENABLED]**
[DISABLED]*

Where	Means
ENABLED	**Specifies that the server will display error messages when an invalid or unsupported command is issued. When the REPORT ERRORS characteristic is set to ENABLED, the invalid command is ignored but error messages are reported. When the REPORT ERRORS characteristic is set to ENABLED, the "ENABLED Characteristics" field of the SERVER CHARACTERISTICS display will list Report Errors.**
DISABLED	**Specifies that the server will not display error messages when an invalid or unsupported command is issued. When the REPORT ERRORS characteristic is set to DISABLED, the invalid command is ignored and error messages are not reported. This is the default for the characteristic.**

Example

```
Xyplex>> DEFINE SERVER REPORT ERRORS ENABLED
```

Support Issues

None

DEFINE|SET SERVER RETRANSMIT LIMIT

Specify the maximum number of times that the server will attempt to re-transmit an unacknowledged LAT message

---

Notes

Use this command to specify the maximum number of times that the server will attempt to re-transmit a message to a LAT service node, when the server receives no acknowledgement messages from the service node.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER RETRANSMIT LIMIT *limit*

Where	Means
limit	**Specifies the maximum number of times that the server will attempt to re-transmit a message to a service node, when the server receives no acknowledgement messages from the service node. When the server reaches the retransmit limit, without receiving an acknowledgement from the service node, it disconnects all connected sessions in the virtual circuit to the node. Valid values for this variable are whole numbers in the range of 4 to 120. The default value is 8.** **The value set for this option principally affects network performance. By changing the retransmit limit value, you can manage the efficiency with which network resources are used. For example, setting a low retransmit limit means that there is less traffic on the network because the server makes fewer attempts to transmit a message to the service node. However, the server may not be able to perform some operations due to a "lack of persistence." A larger retransmit limit means that operations are more likely to be successful, but associated with this is more network traffic because the server makes more attempts to transmit a message to the service node. Thus, you may decide to specify a smaller limit when network performance suffers from heavy use, while lightly loaded networks can support the additional traffic caused by extra retransmission attempts.** **A value of 120 is recommended for servers that will have sessions that must go through bridges that have a low link speed.**

Example

```
Xyplex>> DEFINE SERVER RETRANSMIT LIMIT 4
```

Support Issues

None

DEFINE|SET SERVER RLOGIN

Enable or Disable the RLOGIN connections

Notes

Use this command to specify whether or not users on this server can connect to a UNIX host via the RLOGIN command. Typically, the RLOGIN feature provides a convenient method of logging on to a UNIX host by bypassing the login routine at that host. Refer to the section about Configuring RLOGIN Support and the chapter about Managing Server Resources in the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER RLOGIN [ENABLED]*
[DISABLED]

Where	Means
DISABLED	**Specifies that users on this server can not connect to a UNIX host via the RLOGIN command. You might want to disable the use of RLOGIN in order to prevent unauthorized users from logging on the UNIX host (by forcing users to log on via the host login routine and supplying a login password).**
ENABLED	**Specifies that users on this server can connect to a UNIX host via the RLOGIN command. This is the default.**

Example

```
Xyplex>> DEFINE SERVER RLOGIN DISABLED
```

Support Issues

The server must be running TCP/IP in order to use RLOGIN

DEFINE|SET SERVER SCRIPT SERVER

Specify a UNIX host or MAXserver script server and script directory path

Notes

Use this command to specify a UNIX host or MAXserver script server, as well as the directory path where the login script file is located. You can specify up to 4 hosts as script servers. You must designate one or more script servers to use the dialback feature.

Refer to the chapter on Network Command Script Setup in the *Software Management Guide* for more information.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER SCRIPT SERVER [*domain-name* " *directory-path*"]
[*internet-address* " *directory-path*"]

Where	Means
domain-name	**The domain-name of a network script server.**
internet-address	**The internet-address of a network script server.**
" ***directory-path***"	**Specifies the name of the directory where script files can be located. A valid *directory-path* can be a string up to 40 characters long. Seperate the d*irectory-path* from the *internet-address* or *domain-name* with a space. Enclose the *directory-path* in quotation marks.**

Example

```
Xyplex>> DEFINE SERVER SCRIPT SERVER 140.179.224.10 "/tftpboot/scripts"
```

Support Issues

None

DEFINE|SET SERVER SERVICE GROUPS

Enable or Disable LAT service groups on the server

Notes

Specifies that you will permit or restrict access to local services to remote nodes and users. Local services are represented by the groups listed in the *group-list*. Refer to the chapter on security issues in the *Software Management Guide* for more information about groups.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER SERVICE GROUPS	**[*group-list*]**	**[DISABLED]**
		[ENABLED]*
	[ALL]	**[DISABLED]**
		[ENABLED]*

Where	Means
group-list	**Specifies the group codes that are assigned to local services. When you specify a *group-list*, without specifying the ENABLED or DISABLED keyword, the specified *group-list* replaces the current list for the local services.**
ALL	**Specifies that all groups are enabled or disabled for the local services that are available on the server.**
DISABLED	**Specifies that the groups, listed in the *group-list*, are removed from the list of groups that are available on the server.**
ENABLED	**Specifies that the groups, listed in the *group-list*, are added to the list of groups available on the server.**

Example

```
Xyplex>> DEFINE SERVER GROUPS ALL ENABLED
```

Support Issues

None

DEFINE SERVER SESSION LIMIT

Specify the maximum number of sessions available on a server

Notes

The DEFINE SERVER SESSION LIMIT command allows you to specify the maximum number of user sessions that the server can maintain simultaneously. The setting for this characteristic affects the amount of memory that the server will set aside to support user sessions.

You should be careful to limit this value, as the number of sessions affects other server resources which rely on the server's pool of memory. Depending on your server configuration, your unit may not have sufficient resources to support the number of sessions you specify with this command.

Refer to the *Software Management Guide* for a more thorough description of managing server memory.

Privilege Level

Privileged.

Syntax

DEFINE SERVER SESSION LIMIT *limit*|**NONE**

Where	**Means**
limit	**Specifies the maximum number of active sessions that can be connected simultaneously to all ports of the server.** **For the MAXserver 800, 1100, 1120, 1500, 1520, 1800, 1820, 1600, 1620, and 1640 Standalone Terminal Servers, the MX-TSRVM-J8, MX-TSERV-J16, MX-2120, and MX-2210 Terminal Server Cards, and Network 9000 Terminal Server 720 units, valid values for *limit* are whole numbers in the range of 0 to 255. The default value is 128 for these units.** **For all other units, valid values for *limit* are whole numbers in the range of 0 to 64. The default value is 64.**
NONE	**Specifies that the server will support as many active sessions to be connected simultaneously to all ports as memory permits.**

Example

```
Xyplex>> DEFINE SERVER SESSION LIMIT 100
```

DEFINE|SET SERVER SOFTWARE

Specify the name of the load file for the unit

Notes

For MAXserver 4500/5000/5500 options, specifies that you will define or change the filename which is shown in the "Software" field of server displays. For all other unit types, specifies that you will define or change the name of the load image that the unit will request from a network load server, when the unit is configured to load software remotely.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER SOFTWARE *filename*

Where	Means
filename	**For MAXserver 4500/5000/5500 options, specifies the name of the file which will be shown in the "Software" field of server displays. For all other unit types, specifies the name of the load image that the unit will request from a network load server, when the unit is configured to load software remotely.** **Valid names are 1 to 15 ASCII characters in length. (Do not specify a directory name, filetype extension, or version number.) The default value for this variable varies depending on server type.**

Example

```
Xyplex>> DEFINE SERVER SOFTWARE XPCS00S
```

Support Issues

None

DEFINE SERVER TEXTPOOL

Specify the size of server text pool area.

Notes

Servers contain memory, which is used to: store the server load image and database parameters; support the features you have enabled to run on the unit; store information about sessions, connection destinations, and the connection queue, etc.; and provide session resources for users (e.g., the typeahead buffer). The server must allocate portions of this memory in order to provide these functions in an efficient manner. Since each site's networking communications needs are different, the software provides the means by which the server manager can direct this allocation.

At initialization time, the software allocates "pools" of memory for specific purposes or to store specific types of data. One important memory pool is called the text pool area. The text pool area is a permanently-allocated area of memory, the size of which is fixed at initialization time. The server stores identification strings for nodes, LAT services, and domain-names in the text pool area. The DEFINE SERVER TEXTPOOL SIZE command allows you to specify the size of the textpool area, which is an amount of memory used by the server.

Refer to the *Software Management Guide* for a more thorough description of managing server memory.

Privilege Level

Privileged.

Syntax

DEFINE SERVER TEXTPOOL SIZE *text-pool-size*

Where	Means
text-pool-size	**The total number of bytes of memory that the server will allocate for storing identification strings for nodes, services, locally specified *domain-names*, and learned *domain-names*. For MAXserver 800, 1100, 1120, 1500, 1520, 1600, 1620, 1640, 1800, and 1820 Standalone Terminal Servers, and the MX-TSRVM-J8, MX-TSERV-J16, MX-2120, and MX-2210 Terminal Server Cards and Network 9000 Terminal Server 720 units, valid values are whole numbers in the range of 8192 to 131070. For all other units, the maximum value is 65535. The default value is 16384. Re-initialize the unit after you issue this command.**

Example

```
Xyplex>> DEFINE SERVER TEXTPOOL SIZE 65535
```

DEFINE|SET SERVER TIME

Specify the time that is maintained by the server

Notes

Use this command to specify the time that is maintained by the server will be set or changed.

Note that the load server supplies the default time that is maintained by the unit. This command is useful when time changes occur, such as the change do Daylight Savings Time.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER TIME *hh:mm:ss*

Where	Means
hh:mm:ss	**Specifies the new time which will be maintained by the Xyplex Terminal Server. Specify this time using the following format:** ***hh* is a one or two digit number which is the hour of the day in 24-hour clock format. Valid values for hh are numbers in the range of 00 to 23.** ***m m* is a two digit number which represents the minutes in the hour. Valid values for mm are numbers in the range of 00 to 59.** ***ss* is a two digit number which represents the seconds in the minute. Valid values for ss are numbers in the range of 00 to 59.** **Separate each item in the time with a colon character (:).**

Example

```
Xyplex>> DEFINE SERVER TIME 01:00:23
```

Support Issues

None

DEFINE|SET SERVER TIMEZONE

Specify the server time zone

Notes

Enables the server to determine the local time, based on the Universal Time (formally called Greenwich Mean Time) passed by the load server, after loading via TFTP. If the server does not have a real-time battery-backed-up clock, the local time must be calculated from universal time based on your time zone. (The MAXserver Manager (MAXMAN) card and the MAXserver 1000 Series Terminal Servers have real-time clocks.)

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER TIMEZONE *time*

Where	Means
time	**Specifies the hours and minutes west of Universal Time. Specify this time using the following format: *hh:mm*** ***hh* is a one or two digit number which is the hour of the day in 24-hour clock format. Valid values for *hh* are numbers in the range of 00 to 23.** ***m m* is a two digit number which represents the minutes in the hour. Valid values for *m m* are numbers in the range of 00 to 59.**

Example

```
Xyplex>> DEFINE SERVER 12:00
```

Support Issues

none

DEFINE SERVER TN3270 DEVICE

Create a TN3270 device table

Notes

Use this command to specify that you will create a Tn3270 device table or change entries in a Tn3270 device table. See the *Software Management Guide* for more information about creating and modifying device tables. The terminal server can maintain up to eight Tn3270 device tables.

This is a DEFINE SERVER only command.

Privilege Level

Privileged

Syntax

DEFINE SERVER TN3270

DEVICE ***new-device*** **CREATE** ***existing-device***
PORT ***port-number***

DEVICE ***device-name***
TERMINALTYPE "***termtype***"
TN3278TYPE ***model***
KEYMAP ***key*** "***escape-seq***" "***description***"
SCREENMAP ***action*** "***escape-seq***"
MOVECURSOR ***escape-seq*** **[BASE** ***value*****]**
SGR **[ENABLED]***
[DISABLED]

PORT KEYMAPS **[ENABLED]**
[DISABLED]*

Where	Means
new-device	**Specifies the name of the new device table. Device table names can consist of up to 8 characters.**
CREATE	**Specifies that the server will create the device in the *new-device* variable based on the information in the *existing-device* variable or the information defined at PORT *n*.**
existing-device	**Specifies that the terminal server will copy the device you specify in this variable to create the new device. If this is the first time you have created a new device, the existing devices are ANSI, VT100, VT220-7, and VT220-8.**
PORT	**Specifies that the terminal server will copy the device information defined at the port in the *port-number* variable to create the new device.**
port-number	**Specifies the number of the port that the server will use to create the new device.**
device-name	**Specifies a the name of a device. The device you specify can be one of the Xyplex supplied devices, or one that you have created.**
TERMINALTYPE	**Specifies that you will supply a text description of the terminal type in the *device-name* variable.**
"*termtype*"	**A text description. Describes the terminal in the *device-name* variable. This description can include from 1 to 21 characters, enclosed in quotes.**
TN3278TYPE	**Indicates that you will specify the IBM display station type in the *model* variable.**
model	**Specifies an IBM display station type. The two types of models you can specify in this variable are MODEL2 or MODEL5.**
KEYMAP	**Indicates that you will specify an IBM display station function in the *key* variable that will execute at the local terminal when the user enters the key sequence you specify in the "*escape-seq*" variable.**
key	**Specifies an IBM 3270 display station function. See the *Software Management Guide* for a list of IBM display station functions to use in this variable.**
"*escape-seq*"	**Specifies the byte sequence from the local terminal that the terminal server maps to the IBM display station function in the *key* variable. (You specify the local terminal in the *device-name* variable.) You can specify the characters in the byte sequence in two ways: enter the hexidecimal values, which you obtain from the *Programmer's Reference manual* for the local terminal, or manually press the keys on the terminal. You can use from 0 to 9 hexidecimal values in this variable, and enclose the variable in quotes.**

"***description***"	**A text description. Describes the keymap escape sequence in different keymap displays. These include SHOW PORT KEYMAP and the display that appears when the user presses the SHOWKEYS status key during TN3270 terminal emulation. You can use from 0 to 9 characters in this variable, and enclose the variable in quotes.**
SCREENMAP	**Indicates that you will specify a screenmap action that will execute at the local terminal when the user enters the key sequence in the "*escape-seq*" variable.**
action	**Specifies a screenmap action. See the *Software Management Guide* for a list of actions to use for this variable. (When you specify MOVECURSOR as the screenmap action, you can optionally specify an offset value (BASE value) for the row and column positions, other than the default, which is 1.)**
"***escape-seq***"	**Specifies the hexidecimal value of the screenmap action in the *action* variable. Refer to the *Programmer's Reference Manual* for the local terminal to obtain this hexidecimal value. Enclose the variable in quotes.**
BASE	**Indicates that you will specify a base value for the MOVECURSOR screenmap action.**
value	**Specifies an offset value for the row and column position of the cursor. Valid values for this variable are 0 through 255. The default is 1.**
SGR	**Indicates that you will specify how the server will implement the bold, blink, and underscore screen attributes at the terminal.**
ENABLED	**Indicates that the server will use the SET GRAPHIC RENDITION command to implement the bold, blink, and underscore screen attributes. This is the default setting for this characteristic.**
DISABLED	**Indicates that the server will use ON/OFF escape sequences to implement the bold, blink, and underscore screen attributes.**
PORT KEYMAPS	**Indicates that you will specify whether or not an individual port can maintain and modify its own copy of a keymap. Note that an additional 1 K of memory is required for each port that uses this feature. The copy of the keymap exists only in the operational database, not the permanent database.**
DISABLED	**Specifies that an individual port cannot maintain its own copy of a keymap. This is the default setting for this characteristic.**
ENABLED	**Specifies that an individual port can maintain its own copy of a keymap.**

Support Issues

None

DEFINE SERVER TN3270 DEVICE SCREENMAP COLOR

Specify color screenmaps for use by TN3270 devices

Notes

The server supports the two color modes for IBM 3270 terminal emulation: basic 4-color mode and extended 7-color mode. The basic 4-color mode consists of green, red, blue, and white. The extended 7-color mode includes the four basic colors and pink, yellow, and turquoise. The mode you use depends on the colors that your terminal supports as well as those colors that the IBM host application supports.

To use color, you must define the SCREENMAP escape sequence for each color you will use. In addition, you must enable the TELNET TN3270 XTDATTRS extended attributes characteristic at your port to support the extended 7-color mode.

See the *Commands Reference Manual* for more information about the PORT TELNET TN3270 XTDATTRS feature.

This is a DEFINE SERVER only command.

Privilege Level

Privileged.

Syntax

DEFINE SERVER TN3270 DEVICE *device-name* SCREENMAP COLOR*xxx* "*escape-sequence*"

Where	Means
port-list	**One or more terminal server ports.**
COLOR*xxx* and "*escape-sequence*"	**The following command syntax defines each color. The command description includes the hexidecimal ANSI-standard escape sequences for these colors. Check the documentation for your terminal if the terminal supports other types of escape sequences.**

COLORRED	**"1B 5B 33 31 6D"**	**ANSI-standard for red**
COLORGREEN	**"1B 5B 33 32 6D"**	**ANSI-standard for green**
COLORBLUE	**"1B 5B 33 34 6D"**	**ANSI-standard for blue**
COLORYELLOW	**"1B 5B 33 33 6D"**	**ANSI-standard for yellow**
COLORWHITE	**"1B 5B 33 37 6D"**	**ANSI-standard for white**
COLORPINK	**"1B 5B 33 35 6D"**	**ANSI-standard for pink**
COLORTURQUOISE	**"1B 5B 33 36 6D"**	**ANSI-standard for turquoise**

Example

```
Xyplex>> DEFINE SERVER TN3270 DEVICE TV925 SCREENMAP COLORRED
"1B 5B 33 31 6D"
```

DEFINE SERVER TN3270 TRANSLATIONTABLE

Creating and modifying TN3270 translation tables

Notes

Specifies that you will create a Tn3270 translation table or change entries in a Tn3270 translation table. See the *Software Management Guide* for more information about creating and modifying translation tables.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER TN3270 TRANSLATIONTABLE *new-table* CREATE *existing-table*
TRANSLATIONTABLE *trans-name table offset value*

Where	Means
new-table	**Specifies the name of a new translation table. Translation table names can consist of up to 8 characters.**
CREATE	**Specifies that the server will create the translation table in the *new-table* variable based on the table in the *existing-table* variable.**
existing-table	**Specifies that the translation table that the terminal server will use to create the new translation table. If this is the first time you have created a new translation table, USENGLSH is the name you use in this variable.**
trans-name	**Specifies the name of a translation table that you will modify. You must enter the name of a table you have created in this variable. You cannot modify the USENGLSH table..**
table	**Specifies which part of the translation table you will modify with a new value, depending on the direction of data flow. The two directions you can use in this variable are these:**

Direction	Means
ASCIITOEBCDIC	**Apply the new value to outgoing data from the local terminal to the IBM host.**
EBCDICTOASCII	**Apply the new value to incoming data from the IBM host to the local terminal.**

offset	**Specifies the value in the translation table you will modify. The hexidecimal values 40 through FF apply to the EBCDICTOASCII part of the table, and the values 20 through FF apply to the ASCIITOEBCDIC part of the table. See the *Software Management Guide* for a list of these values.**

value	**Specifies the new hexidecimal translation table entry. The values 20 through FF apply to the EBCDICTOASCII part of the table and the values 40 through FF apply to the ASCIITOEBCDIC part of the table. (This is the reverse of the values in the *offset* variable.)**

Support Issues

None

DEFINE|SET SERVER WELCOME

Specify a server welcome message

Notes

Specifies that you want to change the text that is displayed to users when they log on to the server.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER WELCOME "*message*"

Where	Means

message	**A text message. Specifies the text that will be displayed to users when they log on to the server. This text can be up to 80 ASCII characters long. The text must be enclosed in quotation marks ("). The default message is:**
	
	`Welcome to the Xyplex Terminal Server.`
	
	For a Printer server, the default message is:
	
	`Welcome to the Xyplex Printer Server.`

Example

```
Xyplex>> DEFINE SERVER WELCOME "This is a Xyplex Server"
```

Support Issues

None

DEFINE/SET SERVER XREMOTE PRIMARY FONT SERVER

Specify the primary font server

The DEFINE/SET SERVER XREMOTE PRIMARY FONT SERVER commands specify the domain name or Internet address of the primary font server.

Notes

The XDM host can be a font server, but you must define it as such. If you have defined both a primary and a secondary font server, the terminal server requests the file from both servers. It retrieves the file from the font server that responds first.

Privilege Level

Privileged

Syntax

DEFINE | SET SERVER XREMOTE PRIMARY FONT SERVER *domain-name*/*internet-address*/NONE

Where	Means
domain-name	**The domain name of the font server.**
internet-address	**The Internet address of the font server. You can specify address 0.0.0.0 to remove a previously specified Internet address.**
NONE	**Remove a previously specified domain name.**

Example

This command specifies a domain name for the primary font server.

```
Xyplex>> define server xremote primary font server dev.sun.com
```

DEFINE/SET SERVER XREMOTE SECONDARY FONT SERVER

Specify the secondary font server

The DEFINE/SET SERVER XREMOTE SECONDARY FONT SERVER commands specify the domain name or Internet address of the secondary font server.

Notes

The secondary font server is optional if you have defined a primary font server. If you have defined both a primary and a secondary font server, the terminal server requests the file from both servers. It retrieves the file from the font server that responds first.

Privilege Level

Privileged

Syntax

DEFINE|SET SERVER XREMOTE SECONDARY FONT SERVER *domain-name*/*internet-address*/NONE

Where	Means
domain-name	**The domain name of the font server.**
internet-address	**The Internet address of the font server. You can specify 0.0.0.0 to remove a previously specified Internet address.**
NONE	**Remove a previously specified domain name.**

Example

This command specifies the Internet address of the secondary font server.

```
Xyplex>> define server xremote secondary font server 180.179.23.6
```

DEFINE/SET SERVICE

Specify locally-offered services

Notes

You will use the DEFINE SERVICE and SET SERVICE commands to control the operation of and access to services which are available at the terminal server.

Privileges

Privileged

Syntax:

[DEFINE] SERVICE [*service-name*] [*characteristic(s)*]
[SET]

As shown above, multiple service characteristics can be defined or set with a single command. When you specify more than one service characteristic with one command, separate the characteristics with one or more spaces, a comma, or any combination of commas and spaces. (Note, however, that the maximum length of a command line is 132 characters.) The following list is a summary of syntax for the service characteristics which can be defined.

[CONNECTIONS] [DISABLED]
[ENABLED]*

[IDENTIFICATION] [*identification-string*]

[PASSWORD] [*password*]

[PORTS] [*port-list*] [DISABLED]
[ENABLED]*
[ALL] [DISABLED]
[ENABLED]*

[QUEUE] [DISABLED]
[ENABLED]*

Choices indicated by an asterisk (*) represent implied defaults.

Where	Means
service-name	**Specifies the name of the service which is available at the terminal server.**
CONNECTIONS	**Specifies whether or not the terminal server can accept additional connections to the service specified by the *service-name*. Note that when you issue a DEFINE or SET SERVICE command, the status of any connections that are currently formed is not affected.**
DISABLED	**Specifies that the terminal server cannot accept additional connections to the service specified by the *service-name*.**

ENABLED	**Specifies that the terminal server can accept additional connections to the service specified by the *service-name*. This is the default setting for the CONNECTIONS characteristic.**
IDENTIFICATION	**Specifies that you will define or change the string which is included in multicast messages that are sent to other terminal servers in the network, which notifies these servers of the availability of the service specified by the *service-name*.**
identification-string	**Specifies the contents of the string which is included in multicast messages that are sent to other terminal servers in the network, which notifies these servers of the availability of the service specified by the service-name. The *identification-string* can be up to 40 characters in length, and must be enclosed in quotation marks ("). By default, no string is included in multicast messages. To cancel an existing *identification-string*, specify a null string in quotation marks (i.e., "").**
PASSWORD	**Specifies that you will define or change the password which a user must supply in order to use the service specified by the *service-name*.**
password	**Specifies the password that the user must supply in order to use the service specified by the *service-name*. The *password* can be between 1 and 16 printable ASCII characters in length.**
PORTS	**Specifies that you will define or change the port(s) at which a service is offered or is no longer offered.**
port-list	**Specifies the port(s) at which a service is offered, or is no longer offered.**
ALL	**Specifies that the service, specified by the *service-name*, is offered by all ports, or is no longer offered by all ports.**
DISABLED	**Specifies that the service, specified by the *service-name*, is no longer offered at the port(s) specified in the *port-list* or all ports.**
ENABLED	**Specifies that the service, specified by the *service-name*, is offered at the port(s) specified in the *port-list* or all ports. This is the default setting for the PORTS characteristic.**
QUEUE	**Specifies whether or not the server shall place into a connection queue requests for connection to the service which is specified by the *service-name*.**
DISABLED	**Specifies that the server will not place requests for connection to the service into the connection queue.**
ENABLED	**Specifies that the server will place requests for connection to the service into the connection queue. This is the default.**

DEFINE/SET PARAMETER SERVER

Specify parameter servers

Notes

You will use the DEFINE and SET PARAMETER SERVER command to add a specific parameter server to the list of available parameter servers which the terminal server maintains. The terminal server will insure that parameter information that is stored at the specified parameter server is kept up to date. Typically, you would use the SET PARAMETER SERVER command after you temporarily removed a parameter server using the CLEAR PARAMETER SERVER command.

The SERVER PARAMETER SERVER LIMIT characteristic specifies the maximum number of parameter servers that the server can store in a database.

Privileges

Privileged

Syntax:

DEFINE | SET PARAMETER SERVER ***node-name*** **[ADDRESS** ***ethernet-address*****]**
[INTERNET ADDRESS ***internet-address*****]**

Where	Means
node-name	**Specifies the name of the parameter server to add to the list of parameter servers.**
ADDRESS	**Specifies that you will identify the Ethernet address of the parameter server to be added to the list of parameter servers that the terminal server maintains.**
ethernet-address	**Specifies the unique Ethernet address of the parameter server. Valid values are in the form of six pairs of hexadecimal numbers which are separated by hyphens (e.g., AA-01-04-C9-56-F1).**
INTERNET ADDRESS	**Specifies that you will identify the Internet address of the parameter server to be added to the list of parameter servers that the terminal server maintains.**
internet-address	**Specifies the unique Internet address of the parameter server.**

Example:

1. `Xyplex>> SET PARAMETER SERVER VAX1 ADDRESS AA-00-04-00-56-F1`

   Meaning: Add the node VAX1, whose Ethernet address is AA-00-04-00-56-F1, to the list of parameter servers that the terminal server maintains in the operational database.

2. `Xyplex>> DEFINE PARAMETER SERVER UNIXHOST INTERNET ADDRESS 119.20.112.3`

   Meaning: Add the node, whose *internet-address* is `119.20.112.3`, to the list of parameter servers that the terminal server maintains in the permanent database.

DEFINE/SET XPRINTER

Configuring a Port to Support Novell Printing

The DEFINE/SET XPRINTER command maps terminal server ports to Novell printer servers.

Notes

You use the Novell PCONSOLE utility to create Novell printer servers. (Do not confuse the term Novell printer server with a Xyplex printer server, such as a MAXserver 1450 or 1400A Printer Server unit.) Each of these Novell printer servers can be mapped to a physical port on a terminal server or printer server. The port can be either a serial port or a parallel port. Each Xyplex terminal server or printer server port can be connected to only one Novell printer server.

Xprinter support is only provided on Multi-Megabyte load images.

Refer to Secton 14.4 of the *Software Management Guide* for a discussion of Novell printing in the XPRINTER environment.

Privilege Level

Privileged

Syntax

SET
DEFINE XPRINTER *printer-server printer-number* PORT *port-number*

Where	Means
printer-server	**represents the name of an Novell NetWare printer server, that you set up using the PCONSOLE utility.**
printer-number	**represents the number of a Novell NetWare printer that you set up at the Novell printer server (file server) using the Novell PCONSOLE utility. Novell NetWare allows you to specify up to 16 printers, numbered 0 through 15.**
port-number	**represents a terminal server and printer server port. Each port can be connected to only one Novell Printer Server.**

Example

The following command creates assigns a Novell printer server named "postscript," which is Netware printer number 6 to port 4 of a Xyplex terminal server or printer server.

```
Xyplex>> define xprinter postrcript 6 port 4
```

DISCONNECT

Terminate sessions at ports

Notes

Use the DISCONNECT (or DISCONNECT SESSION) command to terminate one or all sessions to which your terminal is connected. You can use the SHOW SESSION display to determine the number(s) of the session(s) you wish to terminate.

Use the DISCONNECT PORT command to terminate all sessions at a port other than the port which you are logged on to.

Privileges

Non-privileged and secure users can terminate sessions at the port they are logged on to. Only users at privileged ports can terminate a session at a port, other than the port they are logged on to (e.g., use the DISCONNECT PORT command).

Syntax:

DISCONNECT [PORT *port-list*]
[SESSION [*session-number*]
[ALL]

Where	Means
PORT	**Specifies that you will terminate all sessions which are connected at a port other than the port you are currently logged on to.**
port-list	**Specifies the number(s) of the terminal server port(s), other than the port you are currently logged on to, whose terminal server sessions are to be terminated.**
SESSION	**Specifies that you will designate a session that will be terminated.**
session-number	**Specifies the number of the session that will be terminated.**
ALL	**Terminate all sessions to which the port is connected.**

Examples:

The following examples show how you use the DISCONNECT command. For examples 1 through 3, suppose that you are working at a terminal which has three active sessions. Figure 2-5 depicts the SHOW SESSION display for this terminal.

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith          Service Mode     Current Session 1
- Session 1: Connected     Interactive      FINANCEVAX
- Session 2: Connected     Interactive      UNIXVAX
- Session 3: Connected     Interactive      LASER
```

Figure 2-5. Example SHOW SESSION Display.

1. Xyplex> DISCONNECT

Meaning: Terminate only the current active session. Based on the SHOW SESSION display shown in Figure 2-5, the terminal server will disconnect session number 1.

2. Xyplex> DISCONNECT SESSION 2

Meaning: Terminate only session 2. (Based on the SHOW SESSION display shown in Figure 2-5, the terminal server will leave the sessions numbered 1 and 3 connected.)

3. Xyplex> DISCONNECT ALL

Meaning: Terminate all active sessions. (Based on the SHOW SESSION display shown in Figure 2-5, the terminal server will disconnect the sessions numbered 1, 2, and 3.)

4. Xyplex>> DISCONNECT PORT 5

Meaning: Terminate the sessions connected to port 5 of the local terminal server. You must be logged on to a privileged port to use this command.

FORWARDS

Select the next available, higher-numbered session

Notes

Use the FORWARDS command to select the next available, higher-numbered session to which your port or terminal is connected. (The terminal server assigns a session number for each session to which a port is connected.)

For purposes of the FORWARDS command, the terminal server tracks session numbers in a "circular" manner. Therefore, when a port is already connected to the highest numbered session, typing FORWARDS connects the port to the lowest numbered port. When only one session is active at a port, the FORWARDS command re-connects the port to that session.

You can use the forward switch character, if one is defined for your port, instead of the FORWARDS command. Refer to the SET PORT FORWARD SWITCH command).

Privileges

Secure

Syntax:

FORWARDS

Examples:

The following examples illustrate the use of the FORWARDS command. Example 1 is a basic example which shows how to use the FORWARDS command to go from one session to the next higher numbered session. Example 2 is a more complicated example showing how to use the FORWARDS command to connect to sessions from among three different sessions.

1. **Suppose that there are two sessions running at a port, and the SHOW SESSION display for this port appears as shown in Figure 2-6.**

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 1
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Figure 2-6. Example SHOW SESSION Display.

As can be seen in Figure 2-6, the port is connected to two sessions, numbered 1 and 2. Session 1 is the currently active session. If, from the Xyplex> prompt, you type:

```
Xyplex> FORWARDS
```

the terminal server will connect the port to session number 2, and display the message:

```
Xyplex -012- UNIXVAX session 2 resumed
```

Figure 2-7 depicts the SHOW SESSION display after you issue the FORWARDS command.

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 2
- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
```

Figure 2-7. Example SHOW SESSION Display.

2. **Suppose that there are three sessions running at a port, and the SHOW SESSION display for this port appears as shown in Figure 2-8.**

```
Xyplex> SHOW SESSIONS

Port 1:  R. Smith         Service Mode     Current Session 1

- Session 1: Connected    Interactive      FINANCEVAX (FINANCEVAX)
- Session 2: Connected    Interactive      UNIXVAX (UNIXVAX)
- Session 4: Connected    Interactive      LASER
```

Figure 2-8. Example SHOW SESSION Display.

As can be seen in Figure 2-8, the port is connected to three sessions, numbered 1, 3 and 4. Session 1 is the currently active session. If, from the Xyplex> prompt, you type:

```
Xyplex> FORWARDS
```

the terminal server will connect the port to session number 3, which is the next available higher numbered session. If you return to the Xyplex> prompt and again type:

```
Xyplex> FORWARDS
```

the terminal server will connect the port to session number 4.

HELP

Obtain help on using commands

Notes

Use the HELP command to display on-line information about particular commands. The TCP/IP-LAT software provides a brief explanation, and a summary of command options, for each command that is available to the user.

Privileges

Privileged users can display help information about all commands. Non-privileged and secure users can only display help information about the commands they are allowed to execute.

Syntax

HELP [INTRODUCTION]
[*topic*] [*sub-topic(s)*]

Where	Means
INTRODUCTION	**Specifies that the user wants to view the introductory help text displays. These displays describe how the user can get started and quickly "get up to speed" with the TCP/IP-LAT software, and the features available with the user interface.**
topic and sub-topic(s)	**Specifies the command(s) or keyword(s) which you need help information about. All keywords are acceptable.**

Example

1. `Xyplex> HELP INTRODUCTION`

   Meaning: Display the introductory help text displays.

2. `Xyplex> HELP SET PORT`

   Meaning: Display an explanation and list of command options for the SET PORT command.

3. `Xyplex> HELP SET PORT ACCESS`

   Meaning: Display an explanation and list of command options for the SET PORT ACCESS command.

INITIALIZE

Re-initialize the terminal server

Notes

Use the INITIALIZE SERVER command to re-initialize the terminal server, or to cancel a previous INITIALIZE SERVER command. Using the INITIALIZE command, the terminal server returns to a state which is exactly the same as if you powered up the server (i.e., all characteristics are restored to the values specified in the permanent database; values specified using SET commands are reset to the values in the permanent database; users are logged out; and the server image is reloaded).

You can specify a delay period before the terminal server re-initializes. When you issue the INITIALIZE command, without specifying a delay period, the terminal server broadcasts a warning to all ports notifying any users who are logged on (the default is 1 minute). If you specify a delay time which is between 2 and 29 minutes, the server will broadcast a warning immediately, and then every minute for each of the last 5 minutes, until re-initialization. If you specify a delay of 30 minutes or greater, the terminal server will broadcast a message immediately, once every 30 minutes prior to re-initialization, and then once every minute for the last 5 minutes. These messages are broadcast regardless of the setting of the DEFINE/SET SERVER BROADCAST characteristic; however, messages are only displayed at ports for which the SET PORT BROADCAST characteristic is set to ENABLED.

If you specify INITIALIZE DELAY 0, and the initialization cannot be completed because there are unsaved parameters, you will receive the "Warning Configuration Not Saved" error message (message 198). If you specify INITIALIZE DELAY *n*, and a user changes a permanent parameter (i.e., uses a Define command) before *n* minutes expire, the initialization is delayed until the parameters are saved. If the parameter server cannot save the parameters, the user who entered the Define command will receive the 198 error message. If you specify the OVERRIDE keyword, the initialization will proceed regardless of whether or not there are unsaved parameters.

Privileges

Privileged

Syntax

INITIALIZE [SERVER] [DELAY] [*delay-time*] [OVERRIDE]
[CANCEL]

Where	Means
SERVER	**An optional keyword.**
DELAY	**Specifies that you want the re-initialization to occur after a specified period of time.**
delay-time	**Specifies the amount of time, in minutes, that the server will wait, until the re-initialization occurs. Valid values are whole numbers in the range of 0 to 32767 minutes; do not specify units. The default value is 1.**
OVERRIDE	**Specifies that the server will perform the initialization regardless of whether or not there are unsaved parameters. If you do specify "OVERRIDE" and parameters have only been partially updated, the parameter file can become corrupted.**
CANCEL	**Cancel a previously issued INITIALIZE command.**

Example

1. `Xyplex>> INITIALIZE`

   Meaning: Broadcast a warning message immediately, and re-initialize the terminal server in one minute.

2. `Xyplex>> INITIALIZE SERVER DELAY 5`

   Meaning: Broadcast a warning message immediately, and once every minute thereafter, until re-initialization. Re-initialize the terminal server in 5 minutes.

3. `Xyplex>> INITIALIZE SERVER DELAY 5 OVERRIDE`

   Meaning: Broadcast a warning message immediately, and once every minute thereafter, until re-initialization. Re-initialize the terminal server in 5 minutes, even if there are unsaved parameters..

4. `Xyplex>> INITIALIZE CANCEL`

   Meaning: Cancel the previously issued INITIALIZE command. (Shut down warnings may still be displayed at other ports for a time.)

LAT CONNECT

Establish a session between your port and a LAT service

Notes

You will use the LAT CONNECT (or LAT CONNECT SERVICE) command to establish a session by creating a virtual connection between your port (terminal) and a service that is offered at a LAT service node. Most users will use the LAT CONNECT command to establish a session between the port they are logged on to and a host or terminal server. When you use the LAT CONNECT command, without specifying a service-name, the terminal server will attempt to establish a session with a preferred LAT service, when one has been defined.

By using the LAT CONNECT command, you require the terminal server to interpret the command qualifiers as applicable to a LAT service, rather than allowing the server to select a Telnet domain-name that is the same as a LAT service-name.

LAT services can be offered at more than one service node or port. The terminal server assumes that all services which have the same service-name are equivalent. Therefore, when a service is offered at more than one node or port, the terminal server will connect to the node or port which has the highest rating (the relative ability to support additional sessions). LAT CONNECT command options permit you to select the particular service node or port, where the service is offered, to which the terminal server will connect.

Connections to a LAT service are also subject to the following conditions:

1. **both the port and the device offering the LAT service must have a matching group code.**

2. **when a service has reached the maximum number of connections it is allowed to have, additional connection requests are entered into a connection queue, if one is enabled.**

Privileges

Secure

Syntax

LAT CONNECT [[SERVICE] *service-name*] [NODE *node-name*] [DESTINATION *port-name*]

Where	Means
SERVICE	**An optional keyword. Specifies that you will provide a *service-name,* to which the port will be connected.**
service-name	**Specifies the name of the service to which the port will be connected.**
NODE	**Specifies that you will provide the name of the service node at which the service, specified by the *service-name,* is offered. You would use this keyword when a service is offered at more than one service node.**
node-name	**Specifies the LAT node which offers the service specified by the *service-name.***
DESTINATION	**Specifies that you will provide the name of the terminal server port at which the service, specified by the *service-name,* is offered. You would use this keyword when a service is offered at more than one port.**
port-name	**Specifies the port on the terminal server which offers the service specified by the *service-name.***

Examples

1. `Xyplex> LAT CONNECT FINANCEVAX`

   Meaning: Establish a session between this port and the LAT service named FINANCEVAX.

2. `Xyplex> LAT CONNECT`

   Meaning: Establish a session between this port and the LAT preferred service that the user has defined for the port. The system will display an error message if the user has not defined a LAT preferred service for the port.

3. `Xyplex> LAT CONNECT FINANCEVAX NODE VAX1`

   Meaning: Establish a session between the port and the LAT service named FINANCEVAX, which is offered at the node named VAX1, rather than at any other service node where the service named FINANCEVAX is offered.

4. `Xyplex> LAT CONNECT LASER NODE MAX5000 DESTINATION PORT_2`

   Meaning: Establish a session between the port and the LAT service named LASER, which is offered on the node MAX5000 at terminal server port 2, rather than at any other port where the service named LASER is offered.

LAT CONNECT PORT

Establish sessions between a port, other than the port you are logged on to, and a LAT service

Notes

Use the LAT CONNECT PORT command to establish a session by creating a virtual connection between a terminal server port, called the "target" port, and a LAT service. The target port is usually a port other than the port you are currently logged on to.

To use this command, you must specify the name of a LAT service. This can be done either by the LAT CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The PORT ACCESS characteristic for the target port must be set to REMOTE. The target port cannot have a session in progress (you can terminate an active session using the DISCONNECT PORT command).

Privileges

Privileged

Syntax

LAT Connect [POrt *port-number*] [*service-name*] [NODe *node-name*] [DEStination *port-name*]

Where	Means
POrt	**Specifies that you will connect a target port to a LAT service.**
port-number	**Specifies the number of the target terminal server port which will be connected to a LAT service.**
service-name	**Specifies the LAT service to which the target terminal server port, specified by the port-number is connected.**
NODe	**Specifies that you will designate a LAT node which offers the service specified by the service-name. You would use this keyword when there are multiple LAT service nodes which offer the service.**
node-name	**Specifies the LAT service node which offers the service specified by the service-name.**
DEStination	**Specifies that you will designate a terminal server port which offers the service specified by the service-name. You would use this keyword when there are multiple terminal server ports which offer the service.**
port-name	**Specifies the terminal server port which offers the service, specified by the service-name.**

Example

1. Xyplex>> LAT CONNECT PORT 5 LASER

   Meaning: Establish a session between the target port (port 5) and the LAT service named LASER.

2. Xyplex>> LAT CONNECT PORT 5

   Meaning: Establish a session between the target port (port 5) and the LAT dedicated service that the user has defined for the port.

3. Xyplex>> LAT CONNECT PORT 5 LASER NODE MAX5000 DESTINATION PORT_2

   Meaning: Establish a session between the target port (port 5) and the LAT service named LASER, which is offered at terminal server port 2, on the node MAX5000.

LIST

Display information from the permanent database

All LIST commands are described in the section on SHOW commands.

LOCK

Temporarily disable user access to a port

Notes

Use the LOCK command to secure a terminal (temporarily disable user access to active terminal sessions), without disconnecting your current sessions or logging out. The LOCK command requires that you provide a password (which is not displayed) before the terminal is disabled. To re-enable the terminal, you must enter the correct password. If you forget the password, you must have a user at a privileged port logout the port (which disconnects all current sessions) before the port can be used again.

To be able to use the LOCK command, the SERVER LOCK characteristic must be set to ENABLED.

Privileges

Secure

Syntax

LOCK

Example

When you type the command:

```
Xyplex> LOCK
```

the terminal server responds with the prompt:

```
Lock Password>
```

type in a password, of between 1 and 16 characters. The terminal will not display the password on the screen (or printer in the case of a hardcopy terminal). The terminal server then displays the prompt:

```
Verification>
```

Type the same password. If you correctly type the password, the server will respond with a message and prompt similar to the following:

```
Xyplex - 019 - Port 1 locked
Unlock Password>
```

When you are ready to re-enable the terminal, type the password at the Unlock Password> prompt.

LOGOUT PORT

Log out a port and disconnect all sessions

Notes

Use the LOGOUT PORT command to log off of the terminal server, or to log out other ports. LOGOUT PORT also disconnects all sessions.

Privileges

All users can logout their own port. Only a user at a privileged port can logout other ports.

Syntax

LOGOUT [PORT] [*port-list*]
[ALL]

Where	Means
PORT	**Specifies that you will identify the port which is to be logged off of the terminal server.**
port-list	**Specifies the port(s) which are to be logged off. The default value is your own port.**
ALL	**Log off all ports from the terminal server.**

Examples

1. `Xyplex> LOGOUT`

Meaning: Log your port off from the terminal server and disconnect all sessions which are still connected.

2. `Xyplex>> LOGOUT PORT 5`

Meaning: Log off port 5 from the terminal server and disconnect all sessions which are still connected at port 5. The server manager might typically use this command when a user has locked his terminal (using the LOCK command) and has forgotten the unlock password.

MONITOR

Display continuously updated information in the operational database

All MONITOR commands are described with the SHOW commands.

PURGE DOMAIN

Remove domain-name entries from the permanent database

Notes

Use the PURGE DOMAIN command to delete one or all *domain-name* entries from the permanent database. The deleted *domain-name(s)* can be respecified using a DEFINE DOMAIN command. If the *domain-name* is listed in the operational database, it will still be available until the server is re-initialized or it is removed using a CLEAR DOMAIN command. (Refer also to the description of the CLEAR DOMAIN command.)

If the specified *domain-name* is not a fully qualified *domain-name,* the specified name will be concatenated with the default Internet *domain-suffix.* The server will display an error message if you use the PURGE DOMAIN command when the specified Domain name does not exist.

Privileges

Privileged

Syntax

PURGE DOMAIN [*domain-name*]
[ENTRY *entry-number*]
[ALL]

Where	Means
domain-name	**Specifies the name of the local *domain-name* which will no longer be stored in the permanent database.**
ALL	**Specifies that all *domain-names* will be removed from the permanent database.**
ENTRY	**Specifies that you will identify, by *entry-number* shown in the LIST DOMAIN display, the *domain-name/internet-address* combination that will no longer be available to server users.**
entry-number	**Specifies a line shown in the "Entry" column of the LIST DOMAIN display, which represents a *domain-name/internet-address* combination that will no longer be available to server users.** **Note that *domain-name* entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a *domain-name,* you should make sure that you have selected the correct entry number.**

Examples

1. Xyplex>> PURGE DOMAIN FINANCESUN.XYPLEX.COM

   Meaning: Remove the *domain-name* FINANCESUN.XYPLEX.COM from the permanent database.

2. Xyplex>> PURGE DOMAIN ALL

   Meaning: Remove all *domain-names* from the permanent database.

3. Xyplex>> PURGE DOMAIN ENTRY 5

   Meaning: Make unavailable to server users the *internet-address* that is associated with the *domain-name* shown in entry number 5 of the LIST DOMAIN display.

PURGE INTERNET ROTARY

Remove Internet rotary entries from the permanent database

Notes

Use the PURGE INTERNET ROTARY command to delete one or all rotary entries from the permanent database. (A rotary is a group of ports on the server which are assigned the same internet-address.) The deleted rotaries can be respecified using a DEFINE SERVER INTERNET ROTARY command. Since the rotaries are only being deleted from the permanent database, they will remain available until the server is re-initialized or the rotary is removed using a CLEAR SERVER INTERNET ROTARY command. (Refer also to the description of the CLEAR SERVER INTERNET ROTARY command.)

Examine the LIST SERVER INTERNET ROTARY display to determine the entry number for a particular rotary in the permanent database. Note that rotary entries and their associated entry numbers in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a rotary, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE INTERNET ROTARY command when the specified entry does not exist.

Refer to the *Software Management Guide* for a description of the Internet rotaries.

Privileges

Privileged

Syntax

PURGE INTERNET ROTARY [*entry*]
[ALL]

Where	Means
entry	**Specifies the entry number of the rotary which will be deleted from the permanent database. This rotary will no longer be available after the server is re-initialized., unless it is re-enabled with a DEFINE SERVER INTERNET ROTARY command.**
ALL	**Specifies that all internet-rotaries will be removed from the permanent database. These rotaries will no longer be available after the server is re-initialized, unless the internet-rotaries are re-enabled with a DEFINE SERVER INTERNET ROTARY command.**

Example

1. Xyplex>> PURGE INTERNET ROTARY 1

   Meaning: Make only rotary entry number 1 in the permanent database (displayed in the LIST SERVER INTERNET ROTARY display) unavailable, after the server is re-initialized. The rotary can be re-enabled with a DEFINE SERVER INTERNET ROTARY command.

2. Xyplex>> PURGE INTERNET ROTARY ALL

   Meaning: Make all rotaries in the permanent database (e.g., those specified using a DEFINE SERVER INTERNET ROTARY command) unavailable.

PURGE INTERNET SECURITY

Remove Internet Security entries from the permanent database

Notes

This command enables a system manager to remove one or all entries from the Internet Security table in the permanent database. Once purged, an entry can be respecified using the DEFINE PORT INTERNET SECURITY command. (Also, note that the CLEAR INTERNET SECURITY command is used to remove a security table entry from the operational database.)

Examine the output of the LIST PORT INTERNET SECURITY command to determine the entry number in the Internet Security table that you want to remove. Note that security entry numbers in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a security entry, you should make sure that you have selected the correct entry number.

The server will display an error message if the entry you specify does not exist.

The PURGE INTERNET SECURITY command clears the security assignment (allow or deny access) for all ports in the *port-list*, for which the assignment was made. To disable Internet Security for a specific port, use the DISABLE option of the DEFINE PORT INTERNET SECURITY command.

Refer to the *Software Management Guide* for a description of the Internet Security feature.

Privileges

Privileged

Syntax

PURGE INTERNET SECURITY **[*entry*]**
[ALL]

Where	Means
entry	**Corresponds to a number appearing in the Entry field of the LIST PORT INTERNET SECURITY output.**
ALL	**Purges all entries in the Internet Security table.**

Example

```
Xyplex>> PURGE INTERNET SECURITY 3
```

Meaning: Remove Entry 3 in the Internet Security table from the permanent database.

PURGE PARAMETER SERVER

Remove parameter server entries from the permanent database

Notes

This command enables a system manager to remove a parameter server from the list of parameter servers that the server maintains in the permanent database. Once purged, the parameter server can be respecified using the DEFINE PARAMETER SERVER command. (Also refer to the CLEAR PARAMETER SERVER command, which is used to remove a parameter server from the operational database.)

Examine the output of the LIST PARAMETER SERVER command to determine the node name of the parameter server you want to remove.

The server will display an error message if the parameter server you specify does not exist.

Privileges

Privileged

Syntax

PURGE PARAMETER SERVER *node-name*

Where	Means
node-name	**The node name of the parameter server to be purged, which appears in the output of the LIST PARAMETER SERVER command.**

Example

```
Xyplex>> PURGE PARAMETER SERVER UNIXSUN
```

Meaning: Remove the parameter server "UNIXSUN" from the list of parameter servers that the server maintains in the permanent database.

PURGE PORT INTERNET SECURITY

Remove port Internet security entries from the permanent database

Notes

Use the PURGE PORT INTERNET SECURITY command to remove Internet security entries for one or more designated port(s) from the permanent database.

Refer to the *Software Management Guide* for a description of the Internet Security feature.

Privileges

Privileged

Syntax

PURGE PORT [*port-list*] INTERNET SECURITY [ALL]

Where	Means
port-list	One or more terminal server ports.
ALL	Specifies that the command will apply to all ports on the server.
INTERNET SECURITY	Specifies that you want to remove one or all Internet security entries pertaining to the designated port(s) from the Internet Security table in the permanent database. Once cleared, a permanent database entry can be respecified using the DEFINE PORT INTERNET SECURITY command. The server will display an error message if the entry you specify does not exist.

Example

```
Xyplex>> PURGE PORT 4 INTERNET SECURITY
```

Meaning: Remove all entries in the Internet Security table for port 4 from the permanent database.

PURGE SERVER INTERNET ROUTE

Remove internet route entries from the permanent database

Notes

Use the PURGE SERVER INTERNET ROUTE command to delete one or all internet-route entries from the permanent database. The deleted internet-route(s) can be respecified using a DEFINE SERVER INTERNET ROUTE command. Since the internet-route(s) are only being deleted from the permanent database, they will remain available until the server is re-initialized or the route is removed using a CLEAR SERVER INTERNET ROUTE command. (Refer also to the description of the CLEAR SERVER INTERNET ROUTE command.)

Examine the LIST SERVER INTERNET ROUTE display to determine the entry number for a particular internet route in the permanent database. Note that internet-route entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR an internet-route, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE SERVER INTERNET ROUTE command when the specified entry does not exist.

Refer to the section on Configuring Internet Routes in the *Software Management Guide* .

Privileges

Privileged

Syntax

PURGE SERVER INTERNET ROUTE **[*entry*]**
[ALL]

Where	Means
entry	**Specifies the entry number of the internet-route which will be deleted from the permanent database. This internet-route will no longer be available to server users after the server is re-initialized., unless the route is re-enabled with a DEFINE SERVER INTERNET ROUTE command.**
ALL	**Specifies that all internet-routes will be removed from the permanent database. These entries will no longer be available to server users after the server is re-initialized, unless the internet-routes are re-enabled with a DEFINE SERVER INTERNET ROUTE command.**

Examples

1. `Xyplex>> PURGE SERVER INTERNET ROUTE 1`

   Meaning: Make only internet-route entry number 1 in the permanent database (displayed in the LIST SERVER INTERNET ROUTE display) unavailable, after the server is re-initialized. The internet-route can be re-enabled with a DEFINE SERVER INTERNET ROUTE command.

2. `Xyplex>> PURGE SERVER INTERNET ROUTE ALL`

   Meaning: Make all internet-routes in the permanent database (e.g., those specified using a DEFINE SERVER INTERNET ROUTE command) unavailable.

PURGE SERVER MENU

Remove menu entries from the permanent database

Notes

This command enables a system manager to remove an item on the server's menu from the permanent database. Once purged, the menu item can be respecified using the DEFINE SERVER MENU command. (Also refer to the CLEAR SERVER MENU command, which is used to remove a menu item from the operational database.)

Refer to the *Software Manangement Guide* for a description of the Simple Menu Interface feature.

Examine the output of the LIST SERVER MENU command to determine the number of the entry that you want to remove.

The server will display an error message if the entry that you specify does not exist.

Privileges

Privileged

Syntax

PURGE SERVER MENU *item-number*

Where	Means
item-number	**Specifies the item number (1 - 20) within the menu that you want to remove.**

Example

```
Xyplex>> PURGE SERVER MENU 3
```

Meaning: Remove the third item on the server's menu from the permanent database.

PURGE SERVER SCRIPT SERVER

Remove script server entries from the permanent database

Notes

Use the PURGE SERVER SCRIPT SERVER command to delete one or all script server entries from the permanent database. The deleted script servers can be respecified using a DEFINE SERVER SCRIPT SERVER command. Since the script servers are only being deleted from the permanent database, they will remain available until the server is re-initialized or the script server is removed using a CLEAR SERVER SCRIPT SERVER command. (Refer also to the description of the CLEAR SERVER SCRIPT SERVER command.)

Examine the LIST SERVER SCRIPT SERVER display to determine the entry number for a particular script server in the permanent database. Note that script server entries in the permanent database do not need to match the entries in the operational database. Therefore, if you want to PURGE and CLEAR a script server, you should make sure that you have selected the correct entry number.

The server will display an error message if you use the PURGE SERVER SCRIPT SERVER command when the specified entry does not exist.

Privileges

Privileged

Syntax

PURGE SERVER SCRIPT SERVER **[*entry*]**
[ALL]

Where	Means
entry	**Specifies the entry number of the script server which will be deleted from the permanent database. This script server will no longer be available after the server is re-initialized., unless it is re-enabled with a DEFINE SERVER SCRIPT SERVER command.**
ALL	**Specifies that all internet-script servers will be removed from the permanent database. These script servers will no longer be available after the server is re-initialized, unless the internet-script servers are re-enabled with a DEFINE SERVER SCRIPT SERVER command.**

Examples

1. Xyplex>> PURGE SERVER SCRIPT SERVER 1

   Meaning: Make only script server entry number 1 in the permanent database (displayed in the LIST SERVER SCRIPT SERVER display) unavailable, after the server is re-initialized. The script server can be re-enabled with a DEFINE SERVER SCRIPT SERVER command.

2. Xyplex>> PURGE SERVER SCRIPT SERVER ALL

Meaning: Make all script servers in the permanent database (e.g., those specified using a DEFINE SERVER SCRIPT SERVER command) unavailable.

PURGE SERVER TN3270 DEVICE

Remove TN3270 devices from the permanent database

Notes

Use the PURGE SERVER TN3270 DEVICE command to delete a Tn3270 device table from the permanent database. Before if deletes the table from the database, the terminal server checks that the table is not being used by a port. If not, it deletes the table. The server will not delete a table that is currently in use. Tn3270 device tables exist only in the permanent database, so Clear commands do not apply to them. Examine the SHOW/LIST SERVER TN3270 display to determine the Tn3270 devices in the permanent database.

If you delete *all* of the device tables in the database, the terminal server will reenable the Xyplex-supplied tables (ANSI, VT100, VT220-7, and VT220-8) after the server is re-initialized.

The server will display an error message if you use the PURGE SERVER TN3270 DEVICE command when the specified device does not exist, or when it is in use by a Tn3270 port..

Privileges

Privileged

Syntax

PURGE SERVER TN3270 DEVICE [*device-name*]

Where	Means
device-name	**Specifies the name of the of the Tn3270 device table which will be deleted from the permanent database.**

Example

```
Xyplex>> PURGE SERVER TN3270 DEVICE VT100
```

Meaning: Delete the VT100 device table from the permanent database after the server is re-initialized. (To retrieve the VT100 device table, you must delete *all* devices, then re-initialize the terminal server. The terminal server will then reenable all the Xyplex-supplied devices.)

PURGE SERVER TN3270 TRANSLATIONTABLE

Remove TN3270 translation tables from the permanent database

Notes

Use the PURGE SERVER TN3270 TRANSLATIONTABLE command to delete a Tn3270 translation table from the permanent database. Before if deletes the table from the database, the terminal server checks that the table is not being used by a port. If not, it deletes the table. The server will not delete a table that is currently in use. Tn3270 translation tables exist only in the permanent database, so Clear commands do not apply to them. Examine the SHOW/LIST SERVER TN3270 display to determine the Tn3270 translation tables in the permanent database.

The terminal server does not allow you to delete the default table, USENGLSH, that Xyplex supplies with the software. You can only delete tables that you have created on the server with the DEFINE SERVER TN3270 TRANSLATIONTABLE command.

The server will display an error message if you use the PURGE SERVER TN3270 TRANSLATIONTABLE command when the specified entry does not exist, or when it is in use by a Tn3270 port, or if you attempt to delete the USENGLSH table.

Privileges

Privileged

Syntax

PURGE SERVER TN3270 TRANSLATIONTABLE [*trans-name*]

Where	Means
trans-name	**Specifies the name of the of the Tn3270 translation table which will be deleted from the permanent database. This translation table will no longer be available after the server is re-initialized. You can only specify the names of tables that you have created in this variable; you cannot specify USENGLSH, the Xyplex-supplied translation table.**

Example

```
Xyplex>> PURGE SERVER TN3270 TRANSLATIONTABLE SPANISH
```

Meaning: Delete the SPANISH translation table from the permanent database after the server is re-initialized.

PURGE SERVICES

Remove locally-offered LAT services from the permanent database

Notes

Use the PURGE SERVICES command to delete, from the permanent database, the entry for one or all of the services offered locally at the server. The service is permanently removed, and will not again become available when the server is re-initialized. Active local services will still operate until the next time the server is re-initialized, unless they are removed by a CLEAR SERVICES command.

Privileges

Privileged

Syntax

PURGE SERVICES [*service-name*]
[LOCAL]

Where	Means
service-name	**Specifies the name of the local service (e.g., a service which is offered by the server) which will no longer be offered by the server.**
LOCAL	**Specifies that all local services (e.g., services which are offered by the server) will no longer be offered by the server.**

Example

Examples

1. `Xyplex>> PURGE SERVICE LOCAL`

Meaning: Permanently remove (make unavailable) all services which are currently offered at the server.

2. `Xyplex>> PURGE SERVICE LASER`

Meaning: Permanently remove the service named LASER, which is currently offered at the server.

PURGE XPRINTER PORTS

Remove Novell printer services from the permanent database

Notes

Use the PURGE XPRINTER PORTS command to delete, from the permanent database, the entry for the Novell printer services offered at one or more terminal or Xyplex printer server ports. The service is permanently removed, and will not again become available when the server is re-initialized. Active Novell printer services will still operate until the next time the server is re-initialized, unless they are removed by a CLEAR XPRINTER PORTS command.

Privileges **Privileged**

Syntax:

PURGE XPRINTER PORTS **[*port-list*]**
[ALL]

Where	Means
port-list	**Remove the permanent database entry for the Novell printer services offered at one or more terminal or Xyplex printer server ports.**
ALL	**Remove the permanent database entry for the Novell printer services offered at all ports which offer this service.**

Example

```
Xyplex>> PURGE XPRINTER PORTS 1,3-5
```

REMOTE CONSOLE

Establish a session with the terminal server virtual management port

Notes

Use the REMOTE CONSOLE command, at the local server unit, to connect and log on to the console port on a remote server unit. The remote server unit can be a unit that supports the Remote Console Facility. (Many LAT devices support this facility, although some do not and others like the DECsa terminal server support it in an incompatible manner). After the remote console session has been formed, you can issue server unit commands for the remote server unit, as though you were logged on directly at that server unit.

If there is a maintenance password defined for the remote server unit you wish to log on to, you will be required to supply the maintenance password in order to use the REMOTE CONSOLE command. Failure to supply the password will prevent a remote connection from being formed, but this failure will appear as though the server has not responded.

The Console LED will remain lit whenever there is either a local or remote console session.

There are several pre-defined port characteristics (i.e., PORT SPEED) for the remote console port of the remote server unit, when a remote console session has been established. You cannot change the settings for these characteristics. The characteristics are:

Characteristic	Setting
ACCESS	LOCAL
AUTOBAUD	DISABLED
BREAK	DISABLED
CHARACTER SIZE	8
DEDICATED SERVICE	NONE
DIALUP	DISABLED
DSRLOGOUT	DISABLED
DTRWAIT	DISABLED
FLOW CONTROL	XON
INPUT FLOW CONTROL	ENABLED
INPUT SPEED	9600
MODEM CONTROL	DISABLED
OUTPUT FLOW CONTROL	ENABLED
OUTPUT SPEED	9600
PARITY	NONE
PASSWORD	ENABLED
SPEED	9600

When you are in a remote console session, you can use a CONNECT command (at the remote console local command prompt) to establish a session from the remote console. To exit from the session initiated from the remote console port

(i.e., to return to the remote console local command prompt), type a tilde (~) character. To terminate the remote console session, type the <BREAK> character or local switch character, and the DISCONNECT command (at the server unit local command prompt).

Privileges **Privileged**

Syntax

REMOTE CONSOLE [NODE *node-name*] [MAINTENANCE [PASSWORD] *password*] [*ethernet-address*] [MAINTENANCE [PASSWORD] *password*]

Where	Means
NODE	**Specifies that you will identify the *node-name* of the remote server unit to which a remote console session will be established.** **When connecting to a server remote console port by specifying a *node-name*, the target server must offer at least one LAT local service. (If the target server does not offer a local service, you can specify the Ethernet address of the target server in order to establish a remote console connection.)**
node-name	**Specifies the name of the server unit to which a remote console session will be established. Refer to section 2.1.3 for a definition.**
ethernet-address	**Specifies the unique Ethernet address of the remote server unit. Valid values are in the form of six pairs of hexadecimal numbers which are separated by hyphens (e.g., AA-01-04-C9-56-F1).**
MAINTENANCE	**An optional keyword.**
PASSWORD	**Specifies that you will supply the maintenance password for the remote server unit.**
password	**Specifies the maintenance password for the remote server unit. The password is a hexadecimal number in the range of 0 to FFFFFFFFFFFFFFFF (i.e., up to 16 hexadecimal digits long). The password must be in quotation marks ("). The default is 0. The maintenance password at the remote server unit was set using a DEFINE or SET SERVER MAINTENANCE PASSWORD command.**

Examples

1. Xyplex>> REMOTE CONSOLE NODE MX5000

   Meaning: Establish a remote console session between the port the user is logged on to, and the remote console port (port 0) of the remote server unit whose node-name is MX5000. In this example, there may not be a maintenance password defined at the remote server unit.

2. Xyplex>> REMOTE CONSOLE NODE MX5000 MAINT PASSWORD "9C"

   Meaning: Establish a remote console session between the port the user is logged on to, and the remote console port (port 0) of the remote server unit whose node-name is MX5000. The maintenance password defined at the remote server unit is 9C.

3. Xyplex>> REMOTE CONSOLE AA-01-C4-11-73-F8 MAINT PASS "9C"

   Meaning: Establish a remote console session between the port the user is logged on to, and the remote console port (port 0) of the remote server unit whose Ethernet address is AA-01-C4-11-73-F8. The maintenance password defined at the remote server unit is 9C.

4. **This is an example of how you initiate and exit from a session from within a remote console session.**

   a. **Issue the REMOTE CONSOLE command. For example**

      Xyplex>> REMOTE CONSOLE AA-01-C4-11-73-F8 MAINT PASS "9C"

      Press the <RETURN> key until the server unit responds with the login prompt. For example:

      #

   b. **The # prompt (the login password prompt) indicates that you must type in the login password. (The actual password prompt on your server unit may be different, because the server manager can assign a new prompt.) You will need to obtain the login password from the server manager. Type in the login password and press the <RETURN> key. When you type the correct login password, the server unit will display the Enter username> prompt. Note that the login password is not the same password as the maintenance password used in the REMOTE CONSOLE command.**

c. At the Enter Username> prompt, type a username and press the <RETURN> key. You can specify a username that is between 1 and 16 characters long, or type a <CTRL>/<Z> command to automatically assign a username for the port (the assigned username is in the form: PORT_n). The username helps the server manager identify the port where you are logged on, in case there are problems.

The server unit will now display the local command prompt. For example:

```
Xyplex>
```

(The local command prompt on your server unit may be different.) When you see the local command prompt, you are logged on to the remote console port. You can enter all server commands from the local command prompt.

d. Issue the appropriate CONNECT command. For example:

```
Xyplex> CONNECT FINANCEVAX
```

Log on to the service node. While you are logged on to the service node, if you type a tilde (~) character, you will return to the remote console local command prompt. After you have completed work on the service node, log off and return to the local command prompt.

e. Terminate the remote console session by typing the <BREAK> character or local switch character. This will return you to the local command prompt. Type the DISCONNECT command to complete termination of the remote console session. (You could also use the RESUME command to continue the remote console session.)

REMOVE QUEUE

Delete requests for connection to local services, from the server connection queue.

Notes

Use the REMOVE QUEUE command to delete requests for connection to local services, from the terminal server connection queue.

Privileges

Privileged

Syntax

REMOVE QUEUE [ENTRY *entry-number*]
[NODE *node-name*]
[SERVICE *service-name*]
[ALL]

Where	Means
ENTRY	**Specifies that you will remove one specific entry from the connection queue.**
entry-number	**Specifies the number of the connection queue entry that you wish to delete. Use the SHOW QUEUE command to display a list of queue entries to determine the entry-number.**
NODE	**Specifies that you wish to remove from the connection queue all connection requests from a specific node.**
node-name	**Specifies the name of the node whose connection requests will be deleted.**
SERVICE	**Specifies that you wish to remove from the connection queue all connection requests to a specific local service. All connection queue requests to the specified local service will be deleted from the connection queue.**
service-name	**Specifies the name of the local service whose connection queue entries will be deleted. All connection queue requests to the service will be deleted from the connection queue.**
ALL	**Specifies that all connection requests will be deleted from the terminal server connection queue.**

Example

1. Xyplex>> REMOVE QUEUE ENTRY 1

   Meaning: Remove only entry number 1 from the connection queue.

2. Xyplex>> REMOVE QUEUE NODE FINANCEVAX

   Meaning: Remove all entries in the connection queue from the node named FINANCEVAX.

3. Xyplex>> REMOVE QUEUE SERVICE LASER

   Meaning: Remove all entries for connection to the local service LASER from the connection queue.

4. Xyplex>> REMOVE QUEUE ALL

   Meaning: Remove all connection request entries in the terminal server connection queue.

RESET PORT

Clear a "Hung" Parallel Port

Notes

Use the RESET PORT command to clear a parallel port that is stopped "hung." This will allow the next print job in the queue to begin printing.

Privileges **Privileged**

Syntax

RESET PORT *port-list*

Where	Means
port-list	**One or more parallel ports on a Xyplex printer server.**

Example

```
Xyplex>> RESET PORT 3
```

RESUME

Resume a suspended session

Notes

Use the RESUME command to return to a session that you have exited. If you issue a RESUME command, without specifying the session you wish to resume, the terminal server will place you back in the current session. Use the SHOW SESSIONS command to display a list of your connected sessions.

If you issue a RESUME command, without specifying the session you wish to resume, the terminal server will place you back in the current session. Use the SHOW SESSIONS command to display a list of your connected sessions.

You can enter a string of up to 32 characters with the RESUME command. The terminal server sends this string to the application on the host where you have established a session. The string can contain caret ^ control sequences that the terminal server converts to actual control characters before it sends them to the application. For example, you might need to include an ^M^J sequence at the end of a character string to send the Carriage Return and Line Feed characters.

The server does not save the character string in multiple RESUME commands. You enter the string each time you want to send it to the application in the RESUME command.

Privileges

Secure

Syntax

RESUME [[SESSION] ***session-number*****] ["*****character-string*****"]**
[***service-name*****]**
[***domain-name*****]**
[***internet-address*****]**

Where	Means
SESSION	**An optional keyword.**
session-number	**Specifies the number of the session that you wish to resume. The default value is the current session.**
service-name	**Specifies the name of the service with which you wish to resume a session. If there are multiple sessions to the same service-name, the session with the lowest number will be the one that is resumed.**
domain-name	**Specifies the domain name with which you wish to resume a session.**
internet-address	**Specifies the domain name with which you wish to resume a session.**
"***character-string***"	**Up to 32 ASCII characters, including caret control characters. The terminal server converts caret control characters to actual control characters before it sends them to the application. Enclose the character string in quotes.**

Examples

1. `Xyplex> RESUME`

   Meaning: Resume the current active session.

2. `Xyplex> RESUME 1`

   Meaning: Resume session 1.

2. `Xyplex> RESUME FINANCEVAX`

   Meaning: Resume the session currently established with the service or *domain-name* FINANCEVAX.

RLOGIN

Log on to a UNIX host

Notes

The RLOGIN command enables a user to log onto a remote host system by specifying the host system and a username that is recognized by the host. The terminal server passes either the username of the port or the username specified on the RLOGIN command line to the host. Depending on how the RLOGIN implementation at the host is set up, this may be sufficient to allow the user to bypass the login routine of the host (e.g., the user will automatically be logged on to the host, without having to supply a username and password.). Refer to the *Software Management Guide* for a description of the RLOGIN Support feature.

There are advantages and disadvantages to using RLOGIN rather than Telnet to make connections. At some hosts, the RLOGIN implementation can be more efficient at terminating display of output from a program (i.e., when you issue a <CTRL>/<C> command, the user prompt is displayed faster with an RLOGIN connection than a Telnet connection). However, since the RLOGIN protocol is not an Internet-standard protocol, RLOGIN is less widely available and is usually not as well implemented as Telnet. For example, the RLOGIN protocol does not typically support binary session modes, local echoing, or features that are equivalent to the Telnet features such as passing 7-bit CSI escape sequences, and the Telnet "are you there?" and "synchronize" commands. (Refer to the descriptions of the PORT TELNET BINARY SESSION MODE, TELNET ECHO MODE, TELNET CSI ESCAPE, TELNET QUERY, and TELNET SYNCHRONIZE characteristics, respectively).

Privileges

Secure

Syntax

RLOGIN ***domain-name*** **[[USERNAME]** "***username***"**]**
internet-address **[[USERNAME]** "***username***"**]**
NONE

Where	Means
domain-name	**Specifies the domain-name of the host which you will log on to.**
internet-address	**Specifies the internet address of the host which you will log on to.**
USERNAME	**An optional keyword. Specifies that you want to enter a username rather than using the username of the port.**
username	**Enter a quoted string representing a username that will be recognized by the host.**
NONE	**Specifies that the server will connect the port to the preferred service that is defined for that port.**

Examples

1. Xyplex> RLOGIN UNIXSUN

Meaning: Log onto host system "UNIXSUN" using the username of the port.

2. Xyplex> RLOGIN UNIXSUN "JOHNSON"

Meaning: Log onto host system "UNIXSUN" using the username "JOHNSON".

3. Xyplex> RLOGIN

Meaning: Connect the port to the preferred service that is defined for the port.

SCRIPT

Download a script file and execute the commands contained in the file

Notes

Use this command to have the port download a script from a script server and perform the commands contained in the script file.

Refer to the guide *Using the TCP/IP-LAT Terminal Server* and the *Software Management Guide* for more information about using scripts.

Privilege Level

Non-privileged.

Syntax

SCRIPT "*script-name*"

Where	Means
script-name	**The name and directory location of the script file to be executed. (The file and directory location must be specified as a UNIX-style filename. For example, /usr/login). You must enclose the *script-name* in quotation marks ("). The maximum length of the script file name, and directory location is 64 characters. If you do not specify a script file name, the server will try to execute the script file that is normally executed when the user logs on to the port.**

Example

```
Xyplex> SCRIPT "/usr/login"
```

SET - General Information

Alter operational characteristics

You will use the terminal server SET commands to specify or change characteristics for ports or terminals, servers, services, sessions, domain names, and user privilege levels, in the operational database (i.e., when you use the SET command, the permanent characteristics of the terminal server are not altered, and any PORT parameters that have been defined via the SET command are not retained after the port is logged out, SERVER parameters are not retained when the terminal server is re-initialized, etc). In order for a characteristic to be set permanently, you must use a DEFINE command.

SET DOMAIN

Refer to the description of the DEFINE/SET DOMAIN commands.

SET PORT

Refer to the description of the DEFINE/SET PORT commands.

SET SERVER

Refer to the description of the DEFINE/SET SERVER commands.

SET SERVICE

Refer to the description of the DEFINE/SET SERVICE commands.

SET NOPRIVILEGED

Refer to the description of the SET PRIVILEGED/NOPRIVILEGED commands.

SET PARAMETER SERVER

Refer to the description of the DEFINE/SET PARAMETER SERVER commands.

SET PRIVILEGED/NOPRIVILEGED

User Privilege Commands

Notes

Use the SET PRIVILEGED or SET NOPRIVILEGED commands to specify the privilege status of the port at which the command is issued. More than one port on a terminal server can be privileged. Refer to section 1.4 in this manual for a discussion of TCP/IP-LAT software privilege levels.

When you issue the SET PRIVILEGED command, you are required to supply the privileged password. (The privileged password is set via the DEFINE/SET SERVER PRIVILEGED PASSWORD command. The factory default privileged password is SYSTEM. Refer to the the DEFINE/SET SERVER PRIVILEGED PASSWORD description for information about this command.)

The local command mode prompt changes to indicate that the port is a privileged port (unless the command is issued from a console port). For example, the default local command mode prompt for a non-privileged port is Xyplex>. The default local command mode prompt for a privileged port is Xyplex>>.

Privileges

Privileged. Any user who knows the privileged password can use the Set Privileged command.

Syntax

SET [PRIVILEGED]
[NOPRIVILEGED]

Where	Means
NOPRIVILEGED	**Specifies that the port will have non-privileged status. This means that the user can set or change parameters for the current port or session. This is the default privilege level.**
PRIVILEGED	**Specifies that the port will have privileged status. This means that the user at the port can set or change operational and permanent parameters for the server, and any or all ports, sessions, or services.**

Example

1. **When you type the command:**

   ```
   Xyplex> SET PRIVILEGED
   ```

   The port displays the prompt:

   ```
   Password>
   ```

   Type the privileged password (password is not echoed by the terminal). The terminal server will display the privileged local command prompt (the Xyplex>> prompt).

2. `Xyplex>> SET NOPRIVILEGED`

SET SESSION

Specify a session mode

Notes

Use the SET SESSION command to alter the data transparency of the current session. Transparency refers to how the port interprets control characters.

This applies to both LAT and Telnet sessions. For Telnet sessions, when you set the SESSION characteristic to PASSALL or PASTHRU, the terminal server will attempt to negotiate the Telnet binary option.

When the user has finished using the Telnet binary mode and the session successfully negotiates out of binary mode, the terminal server software automatically changes the session type to INTERACTIVE.

Privileges

Secure

Syntax

SET SESSION [INTERACTIVE]
[PASSALL]
[PASTHRU]

Where	Means
INTERACTIVE	**Enable all switch characters, Telnet command characters, server messages, and XON/XOFF flow control (if the SET PORT FLOW CONTROL characteristic is set to XON). Typically, this is the normal mode when a terminal is connected to the port.**
PASSall	**Disable all switch characters, Telnet command characters, server messages, and XON/XOFF flow control. In PASSALL mode, all characters are passed to the connection partner as data. This allows data files that contain control character to be transferred without interference from the terminal server. Typically, you would use this mode for binary file transfers (e.g., transferring a program via modem). PASSALL session**
PASThru	**Disable all switch characters, Telnet command characters, server messages, but leave XON/XOFF flow control enabled. Typically, you would use this mode for ASCII file transfers (e.g., printing on a line printer connected to a port).**

Examples

1. `Xyplex> SET SESSION INTERACTIVE`
2. `Xyplex> SET SESSION PASSALL`
3. `Xyplex> SET SESSION PASTHRU`

SHOW/LIST/MONITOR - General Information

Display permanent or operational port characteristics

Use LIST, MONITOR, and SHOW commands to display information about the terminal server and resources (such as nodes, parameter servers, ports, services, sessions, queues, and users) about which the terminal server maintains information. Table 2-6 describes each of these commands:

Table 2-6. Summary of Display Commands.

Command	Function
LIST	Displays information about values contained in the permanent database.
MONITOR	Displays continuously updated information about values contained in the operational database or the current running status.
SHOW	Displays information about values contained in the operational database, or displays a "snapshot" of the current running status.

The SHOW and LIST commands produce "static" displays of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen. To exit from a MONITOR display:

- **press any keyboard key to terminate the display at the end of the current screenful of information.**
- **press the <BREAK> key to terminate the display immediately.**

For many displays, the first few lines of the display (the "header" lines) contain some fields that are common. For example, the first line of the SHOW PARAMETER SERVER display , shown below, contains the common fields. The common fields are described in the table following the figure. These fields will not be repeated, in order to avoid repetition.

```
Xyplex>> SHOW PARAMETER SERVER

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  X2771                Number:      0

Check Timer:                30            Parameter Server Limit:      4
Retransmit Timer:            5            Parameter Servers:           1
Retransmit Limit:            3            Rejected Servers:            0
Path:                /tftpboot            Bad Parameter Messages       0

Last Update Version:        23            Storage State:            Idle
Last Update Date:  18 Nov 1988            Loaded From:     119.12.119.20
Last Update Time:     12:08:31                                 UNIXHOST

Name           Address            Version Date              Status   Reason
UNIXHOST       119.12.119.20           23 18 Nov 1988 12:08 Current
```

Item (Field)	Description
MaxServer V*x.y*	**Shows the Xyplex product type and the version of the terminal server software, where *x.y* indicates the major and minor software release level.**
Rom *xxxxxx*	**Shows the version, *xxxxxx*, of terminal server ROM software.**
HW *xx.yy.zz*	**Shows the version of the terminal server hardware, where *xx* indicates the version of the terminal server cards, *yy* indicates the type of the MAXserver chassis, and *zz* indicates the version of the MAXserver chassis.**
Lat Protocol V*x.y*	**Shows the version of the LAT protocol running on the terminal server, where *x.y* indicates the major and minor protocol release level.**
Uptime	**Shows the amount of time that the terminal server has been running since it was last initialized. The time is expressed in the form:** **days hours:minutes:seconds.**
Address	**Shows the unique Ethernet address of the terminal server.**
Name	**Shows the name of the terminal server.**
Number	**Shows the number of the terminal server.**

SHOW/MONITOR DESTINATIONS

Display all accessible domain-names and service-names on the network

Notes

Use the SHOW DESTINATIONS or MONITOR DESTINATIONS command to display a list of all accessible *domain-names* and *service-names* on the network. The list will be displayed in alphanumeric order. The SHOW DESTINATIONS command produces a static display. The MONITOR DESTINATIONS command produces a display that is continuously updated.

Privileges

Secure and non-privileged users can use the SHOW DESTINATIONS command. Only users at privileged ports can use the MONITOR DESTINATIONS command.

Syntax

SHOW
MONITOR DESTINATIONS *name*

Where	Means
name	**The *domain-names* and/or *service-names* on the network you wish to view. This allows you to view one or a limited number of destinations, rather than the complete list.**

You can specify a wildcard character to select a subset of the destinations to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW DESTINATIONS AB*, the server will display all accessible *domain-names* and/or *service-names* whose names start with AB. SHOW DESTINATIONS A*BC displays accessible *domain-names* and/or *service-names* whose names start with A and end with BC.

Example

```
Xyplex>> SHOW DESTINATIONS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

DEVVAX                                The Development/Library VAX
FINANCESUN.COM                        192.112.119.200
FINANCEVAX                            Corporate MicroVAX II
MAX_5000                              XYPLEX MAXserver 5000
UNIXHOST.COM                          192.112.119.100
```

Example SHOW/MONITOR DESTINATIONS Display.

After the header line, the first column of the SHOW/MONITOR DESTINATIONS display lists accessible domain-names and service-names. The second column lists either the internet-address to which the domain-name is mapped, or the identification string for the service-name, which is informational text about the LAT service.

SHOW/MONITOR/LIST DOMAIN

Display information about one or all available domain-names

Notes

Use the SHOW DOMAIN or MONITOR DOMAIN command to display information about one or all available domain-names on the network. The SHOW DOMAIN command produces a static display. The MONITOR DOMAIN command produces a display that is continuously updated.

Use the LIST DOMAIN command to display information about domain-names that are defined in the permanent database of the terminal server.

Privileges

Secure and non-privileged users can use the SHOW DOMAIN and LIST DOMAIN commands. Only users at privileged ports can use the MONITOR DOMAIN command.

Syntax

LIST DOMAIN [*domain-name*] [ALL]

SHOW
MONITOR DOMAIN [*domain-name*] [ALL]
[LEARNED]
[LOCAL]

Where	Means
domain-name	**Specifies that the terminal server will display the requested information for the Domain specified by the *domain-name*. If you do not specify a *domain-name*, the display will show all available *domain-names* from the relevant database. If you do not specify a fully-qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix(es)*.** **You can specify a wildcard character to select a subset of the *domain-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW DOMAIN AB*, the server will display all available *domain-names* which start with AB. SHOW DOMAIN A*BC displays available *domain-names* which start with A and end with BC.**
ALL	**Specifies that the terminal server will display information for *domain-names* that it obtained from the primary or secondary Domain name server, as well as those that were specified locally (i.e., using a SET/DEFINE DOMAIN command). This is the default for the LIST/MONITOR/SHOW DOMAIN commands.**
LEARNED	**Specifies that the terminal server will display information about the domain-name(s) that it obtained from the primary or secondary Domain name server.**
LOCAL	**Specifies that the terminal server will display information about domain-names that were specified locally (i.e., using a SET/DEFINE DOMAIN command).**

Example

```
Xyplex> SHOW DOMAIN

Entry Internet                      Domain     19 Jan 1989 08:23:58
      Address         TTL Source    Name

1     192.112.119.100 100 Primary   UNIXHOST.COM
2     192.112.119.200  24 Secondary FINANCESUN.COM
3     192.112.119.240     Local     MAX5000.COM
4     192.112.119.242     Local     MAX5000.COM
```

Example LIST/MONITOR/SHOW DOMAIN Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW DOMAIN display.

Item (Field)	Description
Entry	**Shows the entry number assigned by the software for the *domain-name*.**
Internet Address	**Shows the Internet address of the node.**
TTL	**Shows the amount of time, in minutes (in hours for MX-TSERV-J8 and MX-TSRVL-J16 units), that the terminal server will retain information about the *domain-name(s)* that it obtained from the primary or secondary Domain name server. This is called "time to live." Locally defined *domain-names* have no time to live.**
Source	**Shows the source of the *domain-name* information. The possible values that will be displayed are:** **Local — indicates that the *domain-name* was specified locally (i.e., using a SET/DEFINE DOMAIN command).** **Primary — indicates that the terminal server obtained information about the domain-name from the primary Domain name server.** **Secondary — indicates that the terminal server obtained information about the domain-name from the secondary Domain name server.**
Domain Name	**Shows the *domain-name*.**

SHOW/MONITOR NODES

Display information about one or all available Ethernet nodes on the network

Notes

Use the SHOW NODES or MONITOR NODES command to display information about one or all available Ethernet nodes on the network. The SHOW NODES command produces a static display. The MONITOR NODES produces a display that is continuously updated. Note that the SHOW/MONITOR NODES commands do not display information about Telnet nodes.

Privileges

Secure and non-privileged users can use the SHOW NODES command, however, these users are restricted to viewing information about nodes which are in their authorized groups. Users at privileged ports can view information about any available nodes, regardless of the authorized groups for the port, but only the nodes that are offering services in group-codes that are DEFINED/SET for the server (e.g., if a service node on the network is offering a service in group-code 12, but the server's authorized groups do not include group-code 12, then even a privileged user will not see those services). Only users at privileged ports can use the MONITOR NODES command.

Syntax

SHOW		
MONITOR NODES	**[*node-name*]**	**[COUNTERS]**
		[STATUS]
		[SUMMARY]
	[ALL]	**[COUNTERS]**
		[STATUS]
		[SUMMARY]

Where	Means
node-name	**Specifies that the terminal server will display the requested information for the service node specified by the node-name.**
ALL	**Specifies that the terminal server will display the requested information for the all service nodes that match the authorized group list for the current port.**
COUNTERS	**Specifies that the terminal server will display statistics about current node activity for the specified node or all nodes.**
STATUS	**Specifies that the terminal server will display detailed status information about the availability of the specified node or all nodes, as well as information about the node Ethernet address, group codes, services offered, etc.**
SUMMARY	**Specifies that the terminal server will display a one-line summary for the specified node or all nodes that match the authorized groups for the current port. This is the default display type.**

Examples

```
Xyplex>> SHOW NODES FINANCEVAX COUNTERS

Node FINANCEVAX:                                21 Nov 1988  15:59:40

Seconds Since Zeroed:     156442    Multiple Node Addresses:         0
Messages Received:             0    Duplicates Received:             0
Messages Transmitted:          0    Messages Re-transmitted:         0
Slots Received:                0    Illegal Messages Received:       0
Slots Transmitted:             0    Illegal Slots Received:          0
Bytes Received:                0    Solicitations Accepted:          0
Bytes Transmitted:             0    Solicitations Rejected:          0
```

Example MONITOR/SHOW NODES COUNTERS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW NODES COUNTERS display. The values listed below indicate cumulative values counted since the last time the display counters were reset to zero. There are two ways to reset these counters: use a ZERO COUNTERS command, or re-initialize the terminal server.

Item (Field)	Description
Node node-name	**Shows the name of the node.**
Seconds Since Zeroed	**Shows the number of seconds since the counters were reset to zero.**
Messages Received	**Shows the number of LAT virtual circuit messages that the terminal server received from the node, since the counters were reset to zero.**
Messages Transmitted	**Shows the number of LAT virtual circuit messages that the terminal server transmitted to the node, since the counters were reset to zero.**
Slots Received	**Shows the number of slots that the server received from the node (where a slot represents a message segment for a particular session), since the counters were reset to zero.**
Slots Transmitted	**Shows the number of slots that the server transmitted to the node, since the counters were reset to zero.**
Bytes Received	**Shows the total number of bytes contained in datagrams that have been successfully received by the terminal server, excluding Ethernet header and CRC data, since the counters were reset to zero.**
Bytes Transmitted	**Shows the total number of bytes contained in datagrams that have been successfully transmitted by the terminal server, excluding Ethernet header and CRC data, since the counters were reset to zero.**
Multiple Node Addresses	**Shows the number of times that a node multicast an announcement on the network, with a physical address that was different from the physical address given in a previous announcement, since the counters were reset to zero.**

Duplicates Received	**Shows the number of duplicate messages that the server received from the node, since the counters were reset to zero.**
Messages Re-transmitted	**Shows the number of messages the server retransmitted to the node, since the counters were reset to zero.**
Illegal Messages Received	**Shows the number of illegally formatted messages that the server received from the node, since the counters were reset to zero.**
Illegal Slots Received	**Shows the number of illegally formatted slots that the server received from the node, since the counters were reset to zero.**
Solicitations Accepted	**Shows the number of connection requests that the server has accepted from the node, since the counters were reset to zero. This number includes both queued requests and requests that were immediately satisfied.**
Solicitations Rejected	**Shows the number of connection requests from the node that the server has rejected, since the counters were reset to zero.**

```
Xyplex>> SHOW NODES FINANCEVAX STATUS

Node: FINANCEVAX                        Address:  AA-00-04-00-D0-04
LAT Protocol:     V5.1                  Data Link Frame Size: 1500

Identification: Corporate MicroVAX II

Node Groups:   0

Service Name        Status   Rating  Identification

FINANCEVAX          Available    23  Corporate MicroVAX II
```

Example MONITOR/SHOW NODES STATUS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW NODES STATUS display:

Item (Field)	Description
Node *node-name*	**Shows the name of the service node.**
LAT Protocol V*x*.*y*	**Shows the version number (*x*) and the update level (*y*) of the LAT protocol of the service node software.**
Address	**Shows the Ethernet address of the service node.**
Data Link Frame Size	**Shows the maximum Ethernet data link frame size used by the service node to receive messages.**
Identification	**Shows the identification text string for the node.**
Node Groups	**Shows the group codes enabled for the service node.**
Service Name	**Each entry in this column shows the name of a service offered on the service node.**
Status	**Each entry in this column shows the status of the service (listed in the Service Name column) offered by the service node. Valid values for this column are:**
	Available — **Shows that the service is currently available to server users.**
	n Connected — **Shows that the service is available, and that n currently active sessions with this service were requested.**
	Unavailable — **Shows that all service nodes offering the service are currently unreachable.**
	Unknown — **Shows that the service was available but now may be unavailable. This could be because the server has not recently received a multicast announcement from the service node.**

Rating	**Shows the value assigned to the service by the node, which indicates the relative capacity of the service to accept new connections. A higher number implies that the node is more able to accept connections. The range of values that is displayed is 0 through 255.**
Identification	**Shows a text string which identifies the service.**

```
Xyplex>> SHOW NODES ALL SUMMARY

Node Name           Status       Identification

MAX_5000            Reachable    XYPLEX MAXserver 5000.
FINANCEVAX          Reachable    Corporate MicroVAX II
DEVVAX              Reachable    The Development/Library VAX
SUPPORTVAX          Reachable    The Support/SQA VAX
UNIXVAX             Reachable    ULTRIX-32
```

MONITOR/SHOW NODES SUMMARY Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW NODES SUMMARY display:

Item (Field)	Description
Node node-name	**Shows the name of the service node.**
Status	**Each entry in this column shows the status of the node listed in the Node Name column. Valid values for this column are:**
	***n* Connected** — **Shows that the node is reachable, and that *n* sessions are currently active with services offered by the service node.**
	Reachable — **Shows that the node is currently accessible to server users, although there are currently no active sessions.**
	Requesting — **Shows that a node, that does not currently offer services, has made remote connection requests to the server for access to local services offered at the server.**
	Unknown — **Shows that the node was available but now may be unavailable. This could be because the server has not recently received a multicast announcement about the services which are offered at the node.**
	Unavailable — **Shows that an active session has timed out, or that the service node is currently unreachable.**
Identification	**Shows a text string which identifies the node.**

SHOW/LIST/MONITOR PARAMETER SERVER

Display information about current parameter servers

Notes

Use the SHOW and MONITOR PARAMETER SERVER commands to display information about current parameter servers (nodes which store parameter information) for the terminal server. Use the LIST PARAMETER SERVER command to display information about parameter servers assigned in the permanent database. The SHOW and LIST PARAMETER SERVER commands produce a static display. The MONITOR PARAMETER SERVER command produces a display that is continuously updated.

Privileges

Non-privileged users can use the SHOW or LIST PARAMETER SERVER command. Only users at privileged ports can use the MONITOR PARAMETER SERVER command.

Syntax

SHOW **PARAMETER SERVER**
MONITOR
LIST

Example

```
Xyplex>> SHOW PARAMETER SERVER

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  X2771                Number:      0

Check Timer:                30             Parameter Server Limit:      4
Retransmit Timer:            5             Parameter Servers:           1
Retransmit Limit:            3             Rejected Servers:            0
Path                                       Bad Paramteter Messages      0

Last Update Version:        23             Storage State:            Idle
Last Update Date:  18 Nov 1988             Loaded From: AA-00-04-00-D2-04
Last Update Time:     12:08:31                                  FINANCEVAX

Name           Address            Version Date              Status   Reason
FINANCEVAX     AA-00-04-00-D2-04       23 18 Nov 1988 12:08 Current
```

Example MONITOR/SHOW PARAMETER SERVER Display (when Server is Loaded via MOP or Xyplex Load Server).

```
Xyplex>> SHOW PARAMETER SERVER

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  X2771                Number:      0

Check Timer:                30            Parameter Server Limit:      4
Retransmit Timer:            5            Parameter Servers:           1
Retransmit Limit:            3            Rejected Servers:            0
Path                 /tftpboot            Bad Paramteter Messages      0

Last Update Version:        23            Storage State:            Idle
Last Update Date:  18 Nov 1988            Loaded From:     119.12.119.20
Last Update Time:     12:08:31                                   UNIXHOST

Name           Address            Version Date              Status   Reason
UNIXHOST       119.12.119.20           23 18 Nov 1988 12:08 Current
```

Example MONITOR/SHOW PARAMETER SERVER Display (when Server is Loaded via BOOTP/TFTP Load Server).

The following table describes each of the items (fields) of data in the MONITOR/SHOW PARAMETER SERVER display (except the header lines, which is described in the SHOW/LIST/MONITOR - General Information):

Item (Field)	Description
Check Timer	**Shows the frequency (in minutes) at which the terminal server attempts to locate additional eligible parameter servers.**
Retransmit Timer	**Shows the frequency (in minutes) at which the terminal server attempts to update parameter information at a parameter server that does not acknowledge the attempt.**
Retransmit Limit	**Shows the number of times the terminal server attempts to update parameter information at a parameter server that does not acknowledge the attempt, after the Retransmit Timer period expires.**
Path	**Shows the complete directory pathname to be used when writing parameter files via TFTP.**
Parameter Server Limit	**Shows the maximum number of parameter servers about which the terminal server will retain information.**
Parameter Servers	**Shows the current number of parameter servers about which the terminal server has information.**
Rejected Servers	**Shows the number of parameter servers which have not acknowledged an attempt to update parameter information by the terminal server.**
Bad Parameter Messages	**Shows the number of corrupt parameter messages received by the server.**

Last Update Version	**Shows the version number of the parameter file that is stored in the memory of the terminal server, since it was last initialized. The terminal server creates a new version of the parameter file when parameters are changed using the DEFINE or PURGE commands.**
Storage State	**Shows whether or not the terminal server is attempting to update parameter information at any parameter servers. Idle indicates that the terminal server is not currently attempting an update (this is a normal storage state). All other storage states indicate that an update is being attempted or is in progress.**
Loaded From:	**Shows the Ethernet address or *internet-address* of the unit from which the server obtained its parameters. The Nodename or *domain-name* of this unit is shown below the Ethernet address or *internet-address*.**
Last Update Date	**Shows the date when the terminal server last successfully updated parameter information that is stored at parameter servers.**
Last Update Time	**Shows the time of day when the terminal server last successfully updated parameter information that is stored at parameter servers.**
Name	**Shows the name of a current parameter server.**
Address	**Shows the unique Ethernet address or *internet-address* of a current parameter server.**
Version	**Shows the version number of the parameter file that is currently stored at the parameter server. When this number matches the version indicated by the Last Update Version number, the parameter server and the terminal server have the same version of the parameter file.**
Date	**Shows the date and time when the parameter server was last updated or when an the server made an attempt to update the parameter server.**

Status — Shows the status of attempts by the terminal server to update parameter information at this parameter server. The possible status values are:

- **Ahead** — The parameter server is storing a newer version of the parameter file than the version that is in terminal server memory.
- **Behind** — The parameter server is storing an older version of the parameter file than the version that is in terminal server memory.
- **Current** — The parameter server is storing the same version of the parameter file as the one in terminal server memory.
- **Failed** — The terminal server has failed in attempting to update the parameter information stored at this parameter server (i.e., the parameter server retransmit limit has been reached). The server will attempt to update this parameter server the next time a user issues any DEFINE or PURGE command, or the CHECK PARAMETER SERVER command.
- **Failing** — The terminal server has not yet successfully updated the parameter information stored at this parameter server (i.e., the parameter server retransmit limit has not been reached but the attempt has not yet been successful).

Reason — Shows the reason why the Status column shows an update attempt as Failed or Failing. The possible values that can be shown here are:

- **Invalid** — the server has received an invalid (incorrect or corrupted) parameter file from the parameter server.
- **Open** — the software cannot open the parameter file.
- **Protocol** — a protocol error occurred during the update.
- **Reads** — an error occurred while reading the parameter file.
- **Resource** — the parameter server has a resource problem (e.g., insufficient disk space, memory, etc).
- **Response** — the parameter server has not responded.
- **Writes** — an error occurred while writing to the parameter file.

SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS

Display additional port characteristics

Notes

Use the SHOW/LIST/MONITOR PORTS ALTERNATE CHARACTERISTICS display to view the current values or settings for certain port characteristics that are not displayed on the SHOW/LIST/MONITOR PORTS CHARACTERISTICS display. These include the PORT PAUSE, RESOLVE SERVICE, IDLE TIMEOUT, DTRWAIT, and TYPEAHEAD SIZE, SLIP, and LINE EDITING characteristics, that have been specified for the port.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW|LIST|MONITOR PORTS	**[*port-list*]**	**[ALTERNATE CHARACTERISTICS]**
	[ALL]	
	[ACCESS]	**[DYNAMIC]**
		[LOCAL]
		[REMOTE]
		[NONE]

Where	Means
port-list	**Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**
ALL	**Specifies that the requested information will be displayed about all ports.**
ACCESS	**Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**
DYNAMIC	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
LOCAL	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
REMOTE	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
NONE	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex>> SHOW PORTS ALTERNATE CHARACTERISTICS

Port 1:  J. Smith                              21 May 1990  15:57:32

Resolve Service:               Any     DTR wait:                 Disabled
Idle Timeout:                    0     Typeahead Size:                80
SLIP Address:        192.12.119.74     SLIP Mask:           255.255.255.0
Remote SLIP Addr:    192.13.200.23     Default Session Mode    Interactive
TCP Window Size:               256     Prompt:                      Xyplex
DCD Timeout:                  2000     Dialback Timeout:              10
Stop Bits:                       2     Script Login:             Disabled
XDM Query:                 Specific
XDM Host:            140.179.244.1
TCP Keepalive Timer:             0
```

Example LIST/MONITOR/SHOW PORT ALTERNATE CHARACTERISTICS Display, When Line Editing is Disabled

```
Xyplex>> SHOW PORTS ALTERNATE CHARACTERISTICS

Port 1:  J. Smith                              21 May 1990  15:57:32

Resolve Service:               Any     DTR wait:                 Disabled
Idle Timeout:                    0     Typeahead Size:                80
SLIP Address:        192.12.119.74     SLIP Mask:           255.255.255.0
Remote SLIP Addr:    192.13.200.23     Default Session Mode    Interactive
TCP Window Size:               256     Prompt:                      Xyplex
DCD Timeout:                  2000     Dialback Timeout:              10
Stop Bits:                       2     Script Login:             Disabled
XDM Query:                 Specific
XDM Host:            140.179.244.1
TCP Keepalive Timer:             0

                          Line Editor Characters

Backspace Character:            ^D     Forwards Character:            ^F
Delete Begin Character:         ^U     Delete Line Character:         ^X
End of Line Character:          ^E     Begin Line Character:          ^H
Previous Line Character:        ^B     Next Line Character:           ^N
Quoting Character:              ^V     Insert Character:              ^A
Cancel Character:               ^Z     Redisplay Character:           ^R
```

Example LIST/MONITOR/SHOW PORT ALTERNATE CHARACTERISTICS Display, When Line Editing is Enabled

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT ALTERNATE CHARACTERISTICS display:

Item (Field)	Description
Port *n*	**Shows the number of the terminal server port about which the system is displaying information. The variable *n* represents the number of a physical terminal server port.**

user-name **The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME characteristic.**

Resolve Service **Shows how the terminal server should interpret ambiguous variables in CONNECT commands, DEFINE/SET PORT PREFERRED SERVICE, or DEFINE/SET PORT DEDICATED SERVICE commands. The possible values that will be displayed are:**

Any	**Shows that the terminal server should interpret the variable first as being a LAT service-name, then try to interpret it as a Telnet domain-name or internet-address.**
Lat	**Shows that the terminal server should interpret the variable as being a LAT service-name.**
Telnet	**Shows that the terminal server should interpret the variable as a Telnet domain-name or internet-address.**

Idle Timeout **Shows the amount of time, in minutes, after which an inactive session will be disconnected. Possible values that will be displayed are whole numbers in the range of 0 to 255 (where 0 means that the session will not be disconnected for being inactive). Typically, this characteristic is used to prevent "hanging printer" problems.**

SLIP Address **Shows the *internet-address* assigned to the server port.**

Remote SLIP Addr **Shows the *internet-address* of the remote device.**

TCP Window Size **Shows the size of the TCP window to be used when a TCP/IP session is started.**

DCD Timeout **Shows the period of time, in milliseconds, that the DCD signal can be deasserted, before the software will disconnect the port.**

Stop Bits **Shows the number which maps to the number of stop bits to be used to maintain synchronization of data. The following table indicates how many stop bits will be used for number shown in the display:**

bit-value setting	**Stop Bits Used**
1	**1 stop bit**
2	**2 stop bits**
3	**1.5 stop bits**
4	**Server calculates the number of stop bits to used based on the port speed. This is the default and will be shown in a LIST display. A SHOW or MONITOR display will indicated the actual value in use.**

XDM Query — Shows the method by which the server locates an XDM manager.

- **SPECIFIC** — Search for the host at the location in the *domain-name* or *internet-address* variable, which is the XDM manager.
- **BROADCAST** — Search the network for an XDM manager using the Internet broadcast address.
- **INDIRECT** — Search for the host at the location in the *domain-name* or *internet-address* variable. This host provides a list of XDM managers on the network.

XDM Host — Shows the name of the XDM manager currently in use.

TCP Keepalive Timer — Shows the number of minutes that the terminal server will wait for a response from the Telnet partner before terminating the session. Valid values are the whole numbers 0 through 30. The default is 0, which specifies no keepalive timer.

DTR wait — Shows the conditions under which the port asserts the DTR modem control signal. The possible values that will be displayed are:

- **Disabled** — Shows that the port continuously asserts DTR.
- **Enabled** — Shows that the port asserts DTR when a connection is formed or when the device connected to the port asserts RNG.
- **FORCONNECTION** — Shows that the port will assert DTR when a connection is formed.
- **FORRING** — Shows that the port will assert DTR when the device connected to the port asserts RNG.

Typeahead size — Shows the size of the port type-ahead buffer (the number of bytes or characters that can be temporarily stored pending transmission).

SLIP Mask — Shows the *internet-subnet-mask* which is used by the server when determining whether to forward a packet over a slip link.

Default Session Mode — Shows the mode to which all sessions are initially set. The possible values that will be displayed are:

- **INTERACTIVE** — Shows that the server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are enabled. The server will not attempt to negotiate the TELNET binary option. This is the default.
- **PASTHRU** — Shows that the server will initially set all sessions so that all switching characters and Telnet command characters are interpreted as data, but XON/XOFF flow control is still used in this mode. The server will attempt to negotiate the TELNET binary option.
- **PASSALL** — Shows that the server will initially set all sessions so that all switching characters, Telnet command characters, and XON/XOFF flow control recognition are disabled. The server will attempt to negotiate the TELNET binary option.
- **TRANSPARENT** — Shows that the server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, Telnet command characters, and XON/XOFF flow control recognition. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU.

Prompt — Shows the local command prompt, which is displayed at the devices connected to the server serial port(s).

Dialback Timeout — Shows the amount of time that the remote modem (the modem being called) has to answer a dialback call.

Script Login — Shows whether or not the port(s) can use or will require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence. "Enabled" means that the port(s) will request that a login script file be downloaded from a script server and then executed, prior to completing the login sequence. The port is logged on, even if the server is unable to locate a script file. "Disabled" (the default) means that the port(s) do not need to have a login script file downloaded from a script server and then executed, in order to complete the login sequence. "Required" means that the port(s) require a login script file to be downloaded from a script server and then executed, in order to complete the login sequence. If the server is unable to locate the correct script file, the port is not logged on.

Line Editor Characters

Backspace Character	**Shows whether or not there is a line editing character that will move the cursor one position to the left. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Delete Begin Character	**Shows whether or not there is a line editing character that will delete everything on the current command line, from the cursor position to the beginning of the line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
End of Line Character	**Shows whether or not there is a line editing character that will place the cursor at the end of the current command line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Previous Line Character	**Shows whether or not there is a line editing character that will recall the previous command in the command history. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Quoting Character	**Shows whether or not there is a line editing character that will quote the next character. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Cancel Character	**Shows whether or not there is a line editing character that will cancel an interactive operation (such as changing a password), or delete the current command line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Forwards Character	**Shows whether or not there is a line editing character that will move the cursor one position to the right. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Delete Line Character	**Shows whether or not there is a line editing character that will delete the current command line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Begin Line Character	**Shows whether or not there is a line editing character that will place the cursor at the beginning of the current command line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Next Line Character	**Shows whether or not there is a line editing character that will recall the next command in the command history. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Insert Character	**Shows whether or not there is a editing character that alternates between the insert character and overstrike character modes of operation. If a character is defined, it is shown. If a character is not defined, the server will display "None."**
Redisplay Character	**Shows whether or not there is a line editing character that will re-display the current command line. If a character is defined, it is shown. If a character is not defined, the server will display "None."**

SHOW/LIST/MONITOR PORTS CHARACTERISTICS

Display basic port characteristics

Notes

Use the SHOW/LIST/MONITOR PORTS CHARACTERISTICS command to view the current values for some basic port characteristics that have been defined by the user or the terminal server manager. Among the characteristics shown on this display are items related the actual manner in which data are transmitted by the port to the device (line speed, parity bit error checking, bits per character, flow and modem control, etc), session switching characters, LAT service groups, preferred services, and enabled characteristics. This display is the "default" display shown when you issue a SHOW/LIST/MONITOR PORT command without specifying a port-list (i.e., for your own port) in the command.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW|LIST|MONITOR PORTS	**[*port-list*]**	**[CHARACTERISTICS]**
	[ALL]	
	[ACCESS]	**[DYNAMIC]**
		[LOCAL]
		[REMOTE]
		[NONE]

Where	Means
port-list	**Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**
ALL	**Specifies that the requested information will be displayed about all ports.**
ACCESS	**Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**
DYNAMIC	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
LOCAL	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
REMOTE	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
NONE	**Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex>> LIST PORTS 1 CHARACTERISTICS

Port 1:  J. Smith                        21 Nov 1988  15:56:37

Character Size:            8          Input Speed:        9600
Flow Control:            XON          Output Speed:       9600
Parity:                 None          Modem Control:   Disabled

Access:                Local          Local Switch          ^L
Backward Switch:         ^P           Name:              PORT_1
Break:                 Local          Session Limit:         4
Forward Switch:          ^N           Type:                Soft

Preferred Service: None

Authorized Groups:  0

(Current)  Groups:  0

Enabled Characteristics:

Autoprompt, Broadcast, Input Flow Control, Loss Notification,
Message Codes, Output Flow Control, Verification
```

Example LIST/MONITOR/SHOW PORT CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT CHARACTERISTICS display:

Item (Field)	Description
Port *n*	**Shows the number of the terminal server port, about which the system is displaying information. The variable n represents the number of a physical terminal server port.**
user-name	**The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME characteristic.**
Character Size	**Shows the number of bits per character for data characters that are transmitted or received over the serial connection between the terminal server port and the device connected to the port. The Character Size is 7 or 8 bits.**

Flow Control — **Shows the flow control ("handshaking") method that is used by the serial interface to control data transfer between the terminal server port and the device connected to the port. The possible values which will be shown are:**

- **CTS** — **indicates that the port emulates RTS/CTS flow control by using the DCD and DTR modem control signals to control data transfer between the terminal server port and the device connected to the port.**
- **Disabled** — **indicates that the port does not use any flow control method to control data transfer between the terminal server port and the device connected to the port.**
- **DSR** — **indicates that the port emulates DTR/DSR flow control by using the DCD and DTR modem control signals to control data transfer between the terminal server port and the device connected to the port.**
- **XON** — **indicates that the port uses XON/XOFF flow control to control data transfer between the terminal server port and the device connected to the port.**

Parity — **Shows the method by which the server and the device connected to the port check for single-bit errors in characters transmitted or received by the port. (This is called a parity check because the device provides an extra bit, called a parity bit, for error checking.) The possible values which will be shown are:**

- **EVEN** — **indicates that the port and the device insure that each byte (character) that is transmitted or received contains an even number of 1's, including the parity bit.**
- **NONE** — **indicates that the port and the device do not include a parity bit, and therefore do not check for single bit errors.**
- **ODD** — **indicates that the port and the device insure that each byte that is transmitted or received contains an odd number of 1's, including the parity bit.**

Input Speed — **Shows the rate, in bits per second, at which the device connected to the port transmits data and the server port processes the data. The possible values which will be shown are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 56000, 57600, 64000, 76800, and 115200.**

Output Speed — **Shows the rate, in bits per second, at which the server port transmits data and the device connected to the port processes the data. The possible values which will be shown are: 50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 56000, 57600, 64000, 76800, and 115200.**

Modem Control — Shows whether or not the device connected to the port manipulates modem control signals (e.g., uses DSRLOGOUT or DTRWAIT mode of operation) during data communications. The possible values which can be shown are:

- **Disabled** — indicates that the device connected to the port does not use modem control signals during data communications. (Refer to the description of the SET PORT MODEM CONTROL characteristic for more information.)
- **Enabled** — indicates that the device connected to the port uses modem control signals during data communications. (Refer to the description of the SET PORT MODEM CONTROL characteristic for more information.)

Access — Shows the type of connections which the terminal server allows to the port (e.g., the type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port). The possible values that will be displayed are:

- **Dynamic** — indicates that the port is accessible from either the local command mode, or remotely by service name or node-name and port number.
- **Local** — indicates that the port is accessible only from the local command mode.
- **Remote** — indicates that the port is accessible only remotely by service name or node-name and port number.
- **None** — indicates that the port is not accessible at all (e.g., the server prevents any use of the port).

Backward Switch — Shows the character that causes the terminal server to exit from the current session and connect to the next lower-numbered session, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

Break — Shows which action the port will take when the user presses the <BREAK> key. The possible values which will be shown are:

- **Disabled** — indicates that the terminal server does nothing when the user presses the <BREAK> key.
- **Local** — indicates that the terminal server will return to the local command mode when the user presses the <BREAK> key.
- **Remote** — indicates that the terminal server sends the break to the connection partner when the user presses the <BREAK> key.

Forward Switch — Shows the character that causes the terminal server to exit from the current session and connect to the next higher-numbered session, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

Local Switch — Shows the character that causes the terminal server to exit from the current session and return to the local command mode, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

Name — Shows the server mananger-defined or default name of the port.

Session Limit — Shows the maximum number of sessions that can simultaneously be connected to the port.

Type — Shows the manner in which the attached device produces output, and how the server performs certain device specific functions, when the port is in local command mode. The possible values that will be shown are:

- **ANSI** — indicates that the device produces output on a video display and supports ANSI escape sequences.
- **Hard** — indicates that the attached device produces output on paper. For this type of device, when you delete characters, the deleted characters are echoed between back-slash characters (\).
- **Soft** — indicates that the attached device produces output on a video display, but does not support ANSI escape sequences.

Preferred Service: — Shows the name of the LAT service or Telnet destination to which the port will be connected, whenever the user makes a connect request without specifying a *service-name*.

Dedicated Service: — Shows the name of the LAT service or Telnet destination to which the port will automatically be connected, whenever the port is logged on.

Node: — Shows the name of the LAT service node where the dedicated service or preferred service is offered, when the user wishes to use the service at a specific node from among multiple nodes where the service is offered.

Destination: — Shows the name of the terminal server port where the LAT dedicated service or preferred service is offered, when the user wishes to use the service at a specific port from among multiple ports where the service is offered.

Authorized Groups — Shows the *group-list* which includes the LAT services to which the server manager authorizes the port to have access (i.e., groups in the list represent services to which the port has access, groups not in the list represent services to which the port is denied access).

(Current) Groups — Shows the *group-list* of LAT services to which the user has chosen to have access. The Current Groups list may be identical to or a subset of the Authorized Groups for the port.

Enabled Characteristics

Shows the characteristics which have been enabled for the port using the DEFINE/SET PORT command. Possible values which can be shown are:

Autobaud	**indicates that the port determines the input port speed, parity, and character size for the device connected to the port, and automatically sets matching port characteristics.**
Autoconnect	**indicates that the port automatically connects to either a dedicated service or a preferred service when the user logs on to the port, or that the port will attempt to re-connect a session when a connection failure occurs.**
Autodedicated	**indicates that the unit will automatically log on the port and establish a connection to the dedicated service that is defined for the port when the unit is initialized or the port is logged out.**
Autoprompt	**indicates that the server will automatically prompt the LAT service node to run its login routine whenever a connection is made.**
Broadcast	**indicates that the port can receive messages that are broadcast from other ports on this terminal server.**
Connectresume	**indicates that the CONNECT command will resume an existing session with the specified destination, rather than establishing a new session to that destination.**
Dialback	**indicates that the the port will attempt to dial back to a remote modem The port requires a dialback script in order to be logged in.**
Dial Up	**indicates that the port is considered to be connected to a dial-up line.**
DSRlogout	**indicates that the terminal server will log out the port when the serial interface DCD signal is deasserted.**
DSRWait	**indicates that the terminal server should begin the login sequence when the device asserts the DSR signal.**
Inactivity Logout	**indicates that the server will log out the port after a specified period of inactivity (specified by the SERVER INACTIVITY TIMER characteristic) has elapsed.**
Input Flow Control	**indicates that flow control is used when data are transmitted by the connected device to the port.**
Internet Connections	**indicates that the port will be able to accept an *internet-address*, as well as addresses using the *domain-name* format, in order to connect to a TCP/IP destination.**

Interrupts	**indicates that a local user (e.g., the user at the port) can interrupt a remote session at the port by entering the local switch character, or the <BREAK> character, if the PORT BREAK characteristic is set to LOCAL.**
Kerberos	**indicates that the port provides Kerberos user verification as part of the login process.**
Limited View	**indicates that secure or non-privileged users can not view SHOW/LIST DESTINATIONS, NODES, or SERVICES displays.**
Line Editor	**indicates that the command line editing feature is available at the port.**
Loss Notification	**indicates that the port sends a Bell character to the device connected tothe port, whenever data input by the device are lost due to a receive data error or a data overrun error (e.g., make a terminal beep when the user types a command line that exceeds 132 characters).**
Message Codes	**indicates that the port displays the message code or number associated with a status or error message.**
Menu	**indicates that a user at the port can only perform operations by choosing items from a menu that was defined by the server manager.**
Noloss	**indicates that the port will store data in its typeahead buffer while waiting for a session connection to be made and then pass the data to the connection partner after the session connection is made.**
Output Flow Control	**indicates that flow control is used when data are transmitted by the port to a device connected to the port.**
Password	**indicates that a user must supply a password in order to log on to the port.**
Pause	**indicates the device attached to the port will show terminal server displays 24 lines at a time (by pausing at the end of 24 lines and waiting for the user to press a key before displaying the next 24 lines).**
Privileged Menu	**indicates that the menu is enabled at the port, and the port is privileged.**
Queueing	**indicates that the port can place a received service connection request into a connection queue, when the requested service is busy.**

Remote Modification	**indicates that certain PORT characteristics (of this port) can be changed by a process running at a VMS host.**
Script Echo	**indicates that the port will display the TCP/IP-LAT commands contained in a script file while they are being executed.**
Security	**indicates that the port is set to secure status (i.e., the user is restricted from using some port configuration commands and from viewing information about other ports or sessions, using the SHOW displays).**
Signal Check	**indicates that connections to a service offered at the port are disallowed when the DSR signal is deasserted or that when the DCD signal is deasserted, appropriately configured ports are logged out.**
SLIP	**indicates that Internet SLIP is enabled for the port, and that the port expects all data to be in SLIP packets.**
Verification	**indicates that the port displays informational messages whenever the user connects, disconnects, or switches a session.**

SHOW/MONITOR PORTS COUNTERS

Display statistics about port activity.

Notes

Use the SHOW/MONITOR PORTS display to view statistics about port activity.

Privileges

Secure and non-privileged users can use SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW | MONITOR PORTS [*port-list*] COUNTERS
[ALL]
[ACCESS] [DYNAMIC]
[LOCAL]
[REMOTE]
[NONE]

Where Means

port-list **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL **Specifies that the requested information will be displayed about all ports.**

ACCESS **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

- **DYNAMIC** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
- **LOCAL** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
- **REMOTE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
- **NONE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex>> SHOW PORTS COUNTERS

Port 1:  J. Smith                          21 Nov 1988  15:56:53

Seconds Since Zeroed:      156288      Local Accesses:            4
Framing Errors:                 0      Remote Accesses:           0
Parity Errors:                  0      Idle Timeouts:             0
Overrun Errors:                 0
Input Count:                 1424
Output Count:               13627

                              SLIP Packets
Serial Packets Received:        0  Network Packets Received:      0
Serial Packets Sent:            0  Network Packets Sent:          0
Serial Packets Discarded:       0  Network Packets Discarded:     0
Serial Packet Length Errors:    0
Serial Packet CheckSum Errors:  0
```

Example LIST/MONITOR/SHOW PORT COUNTERS Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT COUNTERS display:

Item (Field)	Description
Port *n*	**Shows the number of the terminal server port, about which the system is displaying information. The variable *n* represents the number of a physical terminal server port.**
user-name	**The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME characteristic.**
Seconds Since Zeroed	**Shows the number of seconds since the counters were reset to zero.**
Framing Errors	**Shows the number of bytes received at the port with illegally formatted frames (e.g., character garbled due to a missing stop bit), since the counter was reset to zero. Frequent framing errors (more than 20 per day for a terminal; 200 per day for a modem, due to line noise) may indicate a problem with the port or the device attached to the port, or mismatched characteristics (such as port speed, parity, character size, etc) between the port and the device connected to the port.**
Parity Errors	**Shows the number of bytes received at the port with parity errors (e.g., a single bit error detected by a parity error check), since the counter was reset to zero. Frequent parity errors (more than 20 per day for a terminal; 200 per day for a modem, due to line noise) may indicate a problem with the port or the device attached to the port, or mismatched characteristics (such as port speed, parity, character size, etc) between the port and the device connected to the port.**

Overrun Errors	**Shows the number of times that characters that were lost because the terminal server input buffers were full, since the counter was reset to zero. Overrun errors indicate that there may be a flow control problem, such as mismatched flow control methods, between the port and the device connected to the port.**
Input Count	**Shows the number of characters (bytes) transmitted to the port by the device connected to the port, since the counter was reset to zero.**
Output Count	**Shows the number of characters (bytes) transmitted by the port to the device connected to the port, since the counter was reset to zero.**
Local Accesses	**Shows the number of times a user has logged on to the port, since the counter was reset to zero.**
Remote Accesses	**Shows the number of times a remote-access connection (e.g., a remote node connected to the port) was established on the port, since the counter was reset to zero.**
Idle Timeouts	**Shows the number of times that the terminal server has disconnected a session, that was initiated by the remote connection queue, for being inactive, since the counter was reset to zero.**
Serial Packets Received	**Shows the number of SLIP packets received from the remote device.**
Serial Packets Sent	**Shows the number of SLIP packets sent by the port to the remote device.**
Serial Packets Discarded	**Shows the number of SLIP packets that have been discarded by the server.**
Serial Packet Length Errors	**Shows the number of SLIP packets received by the port which did not contain the correct number of bytes.**
Serial Packet Checksum Errors	**Shows the number of SLIP packets received by the port which contained incorrectly transmitted data.**
Network Packets Received	**Shows the number of Ethernet packets, received by the server, that have been converted to SLIP packets.**
Network Packets Sent	**Shows the number of Ethernet packets, sent by the server, that have been converted from SLIP packets.**
Network Packets Discarded	**Shows the number of Ethernet packets that have been discarded by the server.**

SHOW/LIST/MONITOR PORTS INTERNET SECURITY

Display Internet Security entries

Notes

Use the SHOW/LIST/MONITOR PORTS INTERNET SECURITYdisplay to view the entries in the Internet Security table. Refer to the *Software Management Guide* for a description of the Internet Security feature.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW | LIST | MONITOR PORTS [*port-list*] INTERNET SECURITY [INBOUND] [ALLOW]
[ALL] [DENY]
[OUTBOUND] [ALLOW]
[DENY]
[*internet-address*]
[ACCESS] [DYNAMIC]
[LOCAL]
[REMOTE]
[NONE]

Where Means

port-list **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL **Specifies that the requested information will be displayed about all ports.**

ACCESS **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

DYNAMIC **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**

LOCAL **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**

REMOTE **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**

NONE **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

INBOUND — **Specifies that you want to view inbound entries. If you do not specify the direction, inbound and outbound entries will both be listed.**

OUTBOUND — **Specifies that you want to view outbound entries. If you do not specify the direction, inbound and outbound entries will both be listed.**

ALLOW — **Specifies that you want to view entries for which inbound or outbound connections are permitted.**

DENY — **Specifies that you want to view entries for which inbound or outbound connections are not permitted.**

internet-address — **A variable -- if you enter an Internet address, the terminal server will inform you whether a connection to the address (outbound) or from the address (inbound) is possible for the specified port.**

Example

```
Xyplex>> SHOW PORT 1 INTERNET SECURITY

Inbound Default:  Allowed      Outbound Default:  Allowed

        Internet          Security
Entry    Address             Mask            Access          Direction

 1  192.12.119.206   255.255.0.0             Allow           Outbound

 2  192.13.119.45    255.255.255.0           Allow           Inbound

 3  192.11.110.40    255.255.255.255         Deny            Outbound
```

SHOW/LIST PORT INTERNET SECURITY DISPLAY.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT INTERNET SECURITY display:

Item (Field)	Description
Inbound Default	**Shows whether inbound connections are allowed or denied by default.**
Outbound Default	**Shows whether outbound connections are allowed or denied by default.**
Entry	**The number of the entry in the port's Internet Security table.**
Internet Address	**The target address of the destination.**
Security Mask	**Describes how to interpret the target address.**
Access	**Either Deny (prevent connection) or Allow (permit connection).**
Direction	**Either Inbound (from the network) or outbound (to the network).**

SHOW/LIST/MONITOR PORTS KEYMAP

Display Tn3270 keymap listings.

Notes

Use the SHOW/LIST/MONITOR PORTS KEYMAP display to view Tn3270 keymap listings.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW|LIST|MONITOR PORTS	**[*port-list*]**	**KEYMAP**
	[ALL]	
	[ACCESS]	**[DYNAMIC]**
		[LOCAL]
		[REMOTE]
		[NONE]

Where Means

port-list **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL **Specifies that the requested information will be displayed about all ports.**

ACCESS **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

- **DYNAMIC** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
- **LOCAL** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
- **REMOTE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
- **NONE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex> SHOW PORT 1 KEYMAP
Address:   08-00-87-00-4F-A4   Name:   X004FA4                Number:    0

Device: VT100       TerminalType: VT100                  Tn3278Type : MODEL2

Keymap:    3270-Key             KeyCode                      Description

           NEWLINE          :   "0A"                         "LF   "
           TAB              :   "09"                         "TAB  "
           BACKTAB          :   "1B 09"                      "ESCTB"
           CURSORUP         :   "1B 5B 41"                   "KEYUP"
           CURSORLEFT       :   "1B 5B 44"                   "KEYBK"
           CURSORRIGHT      :   "1B 5B 43"                   "KEYFW"
           CURSORDOWN       :   "1B 5B 42"                   "KEYDN"
           HOME             :   "1B 68"                      "ESCh "
           DELETE           :   "7F"                         "DEL  "
           ERASEEOF         :   "05"                         "CTRLe"
           ERASEINPUT       :   "1B 69"                      "ESCi "
           INSERT           :   "1B 7F"                      "ESCDL"
           FLUSHINPUT       :   "1B 66"                      "ESCf "
           REFRESH          :   "1B 72"                      "ESCr "
           CENTSIGN         :   "1B 63"                      "ESCc "
           DUPLICATE        :   "04"                         "CTRLd"
           FIELDMARK        :   "06"                         "CTRLf"
           SCROLL           :   "1B 6C"                      "ESCl "
           STATUS ON/OFF    :   "1B 3F"                      "ESC? "
           RESET            :   "12"                         "CTRLr"
           FASTLEFT         :   "16"                         "CTRLv"
           FASTRIGHT        :   "15"                         "CTRLu"
           SHOWKEYS         :   "18"                         "CTRLx"
           PRINT            :   "10"                         "CTRLp"
           PF1              :   "1B 4F 71"                   "NUM 1"
           PF2              :   "1B 4F 72"                   "NUM 2"
           PF3              :   "1B 4F 73"                   "NUM 3"
           PF4              :   "1B 4F 74"                   "NUM 4"
           PF5              :   "1B 4F 75"                   "NUM 5"
           PF6              :   "1B 4F 76"                   "NUM 6"
           PF7              :   "1B 4F 77"                   "NUM 7"
           PF8              :   "1B 4F 78"                   "NUM 8"
           PF9              :   "1B 4F 79"                   "NUM 9"
           PF10             :   "1B 4F 50"                   "PF1  "
           PF11             :   "1B 4F 51"                   "PF2  "
           PF12             :   "1B 4F 52"                   "PF3  "
           PF13             :   "1B 21"                      "ESC! "
           PF14             :   "1B 40"                      "ESC@ "
           PF15             :   "1B 23"                      "ESC# "
           PF16             :   "1B 24"                      "ESC$ "
           PF17             :   "1B 25"                      "ESC% "
```

Example SHOW PORT KEYMAP DISPLAY (part 1 of 2).

```
        PF18            :   "1B 5E"                 "ESC^ "
        PF19            :   "1B 26"                 "ESC& "
        PF20            :   "1B 2A"                 "ESC* "
        PF21            :   "1B 28"                 "ESC( "
        PF22            :   "1B 29"                 "ESC) "
        PF23            :   "1B 5F"                 "ESC_ "
        PF24            :   "1B 2B"                 "ESC+ "
        PA1             :   "1B 2C"                 "ESC, "
        PA2             :   "1B 2E"                 "ESC. "
        PA3             :   "1B 2F"                 "ESC/ "
        SYSREQ          :   "1B 73"                 "ESCs "
        ENTER           :   "0D"                    "ENTER"
        CLEAR           :   "03"                    "CTRLc"
        CURSORSEL       :   "1B 6B"                 "ESCk "
        TEST            :   "1B 74"                 "ESCt "
```

Example SHOW PORT KEYMAP DISPLAY (part 2 of 2).

Item (Field)	Description
Device	**The name of the Tn3270 device in the display.**
TerminalType	**The local terminal type.**
Tn3278Type	**The model of Tn3270 device that the local terminal terminal emulates during a Tn3270 session.**
Keymap	**The table that follows contains the escape sequences that the terminal server uses to translate entries on the local ASCII keyboard into 3270 display station functions.**
3270-Key	**An IBM display station function.**
KeyCode	**The hexidecimal value for the keyboard escape sequence at the local terminal which corresponds to the IBM display station function.**
Description	**A text description of the keyboard function.**

SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS

Display PPP characteristics in use at a port

Notes

The SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS commands display PPP characteristics that will be negotiated by the terminal server on one or more ports.

Privilege Level

SHOW/LIST, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/LIST/MONITOR PORT *port-list* PPP CHARACTERISTICS

Where	Means
port-list	**One or more terminal server ports.**

Example

```
Port 4                          28 Feb 1993

PPP Characteristics

Active:                   Enabled

Charmap:                  000a000
MRU:                         1500
Restart Timer:                  3
Failure Limit:                  3
Configure Limit:                10
```

Example SHOW/LIST/MONITOR PORT PPP CHARACTERISTICS Display

Item (Field)	Description
Port *x*	**The port number whose characteristics are being displayed.**
Active	**Enabled means that the terminal server port can initiate the negotiation of PPP options. Disabled means that the port will wait until the remote device initiates the negotiation of PPP options.**
Charmap	**The character-mask consisting of eight hexidecimal characters, which represents which of the possible ASCII control character options the link will encode prior to transmission or decode upon receipt.**
MRU	**(Maximum Receive Unit). The maximum number of bytes of data and overhead that can be transmitted in a single frame over the PPP link. This number is fixed at 1500.**

Restart Timer	**The amount of time the port waits before sending another option configuration request packet. The value is 1 to 10 seconds .**
Failure Limit	**The maximum number of times the port will object to unacceptable value for a PPP option, before the port rejects further negotiation of the option.**
Configure Limit	**The maximum number of unanswered PPP option configuration request packets that the port will send, before the software concludes that the remote device is unable to respond. When the port has reached this limit, it discontinues further attempts to negotiate PPP options and goes into a passive "listening" state.**

SHOW/MONITOR PORT PPP COUNTERS

Display statistics about PPP activity at a port

Notes

The SHOW/MONITOR PORT PPP COUNTERS commands display statistics about PPP activity at a port.

Privilege Level

SHOW, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/MONITOR PORT *port-list* PPP COUNTERS

Where	Means
port-list	**One or more terminal server ports.**

```
Xyplex>> show port 3 ppp counters


LCP/HDLC Counters                   Received      Transmitted

LCP Config Req:                            2                3
LCP Config Nak:                            0                0
LCP Config Ack:                            2                2
LCP Config Rej:                            0                0
LCP Term Req:                              0                0
LCP Term Ack:                              0                0
LCP Echo Req:                              0                0
LCP Echo Reply:                            0                0
LCP Code Reject:                           0                0
LCP Protocol Reject:                       0                0
HDLC Total Packets:                        8                8
HDLC Framing Errors:                       0                -
HDLC Packet Bad Checksum:                  0                -
HDLC No Packet Errors:                     0                0
HDLC Discards:                             0                -
```

Example SHOW/MONITOR PORT PPP COUNTERS Display.

Item (Field)	Description
LCP Config Req:	**The number of Link Control Protocol (LCP) packets transmitted or received containing proposed option negotiation parameters.**
LCP Config Nak:	**The number of LCP packets transmitted or received containing option negotiation counter-proposals.**
LCP Config Ack:	**The number of LCP packets transmitted or received acknowledging acceptance of proposed option values.**
LCP Config Rej:	**The number of LCP packets transmitted or received rejecting negotiation of the proposed option.**

LCP Term Req:	**The number of LCP packets transmitted or received containing requests to terminate the link.**
LCP Term Ack:	**The number of LCP packets transmitted or received containing acknowledgement that the link will be terminated.**
LCP Echo Req:	**The number of LCP packets transmitted or received which test the ability of the remote device to transmit and receive packets.**
LCP Echo Reply:	**The number of LCP packets transmitted or received in reply to an LCP Echo Request packet.**
LCP Code Reject:	**The number of LCP packets transmitted or received in response to receipt of an unrecognizable LCP packet.**
LCP Protocol Reject:	**The number of LCP packets transmitted or received indicating that the peer attempted to negotiate or use an unsupported protocol.**
HDLC Total Packets:	**The total number of Asynchronous High-Level Data Link Control (HDLC) frames transmitted or received on the link. Asynchronous HDLC is the framing technique used on PPP links.**
HDLC Framing Errors:	**The number of packets received which were framed incorrectly.**
HDLC Packet Bad Checksum:	**The number of packets received which contained an incorrect checksum.**
HDLC No Packet Errors:	**The number of packets trasnmitted or received which were discarded due to insufficient resources.**
HDLC Discards:	**The number of packets received which were discarded for any other reason (than those listed above).**

SHOW/MONITOR PORT PPP INTERNET CHARACTERISTICS

Display PPP Internet characteristics in use at a port

Notes

The SHOW/MONITOR PORT PPP INTERNET CHARACTERISTICS commands display PPP Internet characteristics that will be negotiated by the terminal server on one or more ports.

Privilege Level

SHOW, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/MONITOR PORT *port-list* PPP CHARACTERISTICS

Where	Means
port-list	**One or more terminal server ports.**

```
Xyplex>> sho port 3 ppp internet characteristics

PPP IP Characteristics:

Local IP Address:             0.0.0.0
Remote IP Address:    140.179.248.148
IP Broadcast:               Disabled
VJ Compression:              Enabled
VJ Slots:                          3
```

Example SHOW/MONITOR PORT PPP INTERNET CHARACTERISTICS Display.

Item (Field)	Description
Local IP Address	**The Internet address of the port.**
Remote IP Address	**The Internet address of the remote device, that the port will attempt to negotiate when the remote device does not specify an Internet address on its own.**
IP Broadcast	**Shows whether or not Internet broadcast packets to be transmitted over the PPP link, or whether or not the port will forward broadcast packets received from the remote device to the local area network.**
VJ Compression	**Shows whether or not the port is allowed to negotiate the use of Van Jacobson compression. Enabled means that the port is allowed to negotiate the use of Van Jacobson compression. Disabled means that the port is not allowed to negotiate the use of Van Jacobson compression**
VJ Slots	**Shows the number of sessions (or slots) using Van Jacobson compression operating across the link that the port will attempt to negotiate.**

SHOW/MONITOR PORT PPP INTERNET COUNTERS

Display statistics about PPP Internet activity at a port

Notes

The SHOW/MONITOR PORT PPP COUNTERS commands display statistics about PPP Internet activity at a port.

Privilege Level

SHOW, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/MONITOR PORT *port-list* PPP COUNTERS

Where	Means
port-list	**One or more terminal server ports.**

```
Xyplex>> sho port 3 ppp internet counters


IPCP Counters                 Received         Transmitted

IPCP Config Req:                     2                   1
IPCP Config Nak:                     0                   1
IPCP Config Ack:                     1                   1
IPCP Config Rej:                     0                   0
IPCP Term Req:                       0                   0
IPCP Term Ack:                       0                   0
IP Total Packets:                    0                   0
```

Example SHOW/MONITOR PORT PPP INTERNET COUNTERS Display.

Item (Field)	Description
IPCP Config Req:	**The number of Internet Protocol Control Protocol (IPCP) packets transmitted or received containing proposed option negotiation parameters.**
IPCP Config Nak:	**The number of IPCP packets transmitted or received containing option negotiation counter-proposals.**
IPCP Config Ack:	**The number of IPCP packets transmitted or received acknowledging acceptance of proposed option values.**
IPCP Config Rej:	**The number of IPCP packets transmitted or received rejecting negotiation of the proposed option.**
IPCP Term Req:	**The number of IPCP packets transmitted or received containing requests to terminate the link.**
IPCP Term Ack:	**The number of IPCP packets transmitted or received containing acknowledgement that the link will be terminated.**

IP Total Packets: **The total number of IP datagrams transmitted or received on the link.**

SHOW/MONITOR PORT PPP INTERNET STATUS

Display PPP characteristics in use at a port

Notes

The SHOW/MONITOR PORT PPP INTERNET STATUS commands display shows PPP Internet characteristics that have been negotiated by the terminal server on one or more ports.

Privilege Level

SHOW, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/MONITOR PORT *port-list* PPP CHARACTERISTICS

Where	Means
port-list	**One or more terminal server ports.**

```
Xyplex>> sho port 3 ppp internet status


IPCP State:       OPEN

                       Local               Remote
IP Addresses:      140.179.248.146     140.179.248.148
IP Broadcasts:           Disabled                   -
VJ Compression:           Enabled             Enabled
VJ Slots:                       3                  15
```

Example SHOW/MONITOR PORT PPP INTERNET STATUS Display.

Item (Field)	Description
IP Address	**The Internet address currently used on the link of the port (Local) and of the remote device (Remote).**
IP Broadcast	**Shows whether or not Internet broadcast packets to be transmitted over the PPP link, or whether or not the port will forward broadcast packets received from the remote device to the local area network.**
VJ Compression	**Shows whether or not the port is allowed to negotiate the use of Van Jacobson compression. Enabled means that the port is allowed to negotiate the use of Van Jacobson compression. Disabled means that the port is not allowed to negotiate the use of Van Jacobson compression.**
VJ Slots	**Shows the number of sessions (or slots) using Van Jacobson compression operating across the link.**

SHOW/MONITOR PORT PPP IP commands

The keyword "IP" is synonymous for "INTERNET" for PPP-related displays. See the SHOW/MONITOR PORT PPP INTERNET CHARACTERISTICS, COUNTER, or STATUS command descriptions.

SHOW/MONITOR PORT PPP STATUS

Display PPP characteristics in use at a port

Notes

The SHOW/MONITOR PORT PPP STATUS commands display shows PPP characteristics that have been negotiated by the terminal server on one or more ports.

Privilege Level

SHOW, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/MONITOR PORT *port-list* PPP STATUS

Where	Means
port-list	**One or more terminal server ports.**

```
Xyplex>> sho port ppp status


LCP Status:   NONE

LCP Option                    Local        Remote

Charmap:                       N/A          N/A
Protocol Comp:                 N/A          N/A
Address Comp:                  N/A          N/A
```

Example SHOW/MONITOR PORT PPP STATUS Display.

Item (Field)	Description
Charmap	**Shows the HDLC character encoding currently in use for each direction of the link.**
Protocol Comp	**Shows whether or not protocol field compression is in use for each direction of the link.**
Address Comp	**Shows whether or not address and control field compression is in use for each direction of the link.**

SHOW/LIST PORT SCREENMAP

Display information about the Tn3270 device enabled at a port

Notes

Use the SHOW/LIST SERVER SCREEMAP display to view information about the Tn3270 device enabled at the port. Refer to the *Software Management Guide* for a description of the Tn3270 feature.

Privileges

Non-privileged

Syntax

SHOW|LIST PORT *port-list* SCREENMAP

Where	Means
port-list	**One or more terminal server ports.**

Example

```
Xyplex> SHOW PORT 1 SCREENMAP

Port 1:  Gumby                          19 Jun 1993  07:04:57

 Terminal Function    HexCode

 EraseEOL         :   "1B 5B 4B"
 ClearScr         :   "1B 5B 32 4A"
 MoveCursor       :   "1B 5B F8 3B FA 48"
 Col132           :   "1B 5B 3F 33 68"
 Col80            :   "1B 5B 3F 33 6C"
 Beep             :   "07"
 BoldOn           :   "1B 5B 30 3B 31 6D"
 BoldOff          :   "1B 5B 30 6D"
 Reset1           :   "1B 5B 3F 38 3B 32 68 1B 3D 1B 5B 30 71"
 Reset2           :   "1B 5B 3F 33 3B 37 3B 31 6C 1B 5B 48"
 Reset3           :   "1B 5B 32 4A 1B 5B 34 69"
 MoveCursor Base  :   1
 SGR              :   Enabled
```

Example SHOW/LIST PORT SCREENMAP Display.

The display shows the escape sequences that the terminal server sends to the local terminal to initiate screen functions such as clear the screen, move the cursor, or set the bold attribute.

Terminal Function	**The IBM screen function that occurs on the local terminal when the user enters the escape sequence indicated by the corresponding the Hex Code**
Hex Code	**The hexidecimal value of the escape sequence for the IBM terminal function.**

SHOW/MONITOR PORTS STATUS

Display information about the current session to which the port is connected

Notes

Use the SHOW/MONITOR PORTS STATUS display to view detailed information about the current session to which the port is connected.

Privileges

Secure and non-privileged users can use SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW | MONITOR PORTS	**[*port-list*]**	**STATUS**
	[ALL]	
	[ACCESS]	**[DYNAMIC]**
		[LOCAL]
		[REMOTE]
		[NONE]

Where / Means

port-list — **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL — **Specifies that the requested information will be displayed about all ports.**

ACCESS — **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

- **DYNAMIC** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
- **LOCAL** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
- **REMOTE** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
- **NONE** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

LAT Session:

```
Xyplex>> SHOW PORT 1 STATUS

Port 1:  J. Smith                      Server:               X002771

Access:                 Local          Current Service:      VMSHOST
Status:             Connected          Current Node:
Sessions:                   0          Current Port:

Input XOFFed:              No          Output Signals:          None
Output XOFFed:             No          Input Signals:           None

Last Char Output:          74          Last Char Input:           0d
```

Telnet Session:

```
Xyplex> SHOW PORT 1 STATUS

Port 1:  J. Smith                      Server:               X002771

Access:                 Local          Current Service:       TELNET
Status:             Connected          Current Node:   192.12.119.128
Sessions: 1                            Current Port:              23
Current Domain:                                 FINANCESUN.XYPLEX.COM

Input XOFFed:              No          Output Signals:          None
Output XOFFed:             No          Input Signals:           None

Last Char Output:          74          Last Char Input:           0d

Script Host:       192.12.119.8    unixhost

Script File   /tftpboot/JSmith/login
```

Parallel Printer Port:

```
Xyplex> show port 3 status

Port  3:  (Remote)                     Server:               X0085D4

Access:                  Remote        Current Service:       TELNET
Status:                Connected       Current Node:   192.12.119.128
Sessions:                      1       Current Port:              23
Current Domain:                                 FINANCESUN.XYPLEX.COM


Last Char Output:             6a       Last Char Input:          N/A

Printer Interface:     Centronics
Printer Fault:                 No       Printer Busy:             Yes
Printer Online:               Yes       Printer Paper:            Out
```

Example LIST/MONITOR/SHOW PORT STATUS Displays.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT STATUS display:

Item (Field)	Description
Port *n*	**Shows the number of the terminal server port, about which the system is displaying information. The variable *n* represents the number of a physical terminal server port.**
user-name	**The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME characteristic.**
Server	**Shows the name of the server unit.**
Access	**Shows the type of connections which the server allows to the port (e.g., the type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port). The possible values that will be displayed are:**
	Dynamic — **indicates that the port is accessible from either the local command mode, or remotely by service name or port number.**
	Local — **indicates that the port is accessible only from the local command mode.**
	Remote — **indicates that the port is accessible only remotely by service name or port number.**
	None — **indicates that the port is not accessible at all (e.g., the server prevents any use of the port).**
Status	**Shows the current status of the port. The possible values that can be displayed are:**
	Autobaud — **The port is being autobauded.**
	Available — **A port, whose PORT ACCESS characteristics is set to REMOTE or DYNAMIC, is not busy.**
	Check Modem — **The port is verifying that modem signals are properly asserted.**
	Check Connect — **The port is determining the status (accepted or rejected) of a pending connection.**
	Connected — **The port is currently connected to a LAT service or Telnet destination.**
	Connect Wait — **The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED).**
	Connecting — **The port is currently attempting to connect to a LAT service or Telnet destination.**

Dialback Wait	**The Port is waiting for the remote modem to answer a dial-back call.**
Disconnected	**Shows that a session was disconnected (for example, for being inactive for too long).**
Disconnecting	**Shows that a session is disconnecting from a LAT service or Telnet destination.**
Executing Cmd	**The port is executing a command from the terminal server local command mode.**
Finding Script	**The port is searching for a script file via TFTP read requests.**
First Dialback Login	**The port is making its first attempt to locate a dial-back script.**
Idle	**Shows that the port is not in use.**
Loading Script	**The port has located a script file and is receiving the file from the script server.**
Local Mode	**The port is logged on to the server, and is in the local command mode.**
Locked	**Shows that the user has used the LOCK command to disable the port.**
Login	**The port is waiting for the user to enter a login or Kerberos password.**
Login Wait	**The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed.**
Logout	**The port is being logged out.**
Password	**The port is waiting to enter the password that is required by a password-protected LAT service.**
Reset	**The port is reverting to its stored configuration.**
Retry Connect	**The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).**
Running Script	**Shows that the port is executing the commands contained in a script file.**

	Second Dialback Login	**The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).**
	Slip	**The port is a SLIP port.**
	Suspended	**The user has entered the local-switch character, and the session is being suspended.**
	Test Wait	**The port is performing a TEST SERVICE command.**
	Test Out	**The port is outputting the results of a TEST SERVICE command.**
	Wait Input	**The port is at the local prompt (waiting for the user to enter a command).**
	Wait Logout	**The port is waiting for modem control signals to be deasserted.**
	Wait Output	**The port is completing display output before logging out.**
	Wait Queue	**A connection request from this port is in a queue.**
	Wait Session	**The session is being disconnected.**
Sessions	**Shows the number of active sessions on the port.**	
Current Service	**Shows the currently active service session, or the service session that was interrupted when the user entered local mode. If the user is in a Telnet session, the word TELNET will be displayed.**	
Current Node	**Shows the name of the LAT service node, or the internet-address of the Telnet node, to which the current session is connected. For remote connections to local services, this shows the name or internet-address of the node from which the connection originated.**	
Current Port	**Shows the identification of the port at the service node or at the requesting node. If the user is in a Telnet session, shows the telnet-port-number.**	
Current Domain	**Only displayed when the user is in a Telnet session. Shows the domain-name or internet-address to which the port is connected.**	
Input XOFFed	**Shows whether or not XON/XOFF flow control is enabled for data input to the port from the device connected to the port.**	
Output XOFFed	**Shows whether or not XON/XOFF flow control is enabled for data output from the port to the device connected to the port.**	
Output Signals	**Shows modem control signals that are currently asserted by the port to the device connected to the port. This field is not shown for parallel ports.**	

Input Signals	**Shows modem control signals that are monitored by the port (asserted by the device connected to the port). This field is not shown for parallel ports.**
Last Char Output	**Shows the hexadecimal value of the last character sent by the port to the device attached to the port.**
Last Char Input	**Shows the hexadecimal value of the last character received by the port from the device attached to the port.**
Script Host	**Shows the internet-address/domain-name of the script server where the port obtained a script file to run.**
Script File	**Shows the name of the script file which the port has run, which was obtained from the host shown in the "Script Host" field.**
Printer Information	
Printer Interface	**Shows the type of parallel printer interface used. The possible values that will be displayed are Centronics or Dataproducts.**
Printer Fault	**Shows whether or not the parallel printer is reporting a printer fault. The possible values that will be displayed are Yes and No.**
Printer Busy	**Shows whether or not the parallel printer is currently printing. The possible values that will be displayed are Yes and No.**
Printer Online	**Shows whether or not the parallel printer is currently online (available for printing). The possible values that will be displayed are Yes and No.**
Printer Paper	**Shows whether or not the parallel printer is reporting that it has paper. The possible values that will be displayed are Yes and Out. For the MAXserver 1400 Printer Server the display does not include this field when a Dataproducts interface is used.**

SHOW/LIST/MONITOR PORTS SUMMARY

Display a one-line summary about ports

Notes

Use the SHOW/LIST/MONITOR PORTS SUMMARY display to view a one-line summary showing the access method, connection status, and services in use at the specified port(s). This display is the "default" display shown when you issue a SHOW/LIST/MONITOR PORT command and you include a port-list (i.e., to display information about multiple ports or all ports) in the command.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW|LIST|MONITOR PORTS	**[*port-list*]**	**SUMMARY**
	[ALL]	
	[ACCESS]	**[DYNAMIC]**
		[LOCAL]
		[REMOTE]
		[NONE]

Where / Means

port-list — **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL — **Specifies that the requested information will be displayed about all ports.**

ACCESS — **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

- **DYNAMIC** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
- **LOCAL** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
- **REMOTE** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
- **NONE** — **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex>> SHOW PORTS 1-8 SUMMARY

Port    Access    Status        Services Offered     21 Nov 1988  15:57:19

  1     Local     Executing Cmd
  2     Local     Idle
  3     Local     Idle
  4     Local     Idle
  5     Local     Idle
  6     Local     Idle
  7     Local     Idle
  8     Remote    Connecting    LASER
```

Example LIST/MONITOR/SHOW PORT SUMMARY Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT SUMMARY display:

Port — **Shows the number of the terminal server port, about which the system is displaying information.**

Access — **Shows the type of connections which the terminal server allows to the port (e.g., the type of access the port can have to a service node, and/or the type of access other interactive users and service nodes can have to the port). The possible values that will be displayed are:**

- **Dynamic** — **indicates that the port is accessible from either the local command mode, or remotely by service name or port number.**
- **Local** — **indicates that the port is accessible only from the local command mode.**
- **Remote** — **indicates that the port is accessible only remotely by service name or port number.**
- **None** — **indicates that the port is not accessible at all (e.g., the server prevents any use of the port).**

Status — **Shows the current status of the port. The possible values that will be displayed are:**

- **Autobaud** — **The port is being autobauded.**
- **Available** — **A port, whose PORT ACCESS characteristics is set to REMOTE or DYNAMIC, is not busy.**
- **Check Modem** — **The port is verifying that modem signals are properly asserted.**

Check Connect	**The port is determining the status (accepted or rejected) of a pending connection.**
Connected	**The port is currently connected to a LAT service or Telnet destination.**
Connect Wait	**The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED).**
Connecting	**The port is currently attempting to connect to a LAT service or Telnet destination.**
Dialback Wait	**The Port is waiting for the remote modem to answer a dial-back call.**
Disconnected	**Shows that a session was disconnected (for example, for being inactive for too long).**
Disconnecting	**Shows that a session is disconnecting from a LAT service or Telnet destination.**
Executing Cmd	**The port is executing a command from the terminal server local command mode.**
Finding Script	**The port is searching for a script file via TFTP read requests.**
First Dialback Login	**The port is making its first attempt to locate a dial-back script.**
Idle	**Shows that the port is not in use.**
Loading Script	**The port has located a script file and is receiving the file from the script server.**
Local Mode	**The port is logged on to the server, and is in the local command mode.**
Locked	**Shows that the user has used the LOCK command to disable the port.**
Login	**The port is waiting for the user to enter a login or Kerberos password.**
Login Wait	**The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed.**
Logout	**The port is being logged out.**

	Password	**The port is waiting to enter the password that is required by a password-protected LAT service.**
	Reset	**The port is reverting to its stored configuration.**
	Retry Connect	**The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).**
	Running Script	**Shows that the port is executing the commands contained in a script file.**
	Second Dialback Login	**The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).**
	Slip	**The port is a SLIP port.**
	Suspended	**The user has entered the local-switch character, and the session is being suspended.**
	Test Wait	**The port is performing a TEST SERVICE command.**
	Test Out	**The port is outputting the results of a TEST SERVICE command.**
	Wait Input	**The port is at the local prompt (waiting for the user to enter a command).**
	Wait Logout	**The port is waiting for modem control signals to be deasserted.**
	Wait Output	**The port is completing display output before logging out.**
	Wait Queue	**A connection request from this port is in a queue.**
	Wait Session	**The session is being disconnected.**
Services Offered	**Shows the name(s) of the local service(s) that the terminal server offers at the port.**	

SHOW/LIST/MONITOR PORTS TELNET CHARACTERISTICS

Display the current values for Telnet-related characteristics

Notes

Use the SHOW/LIST/MONITOR PORTS TELNET CHARACTERISTICS display to view the current values for port characteristics which are related to Telnet, that have been defined by the user or the terminal server manager.

Privileges

Secure and non-privileged users can use LIST or SHOW PORTS commands (secure users can only display information about the port they are logged on to). Only users at privileged ports can use the MONITOR PORTS command.

Syntax

SHOW | LIST | MONITOR PORTS [*port-list*] [ALL] [ACCESS] TELNET CHARACTERISTICS [DYNAMIC] [LOCAL] [REMOTE] [NONE]

Where Means

port-list **Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**

ALL **Specifies that the requested information will be displayed about all ports.**

ACCESS **Specifies that the requested information will be displayed about all ports for which the setting of the ACCESS characteristic matches the requested ACCESS characteristic. Refer to the DEFINE/SET PORT ACCESS command description.**

- **DYNAMIC** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to DYNAMIC.**
- **LOCAL** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to LOCAL.**
- **REMOTE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to REMOTE.**
- **NONE** **Specifies that the requested information will be displayed about all ports for which the ACCESS characteristic is set to NONE.**

Example

```
Xyplex>> SHOW PORTS TELNET CHARACTERISTICS

Port 1:  J. Smith                              21 May 1990  15:57:32

Abort Output Character:    None       Newline:                CR/NULL
Attention Character:       None       Newline Filtering           None
Default Port:                23       Query Character:            None
Echo Mode:                 Remote     Remote Port:                2100
Erase Keystroke Character:   ^U       Synchronize Character:      None
Erase Line Character:      None       Transmit:              Immediate
Interrupt Character:       None       Binary Session Mode:    Pasthru
TerminalType               VT100      Tn3270 Device             VT100
TN3270 TranslationTable USENGLSH

Enabled Characteristics:
Tn3270 EOR
```

Example LIST/MONITOR/SHOW PORT TELNET CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW PORT TELNET CHARACTERISTICS display:

Item (Field)	Description
Port *n*	**Shows the number of the terminal server port, about which the system is displaying information. The variable *n* represents the number of a physical terminal server port.**
user-name	**The text which follows the port number shows either the name given by the user to log on to the port, or the name given to the port using the SET/DEFINE PORT USERNAME characteristic.**
Abort Output Character	**Shows the character that, when typed in a Telnet session, causes the terminal server to terminate further display of output (e.g., text file), or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).**
Attention Character	**Shows the character that, when typed in a Telnet session, causes the host to return to the operating system prompt, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).**
Default Port	**Shows the default telnet-port-number (protocol or physical port number).**
Echo Mode	**Shows which connection partner in a Telnet session will echo (return to the video display or printer) characters that the user has typed at the keyboard. The possible values that will be displayed are:** **Local Characters are echoed by the terminal server.** **Remote Characters are echoed by the connection partner.**

Erase Keystroke Character — Shows the character that, when typed in a Telnet session, causes the terminal server to delete the character immediately to the left of the cursor, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

Erase Line Character — Shows the character that, when typed in a Telnet session, causes the terminal server to delete all data in the current line of input, backwards from the cursor position, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

Interrupt Character — Shows the character that, when typed in a Telnet session, causes the terminal server to suspend, interrupt, abort, or terminate a user process, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).

TerminalType — The name of the terminal type that the server sends to a Telnet host while negotiating a Telnet session.

Tn3270 TranslatonTable — The language translation table used at this port during a Tn3270 session. The terminal server software includes one default table (USENGLSH), but you can define others.

Newline — Shows the characters that the terminal server transmits to the connection partner in a Telnet session, when the user presses the <RETURN> key. The possible values that will be displayed are:

- **CR/NULL** — The server transmits a carriage-return and a NULL character to the connection partner when the user presses the <RETURN> key.
- **CR/LF** — The server transmits a carriage-return and a line-feed character to the connection partner when the user presses the <RETURN> key.
- **CR** — The server transmits a carriage-return to the connection partner when the user presses the <RETURN> key.

Newline Filtering — The method, if any, that the terminal server uses to translate Telnet Newline sequences coming from the network and bound for this port. The possible methods are these:

- **None** — The server does not translate Newline sequences
- **CR** — The server translates a CR/NULL or a CR/LF in the data stream to a CR.
- **CR/NULL** — The server translates a CR/NULL or a CR/LF to a CR/NULL.
- **CR/LF** — The server translates a CR/NULL or a CR/LF to a CR/LF.
- **Strip Null** — The server translates a CR/NULL to a CR.

Query Character	**Shows the character that, when typed in a Telnet session, causes the terminal server to provide a visible indication that the system is still up and running, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).**
Remote Port	**Shows the telnet-port-number for which the terminal server will accept a remote connection. This is similar to a logical address at which this physical port can be reached.**
Synchronize Character	**Shows the character that, when typed in a Telnet session, allows the to regain control of a "runaway" process, or None if this is undefined. Control characters are displayed as ^n (e.g., <CTRL>/<B> is shown as ^B).**
Binary Session Mode	**Shows the session mode (Passall or Pasthru) that will be used when the port negotiates the Telnet binary mode, or Interactive if the port should not negotiate the Telnet binary mode.**
TN3270 Device	**The device type used at this port during a Tn3270 session.**
Enabled Characteristics:	**The characteristics that may appear as enabled include these:**

Tn3270 EOR	**An end of record is required prior to binary negotiation when establishing a Tn3270 session.**
Tn3270 XTDATTR	**Extended attributes are enabled at this port.**
Tn3270 ErrorCode	**During a Tn3270 session, the terminal will lock when you press an incorrect key sequence until you press the Reset key.**

SHOW/MONITOR QUEUE

Display the entries in the terminal server service connection queue

Notes

Use the MONITOR QUEUE and SHOW QUEUE commands to display the terminal server service connection queue, which is a list of requests for connection to services that are offered at the terminal server. Typically, you will use the SHOW/MONITOR QUEUE display to examine information about queued connection requests, estimate the effect of deleting entries (i.e., using a REMOVE QUEUE command), or determine the current size of the connection queue in order to adjust the SERVER QUEUE LIMIT characteristic.

The connection queue services requests in first-in-first-out (FIFO) order. When a connection request is queued, the terminal server assigns the request an entry number (i.e., job number) and a position number (i.e., first, second, third, etc). Although entries are processed in FIFO order, a connection request can be dequeued (connection is established) ahead of other entries which have a lower position number, depending on port availability.

Privileges

Non-privileged users can use the SHOW QUEUE command. Only users at privileged ports can use the MONITOR QUEUE command.

Syntax

SHOW|MONITOR QUEUE **[ALL]**
[ENTRY *entry-number*]
[NODE *node-name*]
[PORT *port-number*]
[SERVICE *service-name*]

Where	Means
ALL	**Specifies that the display will list all connection request entries in the terminal server connection queue. This is the default.**
ENTRY	**Specifies that the display will list only a specific connection request that is in the terminal server connection queue.**
entry-number	**A variable. Specifies the number of the entry in the connection queue about which you want information.**
NODE	**Specifies that the display will list only those connection request entries that originated at a specific node.**
node-name	**Specifies the name of a node where the connection request entries originated.**
PORT	**Specifies that the display will list only those connection requests which are made to a specific destination port on the terminal server.**

port-number	**Specifies the number of the port to which the connection request was made. (Note that this could be all connection requests if only one port on the terminal server has queuing enabled.)**
SERVICE	**Specifies that the display will list only those connection requests which are made to a specific service which is offered by the terminal server.**
service-name	**Specifies the name of the service which is offered by the terminal server, to which the connection request was made.**

Example

```
Xyplex>> SHOW QUEUE ALL

Position  Entry  Source Node       Service          Port Name

   1       111   FINANCEVAX        LASER
   2       115   FINANCEVAX                         3
   3       116   ENGINEERING       MODEM            4  PORT_4
```

Example SHOW/MONITOR QUEUE Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW QUEUE display:

Item (Field)	Description
Position	**Shows the current placement of each entry in the connection queue. This is an indication of the relative order of each entry.**
Entry	**Shows the entry number (e.g., the job number) of each queued request.**
Source Node	**Shows the name of the service node which made the connection request that is in the queue.**
Service	**Shows the name of the requested service.**
Port Name	**Shows the port-number and name of the port where the requested service is offered. Information only appears in this column if a port-name was specified in the connection request.**

SHOW/LIST/MONITOR SERVER - General Information

Display information about server-wide settings or statistics

Use the SHOW SERVER or MONITOR SERVER command to display information about operational database parameters for the server. Use the LIST SERVER command to display information about permanent database parameters for the server. The SHOW and LIST SERVER command produces a static display. The MONITOR SERVER command produces a display that is continuously updated.

Non-privileged users can use the SHOW and LIST SERVER command. Only users at privileged ports can use the MONITOR SERVER command.

SHOW/MONITOR SERVER ACCOUNTING

Display information about successful and attempted connections, as well as information about sessions that are disconnected.

Notes

Use the SHOW/MONITOR SERVER ACCOUNTING display to view the accounting log which contains information about successful and attempted connections made to or from the unit, as well as information about sessions that are disconnected. This display can be useful in identifying the cause of problems that are occurring on the server.

Privileges

Non-privileged users can use the SHOW SERVER ACCOUNTING command. Only users at privileged ports can use the MONITOR SERVER ACCOUNTING command.

Syntax

SHOW|MONITOR SERVER ACCOUNTING

Example

```
ENTRY ADDRESS          PORT USERNAME        TYPE DESTINATION      CONNECT TIME          DISCONNECT TIME        BYTES IN BYTES OUT
    1 08-00-87-00-4F-45   1 JSmith          L    UNIXHOST         12 Apr 1991  20:19:40
    1 08-00-87-00-4F-45   1 JSmith          D 0  UNIXHOST         12 Apr 1991  20:19:40 12 Apr 1991  20:19:46         0        20
    2 08-00-87-00-4F-45   0                 R                     12 Apr 1991  20:19:59
    3 08-00-87-00-4F-45   1 JSmith          L    UNIXHOST         12 Apr 1991  20:20:02
    4 08-00-87-00-4F-45   0 A Jones         L    VAX              12 Apr 1991  20:20:43
    4 08-00-87-00-4F-45   0 A Jones         D23  VAX              12 Apr 1991  20:20:43 12 Apr 1991  20:21:04         0         0
    3 08-00-87-00-4F-45   1 JSmith          D 0  UNIXHOST         12 Apr 1991  20:20:02 12 Apr 1991  20:21:04        35     28938
```

Example SHOW SERVER ACCOUNTING DISPLAY

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER ACCOUNTING display:

Item (Field)	Description
Entry	**Shows the entry number**
Address	**Shows the Ethernet address of the server.**
Port	**Shows the port from or to which the connection is made.**
Username	**Shows the name of the user who is logged on to the port.**

Type	**Shows whether the connection is a local access connection or a remote access connection, or if a connection has been disconnected and the reason why the connection was disconnected. Local access connections are indicated by the letter L in the first column. Remote access connections are indicated by the letter R in the first column. Disconnections are indicated by the letter D, followed by a number which represents the reason why the disconnection occurred. The table below lists these numbers and the corresponding reason for a session being disconnected.**
Destination	**Shows the destination LAT service name, domain-name, or internet-address of the connection.**
Connect Time	**Shows the time when the connection was made.**
Disconnect Time	**Shows the time when a connection was disconnected**
Bytes In	**Shows the number of bytes of data that the port received from the device.**
Bytes Out	**Shows the number of bytes of data output by the port to the device.**

Code	Related Error Code	Explanation
0	**None - normal disconnection**	**Connection terminated because the user logged out or disconnected the port.**
1	**211 or 251**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
2	**212 or 252**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
3	**213 or 253**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
4	**214 or 254**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
5	**215 or 255**	**Connection refused because the queue entry id already exists in the queue.**
6	**216 or 256**	**Connection terminated or refused and the LAT virtual circuit is now inactive.**
7	**217 or 257**	**Connection terminated or refused because the server had insufficient memory or resources to make the connection.**
8	**218 or 258**	**Connection terminated or refused because the service node (a host or a remote terminal server offering the service) would not permit the connection.**
9	**219 or 259**	**Connection terminated or refused because the service is not available any more.**

10	**220 or 260**	**Connection terminated or refused because your server would not permit the connection.**
11	**221 or 261**	**Connection terminated or refused because the server had insufficient memory or resources to make the connection.**
12	**222 or 262**	**Connection terminated or refused because the server is being reinitialized or shut down.**
13	**223 or 263**	**Connection terminated or refused because the remote node offering the service intentionally aborted the connection.**
14	**224 or 264**	**Connection terminated or refused because the LAT circuit timer at your server is not set appropriately.**
15	**225 or 265**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
16	**226 or 266**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
17	**227 or 267**	**Connection terminated or refused because the service node failed to respond within the time period defined by DEFINE/SET SERVER RETRANSMIT LIMIT characteristic.**
18	**228 or 268**	**Connection terminated or refused because the server determined that no progress was being made on the existing virtual circuit. This is an indication of how busy the service node is.**
19	**229 or 269**	**Connection terminated or refused because the the service is not offered on the requested port.**
20	**230 or 270**	**Connection terminated or refused because the the service is not offered on the requested port.**
21	**231 or 271**	**Connection terminated or refused because you specified an incorrect password to use the service.**
22	**232 or 272**	**Connection terminated or refused because the requested service is already being used.**
23	**233 or 273**	**Connection terminated or refused because the requested service is no longer offered at your server.**
24	**234 or 274**	**Connection terminated or refused because the service is disabled.**
25	**235 or 275**	**Connection terminated or refused because it was not in the connection queue, as was previously thought.**
26	**236 or 276**	**Connection terminated or refused because you attempted to connect to a busy service that is not configured for queued access.**

27	**237 or 277**	**Connection terminated or refused because of an access violation.**
28	**238 or 278**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
29	**none**	**Connection terminated or refused because of an unexpected event.**
30	**735**	**The service specified in a TEST SERVICE command does not support the specified test.**
31	**793**	**Connection refused because the user supplied a domain-name that was too long or in an invalid format.**
32	**710**	**Connection refused because the requested service is not offered at the node specified, or the service or node name that you specified is not known to the server.**
33	**711**	**Connection refused because the service specified is unknown to the unit, the server node limit has been reached, the server is unable to store information about additional nodes, or you are not authorized to use the service specified.**
34	**REJECT_SERVICE**	
35	**766**	**Connection refused because the user attempted to connect to an internet-address from a port on which the DEFINE/SET PORT INTERNET CONNECTIONS characteristic is DISABLED.**

SHOW/MONITOR SERVER ALTERNATE STATUS

Display server resource levels

Notes

Use the SHOW/MONITOR SERVER ALTERNATE STATUS display to view the current values for server processor and memory usage.

Privileges

Non-privileged users can use the SHOW SERVER ALTERNATE STATUS commands. Only users at privileged ports can use the MONITOR SERVER ALTERNATE STATUS command.

Syntax

SHOW|MONITOR SERVER ALTERNATE STATUS

Example

```
Xyplex> SHOW SERVER ALTERNATE STATUS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:   08-00-87-00-27-71   Name:   MAX5000               Number:     0

Protocol(s): LAT, TELNET

Crate Current State:   No Fault             Crate Transition Count:      0

                        Cur    High     Max    Failures  Last Occurred
Processes:               38      40     132           0
Timers:                  36      39      80           0
Packet Buffers:           8      16      40           0
IPC Messages:             0       1      16           0

                        Cur     Low     Max    Failures  Last Occurred
Free Text Pool:       14528   14368   16384           0
Free Memory:          76784   75552   92080           0

Total Fragment(s) = 4     Start    Size           Start    Size
                     1)   04EC00   76352      2)   061B80     368
                     3)   076440      48      4)   0763F0      32
```

Example MONITOR/SHOW SERVER ALTERNATE STATUS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER ALTERNATE STATUS display:

Item (Field)	Description
Protocol(s)	**Shows the protocols available on your server. Valid values are LAT and Telnet.**
Crate Current State	**For MAXserver 4500/5000/5500 and Network 9000 units, shows whether or not any modules are currently experiencing a fault. For chassis units which have the Redundant Power Supply, this field can also indicate a fault with one of the power supplies. A "No Fault" indication means that there are currently no faults.**
Crate Transition Count	**Shows the number of times a fault has occurred or has been cleared.**

This display shows information which indicates how well the server is operating under the current load, and may be helpful in identifying network trouble or server problems. For each server resource listed, the display shows:

Cur	**Shows the level or amount of the resource that is currently in use.**
High	**Shows the highest amount of the resource that has been used since the server was last initialized.**
Max	**Shows the maximum amount of the resource that can be used (either because of a hardware constraint or because the value shown is the value specified for a server characteristic).**
Failures	**Shows the number of times that a failure has occurred for a given resource.**
Last Occurred	**Shows the most recent occurrence of a failure for a given resource.**
Processes	**Shows the number of processes (for example, user sessions, server "house-keeping" activities, user command line interfaces, etc) occurring on a server.**
Timers	**Shows the number of timers (internal to processes) that are currently in use by the processes that are currently active on the server.**
Packet Buffers	**Shows the number of incoming and outgoing packets that are being buffered in server memory.**
IPC Messages	**Shows the number of interprocess communication (IPC) messages being passed among processes that are active on the server. As an example of when an IPC message is passed, when a user session is terminated, the LAT or TCP/IP process running on the server passes a message indicating that the process has ended to the user interface process, which then informs the user of this event.**

Free Text Pool	**Shows the amount of space used by the server to store identification strings for nodes, LAT services, and domain-names (which is referred to as text pool space), as well as the number of times an operation was attempted, but for which there was insufficient text pool space, and when the last failure occurred. If there are Text Pool Failures, you should consider increasing the size of the SERVER TEXTPOOL SIZE characteristic, or adjusting the number or size of the identification strings for nodes, LAT services, and domain-names that the server must store. (Refer to the discussion on adjusting the SERVER TEXTPOOL SIZE characteristic in the *Software Management Guide.*)**
Free Memory	**Shows the amount of non-text pool space used, the number of times an operation was attempted, but for which there was insufficient non-text pool space, and when the last failure occurred. (Refer to the discussion on adjusting the SERVER TEXTPOOL SIZE characteristic.) If there are Free Memory Failures, you should consider decreasing the size of the SERVER TEXTPOOL SIZE characteristic, or adjusting the number of the nodes, LAT services, and domain-names that the server must store. (Refer to the discussion on adjusting the SERVER TEXTPOOL SIZE characteristic in the *Software Management Guide.*)**
Total Fragment(s) =	**Shows the number of unused fragments of server memory and the largest of these fragments. The number shown in the "Start" column is the hexadecimal memory address of the fragment. The number shown in the "Size" column is the size of the fragment, in bytes.**

SHOW/LIST/MONITOR SERVER CHARACTERISTICS

Display values for server characteristics

Notes

Use the SHOW/LIST/MONITOR SERVER CHARACTERISTICS display to view the current or permanent values for server characteristics that have been defined by the server manager. This is the default display type.

Privileges

Non-privileged users can use the SHOW and LIST SERVER CHARACTERISTICS commands. Only users at privileged ports can use the MONITOR SERVER CHARACTERISTICS command.

Syntax

SHOW|LIST|MONITOR SERVER CHARACTERISTICS

Example

```
Xyplex> SHOW SERVER CHARACTERISTICS

MAXserver V5.0 Rom 410000 HW 00.00.00 Lat Protocol V5.1 Uptime:  0 01:30:25

Address:   08-00-87-00-85-D4   Name:   X0085D4               Number:     0

Identification:  Xyplex Printer Server
Welcome:         Welcome to the Xyplex Printer Server.

Circuit Timer:            80          Password Limit:            3
Console Port:              0          Queue Limit:              24
Inactivity Timer:         30          Retransmit Limit:          8
Keepalive Timer:          20          Session Limit:             8
Multicast Timer:          30          Software:         XYP_MX1400
Node Limit:              100          Identification Size:      63
Textpool Size:          8192          Timezone:              00:00
Accounting Entries:        0
IPX Protocl:        Ethernet
Service Groups:   0

Enabled Characteristics:

Announcements,  Broadcast,  Dump,  Lock,  Parameter Polling
```

Example LIST/MONITOR/SHOW SERVER CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW SERVER CHARACTERISTICS display:

Item (Field)	Description
Identification	**Shows a text message which identifies the server.**
Welcome	**Shows the text message that is displayed when a user logs on to the server.**

Circuit Timer	**Shows the amount of time (in milliseconds) between the transmission of messages to service nodes.**
Console Port	**Shows the number of the port that acts as the console port for server messages.**
Inactivity Timer	**Shows the amount of time (in minutes) that a port can remain logged in to the server and have no connected sessions, before the port is logged off.**
Keepalive Timer	**Shows the amount of time (in seconds) the server will wait before it transmits a null message on an active virtual circuit to service nodes (for the purpose of notifying these nodes that the server is still available on the network).**
Multicast Timer	**Shows the amount of time (in seconds) between transmission of multicast announcements to indicate the availability of local services.**
Node Limit	**Shows the maximum number of service nodes about which the server can retain information.**
Textpool Size	**Shows the maximum amount of server memory that is reserved for storing identification strings for nodes, LAT services, and domain-names.**
Accounting Entries	**Shows the maximum number of entries that can be contained in the server accounting log.**
IPX Protocol	**Shows whether Ethernet or MAC (IEEE 802.3) packets are used for IPX printing.**
Service Groups	**Shows the authorized groups which can have access to services at this server.**
Password Limit	**Shows the maximum number of times that the server will allow a user to incorrectly enter a password.**
Queue Limit	**Shows the maximum number of entries that are allowed in the server connection queue.**
Retransmit Limit	**Shows the maximum number of times the server will attempt to retransmit a message that has not been acknowledged by a service node.**
Session Limit	**Shows the maximum number of sessions permitted among all ports.**
Software	**Shows the name of the software image at the load host.**
Identification Size	**Shows the maximum length of LAT node and service identification strings that the server stores in memory.**
Timezone	**Shows the time zone differential, in hours and minutes, from Universal Time (formally called Greenwich Mean Time) that was passed by the load server, after loading via TFTP.**

Enabled Characteristics

Shows the characteristics which have been enabled for the port using the DEFINE/SET SERVER command. Possible values which can be shown are:

Announcements	**The server will multicast an announcement to indicate that local services are available.**
Broadcast	**The server allows port users to use the BROADCAST command to send messages to other ports.**
Dump	**The server performs a crash dump (e.g., dumps a copy of the contents of its memory into a file at the load host, and then re-initializes) when it detects that a fatal software error has occurred.**
Lock	**The server allows users to execute a LOCK command to secure their port while they are away.**
Parameter Polling	**The server can locate additional eligible parameter servers (the SERVER PARAMETER CHECK characteristic is set to ENABLED).**

SHOW/MONITOR SERVER COUNTERS

Display statistics about server activity

Notes

Use the SHOW/MONITOR SERVER COUNTERS display to view statistics about server activity, and occurrences of error conditions.

Privileges

Non-privileged users can use the SHOW SERVER COUNTERScommand. Only users at privileged ports can use the MONITOR SERVER COUNTERS command.

Syntax

SHOW|MONITOR SERVER COUNTERS

Example

```
Xyplex>> SHOW SERVER COUNTERS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Seconds Since Zeroed:      156361   Frames Sent, 1 Collision:           3
Bytes Received:          23048906   Frames Sent, 2+ Collisions:         1
Bytes Sent:                886180   Send Failures:                      0
Frames Received:           288512   Send Failure Reasons:      0000000000
Frames Sent:                11153   Receive Failures:                3040
Multicast Bytes Rcv'd:   22790945   Receive Failures Reasons:  0000000011
Multicast Bytes Sent:      771197   Unrecognized Destination:      210057
Multicast Frames Rcv'd:    284221   Data Overrun:                       0
Multicast Frames Sent:       7909   User Buffer Unavailable:            0
Frames Sent Deferred:          57   System Buffer Unavailable:          0

Messages Received:           4202   Duplicates Received:                0
Messages Transmitted:        3243   Messages Re-transmitted:            0
Solicitations Accepted:         0   Illegal Messages Rcv'd:             0
Solicitations Rejected:         0   Illegal Slots Rcv'd:                0
Multiple Node Addresses:        0   Illegal Multicasts Rcv'd:           0
```

Example MONITOR/SHOW SERVER COUNTERS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER COUNTERS display. The values listed below indicate cumulative values counted since the last time the display counters were reset to zero. There are two ways to reset these counters: use a ZERO COUNTERS command, or re-initialize the server.

Item (Field)	Description
Seconds Since Zeroed	**Shows the number of seconds since the counters were reset to zero.**
Bytes Received	**Shows the total number of bytes contained in datagrams that have been successfully received from the network by the server, excluding Ethernet header and CRC data, since the counters were reset to zero.**

Bytes Sent	**Shows the total number of bytes contained in datagrams that have been successfully transmitted to the network by the server, excluding Ethernet header and CRC data, since the counters were reset to zero.**
Frames Received	**Shows the total number of datagram frames, including multicast frames, that have been successfully received by the server, since the counters were reset to zero.**
Frames Sent	**Shows the total number of datagram frames, including multicast frames, that have been successfully transmitted by the server, since the counters were reset to zero.**
Multicast Bytes Rcv'd	**Shows the total number of bytes contained in multicast frames that have been successfully received by the server, excluding Ethernet header and CRC data, since the counters were reset to zero.**
Multicast Bytes Sent	**Shows the total number of bytes contained in multicast frames that have been successfully transmitted by the server, excluding Ethernet header and CRC data, since the counters were reset to zero.**
Multicast Frames Rcv'd	**Shows the total number of multicast frames that have been received by the server, since the counters were reset to zero.**
Multicast Frames Sent	**Shows the total number of multicast frames that have been transmitted by the server, since the counters were reset to zero.**
Frames Sent, Deferred	**Shows the number of times when the server deferred transmission of a frame because the data link was in use, since the counters were reset to zero.**
Frames Sent, 1 Collision	**Shows the number of times when the server successfully transmitted a frame on the second attempt after a collision occurred during the first attempt, since the counters were reset to zero.**
Frames Sent, 2+ Collisions	**Shows the number of times when the server successfully transmitted a frame after a collision occurred during the first two or more attempts, since the counters were reset to zero.**
Send Failures	**Shows the number of times the Ethernet interface aborted a transmission request (see Send Failure Reasons), since the counters were reset to zero.**

Send Failure Reasons

Indicates the types of problems encountered which caused send failure(s) to occur. This information is presented in the form of a cumulative mask, in which the following bits are defined (Bit 0 is the rightmost bit):

Bit	Definition
0	Transmission failed to complete after 16 retries.
1	Carrier lost on the Ethernet network during transmission.
4	Transmission aborted because the frame exceeded the maximum allowable length.
5	Late collision during a transmission attempt.
9	Data underflow condition.

Receive Failures

Shows the number of packets that were received with an error (see Receive Failure Reasons, below), since the counters were reset to zero.

Receive Failure Reasons

Indicates the types of problems encountered which caused receive failure(s) to occur. This information is presented in the form of a cumulative mask, in which the following bits are defined (Bit 0 is the rightmost bit):

Bit	Definition
0	Block check error occurred. Indicates that the received packet did not pass the CRC check.
1	Framing error occurred. Indicates that the received packet did not contain an integral number of 8-bit bytes.
2	Message length error occurred. Indicates that the received packet exceeded 1518 bytes.

Unrecognized Destination

Shows the number of times a frame passed through the server hardware, but the server did not recognize the address and discarded the message, since the counters were reset to zero.

Data Overrun

Shows the number of times the server hardware lost an incoming frame because it was unable to keep up with the data rate, since the counters were reset to zero.

User Buffer Unavailable

Shows the number of times the server did not have a user buffer available since the counters were reset to zero.

System Buffer Unavailable

Shows the number of times that a system buffer was unavailable to the server for an incoming frame, since the counters were reset to zero.

Messages Received

Shows the number of LAT virtual circuit messages that have been successfully received by the server since the counters were reset to zero.

Messages Transmitted	**Shows the number of LAT virtual circuit messages that have been successfully transmitted by the server since the counters were reset to zero.**
Solicitations Accepted	**Shows the number of queued LAT connection requests that the server has accepted, since the counters were reset to zero. This number includes both queued requests and requests that were immediately satisfied without queuing.**
Solicitations Rejected	**Shows the number of queued LAT connection requests that the server could not process and has rejected, since the counters were reset to zero.**
Multiple Node Addresses	**Shows the number of times a service node became available with a different Ethernet address since the counters were reset to zero.**
Duplicates Received	**Shows the number of duplicate LAT messages that the server received since the counters were reset to zero.**
Messages Re-Transmitted	**Shows the number of LAT messages that the server retransmitted because they were not acknowledged by the destination service node, since the counters were reset to zero.**
Illegal Messages Rcv'd	**Shows the number of LAT messages that have been received by the server which have an illegal format, since the counters were reset to zero.**
Illegal Slots Rcv'd	**Shows the number of LAT messages that have been received by the server which have an illegal slot format, since the counters were reset to zero.**
Illegal Multicasts Received	**Shows the number of multicast messages that have been received by the server which have an illegal format, since the counters were reset to zero.**

SHOW/LIST/MONITOR SERVER INTERNET CHARACTERISTICS

Display current or permanent values related to Internet addresses or address resolution

Notes

Use the SHOW/LIST/MONITOR SERVER INTERNET CHARACTERISTICS display to view the current or permanent values related to Internet addresses or address resolution for the server.

Privileges

Non-privileged users can use the SHOW and LIST SERVER INTERNET CHARACTERISTICS commands. Only users at privileged ports can use the MONITOR SERVER INTERNET CHARACTERISTICS command.

Syntax

SHOW|LIST|MONITOR SERVER INTERNET CHARACTERISTICS

Example

```
Xyplex> SHOW SERVER INTERNET CHARACTERISTICS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  MAX5000       Number:     0

Identification:  XYPLEX MAXserver 5000

Internet Address:           192.12.119.151      Internet TTL:               64
Internet Broadcast Address: 255.255.255.255



Domain Name:                   DX2771.COM
Domain Suffix:                 .COM|.XYPLEX.COM|.ARPA|.EDU


Domain TTL:                    0               IP Reassembly:         DISABLED
Primary Domain Address:     192.12.119.57      TCP Resequencing:      DISABLED
Secondary Domain Address:   0.0.0.0            TCP Connect Timer:           32

Secondary Domain Address:      0.0.0.0
Primary Gateway Address:       192.12.119.24
Secondary Gateway Address:     0.0.0.0
Subnet Mask:                   255.255.255.0
Subnet Mask Auto-Configure:    ENABLED
```

Example LIST/MONITOR/SHOW SERVER INTERNET CHARACTERISTICS Display.

The following table describes each of the items (fields) of data which follow the display header in the LIST/MONITOR/SHOW SERVER INTERNET CHARACTERISTICS display:

Item (Field)	Description
Internet Address	**Shows the Internet address for this server.**

Internet Broadcast Address	**Shows the Internet address that is used in Internet Broadcast messages.**
Internet TTL	**Shows the maximum amount of time, in seconds, that an Internet data packet can circulate through the network before the packet is discarded (i.e., "time to live").**
Domain Name	**Shows the *domain-name* by which the server is known on the network.**
Domain Suffix	**Shows the default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name*, whenever a user specifies an incomplete *domain-name* (the server appends the suffixes to the incomplete *domain-name*).**
Domain TTL	**Shows the number of hours that a *domain-name* will be retained by the server.**
IP Reassembly	**If enabled, the server reassembles packets that it receives that were fragmented by a gateway or router.**
Primary Domain Address, Secondary Domain Address	**Shows the *internet-address* at which a Domain name server is located. Domain name servers are network objects where the network attempts to resolve a domain-name. The server can use up to two Domain name servers (primary and secondary) to resolve a domain-name. The server will query both the primary and secondary Domain servers (at the same time) to resolve a domain-name.**
TCP Resequencing	**If enabled, shows that the server will accept packets received out of sequence.**
Primary Gateway Address, Secondary Gateway Address	**Shows the internet-address at which an Internet gateway is located. The server can use up to two Internet gateways (primary and secondary) to locate a device on an external network. The server will use the address of the primary gateway to route a transmission to a remote device, until it determines that the primary gateway has failed. Then the server will use the address of the secondary gateway.**
Subnet Mask	**Shows the Internet subnet-mask which server uses to distinguish Internet addresses that can be reached directly from those that must be reached via an IP Gateway.**
Subnet Mask Auto-Configure	**Shows whether or not the software will use an *internet-subnet-mask* specified by the server manager, or one that has been determined automatically by the server. Enabled means that the server will automatically determine the *internet-subnet-mask*. Disabled means that the server will use an *internet-subnet-mask* specified by the server manager.**

SHOW//MONITOR SERVER INTERNET COUNTERS

Display statistics about server IP, TCP, and UDP activity

Notes

Use the SHOW/MONITOR SERVER INTERNET COUNTERS display to view statistics about server IP, TCP, and UDP activity, and occurrences of error conditions.

Privileges

Non-privileged users can use the SHOW SERVER INTERNET COUNTERS command. Only users at privileged ports can use the MONITOR SERVER INTERNET COUNTERS command.

Syntax

SHOW|MONITOR SERVER INTERNET COUNTERS

Example

```
Xyplex> SHOW SERVER INTERNET COUNTERS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1 Uptime:  1 02:20:23

Internet Address:    192.12.119.151
Domain Name:         FINANCESUN.XYPLEX.COM
Domain Suffix:       .COM|.XYPLEX.COM|.|.EDU



IP Packets Received:        58435     IP Packets Transmitted:        834
IP Checksum Errors:             0     IP Header Errors:                0
IP Fragments Received:          0     IP Rx Delivery                   0
IP Unknown Protocol Rcvd:       1     IP Deliveries Rcvd:          58430
IP Failed Reassemblies:         2     IP No Routes Sent:               0
Frags Not Accepted:             0     Frags on Reassembly Que-High:    0

TCP Packets Received:       57823     TCP Packets Transmitted:        38
TCP Retransmissions:          819     TCP Checksum Errors:             0
TCP Active Opens:               2     TCP Passive Opens:               1
TCP Failed Attempts:            5     TCP Establish Resets:            0
TCP Total Resets:               8

UDP Messages Received:        312     UDP Messages Sent:              22
UDP No Port Messages Rcvd:      0     UDP Receive Message Errors:      2
```

Example MONITOR/SHOW SERVER INTERNET COUNTERS Display.

The following table describes each of the items (fields) of data following the display header in the MONITOR/SHOW SERVER INTERNET COUNTERS display:

Item (Field)	Description
Internet Address	Shows the Internet address for this server.
Domain Name	Shows the domain-name by which the server is known on the network.
Domain Suffix	Shows the default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name,* whenever a user specifies an incomplete *domain-name* (the server appends each of the suffixes in turn to the incomplete *domain-name,* until a successful resolution is made).
IP Counters	
IP Packets Received	Shows the total number of IP packets (i.e., the sum of all TCP packets, UDP packets, and ICMP packets) received by the server, since the counters were reset to zero.
IP Checksum Errors	Shows the number of times the server received an IP packet containing a checksum error, since the counters were reset to zero.
IP Fragments Received	Shows the number of times that the server received an IP fragment, since the counters were reset to zero.
IP Unknown Protocol Rcvd	Shows the number of times that the server received an IP packet that was not a TCP, UDP, or ICMP packet.
IP Failed Reassemblies	Shows the number of times that the server discarded an IP message because the server did not receive all of the fragments which were part of the message, within a specified period of time.
Frags Not Accepted	Shows the number of times that the server discarded a packet that it received that was fragmented by a gateway or router.
IP Packets Transmitted	Shows the total number of IP packets (i.e., the sum of all TCP packets, UDP packets, and ICMP packets) transmitted by the server, since the counters were reset to zero.
IP Header Errors	Shows the number of times the server received an improperly formatted IP packet, since the counters were reset to zero.
IP Rx Delivery	Shows the number of times that the server could not deliver an IP packet to a higher level protocol.
IP Deliveries Rcvd	Shows the number of times that the server could deliver an IP packet to a higher level protocol.
IP No Routes Sent	Shows the number of times that the server could not send an IP packet because the server did not know how to reach the destination.
Frags on Reassembly Que-High	Shows the number of highest number of packets that were received out of sequence that the server stored.

TCP Counters

TCP Packets Received	**Shows the total number of TCP packets received by the server, since the counters were reset to zero.**
TCP Retransmissions	**Shows the number of times the server had to retransmit a TCP packet, since the counters were reset to zero.**
TCP Active Opens	**Shows the number of TCP virtual circuits that were initiated by the server**
TCP Failed Attempts	**Shows the number of times that the server was unable to open a TCP virtual circuit.**
TCP Total Resets	**Shows the number of TCP virtual circuits the server aborted or refused.**
TCP Packets Transmitted	**Shows the total number of TCP packets transmitted by the server, since the counters were reset to zero.**
TCP Checksum Errors	**Shows the number of times the server received a TCP packet containing a checksum error, since the counters were reset to zero.**
TCP Passive Opens	**Shows the number of TCP virtual circuits that were initiated by the remote connection partner.**
TCP Establish Resets	**Shows the number of times that the remote connection partner aborted an established TCP virtual circuit with the server.**

UDP Counters

UDP Messages Received	**Shows the total number of UDP packets received by the server, since the counters were reset to zero.**
UDP No Port Messages Rcvd	**Shows the number of times that the server received a UDP message that was addressed to an invalid UDP port on the server.**
UDP Messages Sent	**Shows the total number of UDP packets transmitted by the server, since the counters were reset to zero.**
UDP Receive Message Errors	**Shows the number of times that the server received a UDP broadcast message, and discarded the message.**

SHOW/LIST/MONITOR SERVER INTERNET ICMP COUNTERS

Display statistics about server ICMP activity

Notes

Use the SHOW/MONITOR INTERNET SERVER ICMP COUNTERS display to view statistics about server ICMP activity, and occurrences of ICMP error conditions.

Privileges

Non-privileged users can use the SHOW INTERNET SERVER ICMP COUNTERS command. Only users at privileged ports can use the MONITOR SERVER INTERNET ICMP COUNTERS command.

Syntax

SHOW|MONITOR SERVER INTERNET ICMP COUNTERS

Example

```
Xyplex> SHOW SERVER INTERNET ICMP COUNTERS

MAXserver V5.0 Rom 410000 HW 00.00.00 Lat Protocol V5.1 Uptime:  0 01:30:25

 Internet Address:    192.12.119.151
 Domain Name:         FINANCESUN.XYPLEX.COM
 Domain Suffix:       .COM|.XYPLEX.COM|.ARPA|.EDU



 ICMP Messages Received:       881       ICMP Messages Sent:             5
 Destination Unreachable Rcvd:   3       Destination Unreachable Sent:   0
 Time-to-live Exceeded Rcvd:    10       Time-to-live Exceeded Sent:     0
 Parameter Problem Rcvd:         1       Parameter Problem Sent:         5
 Source Quench Rcvd:             0       Source Quench Sent:             0
 Redirect Rcvd:                 36       Redirect Sent:                  0
 Echo Rcvd:                    784       Echo Reply Sent:                0
 Timestamp Rcvd:                45       Timestamp Reply Sent:           0
 Information Request Rcvd:       2       Information Reply Sent:         0
 Unknown Messages Rcvd:          0
```

Example MONITOR/SHOW SERVER INTERNET ICMP COUNTERS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER INTERNET ICMP COUNTERS display:

Item (Field)	Description
Internet Address	**Shows the Internet address for this server.**
Domain Name	**Shows the *domain-name* by which the server is known on the network.**

Domain Suffix	**Shows the default *domain-name-suffixes* that the server uses to develop a fully-qualified *domain-name*, whenever a user specifies an incomplete *domain-name* (the server appends the suffixes to the incomplete *domain-name*).**
ICMP Messages Received	**Shows the total number of ICMP packets received by the server, since the counters were reset to zero.**
Destination Unreachable Rcvd	**Shows the number of times that the server received an ICMP message indicating that a destination was unreachable, since the counters were reset to zero.**
Time-to-live Exceeded Rcvd	**Shows the number of times that the server received an ICMP message indicating that an IP packet has exceeded its time to live.**
Parameter Problem Rcvd	**Shows the number of times that the server received an ICMP message from a node indicating the server sent an improperly formatted IP packet, since the counters were reset to zero.**
Source Quench Rcvd	**Shows the number of times that the server received an ICMP message from a node, indicating that the node is temporarily unable to accept further data, since the counters were reset to zero.**
Redirect Rcvd	**Shows the number of times that the server received an ICMP message from a gateway, indicating that there is a better path by which the server can route a packet, since the counters were reset to zero.**
Echo Rcvd	**Shows the number of times that the server received an ICMP Echo message, since the counters were reset to zero.**
Timestamp Rcvd	**Shows the number of times that the server received an ICMP message requesting the current time, since the counters were reset to zero.**
Information Request Rcvd	**Shows the number of times that the server received an ICMP message requesting the number of the network to which the server is connected, since the counters were reset to zero.**
Unknown Rcvd	**Shows the number of times that the server received an undefined ICMP packet, since the counters were reset to zero.**
ICMP Messages Sent	**Shows the total number of ICMP packets transmitted by the server, since the counters were reset to zero.**
Destination Unreachable Sent	**Shows the number of times that the server transmitted an ICMP message indicating that a destination was unreachable, since the counters were reset to zero.**
Time-to-live Exceeded Sent	**Shows the number of times that the server transmitted an ICMP message indicating that an IP message has exceeded its time to live, since the counters were reset to zero.**

Parameter Problem Sent	**Shows the number of times that the server has transmitted an ICMP message indicating that it has received an improperly formatted IP packet, since the counters were reset to zero.**
Source Quench Sent	**Shows the number of times that the server transmitted an ICMP message to a node, indicating that it is temporarily unable to accept further data, since the counters were reset to zero.**
Redirect Sent	**Shows the number of times that the server transmitted an ICMP message indicating that there is a better path by which a packet can be routed, since the counters were reset to zero.**
Echo Reply Sent	**Shows the number of times that the server responded to an ICMP Echo message, since the counters were reset to zero.**
Timestamp Reply Sent	**Shows the number of times that the server responded to a request for the current time, since the counters were reset to zero.**
Information Reply Sent	**Shows the number of times that the server transmitted an ICMP message in response to a request for the number of the network to which the server is connected, since the counters were reset to zero.**

SHOW/LIST/MONITOR SERVER INTERNET ROTARY

Display a list of rotaries contained in the operational or permanent database.

Notes

Use the SHOW/LIST/MONITOR SERVER INTERNET ROTARY display to view a list of rotaries contained in the operational or permanent database.

Privileges

Non-privileged users can use the SHOW and LIST SERVER INTERNET ROTARY commands. Only users at privileged ports can use the MONITOR SERVER INTERNET ROTARY command.

Syntax

SHOW|LIST|MONITOR SERVER INTERNET ROTARY

Example

```
Xyplex>> MONITOR SERVER INTERNET ROTARY

       Internet Address  Ports

         140.179.80.5     1-8
```

Example SHOW/MONITOR/LIST SERVER INTERNET ROTARY Display.

The first column of the SHOW/MONITOR/LIST SERVER INTERNET ROTARY display lists the internet-address assigned to the port(s) that are listed in the second column.

SHOW/LIST/MONITOR SERVER INTERNET ROUTES

Display a list of one or all internet-routes contained in the operational or permanent database.

Notes

Use the SHOW/LIST/MONITOR SERVER INTERNET ROUTES display to view a list of one or all internet-routes contained in the operational or permanent database.

Privileges

Non-privileged users can use the SHOWand LIST SERVER INTERNET ROUTES commands. Only users at privileged ports can use the MONITOR SERVER INTERNET ROUTES command.

Syntax

SHOW|LIST|MONITOR SERVER INTERNET ROUTES [ALL]
[*destination*]
[*entry*]

Where	Means
ALL	**Specifies that the server will display a list of all internet-routes contained in the operational or permanent database.**
destination	**A variable. Specifies that the server will display the internet-route entry information for a specific destination.**
entry	**Specifies that the server will display only the specific operational or permanent database internet-route entry. Valid values are whole numbers in the range of 1 through 64.**

Example

```
Xyplex>> MONITOR SERVER INTERNET ROUTES ALL

      Address         Gateway        Mask                   Last Modified

1 192.12.119.255  128.6.201.7  255.255.255.0  NET/FIXED 21 Mar 1993 09:22
2 192.12.120.21   128.6.201.8        0.0.0.0  HOST/VAR  24 Mar 19893 13:58*
```

Example SHOW/MONITOR/LIST SERVER INTERNET ROUTES Display.

The first column of the SHOW/MONITOR/LIST SERVER INTERNET ROUTES display lists the entry number for each internet route. The following table describes the remaining columns:

Item (Field)	Description
Address	**Shows the *internet-address* of the destination host or network.**
Gateway	**Shows the *internet-address* of the gateway to which traffic is sent.**
Mask	**Shows the mask that the server uses to determine the network portion of the *internet-addresses* of the entry and the destination of a server operation. For host entries, this value will always be 0.0.0.0.** **Next to this column, you will see combinations of the following values:** **NET** — **indicates that the entry is a network entry.** **HOST** — **indicates that the entry is a host entry.** **FIXED** — **indicates that the server cannot change this entry based on information in an ICMP Routing Redirect message.** **VAR** — **indicates that the server can change this entry based on information in an ICMP Routing Redirect message.**
Last Modified	**Shows the date and time when the entry was created or last modified. An asterisk character (*) following the time indicates that the internet route was learned from an ICMP message from an Internet gateway.**

SHOW/LIST/MONITOR SERVER INTERNET SECURITY

Display a list of all Internet security entries and the ports to which they apply

Notes

Use the SHOW/LIST/MONITOR SERVER INTERNET SECURITY display to view a list of all Internet security entries and the *port-list* for which each entries applies.

Privileges

Non-privileged users can use the SHOWand LIST SERVER INTERNET SECURITY commands. Only users at privileged ports can use the MONITOR SERVER INTERNET SECURITY command.

Syntax

SHOW|LIST|MONITOR SERVER INTERNET SECURITY

Example

```
Xyplex>> SHOW SERVER INTERNET SECURITY

Ports Set to Default Inbound Allow: 1-8
Ports Set to Default Inbound Deny: 9-16

Ports Set to Default Outbound Allow: 1-8
Ports Set to Default Outbound Deny: 9-16

         Internet        Security
Entry    Address            Mask            Access    Dir        Port(s)

 1  192.12.119.206   255.255.0.0           Allow     Outbound     1,4,5

 2  192.13.119.45    255.255.255.0         Allow     Inbound     0,9,16

 3  192.11.110.40    255.255.255.255       Deny      Outbound    1-4,7
```

SHOW/MONITOR/LIST SERVER INTERNET SECURITY DISPLAY.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW SERVER INTERNET SECURITY display:

Item (Field)	Description
Ports Set to Default Inbound Allow	**Shows which ports allow inbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.**
Ports Set to Default Inbound Deny	**Shows which ports deny inbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.**

Ports Set to Default Outbound Allow	**Shows which ports allow outbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.**
Ports Set to Default Outbound Deny	**Shows which ports deny outbound connections to a connection partner when there is no entry in the Internet Security table for the connection partner.**
Entry	**The number of the entry in the port's Internet Security table.**
Internet Address	**The target address of the destination.**
Security Mask	**Describes how to interpret the target address.**
Access	**Either Deny (prevent connection) or Allow (permit connection).**
Dir	**Either Inbound (from the network) or outbound (to the network).**
Port(s)	**Shows the ports which are affected by the entry.**

SHOW/LIST/MONITOR SERVER INTERNET SNMP CHARACTERISTICS

Display information about how SNMP clients are configured on the unit.

Notes

Use the SHOW/LIST/MONITOR SERVER INTERNET SNMP CHARACTERISTICS display to view information about how SNMP clients are configured on the unit.

Privileges

Non-privileged users can use the SHOWand LIST SERVER INTERNET SNMP CHARACTERISTICS commands. Only users at privileged ports can use the MONITOR SERVER INTERNET SNMP CHARACTERISTICS command.

Syntax

SHOW|LIST|MONITOR SERVER INTERNET SNMP CHARACTERISTICS

Example

```
Xyplex> SHOW SERVER INTERNET SNMP CHARACTERISTICS

MAXserver V5.0 Rom 470002 HW 00.00.00 Lat Protocol V5.1 Uptime:  0 03:03:16

Internet Address:  182.12.118.66               Subnet Mask:  255.255.0.0

System Name:
System Location:   Boxborough
System Contact:    Network Administrator

Get Community:     public
Set Community:     public
Trap Community:    public

Get Client 1:                                  Set Client 1:
Get Client 2:                                  Set Client 2:
Get Client 3:                                  Set Client 3:
Get Client 4:                                  Set Client 4:

Trap Client 1:
Trap Client 2:
Trap Client 3:
Trap Client 4:
```

The SHOW/LIST/MONITOR SERVER INTERNET SNMP CHARACTERISTICS Display

SHOW/LIST/MONITOR SERVER INTERNET SNMP CHARACTERISTICS

The following list describes the fields of the SHOW/LIST/MONITOR SERVER INTERNET SNMP CHARACTERISTICS display:

Item (Field)	Description
Internet Address	**The Internet address of the server.**
Domain Name	**The Domain name of the server.**
Domain Suffix	**The default Internet Domain Name Suffix defined for the server.**
System Name	**The server *domain-name*, as defined via the DEFINE SERVER INTERNET NAME command.**
System Location	**Shows the location of the unit. This information is provided for administrative or informational purposes only.**
System Contact	**Shows the name of a system contact for the unit. This information is provided for administrative or informational purposes only.**
Community	**Shows the name of the SNMP community to which the unit belongs. When a community name has been specified for the unit, only SNMP clients (e.g., a Network Operations Center, or NOC) which belong to the same community are permitted to obtain information from (i.e., perform an SNMP get) or set characteristics (i.e., perform an SNMP set) on a unit.**
Client 1 - 4	**Shows the SNMP clients (e.g., a Network Operations Center, or NOC) which are permitted to set characteristics (i.e., perform an SNMP set) on the unit. Default: 0.0.0.0.**

SHOW/MONITOR SERVER INTERNET SNMP COUNTERS

Display statistics about server SNMP activity

Notes

Use the SHOW/MONITOR SERVER INTERNET SNMP COUNTERS display to view statistics about server SNMP activity, and occurrences of error conditions.

Privileges

Non-privileged users can use the SHOW SERVER INTERNET SNMP COUNTERS commands. Only users at privileged ports can use the MONITOR SERVER INTERNET SNMP COUNTERS command.

Syntax

SHOW|MONITOR SERVER INTERNET SNMP COUNTERS

Example

```
Xyplex> SHOW SERVER INTERNET SNMP COUNTERS

MAXserver V5.0 Rom 470002 HW 00.00.00 Lat Protocol V5.1 Uptime:  0 03:07:04

Internet Address:  182.12.118.66               Subnet Mask:  255.255.0.0

Packets Received:                  29      Get Nexts Received:               24
Packets Transmitted:               29      Set Requests Received:             1
Version Errors:                    0       Too Big Errors:                    0
Community Name Errors:             0       No Such Name Errors:               0
Community Use Errors:              0       Bad Value Errors:                  0
ASN Parse Errors:                  0       Read Only Errors:                  0
Type Errors:                       0       General Errors:                    0
Requested Variables:               28      Get Responses Transmitted:        29
Set Variables:                     1       Traps Transmitted:                 0
Get Requests Received:             4
```

The SHOW/MONITOR SERVER INTERNET SNMP COUNTERS Display

The following list describes the fields of the SHOW/MONITOR SERVER INTERNET SNMP COUNTERS display:

Item (Field)	Description
Packets Received	**The number of SNMP packets the server has received.**
Packets Transmitted	**The number of SNMP packets the server has transmitted.**
Version Errors	**The number of syntactically correct SNMP packets received by the server, which were for an unsupported SNMP version.**
Community Name Errors	**The number of SNMP packets received by the server, which used an SNMP community name unknown to the server.**

Community Use Errors	**The number of SNMP packets received by the server, which represented an SNMP operation not allowed by the SNMP community named in the packet.**
ASN Parse Errors	**The number of ASN.1 parsing errors (either in encoding or syntax) the server encountered while decoding received SNMP packets.**
Type Errors	**The number of SNMP packets of unknown packet type that the server has received.**
Requested Variables	**The total number of Management Information Base (MIB) objects that have been retrieved from the server as the result of SNMP Get-Request and Get-Next packets the server received.**
Set Variables	**The number of MIB objects that have been altered as the result of valid SNMP Set-Request packets the server received.**
Get Requests Received	**The number of SNMP Get-Request packets that the server has received and processed.**
Get Nexts Received	**The number of SNMP Get-Next packets that the server has received and processed.**
Set Requests Received	**The number of SNMP Set-Request packets that the server has received and processed.**
Too Big Errors	**The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "tooBig". (The server creates these packets in response to SNMP packets it receives that would generate a response that is too big.)**
No Such Name Errors	**The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "NoSuch Name". (The server generates these packets in response to SNMP packets it receives that contain an invalid object name.)**
Bad Value Errors	**The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "badValue". (The server generates these packets in response to SNMP packets it receives that contain an invalid value.)**
Read Only Errors	**The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "readOnly". (The server generates these packets in response to SNMP packets it receives that attempt to set a value that is read-only.)**
General Errors	**The number of valid SNMP packets generated by the server, for which the value of the ErrorStatus component is "genErr". (The server creates these packets in response to SNMP packets it receives that generate errors other than "tooBig", "NoSuchName", "badvalue", or "readOnly".)**

Get Responses Transmitted	**The number of SNMP Get-Response packets that the server has generated.**
Traps Transmitted	**The number of SNMP Trap packets that the server has generated.**
Authentication Traps	**Indicates whether the server is configured to generate authentication-failure traps.**

SHOW/MONITOR SERVER INTERNET TRANSLATION TABLE

Display the server ARP table

Notes

Use the SHOW/MONITOR SERVER INTERNET TRANSLATION TABLEdisplay to view information about the internet-address to Ethernet address mappings that it has learned. This is commonly referred to as the ARP table.

Privileges

Non-privileged users can use the SHOW SERVER INTERNET TRANSLATION TABLE commands. Only users at privileged ports can use the MONITOR SERVER INTERNET TRANSLATION TABLE command.

Syntax

SHOW|MONITOR SERVER INTERNET TRANSLATION TABLE

Example

```
Xyplex> SHOW SERVER INTERNET TRANSLATION TABLE

MAXserver V5.0 Rom 470002 HW 00.00.00 Lat Protocol V5.1 Uptime:  0 03:09:51

Internet Address:  182.13.118.66
Domain Name:
Domain Suffix:     .XYPLEX.COM



Entry       Ethernet Address        IP Address      Receive TTL     Send TTL
5           08-00-87-00-4B-A2       182.13.118.61       60              2
10          08-00-87-00-3D-5B       182.13.118.11       60             60
```

The SHOW/MONITOR SERVER INTERNET TRANSLATION TABLE Display

The following list describes the fields of the SHOW/MONITOR SERVER INTERNET TRANSLATION TABLE display:

Item (Field)	Description
Internet Address	**The Internet address of the server.**
Domain Name	**The Domain Name of the server.**
Domain Suffix	**The default Domain Name Suffix for the server.**
Entry	**The entry number assigned by the server for each Ethernet address/Internet address pair.**
Ethernet Address	**An Ethernet address that is mapped to a corresponding Internet address in the IP Address column.**

IP Address	**An Internet address that is mapped to a corresponding Ethernet address in the Ethernet Address column.**
Receive TTL	**The minutes remaining until the server discards the entry. This value is reset to its initial setting, 60 minutes, whenever the server receives a packet from the IP Address for the entry.**
Send TTL	**The minutes remaining until the server discards the entry. This value is reset to its initial setting, 60 minutes, whenever the server sends a packet to the IP Address for the entry.**

SHOW/LIST/MONITOR SERVER KERBEROS

Display information about the Kerberos security feature

Notes

Use the SHOW/LIST/MONITOR SERVER KERBEROS display to view information about how the Kerberos security feature is configured on the unit.

Privileges

Non-privileged users can use the SHOWand LIST xxx commands. Only users at privileged ports can use the MONITOR xxx command.

Syntax

SHOW|LIST|MONITOR SERVER KERBEROS

Example

```
Xyplex> SHOW SERVER KERBEROS

MAXserver V5.0   Rom 480001 HW 00.01.00 Lat Protocol V5.1 Uptime:  2 21:34:43

Address:   08-00-87-00-05-D4   Name:   X00504D               Number:     0

Kerberos Security:                       Login

Kerberos Security:         Login
Kerberos Realm:            IXTLAN
Kerberos Master:           DOLLY
         Address:          182.21.118.23
Kerberos Primary Server:   UNIXHOST
         Address:          182.21.118.44
Kerberos Secondary Server: NONE
         Address:          0.0.0.0

Kerberos Ports Enabled:    6
Kerberos Query Limit:      3
Successful Logins:         0        Unsuccessful Logins: 0

Number of users logged in without Kerberos Verification: 9
Unsuccessful attempts to change Kerberos password:       0
Last Kerberos Error:       0        Occurred:

Attempts to access:          Master          Server1          Server2
Successful:                    1               4                0
Unsuccessful:                  0               0                0
```

The SHOW/MONITOR/LIST SERVER KERBEROS Display

The following list describes the SHOW/MONITOR/LIST SERVER KERBEROS display fields:

Item (Field)	Description
Kerberos Security	**The value LOGIN indicates that the server provides Kerberos user verification. The value NONE indicates that the server does not provide Kerberos verification.**
Kerberos Realm	**The name of the Kerberos realm to which the Master and Server hosts are associated.**
Kerberos Master	**The Domain name and Internet address of the Kerberos Master host. The Kerberos Master maintains the Kerberos database and provides information to Server hosts within a realm. A server must query the Master when a user changes a kerberos password.**
Kerberos Primary Server	**The Domain name and Internet address of the primary Server host. The primary Server host is the first Server host to be queried for user verification.**
Kerberos Secondary Server	**The Domain name and Internet address of the secondary Server host. The server queries the secondary Server host if the primary Server host does not respond.**
Kerberos Ports Enabled	**The server ports for which Kerberos user verification has been enabled.**
Kerberos Query Limit	**The maximum number of queries the server can make when attempting to verify a Kerberos ID or change a password.**
Successful Logins	**The number of successful attempts to log on to a server port for which Kerberos user verification is enabled.**
Unsuccessful Logins	**The number of unsuccessful attempts to log on to a server port for which Kerberos user verification is enabled. (That is, the number of times a user entered an incorrect ID or password, and therefore could not log on to the port.) This value does not reflect unsuccessful attempts to query the Server hosts.**
Number of users logged in without Kerberos Verification	**The number of users logged on to ports for which Kerberos user verification has not been enabled.**
Unsuccessful attempts to change Kerberos password	**The number of times a user attempted to change a Kerberos password but did not supply the required information. (The user did not enter the correct value at the "Old password:" prompt, or was unable to correctly verify the new password.) This value does not reflect unsuccessful attempts to query the Master hosts.**

Last Kerberos Error

The error number of the last Kerberos-related error to have occurred, and the date and time that it occurred. The following kerberos errors can appear here:

1	**Principal expired**
2	**Service expired**
3	**Auth expired**
4	**Protocol version unknown**
5	**Wrong master key version**
6	**Wrong master key version**
7	**Byte order unknown**
8	**Principal unknown**
9	**Principal not unique**
10	**Principal has null key**
20	**Generic error from KDC**
21	**Can't read ticket file**
22	**Can't find ticket or TGT**
26	**TGT expired**
31	**Can't decode authenticator**
32	**Ticket expired**
33	**Ticket not yet valid**
34	**Repeated request**
35	**The ticket isn't for us**
36	**Request is inconsistent**
37	**delta_t too big**
38	**Incorrect net address**
39	**Protocol version mismatch**
40	**Invalid msg type**
41	**Message stream modified**
42	**Message out of order**
43	**Unauthorized request**
51	**Current PW is null**
52	**Incorrect current password**
53	**protocol error**
54	**Error returned by KDC**
55	**Null tkt returned by KDC**
56	**Retry count exceeded**
57	**Can't send request**
61	**Not ALL tickets returned**
62	**Incorrect password**
63	**Protocol error**

70	**Other error**
71	**Don't have TGT**
76	**No ticket file found**
77	**Couldn't access tkt file**
78	**Couldn't lock ticket file**
79	**Bad ticket file format**
80	**tf_init not called first**
81	**Bad Kerberos name format**
82	**No Realm defined**
83	**Bad Service**
84	**Cannot allocate packet**
7205	**Time not within 5 minutes of server**

Attempts to access — **The number of successful and unsuccessful attempts by the server to access the Kerberos Master, Primary Server host (Server 1), and Secondary (Server 2) Server host.**

LIST SERVER LOADDUMP CHARACTERISTICS

Display initialization record information

The LIST SERVER LOADDUMP CHARACTERISTICS command displays the initialization parameters in the initialization records you specify.

Privilege Level

List/Nonprivileged Monitor/Privileged

Syntax

LIST SERVER LOADDUMP [*record*|ALL] CHARACTERISTICS

Where	Means
[*record*]	**One or more of the following initialization records:** **PRIMARY** **SECONDARY** **TERTIARY** **ALL** **The PRIMARY initialization record is the default.**

Display

This sample display shows the primary initialization.

```
Xyplex> list server loaddump primary characteristics
```

```
Primary Record:            Enabled
Internet Load Address      140.179.80.133

Internet Load Host         140.179.119.3
Internet Load Gateway      0.0.0.0
Internet Load File         /usr/xyplex/images/xpcsrv20.sys

Software:                  XPCSRV20

Image Load Protocols Enabled: Card, XMOP, MOP, BOOTP, RARP, DTFTP
Dump Protocols Enabled:       XMOP, MOP, BOOTP, RARP
Parameter Protocols Enabled:  NVS, XMOP, MOP, BOOTP, RARP
```

Field	Means
Primary Record	**The status of the initialization record. This example shows the primary record enabled, but an initialization record can be enabled or disabled.**
Internet Load Address	**The Internet address of the host where the terminal server receives its software load image through DTFTP.**

Field	Means
Internet Load Gateway	**The Internet address of a gateway, if the terminal server requires a gateway to reach the Internet load host through DTFTP.**
Internet Load File	**The name and path of the software load image on the Internet host, that the terminal server loads through DTFTP.**
Software	**The CARD/XMOP/MOP software load image file name.**
Image Load Protocols Enabled	**The protocols that the initialization record can use to obtain the software load image.**
Dump Protocols Enabled	**The protocols that the initialization record can use to transmit a memory dump file.**
Parameter Protocols Enabled	**The protocols that the initialization record can use to obtain the parameter file.**

SHOW/LIST/MONITOR SERVER MENU

Display a list of menu entries

Notes

Use the SHOW/LIST/MONITOR SERVER MENU display to view a list of all menu entries stored in the operational or permanent database. The output of these commands includes the menu items and the corresponding TCP/IP-LAT commands. Refer to the *Software Management Guide* for a description of the Simple Menu Interface feature.

Privileges

Non-privileged users can use the SHOWand LIST SERVER MENU commands. Only users at privileged ports can use the MONITOR SERVER MENU command.

Syntax

SHOW|LIST|MONITOR SERVER MENU

Example

```
Xyplex>> SHOW SERVER MENU

1.  Show Characteristics
    SHOW PORT CHARACTERISTICS; SHOW PORT ALT CHAR
2.
.
.
.
9.  Support
    CONNECT SYSTEM_SUPPORT

10.

11.Connect
    TELNET CONNECT 192.12.119.74
.
.
.
20.

MENU PROMPT
MENU CONTINUE PROMPT
```

Example SHOW/LIST SERVER MENU Display.

For each entry shown in the SHOW/LIST SERVER MENU display, the server shows the command shown on the menu to users who are logged on to ports for which the menu interface is enabled. The second line of the entry shows the corresponding Xyplex LAT-TCP/IP command for the menu item.

SHOW/LIST/MONITOR SERVER SCRIPT SERVER

Display a list of script servers

Notes

Use the SHOW/LIST/MONITOR SERVER SCRIPT SERVER display to view a list of all script servers (i.e., hosts that can download a script file to this server). Refer to the *Software Management Guide* for a description of the Network Scripts feature.

Privileges

Non-privileged users can use the SHOWand LIST SERVER SCRIPT SERVER commands. Only users at privileged ports can use the MONITOR SERVER SCRIPT SERVER command.

Syntax

SHOW|LIST|MONITOR SERVER SCRIPT SERVER

Example

```
Xyplex> SHOW SERVER SCRIPT SERVER

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:   08-00-87-00-27-71   Name:   MAX5000               Number:     0

Script Servers:  140.179.80.12        SCRIPTS
                  UNIXHOST.COM        SCRIPTS
```

Example SHOW/MONITOR/LIST SERVER SCRIPT SERVER Display.

For each entry shown in the SHOW/LIST SERVER SCRIPT SERVER display, the server shows internet-address or domain-name of the script server, and the directory path at the script server where it will search for script files.

SHOW|MONITOR SERVER STATUS

Display detailed information about the current, highest, and permitted maximum levels of port activity, service activity, connection activity, and server resources

Notes

Use the SHOW|MONITOR SERVER STATUS display to view detailed information which shows the current, highest (since server initialization), and permitted maximum levels of port activity, service activity, connection activity, and server resources that can be used, as well as some cumulative errors that have occurred since the server was last initialized.

Privileges

Non-privileged users can use the SHOW SERVER STATUS commands. Only users at privileged ports can use the MONITOR SERVER STATUS command.

Syntax

SHOW|MONITOR SERVER STATUS

Example

```
Xyplex>> SHOW SERVER STATUS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  MAX5000              Number:    0

                     Cur High  Max

Active Ports:          1    1    9   Minutes to shutdown:        N/A
Active Users:          1    1    9   Discarded Nodes:              0
Queue Entries          0    0    3   Resource Errors:              0

Available Services:   21   30  N/A   Port Framing Errors:          0
Local Services:        1    1   10   Port Parity Errors:           0
Reachable Nodes:      18   18  100   Port Overrun Errors:          0

Active Circuits:       0    0   16   Primary Host:        FINANCEVAX
Connected Nodes:       0    0   16   Load Address: AA-00-04-00-C8-04
Connected Sessions:    0    0   64   Dump Address: AA-00-04-00-C8-04
% CPU Used:            4   20  100   Console User:    None Available
% Memory Used:        16   16  100

Selftest Status:  Normal
Software Status:  Normal
```

Example MONITOR/SHOW SERVER STATUS Display (Server Loaded by MOP/Xyplex Load Server).

```
Xyplex>> SHOW SERVER STATUS

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  MAX5000              Number:    0

                     Cur High  Max

Active Ports:          1    1    9   Minutes to shutdown:        N/A
Active Users:          1    1    9   Discarded Nodes:              0
Queue Entries          0    0    3   Resource Errors:              0

Available Services:   21   30  N/A   Port Framing Errors:          0
Local Services:        1    1   10   Port Parity Errors:           0
Reachable Nodes:      18   18  100   Port Overrun Errors:          0

Active Circuits:       0    0   16   Primary Host:           UNIXVAX
Connected Nodes:       0    0   16   Load Address:    192.12.119.200
Connected Sessions:    0    0   64   Dump Address:    192.12.119.200
% CPU Used:            4   20  100   Console User:    None Available
% Memory Used:        16   16  100

Selftest Status:  Normal
Software Status:  Normal
```

Example MONITOR/SHOW SERVER STATUS Display (Server Loaded by BOOTP/TFTP Load Server).

This display shows information which indicates how well the server is operating under the current load, and may be helpful in identifying network trouble or port problems. For each server resource listed, the display shows:

Cur — **the level or amount of the resource that is currently in use. (Note that if the maximum value for the resource was changed since the last time the counters were reset to zero, the value in this column may exceed the value in the Max column.)**

High — **the highest amount of the resource that has been used since the server was last initialized. (Note that if the maximum value for the resource was changed since the last time the server was re-initialized, the value in this column may exceed the value in the Max column.)**

Max — **the maximum amount of the resource that can be used (either because of a hardware constraint or because the value shown is the value specified for a server characteristic).**

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW SERVER STATUS display, after the header lines:

Item (Field)	Description
Active Ports	**Shows the number of ports that have interactive sessions or remote-access connections.**
Active Users	**Shows the number of ports that have interactive sessions connected.**
Queue Entries	**Shows the number of connection requests that are queued in the server connection queue.**
Available Services	**Shows the number of LAT services about which the server has retained information in its memory, and are therefore available to users.**
Local Services	**Shows the number of LAT services offered at the server.**
Reachable Nodes	**Shows the number of LAT nodes (computers, other servers, etc) that offer services and are reachable for service connections.**
Active Circuits	**Shows the number of LAT virtual circuits on which the server has active connections with service nodes.**
Connected Nodes	**Shows the number of service nodes with which the server has an established LAT virtual circuit.**
Connected Sessions	**Shows the total number of sessions which the server has currently connected.**
% CPU Used	**Shows the percentage of processing time that the server has used (calculated every second).**
% Memory Used	**Shows the percentage of the server memory pool that is being used to store information for the node and service database, queued requests, and multiple-service sessions.**
Minutes To Shutdown	**Shows the number of minutes remaining until the server re-initializes (or N/A if no INITIALIZE command has been issued).**
Discarded Nodes	**Shows the number of nodes that could not be included in the server node database because the value set for the SERVER NODE LIMIT characteristic has been reached or because of insufficient memory.**
Resource Errors	**Shows the number of times that insufficient server memory prevented the creation of an internal data structure.**
Port Framing Errors	**Shows the total number of bytes received at all ports which had illegally formatted data characters.**
Port Parity Errors	**Shows the total number of bytes received at all ports which had parity errors.**

Port Overrun Errors	**Shows the total number of times that bytes were lost at any port because the server input buffers were full.**
Primary Host	**Shows the name of the host from which the server was last loaded.**
Load Address	**Shows the Ethernet address or *internet-address* of the host from which the server was last loaded.**
Dump Address	**Shows the Ethernet address or *internet-address* of the node that received the last server memory dump.**
Console User	**Shows the Ethernet address of a remote device at which a user has initiated a session with the console port of this server.**
Selftest Status	**Always Normal (you would not be able to see this display otherwise).**
Software Status	**Always Normal (you would not be able to see this display otherwise).**

SHOW/LIST/MONITOR SERVER SUMMARY

Display the identity of the server and the authorized groups that can have access to the server

Notes

Use the SHOW/LIST/MONITOR SERVER SUMMARYdisplay to view a summary showing the identity of the server and the authorized groups that can have access to this server.

Privileges

Non-privileged users can use the SHOWand LIST SERVER SUMMARY commands. Only users at privileged ports can use the MONITOR SERVER SUMMARY command.

Syntax

SHOW|LIST|MONITOR SERVER SUMMARY

Example

```
Xyplex>> SHOW SERVER SUMMARY

MAXserver V5.0 Rom 430001 HW 00.01.00 Lat Protocol V5.1  Uptime:  1 19:27:53

Address:  08-00-87-00-27-71  Name:  MAX5000              Number:     0

Identification:  XYPLEX MAXserver 5000

Server Groups:  0-7, 100-110
```

Example LIST/MONITOR/SHOW SERVER SUMMARY Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW SERVER SUMMARY display:

Item (Field)	Description
Identification	**Shows a text message which identifies the server.**
Server Groups	**Shows the authorized groups that can have access to this server.**

SHOW|LIST SERVER TN3270

Display the names of available TN3270 devices and translation tables

Notes

Use the SHOW|LIST SERVER TN3270 display to view the names of TN3270 devices and translation tables on this server, and whether the SERVER TN3270 PORT KEYMAPS characteristic is enabled or disabled. Refer to the *Software Management Guide* for a description of the Tn3270 feature.

Privileges

Non-privileged users can use the SHOWand LIST TN3270commands.

Syntax

SHOW|LIST SERVER TN3270

Example

```
Xyplex> SHOW SERVER TN3270

  MAXserver V5.0 Rom 41000 HW 00.01.00 Lat Protocol V5.1 Uptime:  5 23:04:17

  Address:  08-00-87-00-4F-A4  Name X004FA4                   Number:    0

  Port Keymaps : Disabled

  Devices : ANSI, VT100, VT220-7, VT220-8

  TranslationTables : USENGLSH
```

Example SHOW/LIST SERVER TN3270 Display.

The following table describes each of the items (fields) of data in the LIST/SHOW SERVER TN3270 display:

Item (Field)	Description
Port Keymaps	**Indicates whether or not the SERVER TN3270 PORT KEYMAPS characteristic is enabled or disabled on this server. This characteristic controls whether or not individual ports can maintain their own copies of keymaps.**
Devices	**Lists the Tn3270 device types available on this server.**
TranslationTables	**Lists the Tn3270 translation tables available on this server.**

SHOW/LIST SERVER TN3270 DEVICE

Display information about enabled Tn3270 devices

Notes

Use the SHOW/LIST SERVER TN3270 DEVICE display to view information about the Tn3270 devices. Refer to the *Software Management Guide* for a description of the Tn3270 feature.

Privileges

Non-privileged users can use the SHOWand LIST SERVER TN3270 DEVICE commands.

Syntax

SHOW|LIST SERVER TN3270 DEVICE *device-name*

Where	Means
device-name	**Specifies that the server will display information about the device you specify in this variable. This information includes the Tn3270 type, the Model type, and the keymap and screenmap escape sequences.**

Example

```
Xyplex>  SHOW SERVER TN3270 DEVICE VT100

MAXserver V5.0B5 Rom 410000 HW 00.01.00 Lat Protocol V5.1 Uptime:  5 23:23:50

Address:   08-00-87-00-4F-A4   Name:   X004FA4               Number:     0

Device: VT100       TerminalType: VT100                  Tn3278Type : MODEL2

Keymap:    3270-Key             KeyCode                      Description

           NEWLINE          :   "0A"                         "LF   "
           TAB              :   "09"                         "TAB  "
           BACKTAB          :   "1B 09"                      "ESCTB"
           CURSORUP         :   "1B 5B 41"                   "KEYUP"
           CURSORLEFT       :   "1B 5B 44"                   "KEYBK"
           CURSORRIGHT      :   "1B 5B 43"                   "KEYFW"
           CURSORDOWN       :   "1B 5B 42"                   "KEYDN"
           HOME             :   "1B 68"                      "ESCh "
           DELETE           :   "7F"                         "DEL  "
           ERASEEOF         :   "05"                         "CTRLe"
           ERASEINPUT       :   "1B 69"                      "ESCi "
           INSERT           :   "1B 7F"                      "ESCDL"
           FLUSHINPUT       :   "1B 66"                      "ESCf "
           REFRESH          :   "1B 72"                      "ESCr "
           CENTSIGN         :   "1B 63"                      "ESCc "
           DUPLICATE        :   "04"                         "CTRLd"
           FIELDMARK        :   "06"                         "CTRLf"
           SCROLL           :   "1B 6C"                      "ESCl "
           STATUS ON/OFF    :   "1B 3F"                      "ESC? "
           RESET            :   "12"                         "CTRLr"
           FASTLEFT         :   "16"                         "CTRLv"
           FASTRIGHT        :   "15"                         "CTRLu"
           SHOWKEYS         :   "18"                         "CTRLx"
           PRINT            :   "10"                         "CTRLp"
           PF1              :   "1B 4F 71"                   "NUM 1"
           PF2              :   "1B 4F 72"                   "NUM 2"
           PF3              :   "1B 4F 73"                   "NUM 3"
           PF4              :   "1B 4F 74"                   "NUM 4"
           PF5              :   "1B 4F 75"                   "NUM 5"
           PF6              :   "1B 4F 76"                   "NUM 6"
           PF7              :   "1B 4F 77"                   "NUM 7"
           PF8              :   "1B 4F 78"                   "NUM 8"
           PF9              :   "1B 4F 79"                   "NUM 9"
           PF10             :   "1B 4F 50"                   "PF1  "
           PF11             :   "1B 4F 51"                   "PF2  "
           PF12             :   "1B 4F 52"                   "PF3  "
           PF13             :   "1B 21"                      "ESC! "
           PF14             :   "1B 40"                      "ESC@ "
           PF15             :   "1B 23"                      "ESC# "
           PF16             :   "1B 24"                      "ESC$ "
           PF17             :   "1B 25"                      "ESC% "
```

Example SHOW/LIST SERVER TN3270 DEVICE Display (part 1 of 2).

```
            PF18              :   "1B 5E"                          "ESC^ "
            PF19              :   "1B 26"                          "ESC& "
            PF20              :   "1B 2A"                          "ESC* "
            PF21              :   "1B 28"                          "ESC( "
            PF22              :   "1B 29"                          "ESC) "
            PF23              :   "1B 5F"                          "ESC_ "
            PF24              :   "1B 2B"                          "ESC+ "
            PA1               :   "1B 2C"                          "ESC, "
            PA2               :   "1B 2E"                          "ESC. "
            PA3               :   "1B 2F"                          "ESC/ "
            SYSREQ            :   "1B 73"                          "ESCs "
            ENTER             :   "0D"                             "ENTER"
            CLEAR             :   "03"                             "CTRLc"
            CURSORSEL         :   "1B 6B"                          "ESCk "
            TEST              :   "1B 74"                          "ESCt "
Screenmap: Terminal Function      HexCode
            EraseEOL          :   "1B 5B 4B"
            ClearScr          :   "1B 5B 32 4A"
            MoveCursor        :   "1B 5B F8 3B FA 48"
            Col132            :   "1B 5B 3F 33 68"
            Col80             :   "1B 5B 3F 33 6C"
            Beep              :   "07"
            BoldOn            :   "1B 5B 30 3B 31 6D"
            BoldOff           :   "1B 5B 30 6D"
            Reset1            :   "1B 5B 3F 38 3B 32 68 1B 3D 1B 5B 30 71"
            Reset2            :   "1B 5B 3F 33 3B 37 3B 31 6C 1B 5B 48"
            Reset3            :   "1B 5B 32 4A 1B 5B 34 69"
            MoveCursor Base   :   1
            SGR               :   Enabled
```

Example SHOW/LIST SERVER TN3270 DEVICE Display (part 2 of 2).

Item (Field)	Description
Device	**The name of the Tn3270 device in the display.**
TerminalType	**The local terminal type.**
Tn3278Type	**The Tn3270 device model that the local terminal emulates during a Tn3270 session.**
Keymap	**The table that follows contains the escape sequences that the terminal server uses to translate entries on the local ASCII keyboard into 3270 display station functions.**
3270-Key	**An IBM display station function.**
KeyCode	**The hexidecimal value for the keyboard escape sequence at the local terminal which corresponds to the IBM display station function.**
Description	**A text description of the keyboard function.**

ScreenMap	**The table that follows contains the escape sequences that the terminal server sends to the local terminal to initiate screen functions such as clear the screen, move the cursor, or set the bold attribute.**
Terminal Function	**The IBM screen function that occurs on the local terminal when the user enters the escape sequence indicated by the corresponding the Hex Code**
Hex Code	**The hexidecimal value of the escape sequence for the IBM terminal function.**

SHOW|LIST SERVER TN3270 TRANSLATIONTABLE

Display EBCDICTOASCII or ASCIITOEBCDIC translation table information

Notes

Use the SHOW|LIST SERVER TN3270 TRANSLATIONTABLE display to view information in the EBCDICTOASCII or ASCIITOEBCDIC portion of the translation table you specify.

Privileges

Non-privileged users can use the SHOWand LIST SERVER TN3270 TRANSLATIONTABLE commands.

Syntax

SHOW|LIST SERVER TN3270 TRANSLATIONTABLE *trans-name table*

Where	Means
trans-name	**Specifies that the server will display information in the translation table you specify in this variable.**
table	**Specifies which porition of the translation table the server will display. The values you can specify are ASCIITOEBCDIC or EBCDICTOASCII.**

Example

```
Xyplex> SHOW SERVER TN3270 TRANSLATIONTABLE USENGLSH ASCIITOEBCDIC

TranslationTable Name: USENGLSH               Table: ASCIITOEBCDIC
     0x  1x  2x  3x  4x  5x  6x  7x  8x  9x  ax  bx  cx  dx  ex  fx
     ------------------------------------------------------------
x0 | 00  00  40  f0  7c  d7  79  97  00  00  00  00  00  00  00  00
x1 | 00  00  5a  f1  c1  d8  81  98  00  00  00  00  00  00  00  00
x2 | 00  00  7f  f2  c2  d9  82  99  00  00  00  00  00  00  00  00
x3 | 00  00  7b  f3  c3  e2  83  a2  00  00  00  00  00  00  00  00
x4 | 00  00  5b  f4  c4  e3  84  a3  00  00  00  00  00  00  00  00
x5 | 00  00  6c  f5  c5  e4  85  a4  00  00  00  00  00  00  00  00
x6 | 00  00  50  f6  c6  e5  86  a5  00  00  00  00  00  00  00  00
x7 | 00  00  7d  f7  c7  e6  87  a6  00  00  00  00  00  00  00  00
x8 | 00  00  4d  f8  c8  e7  88  a7  00  00  00  00  00  00  00  00
x9 | 00  00  5d  f9  c9  e8  89  a8  00  00  00  00  00  00  00  00
xa | 00  00  5c  7a  d1  e9  91  a9  00  00  00  00  00  00  00  00
xb | 00  00  4e  5e  d2  4a  92  c0  00  00  00  00  00  00  00  00
xc | 00  00  6b  4c  d3  e0  93  6a  00  00  00  00  00  00  00  00
xd | 00  00  60  7e  d4  5a  94  d0  00  00  00  00  00  00  00  00
xe | 00  00  4b  6e  d5  5f  95  a1  00  00  00  00  00  00  00  00
xf | 00  00  61  6f  d6  6d  96  00  00  00  00  00  00  00  00  00
```

Example SHOW/LIST SERVER TN3270 TRANLATIONTABLE ASCIITOEBCDIC Display

```
Xyplex> SHOW SERVER TN3270 TRANSLATIONTABLE USENGLSH EBCDICTOASCII

TranslationTable Name: USENGLSH              Table: EBCDICTOASCII
     0x  1x  2x  3x  4x  5x  6x  7x  8x  9x  ax  bx  cx  dx  ex  fx
    ------------------------------------------------------------
x0 | 20  20  20  20  20  26  2d  20  20  20  20  20  7b  7d  5c  30
x1 | 20  20  20  20  20  20  2f  20  61  6a  7e  20  41  4a  20  31
x2 | 20  20  20  20  20  20  20  20  62  6b  73  20  42  4b  53  32
x3 | 20  20  20  20  20  20  20  20  63  6c  74  20  43  4c  54  33
x4 | 20  20  20  20  20  20  20  20  64  6d  75  20  44  4d  55  34
x5 | 20  20  20  20  20  20  20  20  65  6e  76  20  45  4e  56  35
x6 | 20  20  20  20  20  20  20  20  66  6f  77  20  46  4f  57  36
x7 | 20  20  20  20  20  20  20  20  67  70  78  20  47  50  58  37
x8 | 20  20  20  20  20  20  20  20  68  71  79  20  48  51  59  38
x9 | 20  20  20  20  20  20  20  60  69  72  7a  20  49  52  5a  39
xa | 20  20  20  20  5b  21  7c  3a  20  20  20  20  20  20  20  20
xb | 20  20  20  20  2e  24  2c  23  20  20  20  20  20  20  20  20
xc | 20  20  20  20  3c  2a  25  40  20  20  20  20  20  20  20  20
xd | 20  20  20  20  28  29  5f  27  20  20  20  20  20  20  20  20
xe | 20  20  20  3b  2b  3b  3e  3d  20  20  20  20  20  20  20  20
xf | 20  20  20  2a  7c  5e  3f  22  20  20  20  20  20  20  20  20
```

Example SHOW/LIST SERVER TN3270 TRANSLATIONTABLE EBCDICTOASCII Display

Item (Field)	Description
TranslationTable Name	**The name of Tn3270 language translation table.**
Table	**The portion of the translation table in the display. This can be the ASCIITOEBCDIC portion or the EBCDICTOASCII portion.**

SHOW/LIST/MONITOR SERVER XREMOTE

Display terminal server Xremote characteristics

Notes

Use the SHOW/LIST/MONITOR SERVER XREMOTE commands to display Xremote characteristics on the terminal server, including the primary and secondary font servers.

Privilege Level

SHOW/LIST, Non-privileged MONITOR, Non-privileged

Syntax

SHOW/LIST/MONITOR SERVER XREMOTE

```
Address:     08-00-87-00-4F-4F     Name:  X004F4F       Number:

Xremote Primary Font Server:       HOST.EAST.COM
        Address:                   130.124.80.112

Xremote Secondary Font Server:     HOST.WEST.COM
        Address:                   130.124.80.112

Xremote Ports Enabled              3, 4, 5
Current Number of Xremote Sessions: 3        Current Number of Xclients: 3

Attempts to access                 Server1   Server2
Successful                            2         1
Unsuccessful                          0         1
```

Example Show/List/Monitor Server Xremote Display

Field	Means
Xremote Primary Font Server	**The domain name of the primary font server.**
Address	**The Internet address of the primary font server.**
Xremote Secondary Font Server	**The domain name of the secondary font server.**
Address	**The Internet address of the secondary font server.**
Xremote Ports Enabled	**The ports on the terminal server with the Xremote characteristic enabled.**
Current Number of Xremote Sessions	**The number of Xremote sessions currently established at the ports with the Xremote characteristic enabled. There is one Xremote session per active Xremote port.**

Field	Means
Current Number of Xclients	**The total number of Xclient processes on all ports of the terminal server. This value reflects the number of open X windows, one XDM manager and one window manager for each port with Xremote enabled.**
Attempts to access	**The number of successful and unsuccessful attempts to reach the primary font server and the secondary font server, if you have defined them.**

SHOW/LIST/MONITOR SERVICES CHARACTERISTICS

Display current values for service characteristics

Notes

Use the SHOW/LIST/MONITOR SERVICES CHARACTERISTICS display to view the current values for service characteristics that have been defined by the terminal server manager (using SET/DEFINE SERVICE commands).

Privileges

Secure and non-privileged users can use the SHOW and LIST SERVICES CHARACTERISTICS command, unless the DEFINE/SET PORT LIMITED VIEW characteristics is ENABLED. Only users at privileged ports can use the MONITOR SERVICES CHARACTERISTICS command.

Syntax

SHOW | MONITOR SERVICE	**[*service-name*]**	**[CHARACTERISTICS]**
	[LOCAL]	**[CHARACTERISTICS]**
	[ALL]	**[CHARACTERISTICS]**
LIST SERVICE	**[*service-name*]**	**[CHARACTERISTICS]**
	[LOCAL]	**[CHARACTERISTICS]**

Where — Means

service-name — **Specifies that the terminal server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made.**

You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.

ALL — **Specifies that the terminal server will display the requested information about all services that are available on the network to the user at the port where the request is made.**

LOCAL — **Specifies that the terminal server will display the requested information about all services that are available locally on the terminal server to the user at the port where the request is made.**

Example

```
Xyplex> SHOW SERVICES CHARACTERISTICS ALL

Service: FINANCEVAX                              08 Dec 1988  17:55:59

Identification:  Corporate MicroVAX II



Service: PRINTER                                  08 Dec 1988  17:55:59

Identification:  Terminal Server Printer Queue

Ports: 2, 7

Rating: 127

Enabled Characteristics:

Connections, Queueing

Service: MODEM                                    08 Dec 1988  17:56:00

Identification: MAX5000 Modem Port

Ports: 6

Rating: 255

Enabled Characteristics:

Connections, Password
```

Example LIST/MONITOR/SHOW SERVICES CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the LIST/MONITOR/SHOW SERVICES CHARACTERISTICS display:

Item (Field)	Description
Service	**Shows the name of a service available on the network.**
Identification	**Shows a text string which identifies the service, or describes how to use the service.**
Ports	**Shows the numbers of the port(s) on the terminal server where locally offered services are available.**
Rating	**Shows the relative availability of the service. If there are any available ports which offer the service, then the rating shown is proportional to the number of available ports. If there are no available ports that offer the service, then the rating shown is zero (0).**

Enabled Characteristics

Shows the characteristics that have been enabled for the local service(s) using DEFINE/SET SERVICE commands. The possible values which can be shown are:

Connections **Shows that the server allows connections to the service.**

Password **Shows that the server requires that the requester of the service provide a password, specified by the terminal server manager, before the server permits access to the service.**

Queuing **Shows that the server will place connection requests that cannot be satisfied immediately into a connection queue.**

SHOW/MONITOR SERVICES STATUS

Display detailed information operation and availability of services

Notes

Use the SHOW/MONITOR SERVICES STATUS display to view detailed information about the operational condition and availability of services that are available on the network and/or locally available on the terminal server.

Privileges

Secure and non-privileged users can use the SHOW SERVICES STATUS command, unless the DEFINE/SET PORT LIMITED VIEW characteristics is ENABLED. Only users at privileged ports can use the MONITOR SERVICES STATUS command.

Syntax

SHOW|MONITOR SERVICE [*service-name*] STATUS
[LOCAL]
[ALL]

Where Means

service-name **Specifies that the terminal server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made.**

You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.

ALL **Specifies that the terminal server will display the requested information about all services that are available on the network to the user at the port where the request is made.**

LOCAL **Specifies that the terminal server will display the requested information about all services that are available locally on the terminal server to the user at the port where the request is made.**

Example

```
Xyplex> SHOW SERVICE STATUS

Service PRINTER -    Available

Node Name           Status   Rating  Identification

MAX5000             Reachable   255  Terminal Server Printer Queue

Service LASER -     Available

Node Name           Status   Rating  Identification

MAX5000             Reachable   127  Shared Laser Printer

Service FINANCEVAX - Available

Node Name           Status   Rating  Identification

FINANCEVAX        5 Connected   72  Corporate MicroVAX II
```

Example MONITOR/SHOW SERVICES STATUS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVICES STATUS display:

Item (Field)		Description
Service		**Shows the name of a service available on the network.**
Node Name		**Shows the name of the node where the service is offered.**
Status		**Shows whether or not the service is currently reachable or available. The possible values which can be shown include:**
	***n* Connected**	**Shows that the service is reachable, and that the server has n currently active sessions with this service.**
	Reachable	**Shows that the service is reachable, and that the server has no currently active sessions with the service.**
	Unknown	**Shows that the service was available but now may be unavailable. This could be because the server has not recently received a multicast announcement from the service node(s) which offer(s) the service.**
	Unreachable	**Shows that an active session, or attempt to connect a session has timed out. A service node can also signal that it is unreachable.**
Rating		**Shows the relative capacity of the service to accept additional sessions.**
Identification		**Shows a text string which identifies the service or describes how to use the service.**

SHOW/MONITOR SERVICES SUMMARY

Display a one-line summary about the availability of services

Notes

Use the SHOW/MONITOR SERVICES STATUS display to view a one-line summary about the availability of each service that is available on the network and/or locally available at the terminal server.

Privileges

Secure and non-privileged users can use the SHOW SERVICES SUMMARY command, unless the DEFINE/SET PORT LIMITED VIEW characteristics is ENABLED. Only users at privileged ports can use the MONITOR SUMMARY STATUS command.

Syntax

SHOW|MONITOR SERVICE [*service-name*] SUMMARY
[LOCAL]
[ALL]

Where Means

service-name

Specifies that the terminal server will display the requested information about one or more specific services that are available on the network to the user at the port where the request is made.

You can specify a wildcard character to select a subset of the *service-names* to be displayed. The asterisk symbol (*) is the wildcard character. For example, if one types SHOW SERVICES AB*, the server will display all accessible *service-names* whose names start with AB. SHOW SERVICES A*BC displays accessible *service-names* whose names start with A and end with BC.

ALL

Specifies that the terminal server will display the requested information about all services that are available on the network to the user at the port where the request is made.

LOCAL

Specifies that the terminal server will display the requested information about all services that are available locally on the terminal server to the user at the port where the request is made.

Example

```
Xyplex> SHOW SERVICE SUMMARY

Service Name        Status       Identification

PRINTER             Available    Terminal Server Printer Queue
LASER               Available    Shared Laser Printer
FINANCEVAX          Available    Corporate MicroVAX II
MODEM               Available
```

Example MONITOR/SHOW SERVICES SUMMARY Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVICES SUMMARY display:

Item (Field)	Description
Service Name	**Shows the name of a service on the network.**
Status	**Shows the whether or not the service is currently reachable or available. The possible values which can be shown include:**
	Available — **Shows that at least one service node that offers the service has the status REACHABLE.**
	n Connected — **Shows that the service is reachable, and that the server has n currently active sessions with this service.**
	Unavailable — **Shows that all service nodes that offer the service have the status UNREACHABLE.**
	Unknown — **Shows that none of the service nodes that offer the service have the status REACHABLE, and that at least one of these service nodes has the status UNKNOWN.**
Identification	**Shows a text string which identifies the service, or describes how to use the service.**

SHOW|MONITOR SESSIONS

Display information about service sessions for server ports.

Notes

Use the SHOW/MONITOR SESSIONS command to display information about service sessions for server ports.

Privileges

Secure and non-privileged users can use the SHOW SESSIONS command. Only users at privileged ports can use the MONITOR SESSIONS command. SECURE users can only display information about the port they are logged on to

Syntax

SHOW|MONITOR SESSIONS [PORT *port-list*]
[ALL]

Where	Means
PORT	**Specifies that you will display service session information about one or more ports.**
port-list	**Specifies the port(s) about which the requested information will be displayed. The default is the port you are currently logged on to.**
ALL	**Specifies that you will display service session information about all ports on the server.**

Example

```
Xyplex>> SHOW SESSION ALL

Port 1:  J. Smith         Service Mode     Current Session 1
- Session 1: Connected       Interactive   FINANCEVAX (FINANECEVAX)
- Session 2: Connected       Interactive   192.12.119.200
            [Do Echo]  [Won't Echo]  [Won't Binary]  [Don't Binary]
- Session 3:  Connected      Interactive  ABCDEFGHIJKLMNOPQRSTUVWXYZ.ABCDEF*
[Do Echo]  [Won't Echo]  [Won't Binary]  [Don't Binary]

Port 8:  (Remote)         Service Mode     Current Session 1
- Session 1: Wait         Interactive      (Remote Connect)
```

Example MONITOR/SHOW SESSIONS Display.

In the session display, the first line of information for each port shows port-related information. The line(s) which follow the port-related information list(s) active session information. When a session is terminated, the information for the session is removed and replaced by the information below it in the display. The following table describes the MONITOR/SHOW SESSIONS display:

Item (Field)		Description
Port Information		
Port n		**Shows the number of the physical server port, about which the system is displaying information.**
Username		**Shows the name given by the user to log on to the port, the name given to the port using the PORT USERNAME characteristic, or "(Remote)" for ports which have a remote connection (i.e., a host-initiated connection).**
Mode		**Shows the current port mode (either Local Mode or Service Mode).**
Current Session n		**Shows the number of the currently active session.**
Session Information		
Session n		**Shows the number of the session.**
Status		**Shows the current status of the session. The values that can be displayed are:**
	Available	**Shows that a port, whose ACCESS characteristic is set to REMOTE or DYNAMIC, is not busy.**
	Connected	**The port is currently connected to a service.**
	Disconnecting	**Shows that a session is disconnecting from a service.**
	Dealloc	**The server is deallocating the resources from a session.**
	Fail 2	**Shows that a connection attempt has failed.**
	FWait	**The session is waiting for an internal resource in order to indicate to the software that a connection attempt has failed.**
	Quit	**Shows that a session has been disconnected.**
	QWait	**The session is waiting for an internal resource in order to indicate to the software that a session has been disconnected.**
	Retry	**The session is retrying a connection.**
	Slot	**The session is trying to find a LAT slot on the virtual circuit for this session.**
	Start	**The server is allocating resources for this session.**
	Status	**The session is sending the status of a connection (accepted or rejected) to the software.**

	SWait	**The session is waiting for an internal resource in order to indicate the status of a connection (accepted or rejected) to the software.**
	Wait	**The server is allocating resources for a remote session.**
Service Mode	**Shows the service mode for the session. Valid service modes are:**	
	Interactive	**The server recognizes all special characters.**
	Passall	**The server passes all characters as data.**
	Pasthru	**The server recognizes the XON and XOFF characters, but passes all other characters on as data.**
	Transparent	**The server will initially set all sessions so that a Telnet session will ignore Telnet option messages received from a remotely initiated session and will not send any Telnet option messages from the locally initiated session, in addition to disabling all switching characters, Telnet command characters, and XON/XOFF flow control recognition. For a LAT session, the server tells its partner it is PASSALL but acts locally as if it were PASTHRU.**
Destination (node)	**Shows the currently active LAT service or Telnet destination associated with a session. For LAT services, the display includes within parentheses the name of the service node. For a remote-access connection to the port, the service name is that of the LAT service sought by the requesting node and the name within parentheses is that of the requesting node. Note that if the destination is a domain-name which is too long to fit on the display, the name displayed is truncated and indicated by asterisk (*).**	
Telnet options	**If there is a second line of session information, it shows the Telnet options that have been negotiated for the session. The Telnet Echo and Binary options may be shown. The verbs "Do" and "Don't" indicate whether or not the server will perform option. The verbs "Will" and "Won't" whether or not the connection partner will perform the option.**	

SHOW UNIT

Display hardware type, version, ROM version and software version, level, and protocol(s) available on the unit.

Notes

Use the SHOW UNIT command to display the hardware type, version, ROM version and software version, level, and protocol(s) available on the unit.

Privileges

Secure

Syntax

SHOW UNIT

Example

```
Xyplex> SHOW UNIT

Hardware Type:       42
Hardware Revision:   00.01.00
ROM Revision:        430001
Software Type:       Terminal Server Level 3
Software Revision:   V5.0
Enabled Protocol(s): LAT, TELNET, RLOGIN, SNMP, KERBEROS

Enabled Feature(s):  HELP, INTERNET SECURITY, KERBEROS, MENU, MULTISESSIONS
```

Example SHOW UNIT Display.

The following table describes each of the columns in the SHOW UNIT display:

Item (Field)	Description
Hardware Type *device-type*	**The Xyplex-assigned hardware type for the unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of available *device-types*.**
Hardware Revision *xx.yy.zz*	**Shows the version of the terminal server hardware, where *xx* indicates the version of the terminal server cards, *yy* indicates the type of the MAXserver or Network 9000 chassis, and *zz* indicates the version of the MAXserver or Network 9000 chassis.**
ROM Revision *xxxxxx*	**Shows the version, *xxxxxx*, of terminal server ROM software.**

Software Type: Terminal Server Level *n*	**Indicates the type of features that are available on this Xyplex unit. The value for *n* has the following meaning:** **1 MX-TSERV-J8 without V5.0 or subsequent enhancements.** **2 MX-TSERV-J8 with only Internet Security and Telnet Console enhancements, but no other enhancements.** **3 All other software products running 1 Megabyte load image.** **4 Products running Multi-Megabyte load images** **Refer to the *Software Kit Information* supplied with your software kit for a current list of features that are supported on various types of Xyplex products.**
Software Revision *x.yz*	**Shows the version of Xyplex TCP/IP-LAT software, where *x* indicates the major revision level, *y* indicates the minor revision level, and *z* is a letter/number combination indicating that the software is an Alpha (A), Beta (B), or Special (S) software release.**
Enabled Protocol(s)	**Indicates which protocols (for example, LAT, TELNET, SNMP, RLOGIN, TN3270, or Kerberos protocols) are enabled for this unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of protocols that are supported on various types of Xyplex products.**
Enabled Feature(s)	**Indicates which features (for example, HELP, INTERNET SECURITY, Kerberos , MENU, or MULTISESSIONS features) are enabled for this unit. Refer to the *Software Kit Information* supplied with your software kit for a current list of features that are supported on various types of Xyplex products.**

SHOW/MONITOR USERS

Display which ports are logged on, and the name of the user who is logged on to the port

Notes

Use the SHOW/MONITOR USERS command to determine which ports are logged on, and the name of the user who is logged on to the port.

Privileges

Non-privileged users can use the SHOW USERScommands. Only users at privileged ports can use the MONITOR USERS command.

Syntax

SHOW|MONITOR USERS

Example

```
Xyplex>> SHOW USERS

                                          21 Nov 1993  16:00:41

Port    Username            Status          Service

  1     J. Smith            Executing Cmd

  8     (Remote)            Connecting      (Remote Connect)
```

Example MONITOR/SHOW USERS Display.

The following table describes each of the columns in the MONITOR/SHOW USERS display:

Item (Field)	Description
Port	**Shows the number of the physical terminal server port, about which the system is displaying information.**
Username	**This column lists the name given by the user to log on to the port, the name given to the port using the PORT USERNAME characteristic, or "(Remote)" for ports which have a remote connection (i.e., a host-initiated connection).**
Status	**Shows the current status of the port. The possible values that will be displayed are:**
Autobaud	**The port is being autobauded.**
Available	**A port, whose PORT ACCESS characteristics is set to REMOTE or DYNAMIC, is not busy.**
Check Modem	**The port is verifying that modem signals are properly asserted.**

Check Connect	**The port is determining the status (accepted or rejected) of a pending connection.**
Connected	**The port is currently connected to a LAT service or Telnet destination.**
Connect Wait	**The port is waiting to retry a connection attempt (used when PORT AUTOCONNECT is set to ENABLED).**
Connecting	**The port is currently attempting to connect to a LAT service or Telnet destination.**
Dialback Wait	**The Port is waiting for the remote modem to answer a dial-back call.**
Disconnected	**Shows that a session was disconnected (for example, for being inactive for too long).**
Disconnecting	**Shows that a session is disconnecting from a LAT service or Telnet destination.**
Executing Cmd	**The port is executing a command from the terminal server local command mode.**
Finding Script	**The port is searching for a script file via TFTP read requests.**
First Dialback Login	**The port is making its first attempt to locate a dial-back script.**
Idle	**Shows that the port is not in use.**
Loading Script	**The port has located a script file and is receiving the file from the script server.**
Local Mode	**The port is logged on to the server, and is in the local command mode.**
Locked	**Shows that the user has used the LOCK command to disable the port.**
Login	**The port is waiting for the user to enter a login or Kerberos password.**
Login Wait	**The port has been disabled (for 60 seconds) because an incorrect password has been entered, or because a dial-back attempt has failed.**
Logout	**The port is being logged out.**

Password	**The port is waiting to enter the password that is required by a password-protected LAT service.**
Reset	**The port is reverting to its stored configuration.**
Retry Connect	**The port is trying to connect to a service that was previously unavailable (used when PORT AUTOCONNECT is set to ENABLED).**
Running Script	**Shows that the port is executing the commands contained in a script file.**
Second Dialback Login	**The port is making its second attempt to locate a dial-back script (the port searches the directory path "above" the path specified for this script server).**
Slip	**The port is a SLIP port.**
Suspended	**The user has entered the local-switch character, and the session is being suspended.**
Test Wait	**The port is performing a TEST SERVICE command.**
Test Out	**The port is outputting the results of a TEST SERVICE command.**
Wait Input	**The port is at the local prompt (waiting for the user to enter a command).**
Wait Logout	**The port is waiting for modem control signals to be deasserted.**
Wait Output	**The port is completing display output before logging out.**
Wait Queue	**A connection request from this port is in a queue.**
Wait Session	**The session is being disconnected.**

Service **Shows the currently active LAT service or Telnet destination, or the service connection that was interrupted when the user entered local mode. If a remote connection has been formed with the port, the service will be displayed as (Remote Connect).**

SHOW XPRINTER

View Available Novell Printer Servers

The SHOW/LIST XPRINTER PORTS command shows you the names of all Novell printer servers that are assigned to local Xyplex terminal server or printer server ports.

Notes

You use the Novell PCONSOLE utility to create Novell printer servers. (Do not confuse the term Novell printer server with a Xyplex printer server, such as a MAXserver 1450 or 1400A Printer Server unit.) Novell printer servers can be assigned to a serial or parallel port on a Xyplex terminal server or printer server. You can view the name of any Novell printer server that is assigned to a port on a Xyplex terminal server or printer server using this command.

Refer to the *Software Management Guide* for a discussion of Novell printing in the XPRINTER environment.

Privilege Level

Non-privileged

Syntax

SHOW XPRINTER

Example

```
Xyplex> SHOW XPRINTER

 Available Print Servers

ENGINEERING_PRINTER_SERVER
MANUFACTURING_PRINTER_SERVER
```

Example SHOW XPRINTER Display

SHOW/LIST XPRINTER PORTS

View Status of XPRINTER Ports

The SHOW/LIST XPRINTER PORTS command shows you the status of ports which have local XPRINTER services.

Notes

Novell printer servers can be mapped to a physical port on a terminal server or printer server. The port can be either a serial port or a parallel port. Each Xyplex terminal server or printer server port can be connected to only one Novell printer server. You can view the status of XPRINTER activity using the SHOW/LIST XPRINTER PORTS command.

Refer to the *Software Management Guide* for a discussion of Novell printing in the XPRINTER environment.

Privilege Level

Non-privileged

Syntax

SHOW
LIST XPRINTER PORTS [*port-list*]
[ALL]

Where	Means
port-list	**represents the Xyplex terminal server or printer server ports which have local XPRINTER services assigned to them. If you want to view the status of more than one port, you can specify the individual port-numbers separated by commas or specify a range of port-numbers separated by a hyphen, or a combination of both (do not include spaces). For example, the *port-list*: 1,3-4 refers to the individual ports: 1, 3, and 4.**
ALL	**shows the status of all Xyplex terminal server or printer server ports which have local XPRINTER services assigned to them.**

Example

```
Xyplex> SHOW XPRINTER PORTS 1-4

Port  Status        Print Server                                Printer #

 1    IDLE
 2    IDLE
 3    IDLE          PRINTER                                           3
 4    IDLE
```

Example SHOW/LIST XPRINTER PORTS Display

TELNET CONNECT

Establish a session between your port and a Telnet destination

Notes

Use the TELNET CONNECT command to establish a session by creating a virtual connection between your port (terminal) and a Telnet destination. When you use the TELNET CONNECT command, without specifying a domainname/ internet-address and telnet-port-number, the terminal server will attempt to establish a session with a Telnet preferred destination, when one has been defined.

Privileges

Secure

Syntax

TELNET [CONNECT] **[*domain-name*[:*telnet-port-number*]]**
[*internet-address*[:*telnet-port-number*]]

Where	Means
CONNECT	**An optional keyword.**
domain-name	**Specifies the logical name of the Telnet destination that will be the connection partner in a session with the port which you are logged on to. If the specified domain-name is not a fully qualified domain-name, the specified name will be concatenated with the default Internet domain-name-suffix.** **Note that the first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.**
internet-address	**Specifies the identity or location on the network of the Telnet destination that will be the connection partner in a session with the port which you are logged on to.**
:telnet-port-number	**Specifies the number of the target Internet protocol or physical port number that is used in the session between the port you are logged on to and the connection partner (e.g., host or terminal server). The colon character (:) is required as syntax to separate the telnet-port-number from the domain-name or internet-address. The default value is specified by the PORT TELNET DEFAULT PORT characteristic.**

Examples

1. `Xyplex> TELNET CONNECT FINANCESUN.XYPLEX.COM`

   Meaning: Establish a session between this port and the Telnet destination whose *domain-name* is FINANCESUN.XYPLEX.COM. Note that the user did not specify a *telnet-port-number*. The terminal server will use the default *telnet-port-number* (defined by the PORT TELNET DEFAULT PORT characteristic).

2. `Xyplex> TELNET 128.10.2.30:23`

   Meaning: Establish a session between this port and the Telnet destination whose *internet-address* is 128.10.2.30. Note that the user specified a *telnet-port-number* (23 in this case).

3. `Xyplex> TELNET CONNECT`

   Meaning: Establish a session between this port and the preferred Telnet destination that the user or terminal server manager has defined for the port.

TELNET CONNECT PORT

Establish a Telnet session to a port other than the port you are currently logged on to.

Notes

Use the TELNET CONNECT PORT command to establish a session by creating a virtual connection between a terminal server port (this is called the "target" port), and a Telnet destination. The target port is usually a port other than the port you are currently logged on to.

To use this command, you must specify the name of a Telnet destination. This can be done either by the TELNET CONNECT PORT command, or by defining a dedicated or preferred service for the target port. The target port can not have a session in progress (you can terminate the session using the LOGOUT PORT or DISCONNECT PORT command).

Privileges

Privileged

Syntax

TELNET [CONNECT] [PORT *port-number*] [*domain-name*[:*telnet-port-number*]]
[*internet-address*[:*telnet-port-number*]]

Where	Means
CONNECT	**An optional keyword.**
PORT	**Specifies that you will connect a target port to a Telnet *domain-name/internet-address* and *telnet-port-number*.**
port-number	**Specifies the number of the target terminal server port which will be connected to a Telnet *domain-name/internet-address* and *telnet-port-number*.**
domain-name	**Specifies the logical name of the host or server that will be the connection partner in a session with the target port. If the specified *domain-name* is not a fully qualified *domain-name*, the specified name will be concatenated with the default Internet *domain-name-suffix*.** **Note that the first time the server attempts to connect to any *domain-name* (following initialization) takes 2 seconds to occur because the server must locate a Domain Name Server and then attempt the connection. Subsequent attempts to connect to a *domain-name* occur with no delay, because the server already knows the location of a Name Server.**
internet-address	**Specifies the identity or location on the network of the host or terminal server that will be the connection partner in a session with the target port.**

:telnet-port-number **Specifies the number of the target Internet protocol or physical port number that is used in the session between the target port and the connection partner (i.e., the Telnet destination). Note that the colon character (:) is required to separate the *telnet-port-number* from the *domain-name* or *internet-address*.**

Examples

1. `Xyplex>> TELNET CONNECT PORT 5 LASER`

   Meaning: Establish a session between the target port (port 5) and the host or terminal server whose domain-name is LASER.

2. `Xyplex>> TELNET PORT 5`

   Meaning: Establish a session between the target port (port 5) and the dedicated or preferred service, and default telnet-port-number (defined by the PORT TELNET DEFAULT PORT characteristic) that the user has defined for the port.

3. `Xyplex>> TELNET CONNECT PORT 5 FINANCEVAX.XYPLEX.COM`

   Meaning: Establish a session between the target port (port 5) and the host or terminal server whose domain-name is FINANCEVAX.XYPLEX.COM. Note that the user did not specify a telnet-port-number. The terminal server will use the default telnet-port-number (defined by the PORT TELNET DEFAULT PORT characteristic).

4. `Xyplex>> TELNET CONNECT PORT 5 128.10.2.30:23`

   Meaning: Establish a session between the target port (port 5) and the host or terminal server whose internet-address is 128.10.2.30. Note that the user specified a telnet-port-number (23).

TELNET CONSOLE

Establish a Telnet session with the management (virtual) port

Notes

This command enables a user to access the remote console port of a terminal server (port 0) via Telnet. While connected to port 0, the user interface is identical to the interface when the REMOTE CONSOLE command is used. The target console port cannot have a session in progress. Once you are connected to the remote console port of a terminal server, you can connect to another terminal server's remote console port via Telnet. (You cannot access another remote console port this way using the REMOTE CONSOLE command.)

Additionally, you can suspend a Telnet session with the remote console port of one terminal server (e.g., by pressing the BREAK key) and then initiate a session with another terminal server's remote console port. You can then suspend that Telnet session and resume the original session, or initiate a session with the remote console port of a different terminal server.

The Console LED will remain lit whenever there is either a local or remote console session.

The following port characteristics are predefined for the remote console port of a terminal server. You cannot change the settings for these characteristics.

Characteristic	Setting
ACCESS	LOCAL
AUTOBAUD	DISABLED
BREAK	DISABLED
CHARACTER SIZE	8
DEDICATED SERVICE	NONE
DIALUP	DISABLED
DSRLOGOUT	DISABLED
DTRWAIT	DISABLED
FLOW CONTROL	XON
INPUT FLOW CONTROL	ENABLED
INPUT SPEED	9600
MODEM CONTROL	DISABLED
OUTPUT FLOW CONTROL	ENABLED
OUTPUT SPEED	9600
PARITY	NONE
SPEED	9600

Privileges

Non-privileged

Syntax

TELNET CONSOLE **[*internet-address*[:*telnet-port-number*]]**
[*domain-name*[:*telnet-port-number*]]

Where	Means
internet-address	**The identity or location on the network of the Telnet destination to which you want to establish a session.**
domain-name	**The logical name of the destination to which you want to establish a Telnet session.**
:telnet-port-number	**The physical port number to which you want to establish a Telnet session. The default is 2000.**

Examples

1. `Xyplex>>TELNET CONSOLE 117.29.10.30`

   Meaning: Establish a Telnet session with the remote console port (in this case port 0) of the terminal server whose Internet address is 117.29.10.30.

2. `Xyplex>>TELNET CONSOLE FINANCEVAX.XYPLEX.COM`

   Meaning: Establish a Telnet session with the remote console port of the terminal server whose domain name is FINANCEVAX.XYPLEX.COM. The terminal server uses the default Telnet port number, 2000.

TEST INTERNET

Display the route by which the server communicates with a specified Telnet destination (i.e., perform an Internet "ping").

Notes

Use the TEST INTERNET command display to display the route by which the server communicates with a specified Telnet destination (i.e., perform an Internet "ping").

The server will display one or more internet-addresses which represent the round-trip path that it would use to communicate with the specified Telnet destination.

Privileges

Non-privileged

Syntax

TEST INTERNET [*domain-name*] [RECORDROUTE] [NORECORDROUTE]*
[*internet-address*] [RECORDROUTE] [NORECORDROUTE]*

Where	Means
RECORDROUTE	**Specifies that the server will ask that the route, by which it communicates with the specified destination, be recorded in the packet. The server will display one or more *internet-addresses* which represent the round-trip path that it would use to communicate with the specified Telnet destination.**
NORECORDROUTE	**Specifies that the the server will not ask that the route, by which it communicates with the specified destination, be recorded in the packet. The server will display only the source and destination *internet-addresses*. This is the default for the TEST INTERNET command.**

TEST LOOP

Tests the physical connection between a server and a LAT service node

Notes

When you use the TEST LOOP command, the server tests the physical connection between itself and a LAT service node. The server will display a message indicating whether or not the test was successful. As a TEST LOOP command option, you can specify that an assistant node relay transmission for both outgoing and/or incoming transmissions. For example, you can specify an assistant node at the far end of the Ethernet network so that the test pattern is transmitted along the full length of the network.

Privileges

Privileged

Syntax

TEST LOOP *ethernet-address-t*][Count *n*] [Width *n*] [Help Full Assistant] [*ethernet-address-h*]
[Help Receive Assistant] [*ethernet-address-h*]
[Help Transmit Assistant] [*ethernet-address-h*]

Where	Means
Count n	**Specifies the number of times the test will be repeated. Valid values for n are whole numbers in the range of 1 to 65535. The default value is 1. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.**
Width n	**Specifies the number of data characters per packet. Valid values are whole numbers in the range of 1 to 1470. The default is 0.**
Help Full Assistant	**Specifies that you wish to have an assistant node relay transmission for both outgoing and incoming transmissions.**
Help Receive Assistant	**Specifies that you wish to have an assistant node relay transmissions coming into the terminal server.**
Help Transmit Assistant	**Specifies that you wish to have an assistant node relay transmissions coming from the terminal server.**
ethernet-address-h	**Specifies the unique Ethernet address of the assistant node. Valid values are in the form of six pairs of hexadecimal numbers which are separated by hyphens (e.g., AA-01-04-C9-56-F1). This address must be different than the address of the terminal server or the target service node. Multicast addresses are not permitted.**

TEST PORT

Test the physical connection between the server and a device attached to the port

Notes

When you use the TEST PORT command, the server tests the physical connection between itself and a device attached to the port. To end the test at any time, press the BREAK key (if enabled) or the local switch character. The server will display a repeating pattern of characters that you can observe and check for errors.

Privileges

Non-privileged users can use TEST PORT to verify correct operation of their own port. Only users at a privileged port can use the TEST LOOP command, or use the TEST PORT command to verify operation of a port other than their own port.

Syntax

TEST PORT *port-number* [Count *n*] [Width *n*] [Loopback] [External]
[Internal]

Where	Means
Count n	**Specifies the number of times the test will be repeated. Valid values for n are whole numbers in the range of 1 to 65535. For port tests, the default value is 23. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.**
Width n	**Specifies the number of characters per line. Valid values for are whole numbers in the range of 1 to 132. The default value is 80.** **Notes: If you are using the Count and Width keywords together, Count must precede Width in the command. If your port speed is 38400, the output will appear to be slow unless you set the Width to a value greater than 25.**
Loopback	**Specifies that you define the manner in which a loopback test will be performed on the local or remote port to be tested (this is always a port other than the port where the test is initiated).**
External	**Specifies that the loopback test will be performed by placing a loopback connector on the port to be tested (i.e., in a loopback connector, the transmit data and receive data pins are tied together).**
Internal	**Specifies that the loopback test will be performed by an internal programmable hardware connector on the port to be tested.**

TEST SERVICE

Test end-to-end communication between the terminal server port and a LAT service node

Notes

When you use the TEST SERVICE command, the server tests the end-to-end communication between the port and a LAT service node. The server will send a pattern of characters to the specified service. To end the test at any time, press the BREAK key. The server will display a message indicating whether or not the test was successful.

Privileges

Privileged

Syntax

TEST SERVICE [*service-name*][NODE*node-name*][DEStination *port-name*][Count *n*][Width *n*][Loopback] [External] [Internal]

Where	Means
service-name	**Specifies the name of the service to be tested.**
NODE	**Specifies that a specific node will be used to perform the test, when the service specified by service-name is offered at more than 1 node.**
node-name	**Specifies the name of the node to be used for a test.**
DEStination	**Specifies that you will perform the test to a specific remote port.**
Count n	**Specifies the number of times the test will be repeated. Valid values for n are whole numbers in the range of 1 to 65535. The default value is 1. If you specify NONE, the tests run continuously until you press the BREAK key or type the local switch character.**
Width n	**A keyword. Specifies the number of characters per line for port or service tests, or the number of data characters per packet for loop tests. For port or service tests, valid values for are whole numbers in the range of 1 to 132. For port or service tests, the default value is 80. For loop tests, valid values are whole numbers in the range of 1 to 1470. For loop tests, the default is 0.**
Loopback	**Specifies that you define the manner in which a loopback test will be performed on the local or remote port to be tested (this is always a port other than the port where the test is initiated).**
External	**Specifies that the loopback test will be performed by placing a loopback connector on the port to be tested (i.e., in a loopback connector, the transmit data and receive data pins are tied together).**
Internal	**Specifies that the loopback test will be performed by an internal programmable hardware connector on the port to be tested.**

XCONNECT

Connect to an XDM host

The XCONNECT command attempts to establish a session with an XDM host.

Notes

You can either provide the domain name or Internet address of an XDM host in the command line, or simply enter the XCONNECT command. If you enter the command without specifying a host, the terminal server searches the permanent database for a host that was specified with the DEFINE PORT XDM host command, or uses the BROADCAST query type.

Privilege Level

Secure

Syntax

XCONNECT [*domain-name* /*internet-address*]

Where	Means
domain-name	**The domain name of the XDM host.**
internet-address	**The Internet address of the XDM host.**

Examples

1. This example of the assumes that that you have already defined an XDM host, or the BROADCAST query type. When the user enters the command, the terminal server either searches for the specific or indirect host, or broadcasts a query to the network.

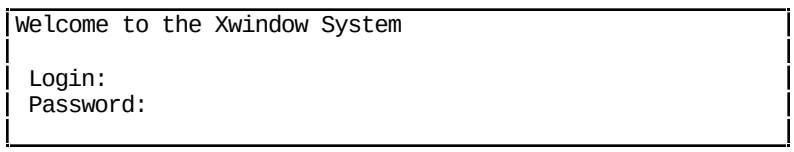
```
Xyplex> xconnect
```

```
Welcome to the Xwindow System

 Login:
 Password:
```

2. This example assumes that you have not defined an XDM host, so the user enters the Internet address of the host with the XCONNECT command.

```
Xyplex> xconnect 143.129.80.200
```



ZERO COUNTERS

Reset counters shown in displays

Notes

Use the ZERO COUNTERS command to reset counters displayed by the SHOW/LIST/MONITOR SERVER, NODES, and/or PORTS commands.

Privileges

Secure and non-privileged users can use the ZERO COUNTERS PORTS command to reset the counters for their own port. All other ZERO COUNTERS commands are privileged only.

Syntax

ZERO COUNTERS [NODE *node-name*]
[PORT *port-list*]
[ALL]

Where	Means
NODE	**Specifies that the server will reset the counters that relate to a specific node. This is the default.**
node-name	**Specifies the name of the node about which the server counters will be reset.**
PORT	**Specifies that the server will reset the counters that relate to a specific port.**
port-list	**Specifies the port number(s) of the ports for which the counters will be reset.**
ALL	**Specifies that the server will reset all counters for all displays.**

Example

1. `Xyplex>> ZERO COUNTERS NODE FINANCEVAX`

   Meaning: Reset to zero the counters that relate to the service node named FINANCEVAX

2. `Xyplex>> ZERO COUNTERS PORT 1-3`

   Meaning: Reset to zero the counters that relate to ports 1 through 3 on the terminal server.

3. `Xyplex>> ZERO COUNTERS ALL`

   Meaning: Reset to zero all counters in the displays shown by the SHOW/LIST/MONITOR SERVER, NODES, and/or PORTS commands.

DEFINE SERVER DAEMON FINGERD

Enable or disable the fingerd daemon.

Notes

`fingerd` **provides a method for exchanging information between hosts about users who are logged on to a server, using a Finger User Information Protocol (RFC 1288). fingerd is supported by implementing software at the server, which responds to requests for information about a user made at a UNIX host.**

Refer to the chapter on Configuring and Managing Daemons in the *Software Management Guide Supplement* for more information. This chapter also shows the type of output that is supplied by the fingerd daemon.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE SERVER DAEMON FINGERD ENABLED/DISABLED

Where	Means
ENABLED	**Enable the fingerd daemon on the server.**
DISABLED	**Disable the fingerd daemon on the server. The daemon is disabled as the factory default.**

Example

```
Xyplex>> DEFINE SERVER DAEMON FINGERD ENABLED
```

DEFINE SERVER DAEMON LPD

Enable or disable the lpd daemon.

Notes

The lpd daemon provides a method for sending print jobs between UNIX systems (in this case, the server behaves as though it was a UNIX host) and managing jobs that are in a print queue, using a protocol that is defined in RFC 1179. lpd is supported by implementing software at the server, which responds to print requests made at a UNIX host using the Berkeley and AT&T System V UNIX lpr, lpc, lprm, and lpq, commands and the lpstat, enable, and disable commands which are only available for AT&T System V UNIX hosts. The lpc, lpq, and lprm commands are also available on the Xyplex terminal server.

Refer to the chapter on Configuring and Managing Daemons in the *Software Management Guide Supplement* for more information. Refer to the *Using the UNIX Line Interface* guide for a description of the lpc, lpq, and lprm commands that are available at the terminal server.

The UNIX Like Interface must be enabled in order to use the lpc, lpq, and lprm commands at the server.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE SERVER DAEMON LPD ENABLED/DISABLED

Where	Means
ENABLED	**Enable the lpd daemon on the server.**
DISABLED	**Disable the lpd daemon on the server. The daemon is disabled as the factory default.**

Example

```
Xyplex>> DEFINE SERVER DAEMON LPD ENABLED
```

DEFINE SERVER DAEMON ROUTED

Enable or disable the routed daemon.

Notes

The routed daemon provides a method for exchanging routing information among gateways or hosts, using the Routing Information Protocol that is defined in RFC 1058.. The terminal server uses this protocol to learn about Internet routes from other hosts or gateways (in this case, the server behaves as though it was a UNIX host). In the Xyplex routed implementation, the server listens for routing messages and updates its internal routing tables, without transmitting any routing information to other gateways or hosts (i.e., the server is a "silent" or "passive" router).

Note that in previous releases, Xyplex servers only updated their internal routing tables by listening to and storing ICMP re-direct messages, or by having routes added by a privileged user via the DEFINE/SET SERVER INTERNET ROUTE command. (These methods are used as well.) Internet routes that are learned via RIP or ICMP re-direct messages are lost when the server is re-initialized. Internet routes learned via RIP expire after 5 minutes, unless the server receives another RIP message with the route. All Internet routes that the server knows can be viewed using the SHOW/LIST/ MONITOR INTERNET ROUTES command

Refer to the chapter on Configuring and Managing Daemons in the *Software Management Guide Supplement* for more information. Refer to the description of the SHOW/MONITOR INTERNET ROUTES command.

You must reinitialize the server for the change to take effect.

Privilege Level **Privileged**

Syntax

DEFINE SERVER DAEMON ROUTED ENABLED/DISABLED

Where	Means
ENABLED	**Enable the routed daemon on the server.**
DISABLED	**Disable the routed daemon on the server. The daemon is disabled as the factory default.**

Example

```
Xyplex>> DEFINE SERVER DAEMON ROUTED ENABLED
```

DEFINE SERVER DAEMON RWHOD

Enable or disable the rwhod daemon.

Notes

The rwhod daemon provides a method for collecting information about domain names on the network by listening to "rwho" messages and adding currently unknown domain-names to the domain-name table.

Note that in previous releases, Xyplex servers only updated their domain name tables when the server itself requested a domain-name from a Domain Name Server, or by having domain-names added by a privileged user via the DEFINE/SET DOMAIN command. (These methods are used as well.) Learned domain-names are lost when the server is re-initialized. When a server receives an "rwho" message that contains a domain-name that the server has already learned, the time-to-live (TTL) for that domain-name is set to 1 day. All domain-names that the server knows can be viewed using the SHOW/LIST/ MONITOR DOMAIN command.

When the server receives an rwho message, if the domain-name already exists in the domain-name table, and its source is either the primary or secondary name server, then the entry is overwritten with "Who" as the source and a time-to-live of 1440. If the the domain-name exists in the table, and its source is "local," the entry is not overwritten.

Refer to the chapter on Configuring and Managing Daemons in the *Software Management Guide Supplement* for more information. Refer to the description of the SHOW/LIST/MONITOR DOMAIN command.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE SERVER DAEMON RWHOD ENABLED/DISABLED

Where	Means
ENABLED	**Enable the rwhod daemon on the server.**
DISABLED	**Disable the rwhod daemon on the server. The daemon is disabled as the factory default.**

Example

```
Xyplex>> DEFINE SERVER DAEMON RWHOD ENABLED
```

DEFINE SERVER DAEMON SYSLOGD

Enable or disable the syslogd daemon.

Notes

The syslogd daemon provides a central facility to log messages about events which occur on the server. These messages can be logged at the server and/or in a file at a UNIX host. This daemon is used as part of the V5.1 Enhanced Event Accounting feature.

The DEFINE SERVER DAEMON SYSLOGD ENABLED/DISABLED command enables or disables the `syslogd` **daemon on the terminal server and specifies a remote host which will receive the accounting entries. The remote host must be running a UNIX implementation.**

Enabling the `syslogd` **daemon provides remote logging of normal or verbose accounting entries. As the terminal server places each entry into the local account log, it sends a message to the host you specify in the command line. The syslogd intercepts the message and routes it to one or more destinations, depending on the settings in the** `/etc/syslog.conf` **file on the host. The entries contain the same information in the remote log file as in the terminal server log file.**

Refer to the chapter on Configuring and Managing Daemons in the *Software Management Guide Supplement* for more information on setting up syslogd. Refer to the chapter on Accounting in the *Software Management Guide Supplement* for more information about setting up and using the accounting feature and a description of syslogd output at a UNIX host. Refer to the description of the SHOW/MONITOR SERVER ACCOUNTING command for a description of event log accounting output at a server.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE SERVER DAEMON SYSLOGD ENABLED *internet-address*
DEFINE SERVER DAEMON SYSLOGD DISABLED

Where	Means
ENABLED	**Enable the syslogd daemon on the server. If you enable the daemon, you must also specify the Internet address of the remote host.**
internet-address	**The Internet address of the host where the destination log file resides.**
DISABLED	**Disable the syslogd daemon on the server. The daemon is disabled as the factory default.**

Example

This command enables the syslogd daemon specifies 140.114.12.6 as the Internet address of the remote host.

```
Xyplex>> define server daemon syslogd enabled 140.114.12.6
```

DEFINE [SERVER] RIP STATE

Enable or disable the routed daemon.

Notes

This command performs the same function as the DEFINE SERVER DAEMON ROUTED ENABLED/DISABLED command. It is included for compatibility with Xyplex router products.

Refer to the description of the DEFINE SERVER DAEMON ROUTED ENABLED/DISABLED command for more information.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE [SERVER] RIP STATE [ENABLED]
[DISABLED]*

SERVER **An optional keyword.**

ENABLED **Enable the routed daemon on the server.**

DISABLED **Disable the routed daemon on the server. The daemon is disabled as the factory default.**

Example

```
Xyplex>> DEFINE SERVER RIP STATE ENABLED
```

DEFINE/SET SERVER LPD QUEUE

Enable or disable a queue for lpd printing.

Notes

You must enable an lpd queue at the server in order for the server to be able to accept lpd print jobs from hosts. The lpd queue name at the server corresponds to a remote printer in the lpd configuration at a host. There can be multiple lpd queues on a server. Multiple ports can also be assigned to service an lpd queue. In this case, a print job submitted to the lpd queue will be serviced by the first available port.

When an lpd queue is enabled, it will accept print jobs from any appropriately configured host. When an lpd queue is disabled, it will reject further print jobs, but will continue to process jobs that are currently in the queue. The host is free to try to resubmit the job at a later time. (To completely eliminate a queue and all jobs in it, use the CLEAR LPD QUEUE command. To remove a specific job from an lpd queue, use the lprm or REMOVE QUEUE ENTRY command. These commands will not work after the job has started.)

Refer to the chapter on Configuring and Managing the LPD Daemon in the *Software Management Guide Supplement* for more information. Refer to the *Using the Xyplex ULI* guide for a description of the lpc, lpq, and lprm commands that are available at the terminal server.

The lpd daemon must be enabled in order to enable an lpd queue. The ULI must be enabled in order to use the lpc, lpq, and lprm commands at the server.

Privilege Level

Privileged

Syntax

DEFINE/SET [SERVER] LPD QUEUE "*queue-name*" PORT *port-list* [ENABLED LFCR [ENABLED]]
[DISABLED]]
[DISABLED LFCR [ENABLED]]
[DISABLED]]

DEFINE/SET [SERVER] LPD QUEUE ALL PORT *port-list* [ENABLED LFCR [ENABLED]]
[DISABLED]]
[DISABLED LFCR [ENABLED]]
[DISABLED]]

DEFINE/SET [SERVER] LPD QUEUE "*queue-name*" [ENABLED]
[DISABLED]
DEFINE/SET [SERVER] LPD QUEUE ALL [ENABLED]
[DISABLED]

DEFINE/SET [SERVER] LPD QUEUE "*queue-name*" PORT *port-list*
DEFINE/SET [SERVER] LPD QUEUE ALL PORT *port-list*

DEFINE/SET [SERVER] LPD QUEUE "*queue-name*" [LFCR ENABLED]
[LFCR DISABLED]
DEFINE/SET [SERVER] LPD QUEUE ALL [LFCR ENABLED]
[LFCR DISABLED]

Where	Means
"queue-name"	**The name of the lpd queue. The queue-name must match the name of a remote printer that you specify at a UNIX host (for example, in the /etc/printcap file or to the AT&T UNIX lpadmin utility). The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks ("). You can specify ALL for all queues.**
PORT	**The lpd queue will exist at one or more ports, other than the current port.**
port-list	**One or more terminal server ports where lpd queue will exist.**
ENABLED	**The lpd queue will be enabled at the port(s).**
DISABLED	**The lpd queue will be disabled at the port(s).** **When you disable an lpd queue, the server will not accept additional print jobs directed to that lpd queue. The server will process print jobs which are currently in the lpd queue.**
LFCR	**Specify whether or not the server will convert line-feed characters into carriage-return/line-feed characters.**
ENABLED	**The server will convert line-feed characters into carriage-return/line-feed characters. Typically, you would set the LFCR characteristic to ENABLED for line printers or printers which are intended to process simple documents. When the LFCR characteristic is ENABLED, the port will imitate the operation of a printer that is directly connected to a UNIX host.**
DISABLED	**The server will not convert line-feed characters into carriage-return/line-feed characters. Typically, you would use set the LFCR characteristic to DISABLED for laser printers, PostScript printers, etc.**

Examples

```
Xyplex>> DEFINE SERVER LPD QUEUE "line-printer" ENABLED

Xyplex>> DEFINE SERVER LPD QUEUE "line-printer" PORT 1-2

Xyplex>> DEFINE SERVER LPD QUEUE "laser-printer" ENABLED

Xyplex>> DEFINE SERVER LPD QUEUE ALL LFCR DISABLED
```

CLEAR/PURGE [SERVER] LPD QUEUE

Terminate printing from an lpd queue

Notes

The CLEAR/PURGE SERVER LPD QUEUE command removes an entire lpd queue and cancels any print jobs currently in the queue. If you use the CLEAR/PURGE SERVER LPD QUEUE command, you should probably update the lpd configuration at any hosts that had access to the queue (i.e., edit the /etc/printcap command to remove the printer associated with the lpd queue at the server).

Refer to the chapter on Configuring and Managing the LPD Daemon in the *Software Management Guide Supplement* for more information. Refer to the *Using the Xyplex ULI* guide for a description of the lpc, lpq, and lprm commands that are available at the terminal server.

Privilege Level

Privileged

Syntax

CLEAR/PURGE [SERVER] LPD QUEUE "***queue-name***"
ALL

Where	Means
queue-name	**The name of the lpd queue that you are removing. The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks (").**
ALL	**Remove all LPD queues.**

Examples

```
Xyplex>> CLEAR LPD QUEUE "line-printer"

Xyplex>> PURGE LPD QUEUE "line-printer"
```

SHOW/MONITOR [SERVER] LPD COUNTERS

Display statistical information about lpd queues

Notes

Use the SHOW/MONITOR SERVER LPD COUNTERS command to view statistical information about print jobs being handled by lpd queues that are enabled on the server. The SHOW command produces a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

Privilege Level

Show is non-privileged. Monitor is privileged.

Syntax

SHOW/MONITOR [SERVER] LPD COUNTERS

Example

LPD Queue	State	LF->LFCR	Total	Active	Waiting	Processed
laser-printer	ENABLED	DISABLED	2	1	1	115
line-printer	DISABLED	ENABLED	0	0	0	38

Example MONITOR/SHOW SERVER LPD COUNTERS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER LPD COUNTERS display.

Item (Field)	Description
LPD Queue	**Shows the name of an lpd queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).**
State	**Shows whether or not the lpd queue can accept job requests. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests.**
LF->LFCR	**Shows whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.**
Total	**Shows the total number of jobs that are currently being processed by the lpd queue. The number shown equals the sum of the jobs shown in the "Active" and "Waiting" columns.**
Active	**Shows the total number of jobs that are actively being printed at ports associated with the queue. (This number can be greater than 1 when the queue exists on more than one port.)**
Waiting	**Shows the total number of jobs pending on the queue. The next job in the queue will be processed when a port associated with the queue becomes available.**
Processed	**Shows the total number of jobs that the queue has previously completed.**

SHOW/LIST/MONITOR [SERVER] LPD QUEUE

Display a list of jobs in lpd queues

Notes

Use the SHOW/LIST/MONITOR SERVER LPD QUEUE command to view the status of all print jobs that are being processed by one or more lpd queues.

The SHOW and LIST commands produce a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

To remove a specific job from an lpd queue, use the lprm or REMOVE QUEUE ENTRY command.

Syntax

SHOW/MONITOR/LIST [SERVER] LPD QUEUE "***queue-name***"
ALL

Where	Means
queue-name	**The name of the lpd queue that you want to view. The name can be up to 16 characters long, and is case sensitive. Enclose the name in double-quotation marks (").**
ALL	**View information about all lpd queues.**

Example

```
Xyplex>> SHOW SERVER LPD QUEUE "laser-printer"

LPD Queue      : laser-printer
Queue Port(s)  : 5, 6
Status         : ENABLED, ACTIVE
LF_>LFCR       : DISABLED

   Job Status        Remote Host     Job #      File Name      File Size   Port
---------------- ---------------- ------- ---------------- ------------ ----
PRINTING/Data     unixhost               1 report1                37651    5
PRINTING/Data     cadstation             2 schematic             223592    6
WAITING/Port      cadstation             3 schematic             111678    0
```

Example MONITOR/SHOW/LIST SERVER LPD QUEUE Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW/LIST SERVER LPD QUEUE display.

Item (Field)	Description
LPD Queue	**Shows the name of an lpd queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).**
Ports	**Shows the ports associated with the lpd queue.**
Status	**Shows whether or not the lpd queue can accept job requests, and whether or not the queue is currently processing any jobs. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests. Active means that the queue is currently processing print jobs.**
LF->LFCR	**Shows whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.**
Job Status	**Shows the current status of a job. Possible states are listed below.**
Remote Host	**Shows the name of the host which originated the lpd print job.**
Job #	**Shows the position of the job within the lpd queue. Jobs are processed on a first-come-first serve basis by the next available port.**
File Name	**Shows the name of the file being processed by the queue.**
File Size	**Shows the size of the file (in bytes).**
Port	**Shows the port assigned to print the job. A zero indicates that the job has not yet been assigned.**

The following are the possible Job Status states.

ABORTED	**The print job was aborted (for example, by an lprm command, REMOVE QUEUE command, etc).**
ABORTED/Flushing	**The queue is discarding data received for an aborted print job.**
ASSIGNED/Port	**The queue has assigned a port to a print job.**
COMPLETED	**The print job is complete.**
ERROR	**An error occurred while the job was being transferred from the remote host to the server.**
INITIALIZED	**The print job was recently created.**
PRINTING/Control	**The queue is receiving (and discarding) an lpd print job control file.**
PRINTING/Data	**The queue is receiving an lpd print job and sending it to the assigned port.**
WAITING/Port	**The print job is on the lpd print queue and is waiting for a port assignment.**

SHOW/MONITOR [SERVER] LPD STATUS

Display summary information about the availability of lpd queues

Notes

Use the SHOW/MONITOR SERVER LPD STATUS command to view summary information about lpd queue availability. The SHOW command produces a "static" display of the requested information. These displays can be viewed on ANSI and non-ANSI terminals (including hard-copy devices). The MONITOR command generates a display that is continuously updated on the terminal display screen.

Privilege Level

Show is non-privileged. Monitor is privileged.

Syntax

SHOW/MONITOR [SERVER] LPD STATUS

Example

```
    LPD Queue      State   LF->LFCR   Ports
----------------- -------- -------- ----------------------------------------
laser-printer     ENABLED  DISABLED  5-8
line-printer      DISABLED ENABLED   9-10
```

Example MONITOR/SHOW SERVER LPD STATUS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW SERVER LPD STATUS display.

Item (Field)	Description
LPD Queue	**Shows the name of an lpd queue (created and enabled/disabled using the DEFINE SERVER LPD QUEUE command).**
State	**Shows whether or not the lpd queue can accept job requests. Enabled means that the queue can accept job requests. Disabled means that the queue cannot accept job requests.**
LF->LFCR	**Shows whether or not the server will convert line-feed characters into carriage-return/line-feed characters. Enabled means that the server will make this conversion. Disabled means that the server will not make this conversion.**
Ports	**Shows the ports associated with the lpd queue.**

CLEAR SERVER ACCOUNTING

Clear the account log

The CLEAR SERVER ACCOUNTING command clears all entries in the account log.

Notes

This command requires that the ACCOUNTING feature be enabled. This command clears the log for both normal and verbose accounting modes.

Privilege Level

Privileged

Syntax

CLEAR SERVER ACCOUNTING

Example

```
Xyplex>> clear server accounting
```

DEFINE/SET SERVER VERBOSE ACCOUNTING

Enable or Disable Verbose Accounting Mode

The DEFINE/SET SERVER VERBOSE ACCOUNTING ENABLED/DISABLED command specifies the status of Verbose Accounting on the terminal server.

Notes

You must enable Verbose Accounting mode to log messages from the UNIX daemons if they are enabled on the terminal server.

You do not have to initialize the terminal server after using the SET command for the change to take effect. You must initialize the server for the DEFINE command to take effect.

Privilege Level

Privileged

Syntax

DEFINE/SET SERVER VERBOSE ACCOUNTING ENABLED/DISABLED

Where	Means
ENABLED	**Enable Verbose Accounting mode.**
DISABLED	**Disable Verbose accounting mode. This is the default setting for this characteristic.**

Example

```
Xyplex>> define server verbose accounting enabled
```

DEFINE/SET SERVER VERBOSE PRIORITY

Set a priority level for the account log

The DEFINE/SET SERVER VERBOSE PRIORITY commands specify a value which the server uses to determine whether or not to write a message from certain software modules to the account log.

Notes

The server uses this value as a filter to determine whether or not to log messages from some software modules in TCP/IP-LAT software V5.1 or greater, such as the UNIX daemons. It logs messages from those modules that submit a priority level equal to or below the priority you specify. It discards messages that submit a greater priority level than the one you specify. This filter affects only SLIP (including compressed SLIP, or CSLIP) and PPP connections, and the following UNIX daemons: `lpd`, `rwhod`, `fingerd`, **and** `routed`.

The server continues to log all traditional accounting messages concerning session activity, regardless of the Verbose Priority number.

Privilege Level

Privileged

Syntax

DEFINE/SET SERVER VERBOSE PRIORITY ***priority-type*** **[LOG FACILITY [USER]] [LOCAL** ***facility-number*****]]**

Where **Means**

priority-type **The priority type that the server will use to filter messages from software modules. Valid values are 0 through 7. The default is 5. Assigning a priority value of 7, which is the highest value, will allow the server to log all messages. The following are the meanings of priority-types 0 through 7.**

Type	Means
0	A severe condition. The server usually broadcasts priority 0 messages to all users because it can affect their ability to work on the host.
1	A condition that the system manager needs to correct immediately, such as a corrupted system database.
2	A critical condition, such as a hard device error.
3	A software error condition.
4	A warning message.
5	Conditions that are not error conditions, but may require specific procedures to adjust them.
6	Normal, informational messages.
7	Messages that contain information useful for test situations only.

LOG FACILITY USER **Specify that the UNIX host will logs the accounting information to the UNIX "KERN" facility. This is the default.**

LOG FACILITY LOCAL *facility number* **Specify that the UNIX host will log the accounting information to a specific UNIX facility. Valid values are 0 through 7 which correspond to the UNIX facilities local0 through local7. The default is 5 (i.e., local5).**

Example

This command sets the value of the of the Verbose Priority Level to 7.

```
Xyplex>> set server verbose priority 7
```

SHOW/MONITOR SERVER ACCOUNTING

Display information about successful and attempted connections, sessions, nested menus, and daemon activity.

Notes

Use the SHOW/MONITOR SERVER ACCOUNTING display to view the accounting log which contains information about successful and attempted connections made to or from the unit, as well as information about sessions that are disconnected. Using verbose accounting the log will also contain information about PPP and SLIP (including compressed SLIP or CSLIP) connections, and informational messages about daemon activity and nested menu file errors . This display can be useful in identifying the cause of problems that are occurring on the server.

Privileges

Non-privileged users can use the SHOW SERVER ACCOUNTING command. Only users at privileged ports can use the MONITOR SERVER ACCOUNTING command.

Syntax

SHOW|MONITOR SERVER ACCOUNTING

Example

```
ENTRY ADDRESS          PORT USERNAME         TYPE DESTINATION       CONNECT TIME          DISCONNECT TIME        BYTES IN BYTES OUT
    1 08-00-87-00-4F-45   1 JSmith           L    UNIXHOST          12 Apr 1991  20:19:40                                    
    1 08-00-87-00-4F-45   1 JSmith           D 0  UNIXHOST          12 Apr 1991  20:19:40 12 Apr 1991  20:19:46         0        20
    2 08-00-87-00-4F-45   0                  R                      12 Apr 1991  20:19:59                                    
    3 08-00-87-00-4F-45   1 JSmith           L    UNIXHOST          12 Apr 1991  20:20:02                                    
    4 08-00-87-00-4F-45   0 A Jones          L    VAX               12 Apr 1991  20:20:43                                    
    4 08-00-87-00-4F-45   0 A Jones          D23  VAX               12 Apr 1991  20:20:43 12 Apr 1991  20:21:04         0         0
    3 08-00-87-00-4F-45   1 JSmith           D 0  UNIXHOST          12 Apr 1991  20:20:02 12 Apr 1991  20:21:04        35     28938
```

Example SHOW SERVER ACCOUNTING DISPLAY (Default Accounting)

```
23 Sep 1993 13:28:20 SLIP Link Startup on Port 11
23 Sep 1993 13:28:46 FINGERD request from 140.179.192.3
23 Sep 1993 13:28:46 FINGERD request :
23 Sep 1993 13:29:13 source:08-00-87-01-CB-A4 dest:140.179.192.3 port:0 user:(Remote) type:Rtelm
23 Sep 1993 13:29:13 source:08-00-87-01-CB-A4 dest:140.179.192.3 port:0 user:(Remote) type:D reason:0 bytes in:1 bytes out:0
23 Sep 1993 13:30:51 source:08-00-87-01-CB-A4 dest:140.179.50.201 port:0 user:(Remote) type:Rtelm
```

Example SHOW SERVER ACCOUNTING DISPLAY (Verbose Accounting)

The following table describes each of the items (fields) of data related to connections in the MONITOR/ SHOW SERVER ACCOUNTING display:

Item (Field)	Description
Entry (default display only)	**Shows the log entry number.**
Address (default display) or source (verbose display)	**Shows the Ethernet address of the server.**
Port	**Shows the port from or to which the connection is made.**
Username (default display) or user (verbose display)	**Shows the name of the user who is logged on to the port.**
Type	**Shows whether the connection is a local access connection or a remote access connection, or if a connection has been disconnected and the reason why the connection was disconnected. Local access connections are indicated by the letter L followed by a connection type. Remote access connections are indicated by the letter R followed by a connection type. Disconnections are indicated by the letter D, followed by a reason number which represents the reason why the disconnection occurred (see "reason" below).The following are the possible connection types that will be displayed:**
Destination (default display) or dest (verbose display)	**Shows the destination LAT service name, domain-name, or internet-address of the connection.**
Connect Time (default display only)	**Shows the time when the connection was made.**
Disconnect Time (default display only)	**Shows the time when a connection was disconnected**
Bytes In	**Shows the number of bytes of data that the port received from the device.**
Bytes Out	**Shows the number of bytes of data output by the port to the device.**

Default	Verbose	Connection Type
la	**lat**	**LAT**
te	**telnet**	**Telnet**
lt	**lat/tel**	**LAT/Telnet**
tn	**tn3270**	**TN3270**
rn	**rcpn**	**Remote console via node name**
rp	**rcpp**	**Remote console via physical port**
rl	**rlogin**	**RLOGIN**
lq	**latq**	**Queued LAT connection**
tm	**telm**	**Telnet maintenance**
xr	**xrem**	**XREMOTE**
xp	**xprn**	**XPRINTER (IPX)**

reason — **Disconnections are indicated by the letter D, followed by a reason number which represents the reason why the disconnection occurred (see "reason" below). The table below lists these numbers and the corresponding reason for a session being disconnected.**

Code	Related Error Code	Explanation
0	None - normal disconnection	Connection terminated because the user logged out or disconnected the port.
1	211 or 251	Connection terminated or refused because the server received messages that violate the LAT protocol.
2	212 or 252	Connection terminated or refused because the server received messages that violate the LAT protocol.
3	213 or 253	Connection terminated or refused because the server received messages that violate the LAT protocol.
4	214 or 254	Connection terminated or refused because the server received messages that violate the LAT protocol.
5	215 or 255	Connection refused because the queue entry id already exists in the queue.
6	216 or 256	Connection terminated or refused and the LAT virtual circuit is now inactive.
7	217 or 257	Connection terminated or refused because the server had insufficient memory or resources to make the connection.
8	218 or 258	Connection terminated or refused because the service node (a host or a remote terminal server offering the service) would not permit the connection.
9	219 or 259	Connection terminated or refused because the service is not available any more.
10	220 or 260	Connection terminated or refused because your server would not permit the connection.
11	221 or 261	Connection terminated or refused because the server had insufficient memory or resources to make the connection.
12	222 or 262	Connection terminated or refused because the server is being reinitialized or shut down.
13	223 or 263	Connection terminated or refused because the remote node offering the service intentionally aborted the connection.
14	224 or 264	Connection terminated or refused because the LAT circuit timer at your server is not set appropriately.

15	**225 or 265**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
16	**226 or 266**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
17	**227 or 267**	**Connection terminated or refused because the service node failed to respond within the time period defined by DEFINE/SET SERVER RETRANSMIT LIMIT characteristic.**
18	**228 or 268**	**Connection terminated or refused because the server determined that no progress was being made on the existing virtual circuit. This is an indication of how busy the service node is.**
19	**229 or 269**	**Connection terminated or refused because the the service is not offered on the requested port.**
20	**230 or 270**	**Connection terminated or refused because the the service is not offered on the requested port.**
21	**231 or 271**	**Connection terminated or refused because you specified an incorrect password to use the service.**
22	**232 or 272**	**Connection terminated or refused because the requested service is already being used.**
23	**233 or 273**	**Connection terminated or refused because the requested service is no longer offered at your server.**
24	**234 or 274**	**Connection terminated or refused because the service is disabled.**
25	**235 or 275**	**Connection terminated or refused because it was not in the connection queue, as was previously thought.**
26	**236 or 276**	**Connection terminated or refused because you attempted to connect to a busy service that is not configured for queued access.**
27	**237 or 277**	**Connection terminated or refused because of an access violation.**
28	**238 or 278**	**Connection terminated or refused because the server received messages that violate the LAT protocol.**
29	**none**	**Connection terminated or refused because of an unexpected event.**
30	**735**	**The service specified in a TEST SERVICE command does not support the specified test.**
31	**793**	**Connection refused because the user supplied a domain-name that was too long or in an invalid format.**
32	**710**	**Connection refused because the requested service is not offered at the node specified, or the service or node name that you specified is not known to the server.**

33	**711**	**Connection refused because the service specified is unknown to the unit, the server node limit has been reached, the server is unable to store information about additional nodes, or you are not authorized to use the service specified.**
34	**none**	**Connection was rejected.**
35	**766**	**Connection refused because the user attempted to connect to an internet-address from a port on which the DEFINE/SET PORT INTERNET CONNECTIONS characteristic is DISABLED.**

DEFINE SERVER NESTED MENU SIZE

Specify the number of bytes in the menu file

The DEFINE SERVER NESTED MENU SIZE command specifies the amount of terminal server memory, in bytes, that you want to reserve for nested menus. Allocating memory with this command also enables the Nested Menu feature. Allocating 0 bytes disables the feature.

Notes

If you allocate memory for nested menus, and then do not use all of it, you can release the unused memory. Use this command and specify only the amount of memory that the menus require. When you initialize the terminal server after you reallocate the memory, the terminal server frees up the unused memory.

The Nested Menu Size field in the SHOW/LIST/MONITOR SERVER CHARACTERISTICS display shows the total amount of memory, in bytes, that you have allocated for nested menus. The Nested Menu Memory field of the SHOW/LIST/MONITOR SERVER STATUS display shows the current amount of memory, in bytes, being used by the menu file.

Privilege Level

Privileged

Syntax

DEFINE SERVER NESTED MENU *menu-size*

Where	Means
menu-size	**The amount of memory, in bytes, that you want to reserve for nested menus. Valid entries are from 0 through 204,800 . A 0 entry disables the nested menu feature and deallocates any previously allocated memory for this feature. The default is 0 bytes (Nested Menus disabled).**

Example

This command allocates 150,000 bytes for nested menus.

```
Xyplex>> define server nested menu size 150000

Xyplex>>
```

Initialize the terminal server to allocate the memory.

DEFINE SERVER NESTED MENU NAME

Specify a name for the menu file

The DEFINE SERVER NESTED MENU NAME command specifies a name for the menu file on the script server.

Notes

When the terminal server initializes with memory allocated for a menu file, searches the Script Server for the filename you specify with this command.

The Menu Name field of the SHOW/LIST/MONITOR SERVER CHARACTERISTICS display shows this name.

Privilege Level

Privileged

Syntax

DEFINE SERVER NESTED MENU NAME "*string*"

Where	Means
"*string*"	**A string of 1 through 16 ASCII characters. Enclose the string in quotes.**

Example

This command defines `n.menu.file` **as the nested menu filename.**

```
Xyplex>> define server nested menu name "n.menu.file"

Xyplex>>
```

DEFINE/SET PORT NESTED MENU

Specify the status of the nested menu feature at one or more ports

The DEFINE/SET PORT NESTED MENU ENABLED/DISABLED/ REQUIRED command enables or disables this feature on a port, or specifies that this feature is required on the port. A user cannot access the Xyplex command interface at a port where nested menus are required.

Notes

You must specify a top level menu number at ports where you enable or require the nested menu feature. The terminal server uses this number to determine which menu to display first.

If nested menus are required at a port, and the terminal server cannot find a menu file on the script server when the user attempts to log on to the port, the user cannot log on. When a user presses the <Exit> key at a port with nested menus required, the terminal server logs out the port.

Privilege Level

Privileged

Syntax

DEFINE/SET PORT *port-list* NESTED MENU ENABLED | DISABLED | REQUIRED

Where	Means
port-list	**One or more ports where you want to specify the status of the Nested Menu feature.**
ENABLED	**Nested menus are enabled, but not required at the ports you specify. If the terminal server cannot find the menu file, it opens the Xyplex command interface at these ports.**
DISABLED	**Disable the nested menu feature at the ports you specify.**
REQUIRED	**This port must use the nested menu feature or the interface logs out the port.**

Example

This command enables nested menus on ports 6-8.

```
Xyplex>> set port 6-8 nested menu enabled

Xyplex>>
```

DEFINE/SET PORT PRIVILEGED NESTED MENU

Enable or Disable the privileged nested menu

This command allows you to include privileged commands in nested menus without explicitly setting the privileged security level within the menu script.

Notes

When you disable the Privileged Nested Menu feature at a port, you also disable the Nested Menu Feature at the port.

If you do not enable this feature, and you want to include a privileged command in a menu, you need to include the SET PRIVILEGE command within the menu script.

If the terminal server cannot access the menu file, and the Privileged Nested Menu feature is enabled at a port, the security level of the port is Nonprivileged when the user logs in to the Xyplex command interface.

Privilege Level

Privileged

Syntax

DEFINE/SET PORT *port-list* PRIVILEGED NESTED MENU ENABLED/DISABLED

Where	Means
port-list	**One or more ports where you want to specify the status of the Privileged Nested Menu feature.**
ENABLED	**Enable Privileged Nested Menus at the ports you specify.**
DISABLED	**Disable Privileged Nested Menus at the ports you specify. This is the default for this feature.**

Example

This command enables Privileged Nested Menus on ports 10-20.

```
Xyplex>> set port 10-20 privileged nested menu enabled

Xyplex>>
```

DEFINE/SET PORT NESTED MENU TOP LEVEL

Specify the top level menu number

The DEFINE/SET PORT NESTED MENU TOP LEVEL command specifies the number of the highest-level menu for the ports you specify. The terminal server displays the highest-level menu first.

Notes

You must specify a top level menu number to use the Nested Menu Feature. If you do not, the terminal server cannot determine which menu to display first. If you do not specify this value, the terminal server issues an error message and does not display a menu when the user logs on to a port with Nested Menus enabled.

You specify menu numbers in the menu script with the `%menu_start` ***n*** **"*menu-title*" command. The variable *n* indicates the menu number. See the section on Creating a Nested Menu Script for more information about this and other nested menu commands.**

Privilege Level

Privileged

Syntax

DEFINE/SET PORT *port-list* NESTED MENU TOP LEVEL *menu-number*

Where	Means
port-list	**One or more ports where you want to specify a top-level menu number.**
menu-number	**The number of the top level menu. Valid values are 0 through 255. The default is 0, which means that no top level menu is specified.**

Example

This command specifies menu 1 as the top level menu for ports 5-10.

```
Xyplex>> set port 5-10 nested menu top level 1

Xyplex>>
```

DEFINE/SET PORT INTERNET CSLIP

Enable or disable compression on SLIP links.

Notes

SLIP links can transmit and receive packets that have been compressed using the Van Jacobson compression algorithm (refer to RFC 1144). Compression allows SLIP links to operate with higher throughput under some circumstances. (The SLIP implementation also supports the transmission of uncompressed packets, since not all remote devices permit the use of compression. Use the DEFINE/SET PORT INTERNET SLIP ENABLED command.)

The DEFINE/SET PORT INTERNET CSLIP ENABLED/DISABLED command allows you to specify whether or not the port can initiate communications with a remote device using Compressed SLIP (CSLIP) packets. For the situation where the port initiates activity on the SLIP link, when the use of compressed SLIP is enabled, the port will immediately begin transmitting compressed packets on the serial link.

For the situation where the remote device initiates activity on the SLIP link, the port will automatically detect whether or not the remote device is using compressed SLIP packets. The port will use the same type (compressed or uncompressed) of packets as the remote device. The port will do this whether you have SLIP or CSLIP enabled.

A SLIP link can have a number of sessions (or slots), using higher-level protocols such as TCP/IP, operating across the link. This can happen, for example, when the SLIP link is used in a gateway configuration that supports several users, or in a configuration where a single node (such as a dial-in PC) is connected to the port and the single node has several windows in use. RFC 1144 allows a SLIP link to use a maximum of 16 slots. (This is because the compression mechanism is very memory intensive. If too many slots use compression, the terminal server or the remote device could run out of memory resources to perform other tasks.) When Van Jacobson compression is in use on a SLIP link, a Xyplex terminal server will allocate sufficient memory to support 16 slots (the maximum permitted), regardless of the number of slots that will actually be used on the link. If the remote device only supports fewer slots, that number will be the actual number of slots used on the link.

The set-up activities for establishing CSLIP links are nearly identical to those which are contained in the V5.0 *Software Management Guide.*

Privilege Level

Privileged.

Syntax

DEFINE/SET PORT ***port-list*** **INTERNET CSLIP [ENABLED]**
[DISABLED]

Where	Means
port-list	**One or more terminal server ports.**
ENABLED	**The port can initiate communications with a remote device using Compressed SLIP (CSLIP) packets.**
DISABLED	**The port cannot initiate communications with a remote device using Compressed SLIP (CSLIP) packets. This is the default.**

Example

```
Xyplex>> DEFINE PORT INTERNET CSLIP ENABLED
```

DEFINE SERVER ULI

Enable or disable the UNIX like interface for the server

Notes

Use the DEFINE SERVER ULI ENABLED/DISABLED command to make the UNIX like user interface available to users on ther server. When enabled, users have access to all of the commands listed in the guide *Using the ULI Interface.*

After the interface is enabled on the server, it must be activated for indivual ports, by using either the DEFINE PORT ULI command, or by typing the ULI command.

The UNIX like interface is only available on certain multi-megabyte load images. Refer to the kit information supplied with your software kit for more information.

Privilege Level

Privileged

Syntax

DEFINE SERVER ULI [ENABLED]
[DISABLED]

Where	Means
ENABLED	**Enable the UNIX like interface on the server. ENABLED is the default.**
DISABLED	**Disable the UNIX like interface on the server.**

Example

```
Xyplex>> DEFINE SERVER ULI DISABLED
```

DEFINE PORT ULI

Enable or disable the UNIX like interface at ports

Notes

Use the DEFINE SERVER ULI ENABLED/DISABLED command to enable or disable the UNIX like user interface at one or more ports. You can also enable this interface so that it is either the primary interface available to a user, or the only interface that is available to the non-privileged or secure user. (Privileged users will continue to have access simultaneously to both the UNIX like and DECserver like user interfaces, regardless of the setting of this port characteristic.)

The UNIX like interface is only available on certain multi-megabyte load images. Refer to the kit information supplied with your software kit for more information.

Privilege Level

Privileged

Syntax

DEFINE PORT *port-number* ULI [ENABLED]
[ONLY]
[PRIMARY]
[DISABLED]

Where	Means
ENABLED	**Enable the UNIX like interface on the port. When the user logs on to the port, the DLI is still activated. In this mode, users still have access to all ULI and DLI . ENABLED is the default.**
ONLY	**Enable only the UNIX like interface on the port. In this mode, users do not have access to DLI commands from the ULI.**
PRIMARY	**When the user logs on to the port, the ULI is activated. In this mode, users still have access to all DLI commands from the ULI.**
DISABLED	**Disable the UNIX like interface on the port. In this mode, users do not have access to ULI commands from the DLI.**

Example

```
Xyplex>> DEFINE PORT 5 ULI DISABLED
```

ULI

Enable or disable the UNIX like interface

Notes

Use the ULI command to execute UNIX like commands, for users who are using the DECserver like command interface. To use this command, the ULI must be enabled at the server and port, but not activated.

The UNIX like interface is only available on certain multi-megabyte load images. Refer to the kit information supplied with your software kit for more information.

Privilege Level

Non-privileged

Syntax

ULI [*uli-command*]

Where	Means
uli-command	**The ULI command that you want to perform. You can activate the ULI by typing ULI by itself (i.e., without including a *uli-command*).**

Examples

1.
```
Xyplex> ULI
Xyplex%
```

2.
```
Xyplex> ULI netstat
```

DEFINE SERVER SECURID ENABLED/DISABLED

Enable or disable the SecurID client.

Notes

SecurID is a system of server software, client software, and accompanying SecurID cards. The system is designed to secure a TCP/IP computer network, preventing unauthorized users from gaining access to resources on a TCP/IP network, but allowing authorized users to gain access easily to these resources.

You use the DEFINE SERVER SECURID ENABLED/DISABLED to specify whether or not SecurID can be used on a given server.

Refer to the *Software Management Guide* for more information about setting up the SecurID client at the Xyplex server.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

```
DEFINE SERVER SECURID ENABLED/DISABLED
```

Where	Means
ENABLED	**The SecurID feature can be used on this server.**
DISABLED	**The SecurID feature cannot be used on this server. This is the factory default.**

Example

Use the following command to enable the SecurID feature at the server:

```
Xyplex>> DEFINE SERVER SECURID ENABLED
```

The server responds with a message similar to:

```
-705- Change leaves approximately nnnnn bytes free.
```

DEFINE SERVER SECURID ACMBASETIMEOUT

Specify the initial time between prompts for a PASSCODE

Notes

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. If the user types an incorrect PASSCODE, the SecurID client will wait for a period of time before again prompting the user to type a PASSCODE. The terminal server manager can specify the length of the initial period that the SecurID client will wait before prompting the user again. The SecurID software requires that for each incorrect PASSCODE, the client must double the period of time that the user must wait until the client again prompts the user.

Use the DEFINE SERVER SECURID ACMBASETIMEOUT command to specify the length of the initial period that the SecurID client will wait before prompting the user to supply a PASSCODE.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE SERVER SECURID ACMBASETIMEOUT *value*

Where	Means
value	**Specifies the initial time between prompts for a PASSCODE. A valid *value* is a number between 1 and 10 (in seconds); the default is 3.**

Example

```
Xyplex>> DEFINE SERVER SECURID ACMBASETIMEOUT 5
```

DEFINE SERVER SECURID ACMMAXRETRIES

Specify the number of times that the Xyplex unit will attempt to connect to the ACE/Servers

Notes

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. The SecurID client then requests authentication from a SecurID server (which is called an ACE/Server). If the first ACE/Server does not respond to an authentication request, the Xyplex client will request authentication from the alternate servers, in order, until it receives a response. If no ACE/Servers respond, the Xyplex client will repeat the process, until it reaches the limit specified by the DEFINE SERVER SECURID ACMMAXRETRIES characteristic.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE SERVER SECURID ACMMAXRETRIES *value*

Where	Means
value	**Specifies the number of times that the Xyplex client will attempt to connect to the ACE/Servers in its list of ACE/Servers (SERVER0 through SERVER4) in order to authenticate a user. A valid *value* is a number between 1 and 10; the default is 5.**

Example

```
Xyplex>> DEFINE SERVER SECURID ACMMAXRETRIES 4
```

DEFINE SERVER SECURID ACM_PORT

Specify the destination UDP port number to use when sending information to ACE/Servers

Notes

Communication between a SecurID client (the Xyplex unit) and server (ACE/Server) are handled using the Internet User Datagram Protocol (UDP). Both the SecurID server and client must be configured with the same SecurID server UDP port number.

Use the DEFINE SERVER SECURID ACM_PORT command to specify the UDP port number which the Xyplex unit (the SecurID client) will use when communicating with one or more ACE/Servers. The value you specify for this characteristic must match the value you specify at one or more ACE/Servers. The specific ACE/Server characteristic that must match the setting for this command is: acm_port.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE SERVER SECURID ACM_PORT *udp-port-number*

Where	Means
udp-port-number	**Specifies the UDP port number to use when sending information to one or more ACE/Servers (SERVER0 through SERVER4) in order to authenticate a user. A valid *udp-port-number* is a number between 1 and 1023; the default is 755. This value must match the value for the acm_port parameter specified at any ACE/Servers which the Xyplex client will use to authenticate a user.**

Example

```
Xyplex>> DEFINE SERVER SECURID ACM_PORT 1023
```

DEFINE SERVER SECURID ENCRYPTION MODE

Specify the encryption method used in SecurID communications

Notes

All data sent between a SecurID client (the Xyplex unit) and server (ACE/Server) are encrypted. The SecurID client implementation supports two methods: the U.S. Department of Defense Encryption Standard (DES), and a proprietary SDI Block Cipher from Security Dynamics, Inc. Both the SecurID server and client must be using the same encryption method.

Use the DEFINE SERVER SECURID ENCRYPTION MODE command to specify the encryption method used. The value you specify for this characteristic must match the value you specify at one or more ACE/ Servers. The specific ACE/Server characteristic that must match the setting for this command is: use_des.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE SERVER SECURID ENCRYPTION MODE *value*

Where	Means
value	**Specifies the the type of encryption that is used by the SecurID client when it needs to communicate with an ACEserver. SecurID supports two encryption methods: DES (Defense Encryption Standard) and SDI BLOCK CIPHER (proprietary Security Dynamics Technologies, Inc. encryption method). The default method is DES.**

Example

```
Xyplex>> DEF SERVER SECURID ENCRYPTION MODE SDI BLOCK CIPHER
```

DEFINE/SET SERVER SECURID QUERY LIMIT

Specify the maximum number of times that a user can attempt to enter a correct PASSCODE

Notes

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. If the user types an incorrect PASSCODE, the SecurID client will wait for a period of time before again prompting the user to type a PASSCODE. The terminal server manager can specify the maximum number of attempts that a user can make, before the port is completely logged off.

Use the DEFINE SERVER SECURID QUERY LIMIT command to specify the maximum number of attempts that a user can make, before the port is completely logged off.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE/SET SERVER SECURID QUERY LIMIT *limit*

Where	Means
limit	**Specifies the maximum number of times that a user at a Xyplex client can enter a PASSCODE before the Xyplex unit will log out the port. A valid *limit* is a number between 1 and 10; the default is 3.**

Example

```
Xyplex>> DEFINE SERVER SECURID QUERY LIMIT 2
```

DEFINE SERVER SECURID SERVERn

Specify the name or address of SecurID authentication servers

Notes

When a user attempts to log on to a port that requires authentication via SecurID, the port requires that the user specify a PASSCODE which consists of a Personal ID Number (PIN) and a pseudo-random number that is generated by a SecurID card. The SecurID client then requests authentication from a SecurID server (which is called an ACE/Server). If the first ACE/Server does not respond to an authentication request, the Xyplex client will request authentication from the alternate servers, in order, until it receives a response. If no ACE/Servers respond, the Xyplex client will repeat the process.

The terminal server manager can specify the internet-addresses or domain-names of up to five SecurID servers. Use the DEFINE SERVER SECURID SERVER*n* command to specify these internet-addresses or domain-names.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Privileged

Syntax

DEFINE SERVER SECURID SERVER*n internet-address*
DEFINE SERVER SECURID SERVER*n domain-name*

Where	Means
SERVER*n*	**Represents SERVER0 through SERVER4, which are SecurID authentication servers. SERVER0 is the primary SecurID authentication server. SERVER1 through SERVER4 are alternate SecurID authentication servers.**
internet-address	**The internet-address of the primary or alternate SecurID authentication servers.**
domain-name	**The domain-name of the primary or alternate SecurID authentication servers. The default domain-name value for SERVER0 is the domain-name"securid_0."**

Example

```
Xyplex>> DEFINE SERVER SECURID SERVER0 192.12.119.12

Xyplex>> DEFINE SERVER SECURID SERVER1 ACM_HOST.XYPLEX.COM
```

DEFINE/SET PORT SECURID

Enable or Disable the SecurID feature at specific ports.

Notes

Use the DEFINE/SET PORT SECURID ENABLED/DISABLED specify which ports will require SecurID authentication for the user to gain access to the port.

The SecurID feature must first be enabled on the server using the DEFINE SERVER SECURID ENABLED command, and other server characteristics must have been configured appropriately. Refer to the *Software Management Guide* for more information about setting up the SecurID feature.

Privilege Level

Privileged

Syntax

DEFINE/SET PORT [*port-list*] SECURID ENABLED/DISABLED

Where	Means
port-list	**One or more ports where you want to specify the status of the SecurID feature.**
ENABLED	**Enable SecurID at the ports you specify. The ports in the *port-list* will require that the SecurID authenticate the user when he or she logs in.**
DISABLED	**Disable SecurID at the ports you specify. This is the default for this feature.**

Example

This command enables SECURID on ports 10-20.

```
Xyplex>> DEFINE PORT 10-20 SECURID ENABLED
```

SHOW/LIST/MONITOR SERVER SECURID

Display SecurID Client Settings

Notes

Use the SHOW/LIST/MONITOR SERVER SECURID display to view the information about the settings that are currently specified for various SecurID-related characteristics, as well as information about successful and unsuccessful authentication attempts and logins using SecurID.

Refer to the *Software Management Guide* for more information about setting up SecurID characteristics at the Xyplex server.

Privilege Level

Show and List are non-privileged. Monitor is privileged.

Syntax

SHOW/LIST/MONITOR SERVER SECURID

Example

```
Xyplex>> show server securid

TS/720 V5.2 Rom 470003 HW 00.00.00 Lat Protocol V5.2 Uptime: 3 15:43:16
                                                 23 Aug 1993  10:58:20

SecurID Server0: SECURID_0                 Resolved Address:     140.179.159.1
SecurID Server1: SECURID_1                 Resolved Address:    140.179.136.20
SecurID Server2: NONE                      Resolved Address:           0.0.0.0
SecurID Server3: NONE                      Resolved Address:           0.0.0.0
SecurID Server4: NONE                      Resolved Address:           0.0.0.0
SecurID ACMMAXRETRIES:     5               SecurID ACMBASETIMEOUT:           3
SecurID ACM_PORT:          755             SecurID Query Limit:              3
SecurID Encryption Mode:   DES

SecurID Ports Enabled:     1, 3

Successful Logins:         1               Last Unsuccessful Login:     Port_3
Logins without SecurID:    4               Username:                     JSmith
Unsuccessful Logins:       1               Reason:                            1

Attempts to access:  Server0      Server1      Server2      Server3     Server4
Successful:                0            0            0            0           0
Unsuccessful:              0            0            0            0           0
```

Example MONITOR/SHOW SERVER SECURID Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW/ LIST SERVER SECURID display.

Item (Field)	Description
SecurID Server0 through SecurID Server 4	**Shows the domain-name of any primary or secondary ACE/Server hosts that have been defined. The "Resolved Address" field next to each SecurID Server refers to the internet-address currently in use that maps to the domain-name.**
SecurID AMCMAXRETRIES	**Shows the number of times that the Xyplex client will attempt to connect to the ACE/Servers in its list of ACE/Servers in order to authenticate a user.**
SecurID ACM_PORT	**Shows the destination UDP port number to use when sending information to one or more ACE/Servers in order to authenticate a user.**
SecurID Encryption Mode	**Shows the type of encryption that is used by the SecurID client when it communicates with an ACEserver.**
SecurID ACMBASETIMEOUT	**Shows the initial time between prompts for a PASSCODE.**
SecurID Query Limit	**Shows the number of times that a user at a Xyplex client can enter a PASSCODE before the Xyplex unit will log out the port.**
SecurID Ports Enabled	**Shows the ports which require that the SecurID host authenticate the user when he or she attempts to log in.**

The following fields are only shown in SHOW or MONITOR SERVER SECURID displays:

Item (Field)	Description
Successful Logins	**Shows the number of times that users were successfully authenticated and logged on to the server.**
Logins without SecurID	**Shows the number of times users logged on to ports at which SecurID is not enabled.**
Unsuccessful Logins	**Shows the number of times that users attempted to log on to the server, but were unsuccessful at passing SecurID authentication.**
Last Unsuccessful Login	**Shows the name of the last port at which user was not able to be authenticated and logged on. If there have been no unsuccessful login attempts, the display will say "None."**
Username	**Shows the username specified by the last user who was unsuccessful at being authenticated and logged on.**
Reason	**Shows the reason code explaining why the last unsuccessful user was unable to be authenticated. The reason codes that can be shown are:**
Attempts to access: Server0 through Server4	**Shows the number of times that the client attempted to access a primary or alternate ACE/Servers to authenticate a user. When the client received a response from a given ACE/Server, it is listed as a successful attempt to access that ACE/Server. When the client did not receive a response from a given ACE/Server, it is listed as an unsuccessful attempt to access that ACE/Server.**

Code	Explanation
1	Memory allocation failure.
2	User did not enter a PASSCODE.
3	User entered an invalid PASSCODE.
4	User did not enter a new PIN.
5	User entered an invalid new PIN.

DEFINE SERVER PROTOCOL ARAP ENABLED/DISABLED

Enable or disable the ARAP feature at a server.

Notes

The AppleTalk Remote Access Protocol (ARAP) allows a Macintosh user to connect to an AppleTalk network through a Xyplex server. The server transfers AppleTalk packets between the remote Macintosh and the AppleTalk network in such a way that the Macintosh acts as though it were directly connected to the network.

Use the DEFINE SERVER PROTOCOL ARAP ENABLED/DISABLED command to specify whether or not ARAP can be used on a given server.

Refer to the *Software Management Guide* for more information about setting up ARAP at the Xyplex server.

You must reinitialize the server for the change to take effect.

Privilege Level

Privileged

Syntax

DEFINE SERVER PROTOCOL ARAP ENABLED/DISABLED

Where	Means
ENABLED	**The ARAP feature can be used on this server.**
DISABLED	**The ARAP feature cannot be used on this server. This is the factory default.**

Example

Use the following command to enable the ARAP feature at the server:

```
Xyplex>> DEFINE SERVER PROTOCOL ARAP ENABLED
```

The server will respond with the following prompt:

```
ARAP Password>
```

Enter the protocol password at this password prompt. The server will not "echo" the protocol password to the display. Press the <RETURN> key. When you supply the correct password, the following messages appear:

```
Press <RETURN> to modify configuration, any other key to abort.
```

Press the RETURN key when you see this prompt. The server displays the following message:

```
-705- Change leaves approximately nnnnn bytes free.

Xyplex>>
```

DEFINE/SET SERVER ARAP NODE NAME

Specify a name by which the server is known on an AppleTalk network.

Notes

When a remotely connected AppleTalk user connects to the network via a Remote Access server, the name of the Remote Access server is displayed in the Remote Access Status display. The DEFINE/SET SERVER ARAP NODE NAME command allows the server manager to specify the AppleTalk node name that the remote user sees.

The default ARAP node-name is NONE. If you do not specify a node name, the unit will use the server-name specified by the SET/DEFINE SERVER NAME command or, if one is not specified by this command a seven-character name in the form X*nnnnnn*, where *nnnnnn* represents the last 6 digits of the server Ethernet address. (For servers that operate with a parameter server that is a VAX/VMS node, the default name is the DECnet node name that has been assigned by the system manager of that node.)

Privilege Level

Privileged

Syntax

DEFINE/SET [SERVER] ARAP NODE NAME "*node-name*"/NONE

Where	Means
node-name	**Specifies the server's AppleTalk node name. The node name is a quoted, case-sensitive text string that can be up to 32 characters in length and may not contain the double-quote (") character.**
NONE	**Specifies that the server will not have an AppleTalk node name assigned to it. In this case, the server will revert to using the default, which is the server-name. This is the default.**

Example

Use the following command to specify the AppleTalk node name "REMOTEMACS" at the server:

```
Xyplex>> DEFINE SERVER ARAP NODE NAME "REMOTEMACS"
```

DEFINE SERVER ARAP DEFAULT ZONE

Specify the default AppleTalk zone to which the server should connect.

Notes

All AppleTalk devices are found in an AppleTalk zone, which can be an EtherTalk zone, a TokenTalk zone, a LocalTalk zone, etc. There is always a default choice for the zone which the device will join. Xyplex communication servers join an EtherTalk zone.

The DEFINE/SET SERVER ARAP DEFAULT ZONE command allows the server manager to specify the default EtherTalk zone that the server joins after it is initialized. If there is no zone of that name available on the network segment the server will join the default zone for the segment.

Privilege Level

Privileged

Syntax

DEFINE [SERVER] ARAP DEFAULT ZONE "*zone-name*"/NONE

Where	Means
zone-name	**Specifies the AppleTalk zone that the server will attempt to join when it is initialized. The zone name is a quoted, case-sensitive text string that can be up to 32 characters in length and may not contain the double-quote (") character.**
NONE	**Specifies that the server will not be assigned to a specific AppleTalk zone. This is the default.**

Example

Use the following command to specify that after the server initializes, it will attempt to join the AppleTalk zone named "REMOTEZONE":

```
Xyplex>> DEFINE SERVER ARAP DEFAULT ZONE "REMOTEZONE"
```

DEFINE/SET SERVER ARAP PASSWORD

Specify an ARAP login password.

Notes

The server manager can configure a server so that when Remote Access users try to connect, the users must type a login password. There is only one Remote Access login password per server.

Use this command to specify the password that Remote Access users must type when they log on. If you type the password on the DEFINE/SET SERVER ARAP PASSWORD command line, enclose the password in quotation mark characters ("). If you do not type the password on the DEFINE/SET SERVER ARAP PASSWORD command line, the server will prompt you for a password. In this case, do not enclose the password in quotation mark characters. (Also, in this case, the server will not echo the password.)

Privilege Level

Privileged

Syntax

DEFINE/SET [SERVER] ARAP PASSWORD ["***password***"**]**

Where	Means
password	**Specifies the new password that Remote Access users must type when they log on to a server port. The password can be up to 8 characters in length and can not contain the double-quote (") character. Enclose the password in double-quote characters. The password is case-sensitive. The default ARAP password is "access".**

Example

```
Xyplex>> DEFINE SERVER ARAP PASSWORD "REMOTE"
```

REFRESH SERVER CCL NAME

Download a new version of a CCL script to ports which use that script.

Notes

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP). Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command.

Occasionally, you may want to change the contents of a CCL script and then make the server load that CCL script. The REFRESH SERVER CCL NAME command causes the server to re-load the CCL script. Ports that are currently running the CCL script of that name will continue to execute the old version of the script until they exit.

Refer to the documentation supplied with APDA Modem Tool Kit for a description of the CCL script language. Refer to the *Software Management Guide* for a description of how to configure and use script servers.

Xyplex supplies a number of CCL scripts for use with a variety of modems that can be connected to either the communication server serial port or to the Macintosh computer. These are listed in the *Software Kit Information* supplied with your software kit.

Privilege Level

Privileged

Syntax

REFRESH [SERVER] CCL [NAME] "***ccl-name***"

Where	Means
ccl-name	**The name of the CCL script to be loaded at ports which use that script.**

Example

```
Xyplex>> REFRESH SERVER CCL NAME "SupraFAXModem_V.32bis"
```

When you issue the REFRESH SERVER CCL command, if there are any syntax errors in the CCL script, the server will report the number of the line in the script which is in error, and a description of the problem. The following table lists the errors that can be indicated:

Message	Comments/Corrective Action
Memory allocation failure	**There is insufficient free memory left on the server to run the CCL script. Refer to the Chapter on Managing Server Resources in the *Software Management Guide* for some stategies to resolve this problem.**
Unknown instruction name	**A bad instruction was contained in the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**
Value out of range	**An illegal argument value was contained in the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**
Argument missing	**Command requires an argument that is missing. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**
Illegal backslash expresson in string	**In a CCL script, the Backslash (\) character can only be followed by one of the following:** • **two decimal digits** • **the \ character** • **the ^ character** **Refer to the documentation supplied with APDA Modem Tool Kit for more information.**
Numeric argument expected	**A numeric value was expected but not found. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**
String exceeds maximum length	**A text string that was too long was found in the CCL script. The maximum length of a text string is 255 characters. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**
@ANSWER entrypoint missing @HANGUP entrypoint missing @ORIGINATE entrypoint missing	**One of these mandatory commands was missing from the CCL script. Check for the syntax of the command in the documentation supplied with APDA Modem Tool Kit.**

CLEAR SERVER CCL NAME

Delete a CCL script assignment.

Notes

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP). Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command.

Occasionally, you may want to change the name of the CCL script assigned to some ports or stop using a certain CCL script altogether (this is called "unloading" a CCL script.). The CLEAR SERVER CCL NAME command causes the server to unload the CCL script *ccl-name* and free the associated memory. This command will fail if any ports are currently set to run the CCL script *ccl-name*.

Privilege Level

Privileged

Syntax

CLEAR [SERVER] CCL [NAME] "***ccl-name***"

Where	Means
ccl-name	**The name of the CCL script to be unloaded at ports which use that script.**

Example

```
Xyplex>> CLEAR SERVER CCL NAME "SupraFAXModem_V.32bis"
```

DEFINE PORT ARAP ENABLED/DISABLED

Enable or disable the ARAP feature at a port.

Notes

The AppleTalk Remote Access Protocol (ARAP) allows a Macintosh user to connect to an AppleTalk network through a Xyplex server. The server transfers AppleTalk packets between the remote Macintosh and the AppleTalk network in such a way that the Macintosh acts as if it were directly connected to the network.

You use the DEFINE PORT ARAP ENABLED/DISABLED to specify whether or not ARAP can be used on a given port. When ARAP is enabled on a port, interactive sessions and other protocols will not be available on the port (i.e., the port is dedicated only to Remote Access connections).

The unit will verify that certain port characteristics are set properly before enabling Remote Access on the port. These characteristics are:

Characteristic	Setting
PORT ACCESS	LOCAL
PORT FLOW CONTROL	CTS or NONE (depending on configuration)
PORT MODEM CONTROL	DISABLED
PORT AUTOBAUD	DISABLED

There is no SET command for enabling or disabling Remote Access on a port.

Refer to the *Software Management Guide* for more information about setting up Remote Access at the Xyplex server.

The ARAP protocol must be enabled for the server in order to enable Remote Access (ARAP) at one or more ports.

Privilege Level

Privileged

Syntax

DEFINE PORT [*port-list*] ARAP ENABLED/DISABLED

Where	Means
port-list	**One or more ports where you want to specify the status of the Remote Access feature (ARAP).**
ENABLED	**The Remote Access feature (ARAP) can be used on this port.**
DISABLED	**The Remote Access feature (ARAP) cannot be used on this port. This is the default.**

Example

Use the following command to enable ARAP at ports 1 through 5:

```
Xyplex>> DEFINE PORT 1-5 ARAP ENABLED
```

DEFINE PORT ARAP ZONE ACCESS

Specify AppleTalk zones that are available from a given port.

Notes

All AppleTalk devices are found in an AppleTalk zone, which can be an EtherTalk zone, a TokenTalk zone, a LocalTalk zone, etc. There is always a default choice for the zone which the device will join. Xyplex communication servers join an EtherTalk zone. The user can select Chooser entities (printers, file servers, Public Folders, or other peripheral devices) located in other zones.

The DEFINE/SET SERVER ARAP ZONE ACCESS command allows the server manager to specify which AppleTalk zones are available to users at a specific port. This command can be used to restrict remote access to devices in one or more AppleTalk zones.

There is no SET command for changing the ARAP zone access on a port.

Privilege Level

Privileged

Syntax

DEFINE PORT [*port-list*] ARAP ZONE ACCESS ALL/LOCAL/NONE/"*zone-name*"

Where	Means
port-list	**One or more ports.**
ALL	**Users at this port have access to all AppleTalk zones. This is the default.**
LOCAL	**Users at this port have access only to the AppleTalk zone that the server is in.**
NONE	**Users at this port have access to no AppleTalk zones. While users cannot see services on the network, they can still provide services to others.**
zone-name	**Users at this port have access to the specific AppleTalk zone specified by the zone-name, in addition to the zone that the server is in. The zone name is a quoted text string that can be up to 32 characters in length and may not contain the double-quote (") character.**

Example

```
Xyplex>> DEFINE PORT 1-5 ARAP ZONE ACCESS NONE
```

DEFINE PORT ARAP MAXIMUM CONNECT TIME

Specify the maximum time users can remain connected.

Notes

The server manager can configure a port so that ARAP users have a limited amount of time in which to remain connected. When the ARAP session reaches the limit, the server will disconnect the session. Use the DEFINE PORT ARAP MAXIMUM CONNECT TIME command to specify this limit.

There is no SET command to change this value temporarily.

Privilege Level

Privileged

Syntax

DEFINE PORT [*port-list*] ARAP MAXIMUM CONNECT TIME *time*/UNLIMITED

Where	Means
port-list	**One or more ports.**
time	**Users at this port can remain connected for a limited amount of time. Specify the amount of time in minutes.**
UNLIMITED	**Users at this port can remain connected for an indefinite amount of time. This is the default.**

Example

Use the following command to limit the amount of time users at ports 1 through 5 can remain to 30 minutes.

```
Xyplex>> DEFINE PORT 1-5 ARAP MAXIMUM CONNECT TIME 30
```

SET PORT ARAP TIME REMAINING

Specify how much time remains in an active Remote Access session before the server disconnects the session.

Notes

The server manager can configure a port so that Remote Access users have a limited amount of time in which to remain connected using the DEFINE PORT ARAP MAXIMUM CONNECT TIME command. The manager can use the SET PORT ARAP TIME REMAINING command to change this for one or more ports, while there are active Remote Access sessions. This changes the remaining amount of time the user has available for the session. The user of the session will be notified that the server manager has changed the time remaining for the current session, and how much time remains. This gives users an opportunity to finish whatever they are doing and log out the port. The next time a user logs on to the port, that user will be allowed to remain connected for the period of time specified by the PORT ARAP MAXIMUM CONNECT TIME characteristic.

Note: A server manager does not need to use this command prior to reinitializing the server, in order to notify users that the server will be reinitializing. When you use the INITIALIZE DELAY *time* command, and *time* is greater than 1 minute, the server notifies all logged in ports. Refer to the description of the INITIALIZE command in the *Commands Reference Guide*.

There is no DEFINE command for changing this value.

Privilege Level

Privileged

Syntax

SET PORT [*port-list*] ARAP TIME REMAINING UNLIMITED/NONE/*time*

Where	Means
port-list	One or more ports.
UNLIMITED	Users at this port can now remain connected for an indefinite amount of time.
NONE	Users at this port will be disconnected immediately (i.e., they have no more time).
time	Users at this port can now remain connected only for the specified amount of time. Specify the amount of time in minutes. The user will be notified of the change.

Example

```
Xyplex>> DEFINE PORT 1-5 ARAP TIME REMAINING 5
```

DEFINE PORT ARAP GUEST LOGINS ENABLED/DISABLED

Enable or Disable guest logins to the server by remote access users.

Notes

When a user connects to the network via Remote Access, the Remote Access login window includes an option to allow users to log on to the device as a "guest" user (no password is required to log in as a guest user), rather than as a "registered" user. Administrators of AppleTalk Remote Access servers can control whether or not guest logins are permitted on one or more ports.

The DEFINE PORT ARAP GUEST LOGINS command allows the server manager to specify whether or not users can login to the Remote Access server as a guest.

There is no SET command.

Privilege Level

Privileged

Syntax

DEFINE PORT [*port-list*] ARAP GUEST LOGINS ENABLED/DISABLED

Where	Means
port-list	**One or more ports.**
ENABLED	**A user at this port can login as a guest user.**
DISABLED	**A user at this port can not login as a guest user. This is the default.**

Example

```
Xyplex>> DEFINE PORT 1-5 ARAP GUEST LOGINS ENABLED
```

DEFINE PORT CCL NAME

Specify which CCL script will apply to a port.

Notes

CCL scripts are ASCII text files which contain commands that specify initialization and operational characteristics for the specific type of modem that is connected to a port. CCL scripts are stored at script servers (hosts which can transfer a file to the server via TFTP) and usually indicate the type of the modem connected to the port. Individual ports can be configured to use a specific CCL script using the DEFINE PORT CCL NAME command. If no CCL script is specified on the port, the server manager must manually configure the port and modem properly for Remote Access operation.

Xyplex supplies CCL scripts for use with a variety of modems. These are listed in the *Software Kit Information* supplied with your software kit.

There is no SET command.

***Note Regarding MAXserver 800 and 1600 Terminal Servers:* CCL scripts can instruct a port to use a port speed (baud rate) higher than 38,400 bits per second. (In a CCL script, these instructions use either the CCL script language "serreset" or "setspeed" commands.) However, the maximum port speed for a MAXserver 800 and 1600 Terminal Server is 38,400 bps. The server will not load a script which contains instructions to set the port to a speed that is higher than the maximum. You can determine that this situation is occurring either by issuing the REFRESH CCL "*ccl-name*" command or by examining the SHOW/MONITOR PORT STATUS display. This display will continously switch between the ARAP Initializing and ARAP Enable Wait states. To correct this problem, edit the CCL script and remove or comment out the offending commands.**

Refer to the the documentation supplied with APDA Modem Tool Kit for a description of the CCL script language. Refer to the *Software Management Guide* for a description of how to configure and use script servers.

Privilege Level

Privileged

Syntax

DEFINE PORT [*port-list*] CCL [NAME] "*ccl-script-file*"/NONE

Where	Means
port-list	**One or more ports.**
"*ccl-script-file*"	**The name of a CCL script, which is located in a /CCL sub-directory at a script server.** **For purposes of configuring a script server, the complete location (directory path and name) for the ccl-script-file is:** ***directory-path*/CCL/*ccl-name*** **In this case, *directory-path* represents the directory on the script server where scripts are stored. You use the DEFINE SERVER SCRIPT SERVER command to specify the *directory-path*. The *directory-path* is usually the TFTP home directory on a UNIX host. CCL scripts are contained in a /CCL sub-directory of the *directory-path*. *ccl-name* is a file name which usually indicates the type of the modem connected to the port. Refer to the *Software Management Guide* for a description an Network Command Script Setup.** **All space characters are removed from the name before it is concatenated with the directory path. The '/' characters above indicate where the separator character will be inserted in the path.**
NONE	**The port will not be a assigned CCL script. This is the default.**

Example

```
Xyplex>> DEFINE PORT 1-5 CCL NAME "Telebit_T3000"
```

DEFINE/SET PORT CCL MODEM AUDIBLE/INAUDIBLE

Specify whether or not the modem speaker should be audible while the modem establishes a connection.

Notes

Server managers can configure a port so it indicates to the CCL script whether or not the modem speaker should be audible while the modem establishes a connection. Whether or not the modem speaker is audible has no effect on CCL script execution.

Privilege Level

Privileged

Syntax

DEFINE/SET PORT [*port-list*] CCL [MODEM] AUDIBLE/INAUDIBLE

Where	Means
port-list	**One or more ports.**
AUDIBLE	**Indicate to the CCL script that the modem should be audible while the modem establishes the connection.**
INAUDIBLE	**Indicate to the CCL script that the modem should not be audible while the modem establishes the connection. This is the default.**

Example

```
Xyplex>> DEFINE PORT 1-5 CCL MODEM INAUDIBLE
```

SHOW/LIST SERVER ARAP CHARACTERISTICS

Display information about Remote Access server settings.

Notes

Use the SHOW/LIST SERVER ARAP CHARACTERISTICS display to view information about the settings that are currently specified for various ARAP characteristics, and at which ports the ARAP feature is enabled.

Privilege Level

Non-privileged.

Syntax

SHOW/LIST [SERVER] ARAP [CHARACTERISTICS]

Example

```
Xyplex> show server arap characteristics

ARAP Node:           REMOTEMAC
ARAP Default Zone:   REMOTEZONE
ARAP Current Zone:   AppleTalk
ARAP Ports:          1, 2, 3
```

Example SHOW SERVER ARAP CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the SHOW/LIST SERVER ARAP CHARACTERISTICS display.

Item (Field)	Description
ARAP Node:	**Shows the server's AppleTalk name.**
ARAP Default Zone:	**Shows the name of the AppleTalk/EtherTalk zone that the server will attempt to join when it is initialized.**
ARAP Current Zone:	**Shows the name of the AppleTalk zone to which the server currently belongs. (This field is only displayed when you use the SHOW command.)**
ARAP Ports:	**Shows the ports at which the ARAP feature is enabled.**

SHOW SERVER CCL

Display a list of CCL scripts loaded on the server.

Notes

Use the SHOW SERVER CCL display to view the names of loaded CCL scripts and the ports to which they are assigned.

Privilege Level

Non-privileged.

Syntax

SHOW [SERVER] CCL [*"ccl-name"*]
[ALL]

Where	Means
ccl-name	**Show the ports at which a specific CCL script is loaded.**
ALL	**Show a display listing all CCL scripts that are loaded at port on this server, and indicate which ports the scripts are loaded on. This is the default.**

Example

```
Xyplex> show server ccl all

CCL script "SupraFAXModem_V.32bis" loaded, not used by any port
CCL script "ZOOMV32.ARA" loaded, not used by any port
CCL script "Telebit_T3000" loaded, in use by port(s) 1 2
```

Example SHOW SERVER CCL Display.

SHOW/LIST/MONITOR PORT ARAP CHARACTERISTICS

Display information about port ARAP settings.

Notes

Use the SHOW/LIST/MONITOR SERVER ARAP display to view information about the settings that are currently specified for various ARAP characteristics at a port.

Privilege Level

Show and List are non-privileged. Monitor is privileged.

Syntax

SHOW/LIST/MONITOR PORT [*port-list*] ARAP [CHARACTERISTICS]

Where	Means
port-list	**One or more ports.**

Example

```
Xyplex> show port 1 arap characteristics

Port 1:  Mac1                              04 Aug 1993  19:51:53

ARAP Enabled:               Enabled
ARAP Zone access:           All
ARAP Guest Logins:          Disabled
ARAP Maximum Connect Time:  0:60:00
Time Connected:             0:29:44
Time Remaining:             0:30:16
```

Example MONITOR/SHOW/LIST PORT ARAP CHARACTERISTICS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW/ LIST PORT ARAP CHARACTERISTICS display.

Item (Field)	Description
Port *n*:	**Shows the number of the port, *n*, and the username of the user who is logged on to the port.**
ARAP Enabled:	**Shows whether or not Remote Access is enabled at the port. Enabled means that the port is configured to support Remote Access connections. (In this case, other types of connections are not allowed.) Disabled means that the port is not configured to use Remote Access connections.**
ARAP Zone access:	**Shows which, if any AppleTalk zones that are available to users at this port. If a specific zone-name is listed, the user only has access to that zone, in addition to the zone that the server is in. Otherwise, one of the following will be listed:** **All** — **The user at this port has access to all AppleTalk zones.** **Local** — **The user at this port has access only to the zone that the server is in.** **None** — **The user at this port has access to no AppleTalk zones.**
ARAP Guest Logins:	**Shows whether or not users at this port can log on to the device as a "guest" user (no password is required to log in as a guest user), rather than as a "registered" user. Enabled means that users can log on in as a guest user (or, optionally, as a registered user). Disabled means that the user must log on as a registered user.**
ARAP Maximum Connect Time:	**Shows the maximum amount of time (in minutes) that a user can remain connected to this port, if the port has been configured with a time limit. If there is no time limit, this field will show that the user can be connected for an "Unlimited" amount of time. When the ARAP session reaches the limit, the server will disconnect the session.**
Time Connected:	**Shows the amount of time that the user in the current session has been connected to this port. (This field is only displayed in SHOW or MONITOR displays and only when ARAP is enabled at the port.)**
Time Remaining:	**Shows the maximum amount of time (in minutes) that a user can remain connected to this port If there is no time limit for the currently connected session, this field will show that the user can be connected for an "Unlimited" amount of time. (This field is only displayed in SHOW or MONITOR displays and only when ARAP is enabled at the port.)**

SHOW/MONITOR PORT ARAP COUNTERS

Display information about Remote Access activity.

Notes

Use the SHOW/MONITOR PORT ARAP COUNTERS display to view information about the activity at ports which are configured to use Remote Access.

Counters in this display correspond to the interface counters in the SNMP MIB.

Privilege Level

Show is non-privileged. Monitor is privileged.

Syntax

SHOW/MONITOR PORT [port-list] ARAP COUNTERS

Where	Means
port-list	**One or more ports.**

Example

```
Xyplex> show port arap counters

Port 1:  Mac1                              04 Aug 1993  19:51:53

Number of bytes received:                                  0
Number of bytes transmitted:                               0
Number of uni-cast packets received:                       0
Number of uni-cast packets transmitted:                    0
Number of received packets discarded:                      0
Number of transmitted packets discarded:                   0
Number of received packets in error:                       0
Number of received packets of unknown type:                0
Length of transmit packet queue:                           0
```

Example MONITOR/SHOW PORT ARAP COUNTERS Display.

The following table describes each of the items (fields) of data in the MONITOR/SHOW PORT ARAP COUNTERS display.

Item (Field)	Description
Port *n*:	**The number of the port, *n*, and the username of the user who is logged on to the port.**
Number of bytes received:	**The total number of bytes received by the serial port, since the counters were last reset to zero.**
Number of bytes transmitted:	**The total number of bytes sent by the serial port, since the counters were last reset to zero.**
Number of uni-cast packets received:	**The total number of ARAP unicast packets that have been received by the serial port, since the counters were last reset to zero.**
Number of uni-cast packets transmitted:	**The total number of ARAP unicast packets that have been transmitted by the serial port, since the counters were last reset to zero.**
Number of received packets discarded:	**The number of ARAP packets that have been received and discarded, since the counters were last reset to zero. A large value usually indicates poor telephone line quality or insufficient buffer (typeahead) capacity.**
Number of transmitted packets discarded:	**The number of ARAP packets that were not transmitted, since the counters were last set to zero.**
Number of received packets in error:	**The number of ARAP packets that have been received and discarded because they contained an error, since the counters were last reset to zero. A large value usually indicates poor telephone line quality.**
Number of received packets of unknown type:	**The number of packets that have been received and discarded because they did not appear to be ARAP packets, since the counters were last reset to zero. A large value could indicate poor telephone line quality.**
Length of transmit packet queue:	**The number of ARAP packets that have not yet been transmitted, since the counters were last reset to zero. A large value (greater than 3) means that the link is running slowly or that packets are being received from the Ethernet network too quickly to be processed.**

Index

A

B

C

D

E

F

G

H