DIGITAL NetRider

Network Access Server Command Reference

Part Number: AA-PW5WE-TE

June 1997

Revision/Update Information: This is a revised document.

Software and Version: DECserver Network Access Software, Version 2.2

Contents

3 CLEAR/PURGE Commands

4 SET/DEFINE/CHANGE Commands

5 SHOW/MONITOR/LIST Commands

Preface

About This Manual

The *Network Access Server Commands* manual is written for the person who sets up, maintains, and manages any one of the Digital Equipment Corporation family of network access servers. This individual must be familiar with the use of a terminal on a DIGITAL Network Access Server.

Using This Manual

This manual details the commands you need to operate and manage your access server, and should be used with the *Network Access Server Management* manual.

If you have an optional network management product, such as Terminal Server Manager (TSM) software, review the documentation for the product before you read this manual and other access server documents. TSM software affects the way you install and manage access servers.

Associated Documents

For additional information on DIGITAL networking products, please refer to the following manuals:

- *LAT Network Concepts* — Provides an overview of the LAT protocol.
- *Terminal Server Manager Installation and Use* — Provides the procedures to install and use TSM.
- *DECserver 700 Site Preparation and Maintenance* — Provides the procedures to prepare the site before installing the DECserver 700 hardware.
- *DECserver 90TL/DECserver 90M Owner's Manual* — Provides the procedures to install and operate the DECserver 90TL/DECserver 90M hardware.
- *DECserver 900TM Installation* — Provides the procedures to install and operate the DECserver 900TM hardware.

- *VMS VAXcluster Manual* — Provides the procedures to configure a VAXcluster system, including the procedure to configure the system for remote printing.
- *ULTRIX Guide to System Environment Setup* — Provides the procedures to configure the ULTRIX system environment, including the procedure to configure print systems.
- *Release Notes* — Provides the latest information about the access server. The release notes are available with the software distribution kit and are stored in the load host directory with the other software distribution files.
- *DECserver Network Access Software Installation* — Describes how to install the network access software on Microsoft Windows 95 or Windows NT, OpenVMS, DIGITAL UNIX, ULTRIX, or UNIX operating systems.
- *Network Access Server Management* — Provides the procedures to perform management tasks for the various access servers.
- *Network Access Server Problem Solving* — Describes problem-solving tools and procedures for the various access servers.

Conventions

Overview

This book uses the following conventions:

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

Convention	Description
`special type`	Special type indicates the following: an example of system output or user input, directories, scripts, and file names. User input is in bold.
Boldface text	Boldface text, in summaries of characteristics, indicates default values.
lowercase italic text	Lowercase italic text indicates variables for which you specify or the system supplies actual values.
UPPERCASE TEXT	Uppercase text in command lines indicates keywords that must be entered. You can enter them in either uppercase or lowercase. You can abbreviate command keywords to the first three characters or to the minimum unique abbreviation.
/	A slash indicates related alternate commands or options. For example, SET/DEFINE/CHANGE PORT refers to the SET PORT, DEFINE PORT, and CHANGE PORT commands. The slash (/) is not part of the command syntax.
[]	Brackets in the command syntax indicate that the enclosed values are optional. You can enter one or none. (Do not type the brackets.)
{}	Braces in the command syntax indicate that you must choose one of the enclosed options. (Do not type the braces.)
Ctrl/*n*	This syntax indicates a keying sequence for which you must hold down the Ctrl key while pressing the key specified by the variable *n*.

How to Order Additional Documentation

To order additional documentation, use the following information:

To Order:	Contact:
By Telephone	USA (except Alaska, New Hampshire, and Hawaii): 1-800-DIGITAL (1-800-344-4825) Alaska, New Hampshire, and Hawaii: 1-603-884-6660 Canada: 1-800-267-6215
Electronically (USA only)	Dial 1-800-DEC-DEMO (For assistance, call 1-800-DIGITAL)
By Mail (USA and Puerto Rico)	DIGITAL EQUIPMENT CORPORATION P.O. Box CS2008 Nashua, New Hampshire 03061 (Place prepaid orders from Puerto Rico with the local DIGITAL subsidiary: 809-754-7575)
By Mail (Canada)	DIGITAL EQUIPMENT of CANADA LTD. 940 Belfast Road Ottawa, Ontario, Canada K1G 4C2 Attn.: A&SG Business Manager
Internationally	DIGITAL EQUIPMENT CORPORATION Attn.: A&SG Business Manager c/o local DIGITAL subsidiary or approved distributor
Internally	U.S. Software Supply Business (SSB) DIGITAL EQUIPMENT CORPORATION 8 Cotton Road Nashua, New Hampshire 03063

Correspondence

Documentation Comments

If you have comments or suggestions about this document, send them to the DIGITAL documentation organization.

Attn: Documentation Project Manager

Fax: (508) 486-5655

E-mail: doc_quality@lkg.mts.dec.com

Online Services

To locate product-specific information, refer to the following online services:

BBS

To read the Bulletin Board System, set your modem to 8 bits, no parity, 1 stop bit, and dial 508-486-5777 (U.S.). Outside of the U.S., dial (access code) 1-508-486-5777.

WWW

The Digital Equipment Corporation Network Products Business Home Page on the World Wide Web is at the following addresses:

North America:	http://www.networks.digital.com
Europe:	http://www.networks.europe.digital.com
Australia:	http://www.digital.com.au/networks

Chapter 1

Using Network Access Server Commands

Overview

Introduction

This chapter briefly describes features of the access server that you should be familiar with to effectively use the access server commands.

Reference

For more information about using the commands in this manual to manage your access server, refer to the *Network Access Server Management* manual.

Each command in the following chapters will be presented with the following information:

- Syntax
- Description
- Functionality
- Security level to the lowest level
- Description of command characteristics, if any

Where applicable, command restrictions and examples are also provided.

Command keywords can be abbreviated to the smallest number of characters that distinguish the keyword to the access server. The command syntaxes in this chapter use the graphic conventions outlined in the Preface.

Online Help

Introduction

You can display brief descriptions of all access server commands and characteristics available for the security level of your port by typing HELP at the access server prompt. The access server also offers tutorial help, which describes various end-user tasks.

User Security Levels

Three levels of security are available for access server ports:

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

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

- **Nonprivileged status** — Nonprivileged status is the default for all interactive ports. Users at a nonprivileged port cannot access commands that change the state of the access server or other ports, but they can use all commands required for connecting to LAT services, Internet hosts, and network connections from an interactive port.

  Nonprivileged users can also modify certain port characteristics and display information about the access server, its ports, and service nodes. Chapter 2 identifies the commands available to nonprivileged users.

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

Chapter 2 identifies all the commands that you can enter from a secure port by the designation "available to all users." To view all secure commands, SET PORT SECURITY ENABLED and then access online help. The commands listed will be those available to secure users.

Naming Conventions

Naming Conventions for Access Servers and LAT Services

Some commands require you to enter an access server, node, port, or service name. All of these names must be a string of 1 to 16 characters and cannot be abbreviated. Allowable characters are A to Z, 0 to 9, $, - (hyphen), _ (underscore), and . (period). The access server converts all lowercase letters to uppercase letters.

The exception is DECnet node names. DECnet node names (not LAT node names) must have 1 to 6 alphanumeric characters, including at least one alphabetic character.

DECnet node names and access server names must be unique on a local area network (LAN), and port names must be unique on a network access server. Digital recommends that you set the server name to match the DECnet node name for the server. LAT service names must be unique for each service on the LAN; however, one service may be offered by multiple service nodes.

These naming conventions do not apply to user names, access server, or service identification messages.

Reference

For more details, refer to the *Network Access Server Management* manual.

Naming Conventions for Internet Host Names

Each Internet node, called a host, is given an Internet domain name. The format of a domain name is the concatenation of all the labels of the domains from the host up to the root. A label is the name of a single level or domain in a tree-structured name space. The labels that compose a domain name are printed or read left to right, from the most specific (lowest, farthest from the root) to the least specific (highest, closest to the root). The labels are separated by dots or periods. Each label can be one to 63 characters in length. The maximum number of characters that can represent a domain name is 255. For example, the domain name **falcon.nac.tmp.com** contains 4 labels (**falcon, nac, tmp,** and **com**), which along with the periods comprise a total of 18 characters. Any suffix of labels in a domain name is called a domain. In the above example, the lowest level domain is **falcon.nac.tmp.com**; the second level domain is **nac.tmp.com**; the third level domain is **tmp.com**; and the top level domain is **com**. The root domain is specified by a dot.

Domain names can be of two types, either absolute (fully qualified) or relative. An absolute domain name has all the labels from the host to the root present in the name. A relative domain name has fewer labels, and is a domain name prefix. For example,

falcon.nac.tmp.com is a fully qualified domain name for the host **falcon**, and **falcon** is a relative domain name for the host **falcon**. Thus, a relative domain name becomes an absolute domain name by appending the current default domain **nac.tmp.com**.

A default domain, such as **nac.tmp.com**, can be specified in the access server name resolution database using the SET/DEFINE/CHANGE NAME RESOLUTION command. If specified, the access server appends this information when it receives a user query for a relative domain name, such as **falcon**. Relative domain names can also consist of multiple labels, for example **falcon.nac**. In this case, appending the default domain name **nac.tmp.com** probably will not form the correct fully qualified domain name. The access server then reforms the name with higher level domains taken from the default domain string. For example, for **falcon.nac** it tries this sequence of names:

falcon.nac.nac.tmp.com

falcon.nac.tmp.com

and finally the relative domain name itself

falcon.nac

If the user types **falcon.nac.** with the dot at the end, the access server assumes that this is a fully qualified domain name. In this case, it tries only that name and does not use the default domain labels to construct names.

Naming Conventions for Kerberos Principal Names

In Kerberos, both servers and clients (users) are named with a Kerberos principal name. The format of a principal name is **name.instance@realm**. The **name** is the name of the user or service. These Kerberos principal names can be up to 40 ASCII characters. The **instance** may entail special privileges (much as the UNIX “root” user). The **realm** is the name of an administrative entity or domain that contains authentication data for all its members. Realm names are formatted like a DNS domain. For example: Jones@finance.acme.com or Jones.superuser@finance.acme.com.

Naming Conventions for Other Authentication Services

The Access Server uses the Kerberos realm name concept for other supported authentication services, for example, RADIUS, SecurID, and the Local User Database. The realm name selects the available authentication protocols and servers.

Specifying Passwords

Conventions for Specifying Passwords

Unless Chapter 2 states otherwise, all passwords have 1 to 16 ASCII characters. When specifying passwords in access server commands, either enclose the password in quotation marks and include it in the command line, or enter the command without the password and let the access server prompt you for it.

You can omit the password value and be prompted only if the password characteristic is the only characteristic in the command line.

The access server does not echo a password that is entered in response to a password prompt. When you specify a new password, the access server displays a verification prompt and waits for you to reenter the password (which is again not echoed). If both entries match, the password is established and the local mode prompt is displayed. If they do not match, the access server returns to the local mode prompt. Some examples of password specification follow:

```
Local> SET SERVER LOGIN PASSWORD "SECRET"
Local> SET SERVER LOGIN PASSWORD
Password> SECRET (not echoed)
Verification> SERCET (not echoed)
Local -742- Password verification failed
Local> SET SERVER LOGIN PASSWORD
Password> SECRET (not echoed)
Verification> SECRET (not echoed)
```

Press Ctrl/Z at any time to interrupt password processing and return to the local mode prompt.

You can change the access server characteristics LOGIN PASSWORD, REMOTE PASSWORD, and PRIVILEGED PASSWORD, but you cannot clear them; you can change or clear the service characteristic PASSWORD and the access server characteristic MAINTENANCE PASSWORD.

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

To clear MAINTENANCE PASSWORD, you can specify “0” in the command line or enter 0 in response to the password prompt. For details, refer to the command descriptions in Chapter 2.

Specifying a Port List

Conventions for Specifying a Port List

When specifying a port list in an access server command, the port-list line can contain either a single port or a port range (low to high or high to low). Use the DEFINE PORT command to change the port characteristics that take effect when the port is logged in to next time. Use the SET PORT command to change the port characteristics that you wish to take effect immediately, but stay in effect only until you log out. Use the CHANGE PORT command to perform both DEFINE and SET PORT.

When setting port characteristic(s) for one or more port characteristics options, you can embed spaces in the *port-list* value. Some examples for port-list specification follow:

```
Local> SET PORT 1, 2, 3
Local> SET PORT 1-4
Local> SET PORT 1, 2, 3, 7-9
Local> SET PORT 7-9, 3, 2, 1
```

Entering Commands

Entering Commands

This section describes command line editing features for entering access server commands.

Command Prompting

If you type a question mark (?) at any point in a command, the access server will display a list of all the legal keywords or data types at that point in the command.

In the following examples, the words that start with capital letters are KEYWORDS. The capital letters indicate the minimum abbreviation for the keyword.

Uncapitalized words are data types. In the second example, internet_addr starts with a lower case letter, and indicates that the server is looking for an Internet address. In the third example, only the carriage return is allowed.

If you use command recall after the command prompter has displayed the list, the question mark will not appear and you can simply type the keyword you select at the end of the recalled line.

Examples: Prompting for Commands

```
Local> SET ?
COMmand         INTernet        KERberos        MENu
NOPrivileged    POrt            PRIvileged      SERVEr
SERVIces        SESsions        SNMP            SYStem
TELnet          TN3270

Local> SET INTERNET ?
ADdress         ARP             GATeway         HOSt
MASk            NAMEServer      NAme            SUBnet

Local> SET INTERNET ADDRESS ?
NONe            internet_addr
Local> SET INTERNET ADDRESS 16.20.49.33 ?   <Return>
```

Command Line Editing and Recall

The access server supports command line editing and recall.

Note

For command line editing and recall to work on a particular port, the port type characteristic must be set to ANSI (this is the default). For more information, refer to the SET/DEFINE/CHANGE PORT TYPE command.

Command line editing enables you to use the left arrow and right arrow keys and the delete key on your keyboard to modify the access server local command currently being entered.

Command line recall enables you to use the up arrow and down arrow keys on your keyboard to restore previously executed access server local commands. Once restored, the command can also be edited using the command line editing feature.

Command Requirements and Restrictions

You can enter the access server commands in either uppercase or lowercase characters, or a combination of both. Separate the words in a command line by one or more spaces.

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

You can interrupt current local mode output by pressing the Break key or by entering your local switch character. When a TN3270 session is interrupted with the Break or the local switch character, you are placed in the local mode with the cursor positioned at the last row of the screen.

When a command executes, or fails to execute, you get a status or error message. If you make an error in a command line, the access server rejects the entire command line. If you get an error message, check the command syntax and reenter all or part of the command as necessary. When a command has executed successfully, the access server displays a local mode prompt.

Special Keys

Special Keys Table

The following table describes the special keys that you can use when entering commands:

Key	Function
Delete	Deletes the last character entered in the current command line.
Ctrl/U	Deletes the entire current command line.
Ctrl/Z	Operates like Ctrl/U except when entered in response to a password prompt or password verification prompt. In that case, it cancels the password processing and causes the access server to return to local mode. A Ctrl/Z in response to a username prompt causes the defined port name to be used for the user names. Exception: Ctrl/Z does not unlock a locked terminal. (Refer to the LOCK command.)
Ctrl/R	Retypes the current command line (helpful after using the delete key on a hardcopy terminal).
Return	Executes the current command line.

Chapter 2

Command Descriptions

Command Descriptions Overview

Introduction

This chapter describes the access server commands that are not explained in one of the following command categories: Clear/Purge, Set/Define/Change, or Show/Monitor/List.

Reference

For more information about the commands used in this chapter, refer to the *Network Access Server Management* manual.

Getting Help

To get help at any time with commands, enter a question mark (?) at the prompt. A list of all the legal keywords or data types you can use at that point in the command will appear.

Commands BACKWARDS - CRASH

BACKWARDS (secure)

Syntax

BACKWARDS

Description

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

Note

Using the BACKWARDS command within a TN3270 session will cause the screen to be cleared and the TN3270 screen displayed. The information displayed will be the information that existed prior to the interrupt.

Restriction

You cannot use the BACKWARDS command on a port that has the MULTISESSIONS characteristic set to ENABLED. For more information, refer to the PORT MULTISESSIONS (secure).

BROADCAST (nonprivileged)

Syntax

Description

This nonprivileged command sends a message to other access server ports.

Keywords

PORT *port-list*

Specifies one or more ports to receive your message. For more information, refer to Chapter 1.

ALL

Is a privileged parameter specifying that the message is sent to all ports on the access server.

message-text

Is the text of the message (maximum of 115 characters, as space permits on the command line). The access server broadcasts the message in uppercase letters unless you enclose it in quotation marks. You cannot embed quoted text within the message.

Your message is sent unless one of the following conditions exists:

- The port has the port characteristic BROADCAST set to DISABLED. (A warning message is displayed.)
- A currently active LAT session on the port is set to PASSALL or PASTHRU mode. For more information, refer to the SET SESSION LAT command.
- The port is logged out or has a dedicated service.
- The port has an active SLIP or PPP session.
- Output flow control from the access server to the port is turned off.

Restriction

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

Example: BROADCAST

```
Local> BROADCAST PORT 7 "Lunch today?"
```

This command sends the string “Lunch today?” to port 7.

CLOSE PORT (secure)

For information on CLOSE and CLOSE PORT, refer to DISCONNECT/CLOSE PORT (privileged).

CONNECT (secure)

Syntax

Description

This secure command requests a connection to the LAT service. For more information, refer to the CONNECT ANY (secure), CONNECT AUTOLINK (secure), CONNECT [DIAL] (secure), CONNECT PORT (privileged), CONNECT PPP (secure), CONNECT SLIP (secure), and CONNECT/OPEN TELNET (secure).

Keywords

service-name

Specifies the named service on an access server to which you want to connect (default: your preferred service if defined). If the service is offered by multiple service nodes, the access server connects to the node with the highest service rating.

NODE *node-name*

Specifies a particular service node to which you want to connect. (The default is the highest-rated node offering the service.)

DESTINATION *port-name*

Specifies a particular access server port to which you want to connect. (The default connects you to the first available port offering the service.) Users who specify DESTINATION without specifying NODE are connected to the specified port on the local access server node, provided it offers the service.

PORT

Specifying PORT will connect you to the port's preferred service.

LAT or SERVICE (Optional keywords)

Specifies that only LAT will be used to attempt connection. If missing from the command line, the access server will use the port default protocol. LAT protocol is the factory-set default protocol.

Example: CONNECT

```
Local> CONNECT

Local> CONNECT SALES

Local> CONNECT METDATA NODE DATAserver DESTINATION PORT_6
```

The first command connects the port to its preferred service, provided one is defined. The second command connects the port to the service SALES. The last command connects the port to the service METDATA at PORT_6 on the access server DATA-server.

CONNECT ANY (secure)

Syntax

CONNECT [ANY] [*host-name*]

Description

This command (available to all users) determines whether a specified host is using the LAT or Telnet protocol. The access server first checks the LAT protocol; if that fails, the server checks the Telnet protocol. When a protocol is found, the access server establishes a connection to that host.

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

Keyword

host-name

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

Restriction

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

Example: CONNECT ANY

```
Local> CONNECT ANY FALCON
```

This command checks the host FALCON to see if it uses the LAT protocol or the Telnet protocol, then connects to the host FALCON.

CONNECT AUTOLINK (secure)

Syntax

CONNECT [AUTOLINK]

Description

This command (available to all users) allows a dial-in port to be configured for both PPP and SLIP protocols, and for character-cell terminal use.

Restrictions

- The port must have SLIP or PPP enabled.
- Only one SLIP or PPP session per port is allowed at any given time.
- The incoming data must use either PPP or SLIP protocol, or be an interactive terminal session.
- Both Multisessions and ODL must be disabled.

Example: CONNECT AUTOLINK

```
Local> CONNECT AUTOLINK
```

This command examines incoming data. If a PPP or SLIP packet is detected, the session attempts to change itself into a PPP or SLIP session. If a single carriage return is detected or a user-settable timeout occurs, the session will be interactive.

CONNECT [DIAL] (secure)

Syntax

CONNECT [DIAL] *dial-service-name*

Description

This command requests a connection be established using the given dial service. It is functionally equivalent to the DIAL command. On a port that defaults to the DIAL protocol, the DIAL keyword in this command is optional. If the selected dial service does not define the mode or the phone number for the new session, you will be prompted for this information.

Keywords

dial-service-name

The name of the dial service to which you wish to connect.

If a name is not specified, the port's preferred service is used. If the preferred service contains an asterisk (*) as the number specified in the dialer service, the access server prompts the user to enter a telephone number. Likewise, if the dialer service specifies ANY as the mode, the access server prompts the user to enter a mode (LOGIN, LOCAL, SLIP, or PPP).

If the port does not have a preferred service name set, the command fails.

Restriction

The default protocol must be dial.

Example: CONNECT [DIAL]

```
Local> CONNECT [DIAL] AT_TRADESHOW
```

This command connects the dial service AT_TRADESHOW.

CONNECT PORT (privileged)

Syntax

CONNECT PORT {*port-number*}

Description

This privileged command connects a dedicated port on your access server (a port other than your own) to a host system. For example, you can use this command to connect a printer to a host system. Once connected, the host could then send print jobs to the printer. You can use this command for LAT, Telnet, PPP, and SLIP connections.

Restriction

You cannot use this command for a port with a password-protected, dedicated service. The target port must be set to LOCAL or DYNAMIC access and must have a dedicated service defined for the port. In addition, the port cannot have a session in progress.

Example: CONNECT PORT

```
Local> CONNECT PORT 3
```

This command connects port 3 to its dedicated service.

CONNECT PPP (secure)

Syntax

CONNECT [PPP]

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

Restrictions

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

Example: CONNECT PPP

```
Local> CONNECT PPP
```

This command starts a PPP session on the current port.

CONNECT SLIP (secure)

Syntax

CONNECT [SLIP]

Description

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

Note

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

Restrictions

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

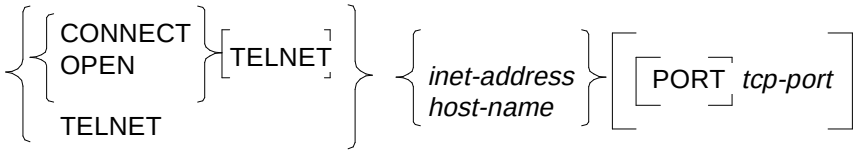
Example: CONNECT SLIP

```
Local> CONNECT SLIP
```

This command starts a SLIP session on the current port.

CONNECT/OPEN TELNET (secure)

Syntax



Description

This command (available to all users) requests a connection to the specified target. The target can be an Internet address or an Internet host name. Before granting the connection, the access server checks the protocol enabled on the requested port. (This command is functionally the same as OPEN/TELNET.)

When making connections, use either of the following methods:

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

Keywords

CONNECT, OPEN, or TELNET

Specifies that only Telnet will be used to attempt the connection. If Telnet is missing from the command line, the access server will use the port's default protocol. LAT is the factory-set default protocol.

TELNET

You must specify TELNET if Telnet is not the port's default protocol. If the TN3270 model is defined (see SET PORT TN3270) then Telnet will allow TN3270 to be negotiated with the host. If the TN3270 model is not defined a conventional Telnet connection will be established.

inet-address

The Internet address of a host. The address must be specified in dot-notation (for example, 195.1.1.60).

host-name

The Internet domain name of a host. The name may be absolute (for example, tom.pubs.dec.com) or relative (for example, tom).

[PORT] ***tcp-port***

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

Example: CONNECT TELNET

```
Local> CONNECT TELNET BAKER 2001
```

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

CRASH (privileged)

Syntax

CRASH

This privileged command shuts down the access server and initiates an upline dump. When this command is entered, users cannot access the access server until the upline dump completes and the access server reinitializes.

Restriction

If DUMP is set to DISABLED, the CRASH command will only reboot the access server (no upline dump will be performed).

Commands DIAL - FORWARDS

DIAL (secure)

Syntax

DIAL *dial-service-name*

Description

This command establishes a session using a dial service offered on the server. The DIAL command is a synonym for CONNECT DIAL.

Keyword

dial-service-name

The name of the dial service to which you wish to connect, or the phone number to be dialed. If a phone number is specified, the port must have a preferred dial service name set.

If the DIAL command line or the selected dial service does not define the mode (LOGIN, LOCAL, SLIP, PPP) for the new session, the user is prompted for this information. Likewise, if the phone number to be dialed is not defined, the user is prompted for the number.

Examples: DIAL

```
Local> DIAL
```

```
Local> DIAL 1-800-555-1212
```

This first command connects the default dial service. The second command connects to the preferred dial service and supplies the dial-service telephone number in the command line.

DISCONNECT/CLOSE (secure)

Syntax

Description

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

Keywords

ALL

Terminates all sessions on a port.

SESSION *session-number*

Terminates a particular session. (The default is your current session.)

Examples: CLOSE/DISCONNECT SESSION

```
Local> CLOSE SESSION 1
```

This command disconnects session 1.

```
Local> DISCONNECT ALL
```

This command disconnects all sessions on the port.

DISCONNECT/CLOSE PORT (privileged)

Syntax

{DISCONNECT / CLOSE} PORT *port-number*

Description

This privileged command is used to terminate a session to a dedicated service on another port. To disconnect sessions of interactive users, use the LOGOUT PORT command.

Keywords

port-number

Specifies the port you want to terminate.

Example: DISCONNECT/CLOSE PORT

```
Local> DISCONNECT PORT 3
```

This command terminates the sessions on port 3.

DO *command_group*

Syntax

DO command_group [p1,p2,p3.....p8]

Description

The DO command is used by the access server user to execute a set of commands contained within the command group.

The user can enter this command from the Local> prompt, if privileged, or from one of the ports associated with the command group *port-list*.

***command_group* [p1, p2, p3,...p8]**

The command group is created using the SET/DEFINE/CHANGE COMMAND GROUP command and one or more SET/DEFINE/CHANGE COMMAND GROUP LINE commands.

P1 through p8 are text string parameters that are to be substituted as the command group is interpreted. Quotation marks (" ") must be used around any text string that is a null string, contains spaces, or contains lowercase letters that are not to be interpreted as uppercase. This text string substitution capability is a general one. The parameter may be used to pass parameters such as the service name in a connect command. The parameter may also be used to pass keywords or portions of keywords.

Note

If this command is invoked from a menu, port-list and privilege checking are not performed.

Example: DO *command_group*

```
Local> DO Bob ENABLED
```

This command executes command group Bob and substitutes the text string ENABLED for parameter %P1 contained within the command group.

ENTER MENU

Syntax

ENTER MENU [menu_name]

Description

If this command is entered in response to the Local> prompt, the specified menu must have previously been enabled for the port or the user must be privileged.

When executed, this command puts the user's port into menu mode, displays the specified menu, and positions the cursor at the first choice of that menu.

Keywords

[*menu_name*]

Allows the user to select the specific menu to be displayed. If the menu name is not given, the default menu for the port will be displayed, if a default menu exists.

FORWARDS (secure)

Syntax

FORWARDS

This command (available to all users) resumes the session that follows your current session in the session list, which you can display with the SHOW SESSIONS command. The FORWARDS command connects you to the session with the next higher session number than your current session. If your current session has the highest session number, FORWARDS connects you to the session with the lowest session number.

Note

Using the FORWARDS command within a TN3270 session will cause the screen to be cleared and the TN3270 screen displayed. The information displayed will be the information that existed prior to the interrupt.

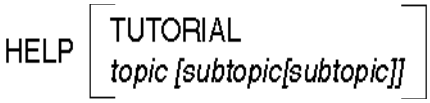
Restriction

You cannot use the FORWARDS command on a port that has the MULTISESSIONS characteristic set to ENABLED. For more information, refer to the SET/DEFINE/ CHANGE PORT MULTISESSIONS command.

Commands HELP - MONITOR

HELP (secure)

Syntax



Description

This command displays conventional online HELP for the access server. Chapter 1 provides an overview of the most common form of online help.

Help displays differ for privileged, nonprivileged, limited view and secure users. For example, if you enter HELP at a nonprivileged port, the resulting displays include only those commands and characteristics that can be specified by a nonprivileged user.

Keywords

TUTORIAL

Describes the tasks performed by end-users on the access server.

***topic* [*subtopic*]**

Specifies a command keyword and possible options for which you want online help information.

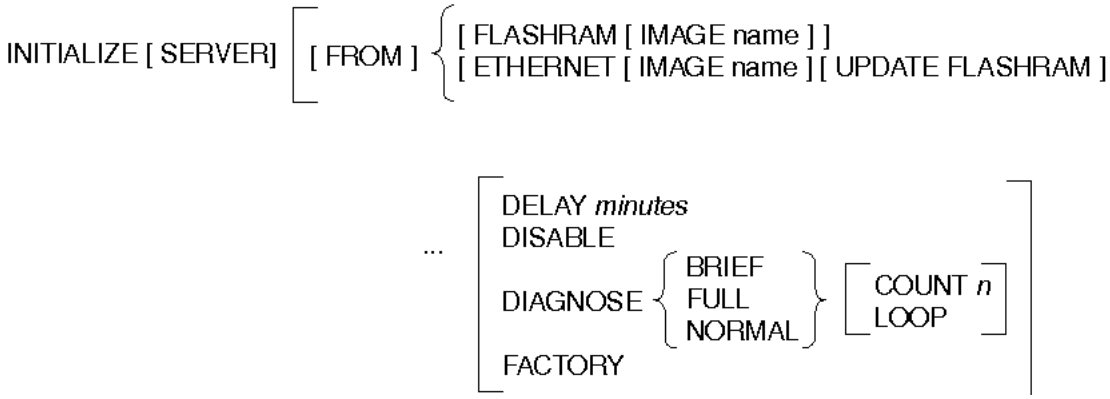
Example: HELP DEFINE PORT ACCESS

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

This command initiates online help documentation for defining the port characteristic ACCESS in the permanent database.

INITIALIZE (privileged)

Syntax



Description

This privileged command reinitializes the access server. By default, the access server delays initialization for about 1 minute after it processes this command. You can specify no delay, or you can delay initialization for a longer time in order to perform an orderly shutdown. You can also execute a diagnostic test on the access server.

Keywords

FROM

The optional FROM command allows the user to specify which device is to be used for loading. If the FROM option is specified, the reload will be from a specified device. If the FROM option is omitted, the standard reboot sequence will take effect.

FLASHRAM

The load image loads from an internal Flash RAM.

ETHERNET

The load image loads over the Ethernet port, using either MOP or BOOTP.

IMAGE name

A specified image name that overrides the image name stored in NVRAM.

UPDATE FLASHRAM

The access server copies the load image to Flash RAM, after loading through the network, but before completing initialization.

DELAY *minutes*

Specifies that the initialization procedure is delayed by the specified number of minutes (range: 0 to 1440; default: 1 minute).

DISABLE

Prevents the CONNECT command and the AUTOCONNECT function after an initialization. To enable CONNECT and AUTOCONNECT, enter INITIALIZE without the DISABLE option.

DIAGNOSE

Specifies that a test is to be done on the access server hardware. You can specify the self-test you want to perform. If you omit DIAGNOSE, the access server performs the standard self-test (NORMAL).

BRIEF

Performs internal self-test functions only.

FULL

Performs extended tests, including in-depth memory test.

NORMAL

Performs the standard self-test.

COUNT *n*

Specifies that the test repeats *n* times, range: 1 (default) to 32767.

LOOP

Specifies that the test runs indefinitely. You must interrupt the access server power source to stop the test.

FACTORY

Performs the software equivalent of holding down the reset-to-factory button.

Example: INITIALIZE

```
Local> INITIALIZE DELAY 5
```

This command specifies initialization of the access server after 5 minutes have elapsed.

Restriction

If the specified load from Flash RAM fails, the firmware will print a warning message and then attempt a reboot. Flash RAM must be installed on your system for the program to support Flash RAM.

INITIALIZE CANCEL (privileged)

Syntax

INITIALIZE [SERVER] CANCEL

Description

This privileged command terminates a previous INITIALIZE command (provided the initialization process has not yet begun).

LEAVE MENU (secure)

Syntax

LEAVE MENU

Description

This command will cause the access server to leave the menu and return the user to the Local> prompt.

LOCK (secure)

Syntax

LOCK

Description

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

The access server responds to a LOCK command by prompting for a lock password, provided the access server characteristic LOCK is ENABLED and the DEFINE PORT characteristic LOCK is ENABLED.

The password is your choice of 1 to 16 characters. After you enter the password, which is not displayed on your terminal, the access server prompts you to enter it again for verification. If both password entries match, the access server displays an unlock password prompt (Unlock Password>). Your terminal remains locked until you enter the password again, returning you to local mode. For more information on specifying passwords, refer to Chapter 1.

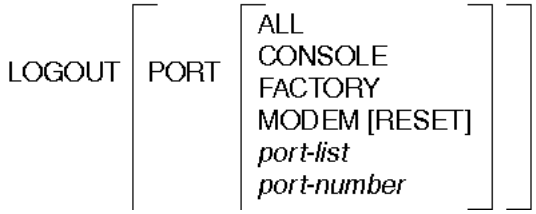
Example: LOCK

```
Local> LOCK

Lock Password> FROGS (not displayed)

Verification> FROGS  (not displayed)

Local -019- Port 6 locked

Unlock Password> FROGS (not displayed)

Local>
```

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

LOGOUT (secure)

Syntax



Description

This command logs out a port on the access server and disconnects any sessions associated with the port. After you log out a port, the port characteristics in the operational database for that port are reset to the values defined in the permanent database. For more information, refer to the *Network Access Server Management* manual.

On ports that have the MULTISESSIONS characteristic set to ENABLED (refer to the SET/DEFINE/CHANGE PORT MULTISESSIONS command), LOGOUT only closes your current terminal session. Use LOGOUT PORT to perform a full logout with MULTISESSIONS ENABLED. For more information about using LOGOUT on access servers that support session management, refer to the *Network Access Server Management* manual.

If a port has modem control or signal control enabled, the LOGOUT command causes outgoing modem signals to be dropped.

Keywords

PORT

Specifies a full logout from your own port, regardless of the current multisessions characteristic setting.

ALL

Is a privileged option that logs out all ports except the port where the command is entered.

CONSOLE

Is a privileged option that logs out the port being used as a remote management console port.

port-list

Is a privileged option specifying the port(s) to be logged out. (The default is your own port.) If your port is not specified in the list, it will not be logged out. For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

port-number

Is a privileged option specifying the port you want logged out. (The default is your own port.)

FACTORY

Is a privileged option that resets the port characteristics to their factory defaults.

MODEM [RESET]

Asserts a reset signal to the DECserver 900MC modem port. If you issue this command on a platform other than a DECserver 900MC platform, the software performs a simple logout.

Examples: LOGOUT

```
Local> LOGOUT

Local> LOGOUT PORT 5
```

The first command logs out the port where the command is entered and disconnects all sessions on that port. The second command disconnects all sessions and logs out of port 5.

LOOP

For information on this command, refer to the TEST LOOP command.

MONITOR

For information on this command, refer to the SHOW/MONITOR/LIST and SHOW/MONITOR commands in Chapter 5.

Commands OPEN/TELNET - ZERO SERVER AUTHENTICATION COUNTERS

OPEN/TELNET (secure)

For information on this command, refer to the CONNECT/OPEN TELNET (secure) command.

PING/TEST INTERNET (nonprivileged)

Syntax

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

Description

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

PING tests for the availability of the target by establishing a PING session on the port. Testing continues until the PING succeeds (and sends a verification message) or until the time-out period is exceeded (30 seconds). The timer begins when the user receives a “Pinging...” message. To stop PING, the user can disconnect the session with the DISCONNECT/CLOSE SESSION command.

Keywords

PING or TEST INTERNET

Specifies that an Internet Control Message Protocol (ICMP) request be sent to the specified target. If the target receives the message, it will return an ICMP Reply message.

host-name

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

inet-address

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

Restriction

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

Example: PING

```
Local> PING 195.1.1.60
```

This command tests Internet connectivity to the Internet address 195.1.1.60.

REMOVE QUEUE (privileged)

Syntax

REMOVE QUEUE { ALL | ENTRY *entry-name* | NODE *node-name* | SERVICE *service- name* }

Description

This privileged command removes queued LAT connection requests (for remote access to access server ports) from the access server queue.

When you remove an entry from the access server queue, the access server sends a message to the service node that requested the remote access. The message reports that the queued entry was deleted by an access server user.

Keywords

ALL

Specifies that all entries in the queue are removed.

ENTRY *entry-number*

Specifies a particular entry by number.

NODE *node-name*

Specifies all entries initiated from the specified node.

SERVICE *service-name*

Specifies all entries initiated from the specified service node.

Example: REMOVE QUEUE ENTRY

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

This command removes entry 2 from the access server queue.

RESUME (secure)

Syntax

RESUME [SESSION *session-number*]

Description

This command (available to all users) resumes an interactive session from local mode. When a TN3270 session is resumed, the screen will be cleared and the 3270 screen will be displayed with the information that existed when the session was interrupted.

Keywords

SESSION *session-number*

Specifies the session you want to resume. If you omit this parameter, the access server resumes your current session. You can enter the session number without the keyword SESSION.

Restriction

You cannot specify a session number on a port that has the MULTISESSIONS characteristic set to ENABLED. (Refer to the PORT MULTISESSIONS (secure) command.)

Reference

For more information on resuming sessions while using session management, refer to the *Network Access Server Management* manual.

Examples: RESUME

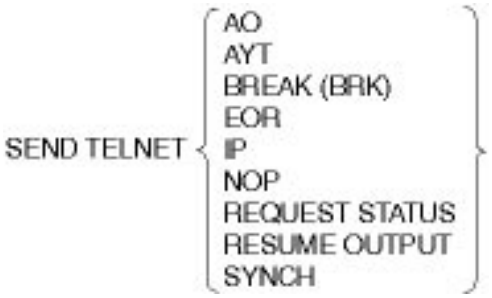
```
Local> RESUME
```

```
Local> RESUME SESSION 3
```

The first command resumes your current session. The second command resumes session 3 in your session list.

SEND TELNET (secure)

Syntax



Description

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

Keywords

AO (Abort Output)

Causes any output currently on its way to the user's terminal to be aborted.

AYT (Are-You-There)

Solicits a response from the remote Telnet implementation. This causes the remote host to send back a message indicating that it is still up and running.

BREAK (BRK)

Entering either BREAK or BRK will causes a Telnet Break command to be sent to the remote host. This is intended to indicate that the Break key or the Attention key was pressed, but it may be interpreted differently by some remote hosts.

EOR (End-of-Record)

Causes a Telnet End-of-Record command to be sent to the remote host. This command indicates the end of the current input record.

IP (Interrupt Process)

Sends a Telnet command to the remote host that interrupts or aborts the remote process.

NOP (No-Operation)

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

REQUEST STATUS

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

RESUME OUTPUT

Causes a session to resume after an Abort Output signal has been sent and the port hangs.

SYNCH

Causes all input currently on its way to the remote process to be dropped. This includes input queued both by the local access server and the remote host.

Example: SEND

```
Local> SEND TELNET AO
```

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

Restrictions

- The session must be resumed to see a AYT response.
- The session must be resumed to view a REQUEST STATUS response.
- The command SEND TELNET RESUME OUTPUT should only be used after an Abort Output signal has been sent. It does not work in any other context. The Abort Output signal may have been sent either by entering a SEND TELNET AO command or by typing the keyboard character defined as AO. This assumes that the port Telnet client or Telnet session characteristic AUTOSYNCH AO is ENABLED.

SETUP PRINTER (privileged)

Syntax

SETUP PRINTER

This command allows the user to configure an access server port(s) to be connected to a printer(s). After the command is entered, the system will prompt the user for the needed configuration parameters. The following is an example of the display. After you have entered all required information, you can confirm your entries by answering yes to the “Display commands generated” request.

Example: SETUP PRINTER

```
Local>SETUP PRINTER

             ***** PRINTER SETUP ASSISTANCE *****
Port or ports to configure for printer [max port = 16]      16
Printer port speed                                        4800
Printer character size[7,8]                                 8
Printer stop bits (D=Dynamic)[1,2,D]                         D
XON/XOFF, CTS/RTS, or None flow control [XON,CTS,None]       X
LAT, Telnet, or Both protocols[LAT,Telnet,Both]              L
Announced LAT service?[Y,N]                                  Y
LAT printer service name (1-16 characters)          OURPRINTER
LAT svc identification string (0-40 characters)      <Return>
LAA Printer Enable LAT queueing for this service?[Y,N]       y
LAT group code(s) for this service:                        4-6
End of setup printer dialog.
Display commands generated?[Y,N]                             y
DEFINE PORT 16 PARITY NONE
DEFINE PORT 16 TYPE ANSI
DEFINE PORT 16 AUTOBAUD DISABLED
DEFINE PORT 16 AUTOPROMPT DISABLED
DEFINE PORT 16 BREAK DISABLED
DEFINE PORT 16 ACCESS REMOTE DEFINE PORT 16 AUTOCONNECT DISABLED
DEFINE PORT 16 DSRLOGOUT ENABLED
DEFINE PORT 16 INACTIVITY LOGOUT DISABLED
DEFINE PORT 16 LONGBREAK LOGOUT DISABLED
DEFINE PORT 16 SIGNAL CONTROL DISABLED
DEFINE PORT 16 SPEED 4800
DEFINE PORT 16 CHARACTER SIZE 8
DEFINE PORT 16 STOP BITS DYNAMIC
DEFINE PORT 16 FLOW CONTROL XON
DEFINE SERVICE OURPRINTER PORT 16
DEFINE SERVICE OURPRINTER IDENTIFICATION “LAA Printer”
DEFINE SERVICE OURPRINTER QUEUE ENABLED
DEFINE SERVER SERVICE GROUPS 4-6 ENABLED
DEFINE PORT 16 AUTHORIZED GROUPS 4-6
EXECUTE PRINTER SETUP?[Y,N]                                  y
```

TEST INTERNET

For information on this command, refer to PING/TEST INTERNET (nonprivileged).

TEST LOOP (privileged)

Syntax

Description

This privileged command tests the connectivity between your access server and another Ethernet node on the network. For more information about loop node testing, refer to the Network Access Server Problem Solving manual.

Keywords

e-address1

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

HELP

Specifies the type of help desired from an assistant node.

FULL

Relays both outgoing and returning access server transmissions.

RECEIVE

Relays transmissions returning to the access server.

TRANSMIT

Relays outgoing access server transmissions.

ASSISTANT *e-address2*

Specifies the Ethernet address of the assistant node.

Example: TEST LOOP

```
Local> TEST LOOP 08-00-2B-02-24-43 HELP TRANSMIT ASSISTANT
08-00-2B-00-16-C3
```

This command specifies that node 08-00-2B-00-16-C3 should relay outgoing access server transmissions to target node 08-00-2B-02-24-43.

TEST PORT (secure)

Syntax

TEST [PORT *port-number*] [COUNT n] [WIDTH *n*] [LOOPBACK { EXTERNAL / INTERNAL }]

Description

This command (available to all users) tests a port on the access server. This command causes the access server to send a stream of characters to the specified port. Irregularities in the rotating ASCII pattern indicate possible problems with the terminal or with the connection of the port to the access server. For more information about this test, refer to the *Network Access Server Problem Solving* manual.

Keywords

PORT *port-number*

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

COUNT *n*

Specifies the number of test lines to be sent. (The range is 1 to 65535; the default is 23 lines.)

WIDTH *n*

Specifies the number of characters per line (range: 1 to 132; default: 80).

LOOPBACK

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

Restrictions

- If you are testing a port that is not logged in, you must set AUTOBAUD DISABLED for that port.
- You cannot specify LOOPBACK from the port you are testing; you must enter the TEST PORT *n* LOOPBACK command from another port.
- Only privileged users can specify the LOOPBACK parameter and can test a port other than their own. For more information, refer to the port-number parameter.

Example: TEST PORT

```
Local> TEST PORT 3 COUNT 90 WIDTH 60 LOOP INTERNAL
```

This command directs the access server to loop internally ninety 60-character lines to port 3.

TEST SERVICE (privileged)

Syntax

TEST SERVICE *service-name* [NODE *node-name* | DESTINATION *port-name* | COUNT n | WIDTH *n* | LOOPBACK { EXTERNAL | INTERNAL }]

Description

This privileged command tests the end-to-end access servers over the LAT network. The test is performed between the access server and a service node. When the test is completed, the access server displays a report of the test results.

Keywords

service-name

Specifies the name of the service to be tested.

NODE *node-name*

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

DESTINATION *port-name*

Specifies which port offering the service is to be tested.

COUNT *n*

Specifies the number of test buffers to be sent. (The default is 1.)

WIDTH *n*

Specifies the number of characters per buffer. (The range is 1 to 180; the default is 80.)

LOOPBACK

Specifies that test data is looped back from the external target port connector or from the internal target port hardware. If you omit LOOPBACK, the test data is returned by the LAT protocol software on the target service node.

Restriction

This command is valid only on ports with MULTISESSIONS DISABLED.

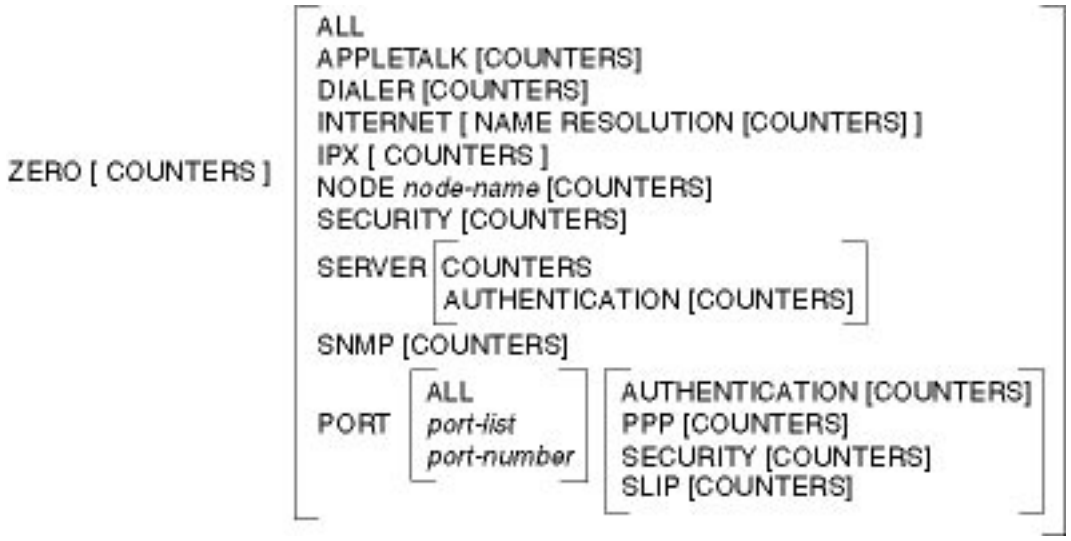
Example: TEST SERVICE

```
Local> TEST SERVICE SALES DESTINATION 6 WIDTH 132 LOOP
EXTERNAL
```

This command directs the access server to loop externally a one-buffer display of 132-character lines to the service SALES on port 6.

ZERO COUNTERS (privileged)

Syntax



Description

This privileged command resets counters for the access server, nodes, ports, and devices (where applicable). If you enter this command with no parameters, only the access server counters are set to zero.

The ZERO [COUNTERS] command does not zero the uptime counter in displays. This counter is reset only after an initialization or after turning on the power of the access server.

Keywords

ALL

Specifies that access server, LAT node, port, port SLIP, port PPP, Internet, Internet name resolution, IPX, and SNMP counters are set to zero (0). Note that AppleTalk and access server authentication counters are not reset with this command.

APPLETALK

All current access server-wide AppleTalk counters are set to zero (0).

INTERNET

Clears the Internet counters associated with the specified entity.

NAME RESOLUTION

Specifies that only Internet domain name system Internet counters are cleared.

IPX

All current access server-wide IPX counters are set to zero (0).

NODE *node-name*

Specifies that counters for data exchanges between the access server and the specified service node (LAT) be set to zero.

ALL

Specifies all access server ports.

port-list

Specifies that error counters and status counters for the specified port(s) are to be set to zero. For more information on specifying port-list, refer to Chapter 1 for examples and conventions.

DIALER

All Dialer counters are set to zero.

SLIP

Clears the SLIP counters associated with the specified port.

PPP

Clears the PPP counters associated with the specified port.

AUTHENTICATION

Clears the authentication counters associated with the specified port.

SECURITY AUTHENTICATION

All Security Authentication counters are set to zero.

SERVER AUTHENTICATION

Clears the server authentication counters.

SNMP

Clears all SNMP error and access counters.

Examples: ZERO COUNTERS

```
Local> ZERO APPLETALK COUNTERS
```

This command specifies that all AppleTalk counters be set to zero.

```
Local> ZERO INTERNET
```

This command clears the access server Internet counters.

```
Local> ZERO COUNTERS NODE SALES_1
```

This command zeroes the counters for data exchanges between the service node SALES_1 and the access server. The counters listed in the display for SHOW NODE SALES_ 1 COUNTERS read “0” immediately after you execute this command.

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

This command zeroes the SLIP-specific counters for port 5.

```
Local> ZERO SNMP COUNTERS
```

This command specifies that all SNMP access and error counters be set to zero.

Chapter 3

CLEAR/PURGE Commands

Overview

Introduction

This chapter describes the CLEAR and PURGE commands. Both the CLEAR and PURGE commands delete whatever is specified by the keyword from the access server databases.

Use the **CLEAR** command to remove information from the operational database.

Use the **PURGE** command to remove information from the permanent database.

Reference

For more information about using the CLEAR/PURGE commands in this chapter, refer to the *Network Access Server Management* manual.

Note

To get help at any time with commands, enter a question mark (?) at the prompt. A list of all the legal keywords or data types you can use at that point in the command will appear.

Commands COMMAND GROUP - INTERNET DHCP

COMMAND GROUP (privileged)

Syntax

Description

This privileged command removes the specified command group from the access server database.

Keywords

ALL

Specifies that all of the command groups are to be removed from the access server database.

command_group

Specifies the name of the command group being removed from the database.

COMMAND GROUP LINE (privileged)

Syntax

Description

This privileged command removes the specified line from the specified command group in the access server database.

Keywords

command_group

Specifies the name of the command group from which a line will be deleted.

n

The number of the line to be removed.

DIALER SCRIPT (privileged)

Syntax

{CLEAR / PURGE} DIALER SCRIPT [NAME] {*script-name* / ALL}

Description

This privileged command removes a modem script configuration entry from the permanent or volatile database.

DIALER SERVICE (privileged)

Syntax

{CLEAR / PURGE} DIALER [SERVICE] {*dial-service-name* / ALL}

Description

This privileged command removes a dialer service from the volatile or permanent database.

INTERNET ARP ENTRY (privileged)

Syntax

{CLEAR / PURGE} INTERNET ARP ENTRY {ALL / *inet-address*}

Description

This privileged command deletes existing address resolution protocol (ARP) entries from the access server ARP database.

Keywords

ALL

Specifies that all existing Internet ARP entries in the access server database are to be deleted.

inet-address

Specifies the Internet address of the Internet ARP entry to be deleted.

Examples: CLEAR/PURGE INTERNET ARP ENTRY

```
Local> CLEAR INTERNET ARP ENTRY ALL
```

This command deletes all Internet ARP entries from the access server ARP operational database.

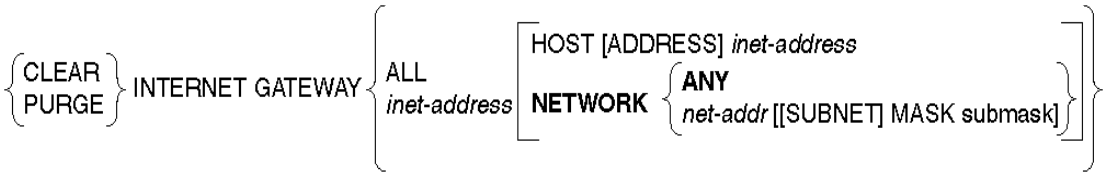
```
Local> PURGE INTERNET ARP ENTRY 195.1.1.60
```

This command deletes the ARP entry for the Internet address 195.1.1.60 from the access server ARP permanent database.

Commands INTERNET GATEWAY - MENU LINE

INTERNET GATEWAY (privileged)

Syntax



Description

This privileged command deletes existing gateway entries from the access server database.

Keywords

ALL

Specifies all existing gateway entries in the access server database.

inet-address

Specifies the local network Internet address of the gateway to be deleted. When this option is used, the NETWORK *net-address* and HOST *inet-address* options are also available. If you do not use the NETWORK or HOST options, NETWORK ANY is the default. The specified Internet address must be expressed as *n.n.n.n*, where *n* is a decimal number in the zero (0) to 255 range.

HOST [ADDRESS]

Specifies the gateway entry for traffic from the server to the specified host.

net-addr

Specifies the gateway entry for traffic from the access server to the specified network. This is useful when removing only one leg of a gateway.

ANY

Specifies the gateway entry for traffic from the access server to any network. This is the default if you do not specify an option with an *inet-address*.

[SUBNET] MASK submask

When combined with NETWORK, deletes the entry mapping traffic from the exact subnet to this gateway. If the mask option is omitted, the Internet subnet mask in the access server operational database is the default.

Restrictions

- The CLEAR command does not remove gateway entries with active connections. The PURGE command does remove gateway entries with active connections because it affects only the permanent database.
- The HOST and NETWORK characteristics are not valid with the ALL characteristic.

Examples: CLEAR/PURGE INTERNET GATEWAY

```
Local> CLEAR INTERNET GATEWAY ALL
```

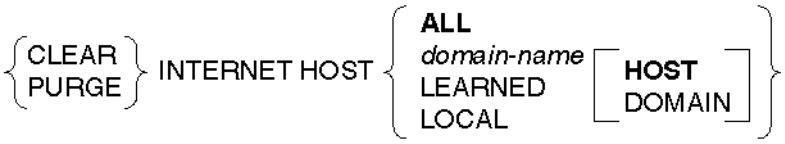
This command deletes all Internet gateway entries from the access server operational database.

```
Local> PURGE INTERNET GATEWAY 195.1.1.60 NETWORK
195.1.1.61
```

This command deletes the Internet gateway with the above Internet address and network address from the access server permanent database.

INTERNET HOST (privileged)

Syntax



Description

This privileged command deletes existing Internet hosts from the access server Internet domain name system (DNS) database.

Note

Whenever a CLEAR INTERNET HOSTS ALL or LEARNED command is entered, the access server automatically relearns the host names of secondary name servers for the default domain and the root domain (if defined). It might appear that the host names for these name servers are not cleared when you enter the SHOW INTERNET HOST command, but in fact, the host names have been cleared and relearned.

Keywords

ALL

Specifies that all hosts in the DNS cache will be deleted.

domain-name

Specifies the *domain-name* of a host or a domain.

HOST

This option (the default) is valid only when specifying a *domain-name*. Only the host specified will be deleted.

The domain name for HOST can be an absolute or a relative name. If a relative name is specified, the default local domain will be automatically appended to the host name. The domain name for DOMAIN must be an absolute name.

DOMAIN

This option identifies the domain-name as a domain name for a domain. All hosts within the specified domain and its subdomains will be deleted. This option is valid only when specifying a host name.

LEARNED

Specifies that only hosts that the access server has learned about will be deleted.

LOCAL

Specifies that only hosts that have been defined locally at the access server will be deleted.

Restriction

The LEARNED characteristic is not valid with the PURGE command.

Example: CLEAR/PURGE INTERNET HOST

```
Local> CLEAR INTERNET HOST LEARNED
```

This command acts on the access server operational database. It deletes all Internet hosts from the name server database that were learned about over the network.

```
Local> PURGE INTERNET HOST ALL
```

This command acts on the access server permanent database. It deletes all Internet hosts from the domain name server.

```
Local> CLEAR INTERNET HOST FALCON HOST
```

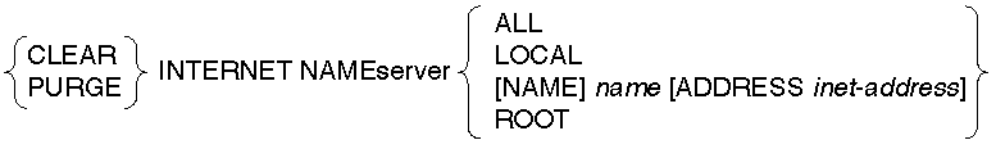
This command acts on the access server operational database. It deletes Internet host FALCON from the domain name server.

```
Local> CLEAR INTERNET HOST DEC.COM DOMAIN
```

This command acts on the access server operational database. It deletes all Internet hosts in domain dec.com from the domain name server.

INTERNET NAMEserver (privileged)

Syntax



Description

This privileged command deletes existing Internet domain name servers from the access server domain name system (DNS) database.

Keywords

ALL

Specifies that all domain name servers will be deleted.

LOCAL

Specifies that all local domain name servers will be deleted.

NAME *name*

Specifies the name of the domain name server to be deleted.

ADDRESS *inet-address*

Specifies the address of the domain name server to be deleted. This option is useful when there are two or more defined name servers with the same name. The address must be a valid Internet address of the form *n.n.n.n*, where *n* is a decimal number in the zero (0) to 255 range.

ROOT

Specifies that all root domain name servers will be deleted.

Examples: CLEAR/PURGE INTERNET NAMEserver

```
Local> CLEAR INTERNET NAMEserver ROOT
```

This command deletes all root name server entries from the access server DNS operational database.

```
Local> PURGE INTERNET NAMEserver ALL
```

This command deletes all name server entries from the access server DNS permanent database.

```
Local> CLEAR INTERNET NAMEserver NAME Nserver.LKG.DEC.COM
```

This command deletes the name server Nserver.LKG.DEC.COM from the access server DNS operational database.

IPX (privileged)

Syntax

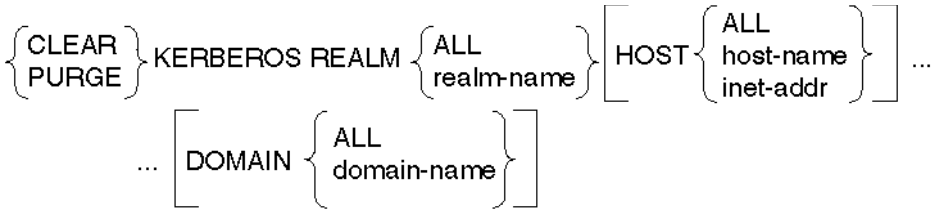
Description

RIP deletes all unique networks from the RIP database that have been learned from RIP protocol requests. Also, all routes associated with these networks are also deleted.

SAP clears all SAP service entries in the SAP database that have been learned by SAP Get Nearest Service (GNS) protocol requests (use SHOW IPX STATUS for current entries).

KERBEROS REALM (privileged)

Syntax



Description

This privileged command removes one or more REALM and/or key distribution centers (KDCs). The keyword HOST refers to the KDCs.

The command gives the option of removing:

- ALL realms, including all KDCs and all DOMAINs
- A single realm, including all of its KDCs and all DOMAINs
- A single KDC within a single realm
- ALL KDCs within a single realm
- A single DOMAIN within a single realm
- ALL DOMAINs within a single realm

Restriction

The HOST or DOMAIN options cannot be used with the REALM ALL option.

MENU (privileged)

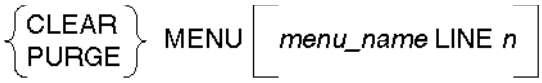
Syntax

Description

This privileged command removes a menu or ALL menus from the access server database.

MENU LINE (privileged)

Syntax



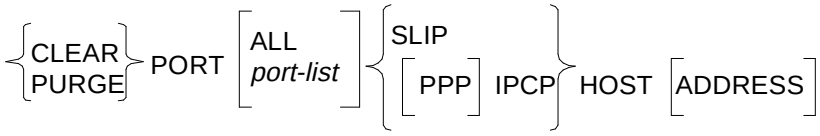
Description

This privileged command removes a specified line from the specified menu in the access server database.

Commands PORT PPP/SLIP HOST ADDRESS - USERACCOUNT

PORT PPP/SLIP HOST ADDRESS (privileged)

Syntax



Description

This privileged command deletes the Internet address of the port's attached device.

Keywords

ALL

Specifies all access server ports.

port-list

Specifies one or more ports. For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

Note

A port has only one Internet address associated with it. PPP, IPCP, and SLIP use the same address. In this command, keywords PPP, IPCP, and SLIP are interchangeable.

Restriction

You cannot use the CLEAR command with an Internet address on a port with an existing SLIP or a PPP session.

Example: PORT PPP/SLIP HOST ADDRESS

```
Local> CLEAR PORT 5 SLIP HOST ADDRESS
```

This command deletes the Internet address of the SLIP host at port 5 from the access server operational database.

PRINTER

Syntax

Description

This command deletes the LPD printer name and disassociates the printer from a port.

Keywords

printer-name

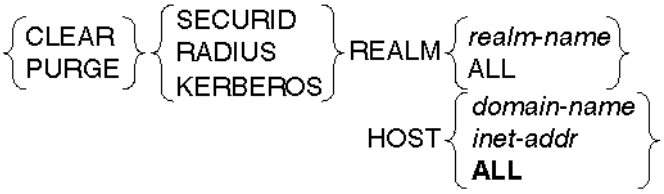
Specifies the name of the printer to be deleted.

ALL

Specifies that all of the printers associated with a port will be deleted.

REALM (privileged)

Syntax



Description

This privileged command deletes the various realms used to identify particular administrative domains.

The HOST clause associates a host with a realm. The DECserver software will use this host to resolve authentication requests. The DECserver software will accept either a Domain name or an IP address as a host identifier.

SERVER REALM (privileged)

Syntax

Description

This privileged command deletes the various realms used to identify particular administrative domains. This is simply an extension of the existing syntax for setting up and tearing down Kerberos.

SERVICES (privileged)

Syntax

Description

This privileged command deletes an entry for one or all local LAT services from the access server database.

Keywords

service-name

Specifies the name of a LAT service to be deleted. If a service is not specified, the access server purges the locally defined LAT services.

LOCAL

Specifies that all locally defined LAT services are deleted. LOCAL is the default.

You will receive an error message if you enter the CLEAR SERVICES command under the following conditions:

- Sessions are established with the service.
- The access server queue contains CONNECT requests for the specified service.
- The requested service does not exist.

Example: CLEAR/PURGE SERVICES

```
Local> PURGE SERVICE LABWORK
```

This command clears all information for service LABWORK from the permanent database so that it is no longer a locally defined service.

SNMP COMMUNITY (privileged)

Syntax

Description

This privileged command deletes an SNMP community name from the access server database.

Keywords

ALL

Specifies all SNMP communities currently defined in the community database, except for the default community PUBLIC.

community-name

Specifies a community name or a community's characteristics in the access server community database. The *community-name* is an ASCII string, maximum length 32 characters, enclosed in double quotes. If the *community-name* entered is longer than 32 characters, it will be truncated to 32 characters. For more information, refer to SNMP (privileged) under *community-name* length restrictions.

Example: CLEAR/PURGE SNMP COMMUNITY

```
Local> PURGE SNMP COMMUNITY "Central Engineering"
```

This command deletes the SNMP community name "Central Engineering" from the permanent database.

TCP LISTENER(privileged)

Syntax

Description

This privileged command resets a predefined TCP listener in the access server database to the factory-set defaults. The access server defaults are: Connections: DISABLED, Ports: NONE, and Type: TCP. The listener type will remain RAW TCP.

When you enter the CLEAR TCP LISTENER command.you will get an error message if there are sessions active that were established from the specified listener. When this occurs, log out the ports on which these sessions are established before attempting the CLEAR command.

Keywords

listener-id

This keyword identifies the listener to be reset. If the listener is in the range of 2001 to 2032, that port is reset to Connections: DISABLED, Ports: NONE, and Type: TCP.

ALL

Specifies that all Telnet listeners with type RAW TCP are currently defined in the designated database.

Restrictions

- You cannot use the CLEAR TCP LISTENER command with an active session.
- The specified listener must be type RAW TCP.
- Listener 23 cannot be type RAW TCP.

Example: CLEAR TCP LISTENER

The following example resets the Telnet listener (type RAW TCP) mapped to TCP port 2010 to factory-set defaults:

```
Local> CLEAR TCP LISTENER 2010
```

TELNET LISTENER (privileged)

Syntax

Description

This privileged command resets a predefined Telnet listener in the access server database back to the factory-set defaults. This command sets the Telnet listener's IP address to 0.0.0.0.

When you enter the CLEAR TELNET LISTENER command, you will get an error message if there are sessions active that were established from the specified listener. When this occurs, log out the ports on which these sessions are established before attempting the CLEAR command.

Keywords

listener-id

Specifies the listener to be reset. If the listener specified is in the range from 2001 to 2032, that port is reset to Connections: DISABLED, Ports: NONE, and Type: TELNET. If the listener specified is 23, used for Telnet remote console, that port is reset to Connections: ENABLED and Ports: CONSOLE.

ALL

Specifies all Telnet listeners currently defined in the designated database.

Restriction

You cannot use the CLEAR TELNET LISTENER command with an active session.

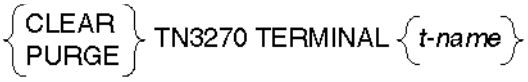
Example: CLEAR/PURGE TELNET LISTENER

```
Local> CLEAR TELNET LISTENER 2010
```

This command resets the Telnet listener mapped to TCP port 2010 to factory-set defaults. (The factory-set defaults are Connections: DISABLED, and Ports: NONE.)

TN3270 TERMINAL (privileged)

Syntax



Description

This privileged command removes a customized TERMINAL entry. The keymap associated with TERMINAL is deleted unless it is currently used by another TERMINAL.

Keywords

t-name

The name of a terminal type. The CLEAR command is restricted from clearing *t-name* if one or more ports currently have the *t-name* defined in its operational database. Port definitions must be changed for command operation.

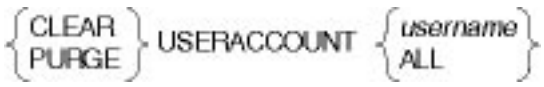
The PURGE command is restricted from purging *t-name* if one or more ports currently have *t-name* defined in NVRAM.

Restriction

You cannot use this command with ANSI, VT100, VT220, VT320, or VT420.

USERACCOUNT (privileged)

Syntax



Description

The CLEAR/PURGE command allows local database entries to be deleted.

Restriction

The ACCOUNT *username* has a maximum length of 40 characters.

Chapter 4

SET/DEFINE/CHANGE Commands

Overview

Introduction

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

Use **SET** commands to change characteristics and options stored in the operational database of the access server. SET commands take effect immediately but continue only until logout occurs (for port characteristics) or until the server is rebooted (for all other characteristics).

Use **DEFINE** commands to change characteristics stored in the permanent database of the access server. DEFINE commands take effect when the server is rebooted (for server-based commands, such as DEFINE ACCOUNTING) or when port reinitialization occurs (for port-based commands, such as DEFINE IPX) by logging out and logging in.

Use **CHANGE** commands to change characteristics stored in the permanent and operational databases of the access server. The CHANGE command is equivalent to both the DEFINE and SET commands. If either the DEFINE or SET command produces an error, neither database will be modified by the CHANGE command.

Reference

For more information about using the SET, DEFINE, and CHANGE commands in this chapter, refer to the *Network Access Server Management* manual.

Note

To get help at any time with commands, enter a question mark (?) at the prompt or within a command. A list of all the legal keywords or data types you can use at that point in the command will appear.

ACCOUNTING - COUNTRY

ACCOUNTING CONSOLE (privileged)

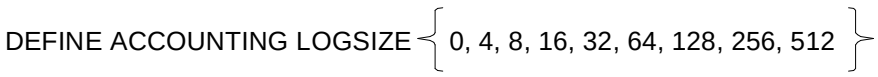
Syntax

Description

This privileged command allows you to display accounting events on the access server console port. If ENABLED, every accounting event is displayed on the access server console port as it occurs. If the access server console port is set to NONE, no console logging occurs. For more information and a list of events, refer to the *Network Access Server Management* manual.

ACCOUNTING LOGSIZE (privileged)

Syntax



Description

This privileged command specifies the amount of memory (in kilobytes) that is reserved at initialization time for storing accounting events. When you reinitialize the access server, the defined logsize is allocated in memory. If the defined logsize is 0 or there is not enough space in memory, no storing of accounting events occurs. If the accounting log becomes full, new events will replace old events in the log. A newly entered value will not take effect until reinitialization occurs.

ACCOUNTING THRESHOLD (privileged)

Syntax

Description

This privileged command specifies the points at which a notification is sent to indicate that the accounting log has crossed the defined threshold. This command is useful in preventing loss of log entries.

NONE indicates that notification is not sent upon reaching the threshold.

END indicates to send notification when the end of the log is reached.

HALF indicates to send notification when reaching the halfway point and end of the log.

QUARTER indicates to send notification when reaching the quarter, halfway, three-quarter, and end of the log.

EIGHTH indicates to send notification when reaching the one-eighth, quarter, three-eights, halfway, five-eighths, three-quarter, seven-eighths, and end of the log.

APPLETALK (privileged)

Syntax

Description

This privileged command enables AppleTalk on the access server.

Note

It is possible to issue SET or CHANGE APPLETALK ENABLE commands; however, it is not possible to issue SET or CHANGE APPLETALK DISABLE commands.

Keywords

ENABLED/DISABLED

If ENABLED, the access server provides AppleTalk functionality.

If DISABLED, the access server does not provide AppleTalk functionality. To become effective, the privileged user must DEFINE the characteristic DISABLED and then reinitialize the access server. If you enter any subsequent AppleTalk commands, you receive an error message. If AppleTalk has been disabled, no memory is allocated. In addition, the access server rejects all SNMP queries for AppleTalk information and transmits a "No Such Name" error message.

APPLETALK [ADDRESS] CACHE (privileged)

Syntax

DEFINE APPLETALK [ADDRESS] CACHE [SIZE] *n*

Description

This privileged command specifies the maximum number of AppleTalk addresses the access server should acquire for hosts attaching through the access server asynchronous lines.

Note

This characteristic can be modified in NVRAM only. There is no corresponding SET or CHANGE command.

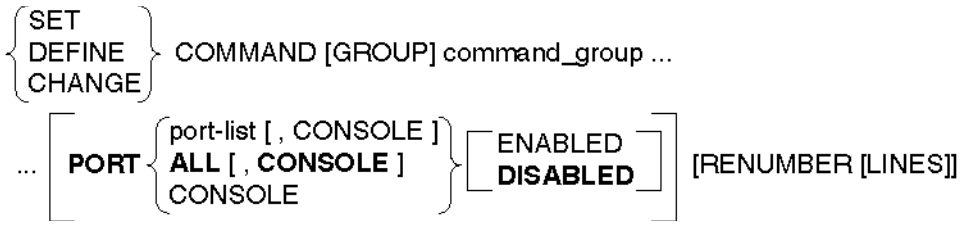
Keywords

n

The number of addresses the access server should preacquire. The supported range of *n* is from 1 to the number of asynchronous ports. The default is the number of asynchronous ports divided by 8.

COMMAND GROUP (privileged)

Syntax



Description

This command creates a command group with a name and an associated port list. A command group can be invoked with the DO command, provided you have privilege access or are logged in to one of the ports in the associated port list.

If the command group already exists, this command can change the port list associated with it, or renumber the lines in it. The SET/DEFINE/CHANGE COMMAND GROUP LINE command is used to fill in the contents of the command group.

Keywords

command_group

Specifies the name for this command group and appears as the parameter in a DO command. The maximum length of a command group name is 16 characters.

port-list

Specifies one or more physical ports that have access to this command group.

ALL

Specifies all of the physical ports. The remote management console is not included.

CONSOLE

Specifies the remote management console, available with either Telnet or MOP.

ENABLED/DISABLED

If ENABLED, the ports specified are added to the list of ports allowed to use this command group. If DISABLED, the ports specified are removed from the list of ports allowed to use this command group. If DISABLED or ENABLED are not specified, the list of ports specified becomes the list of ports allowed to use the command group.

RENUMBER

If RENUMBER LINES is requested, the line numbers of the lines in the group are modified. The first line is given the number 10, and each line number thereafter is 10 greater than the preceding one.

Note

If a command group is invoked at the user's menu, neither privilege checking nor port list checking is performed. This results because the access server manager has already given the user permission to use the command group.

COMMAND GROUP LINE (privileged)

Syntax

{SET / DEFINE / CHANGE} COMMAND [GROUP] command_group LINE *n* [command_group_line]

Description

This privileged command creates or modifies a line in a command group.

Keywords

command_group

Specifies the name of the command group whose line will be created or replaced. The maximum length of *command_group* is 16.

n

The number of the line in the command group being created or replaced.

command_group_line

A string of text that can be up to 80 characters long and that will be interpreted as an access server command. The *command_group_line* value should be surrounded with quotation marks (" ") if it contains blanks or lowercase letters that should not be converted to uppercase.

If a *comman_group_line* value is not entered, the access server will prompt you for it.

Parameter substitution is indicated wherever a substring of the form "%P*n*" occurs. The *P* following the percent sign may be either uppercase or lowercase. The *n* may be any number between 1 and 8 inclusive.

COUNTRY

Syntax

DEFINE COUNTRY *country-number*

Description

This command modifies the country code setting for the modems in a DECserver 900MC access server. When you change the country code, you must re-initialize the access server to have the new country code take effect.

Restrictions

- Set the country code for the modems before you connect the modems to telephone lines.

Keyword

country-number

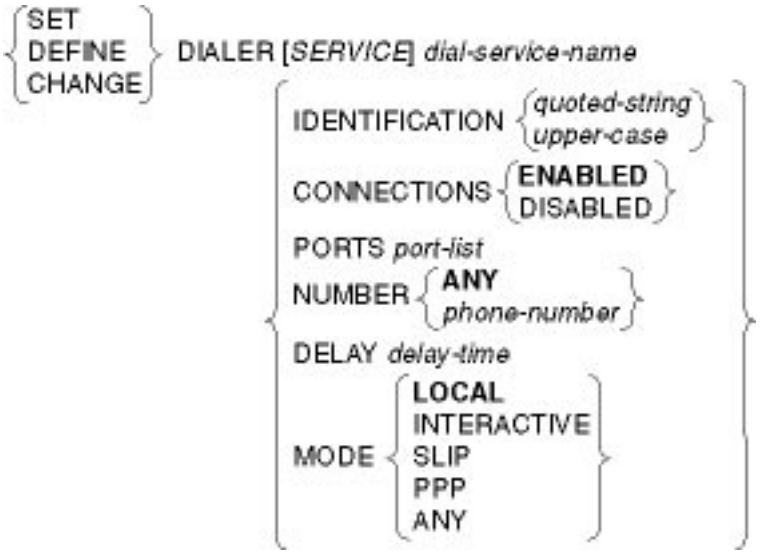
A code specific to a country's modem standards. The following table lists the supported country codes:

Country	Code	Country	Code
Australia	20	Japan	13
Austria	22	Netherlands	5
Belgium	23	New Zealand	11
Czech Republic	18	Norway	8
Denmark	10	Poland	19
Finland	9	South Africa	16
France	25	Spain	6
Germany	17	Sweden	7
Ireland	24	Switzerland	14
Israel	15	United Kingdom	2
Italy	3	United States	1
Italy SIP	4		

DIALER [SERVICE] - KERBEROS USER PASSWORD

DIALER [SERVICE] (privileged)

Syntax



Description

This privileged command creates or modifies a dialer service. A dialer service is used to establish a dial-back session. The dial-service-name specifies the name of the service to be created or modified. The length of the dial-service-name must be 16 or fewer characters.

Keywords

IDENTIFICATION

Allows an identifying string (40-character maximum) to be associated with a given service.

CONNECTIONS

Specifies whether or not a user may currently connect to this service.

PORTS

Is a list of one or more physical ports that are to offer this dialer service. Modems are assumed to be connected to these ports.

NUMBER

Indicates the allowable phone numbers for use with this service. The default is ANY, which means the user may specify any number within security constraints. If a number is specified, this is the *only* number that may be dialed using this service. The maximum length of a phone number is 80 characters.

DELAY

Indicates the delay (in seconds) before the dialer engine should attempt to initiate the dialback/dialout (defaults to 30 seconds). The minimum allowed delay is 15 seconds, while the maximum possible delay is 3600 seconds (1 hour).

MODE

Indicates the type of session that the dialer service will create after successfully completing the modem connection.

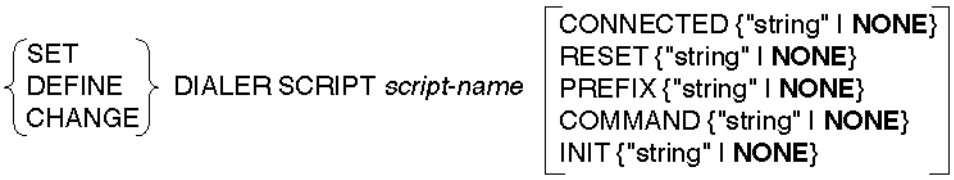
Table: Mode Descriptions

Mode	Description
LOCAL	Interactive non dedicated session
PPP	Dedicated PPP session
SLIP	Dedicated SLIP session
LOGIN	Interactive dedicated session, based on port and/or user authorization information
* or ANY	Any mode allowed (within user security constraints)

A dial-back request implies that the current session will be logged out and the client's modem hung up in anticipation of a return call from the server.

DIALER SCRIPT [NAME] (privileged)

Syntax



Description

This privileged command is used to define a modem script/type and its characteristics. The script name may be a maximum of 16 characters. Parameters define the character strings that make up various modem commands. The functions and default values of each string are shown in Table: Dialer Script Strings. Each associated string can be up to 40 characters in length.

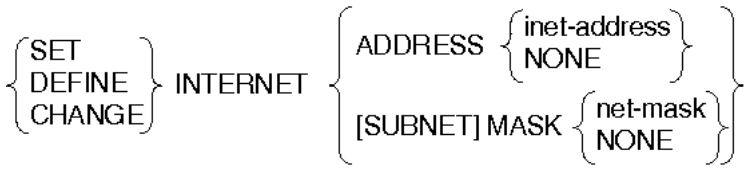
Table: Dialer Script Strings

String Type	Default Value	Usage
COMMAND	"AT"	Appended to all other command strings.
INIT	None	Before initiating an outbound connection.
PREFIX	"DT"	Before digits of phone number.
CONNECTED	"Connect"	Verifies successful connection.
RESET	"H0Z" (The second character is zero.)	After session is disconnected.

The size of a modem dialer script string is restricted by the amount of remaining unallocated NVRAM for the modem pool (total of 2K bytes for 8- and 16-port servers, and 4K for 32-port servers) and by the command line restrictions. The script name may be a maximum of 16 characters.

INTERNET (privileged)

Syntax



Description

This privileged command modifies the access server Internet address and subnet mask.

The Internet address must be defined in the access server database for the access server to function in the Internet environment. You must configure the Internet address in both the permanent and operational databases after downline loading takes place. You will not have to redefine the Internet address on successive loads as long as that address resides in the permanent database. If an Internet address has not been defined on the access server, the access server can use the BOOTP protocol to obtain its Internet address from a network host.

The subnet mask defaults to a Class A, B, or C mask depending on the class of the Internet address defined. If the default subnet mask is satisfactory, you do not have to set the subnet mask.

Keywords

ADDRESS

Specifies the access server Internet address.

inet-address

The Internet address must be a valid Internet address of the form *n.n.n.n*, where *n* is a decimal number in the 0 to 255 range.

NONE

If the DEFINE INTERNET ADDRESS NONE command is entered, it deletes the previously defined Internet address from the access server permanent database.

[SUBNET] MASK

Specifies the access server subnet mask used to partition the host section of an Internet address into subnets.

net-mask

The subnet mask must be of the form *n.n.n.n*, where *n* is a decimal number in the 0 to 255 range. (Default: If you do not specify a subnet mask, the access server defaults to either a Class A, B, or C subnet mask depending on the current access server Internet

address. The default for a Class A subnet mask is 255.0.0.0; for a Class B, 255.255.0.0; and for a Class C, 255.255.255.0. If an Internet address has not been defined, there is no default subnet mask.)

NONE

Deletes a previously defined Internet subnet mask.

Restrictions

- The Internet address cannot be changed while the Internet protocols are running.
- If you do not want to use the default subnet mask, you must configure the subnet mask before configuring the Internet address; otherwise, the access server will choose the default subnet mask.
- The NONE characteristic cannot be used with the SET INTERNET ADDRESS or CHANGE INTERNET ADDRESS command.

Example: DEFINE/SET/CHANGE INTERNET

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

This command enters the Internet address 195.1.1.60 into both the operational and permanent databases.

INTERNET ARP ENTRY (privileged)

Syntax

{SET, DEFINE, CHANGE} INTERNET ARP ENTRY inet-addr ETHERNET eth-addr [NOPURGE]

Description

This privileged command enters an Internet address resolution protocol (ARP) entry into the access server ARP database. These entries can be purged by the access server.

Keywords

inet-addr

Specifies the Internet address of the Internet ARP entry. (The address must be a valid Internet address of the form *n.n.n.n*, where *n* is a decimal number of the 0 to 255 range.)

eth-addr

Specifies the Ethernet address of the Internet ARP entry. (The address must be a valid Ethernet address of the form HH-HH-HH-HH-HH-HH.)

[NOPURGE]

Specifies that the ARP entry will not be purged. The ARP entry is dynamically purged by default unless the NOPURGE option is specified. The dynamic purging mechanism affects entries in the current (operational) database only. However, if you would like the ARP entry permanently defined as a NOPURGE entry, specify the NOPURGE option with the CHANGE or DEFINE command.

Restriction

There can be only one ARP entry per Internet address in the ARP database. When you use the SET/DEFINE/CHANGE command with an ARP entry, the software checks to determine whether the specified Internet address is already defined in the ARP database. If it is, the new Ethernet address will overwrite the previously defined Ethernet address.

Example: SET/DEFINE/CHANGE INTERNET ARP ENTRY

```
Local> SET INTERNET ARP ENTRY 195.1.1.60 ETHERNET 00-2B-
00-26-00-1A
```

This command creates an Internet ARP entry associating IP address 195.1.1.60 with an Ethernet address 00-2B-00-26-00-1A.

INTERNET DHCP (privileged)

Syntax

{ SET / DEFINE / CHANGE } INTERNET DHCP { **ENABLED** / DISABLED }

Description

This privileged command enables or disables all DHCP functionality on the access server.

Keywords

ENABLED/DISABLED

Enabling DHCP specifies that the access server uses DHCP to try to autoconfigure its IP parameters (excluding the access server's IP address). ENABLED is the default. Disabling DHCP means that the access server obtains its IP parameters from other sources (for example, a BOOTP server or access server commands that you enter).

INTERNET GATEWAY (privileged)

Syntax

Description

This privileged command enters a gateway into the access server gateway database.

Keywords

inet-address

Specifies the Internet address of the gateway being defined. This address must be located in the same network as the access server and it must be a valid Internet address in the form *n.n.n.n*, where *n* is a decimal number in the 0 to 255 range.

Note

If inet-address is specified without the NETWORK characteristic, then NETWORK ANY is the default.

HOST [ADDRESS] inet-address

Specifies a host that is reachable through the gateway. This option is used to define a gateway to a specific host, rather than to a network.

ANY

Specifies that ANY network address is accessible through the defined gateway. This is the default.

net-address

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

[SUBNET] MASK submask

When used with NETWORK, determines the exact SUBNET that the user can access through the defined GATEWAY. If the SUBNET MASK option is omitted, the subnet mask in the access server operational database is the default. Avoid overlapping subnets (similar subnet mask addresses).

Restrictions

- There can be only 16 gateway entries defined in the permanent database.
- To ensure clearly defined gateways, avoid overlapping subnets (gateways with similar subnet addresses).
- While it is possible to use the SET/DEFINE/CHANGE command with various network addresses for the same gateway (using the same Internet address), you must use a separate SET/DEFINE/CHANGE INTERNET GATEWAY command to assign the same inet-address to each network.

Example: SET/DEFINE/CHANGE INTERNET GATEWAY

```
Local> CHANGE INTERNET GATEWAY 195.1.1.60 NETWORK
127.10.1.0
```

This command enters an Internet gateway with an Internet address of 195.1.1.60 and a network address of 127.10.1.0 in the access server operational and permanent databases. Because the SUBNET MASK option is omitted, the server uses the current Internet subnet mask in the server operational database (and no subnet mask in the server permanent database). In the above example, all connections to the hosts beginning with address 127.10 will go through the gateway address 195.1.1.60.

INTERNET HOST (privileged)

Syntax

Description

This privileged command enters Internet hosts into the access server domain name system (DNS) database.

Keywords

host-name

Specifies a name for the Internet host. Valid name length is 1 to 255 characters.

inet-address

Specifies the Internet address of the Internet host. (The address must be a valid Internet address of the form *n.n.n.n,* where *n* is a decimal number of the 0 to 255 range.)

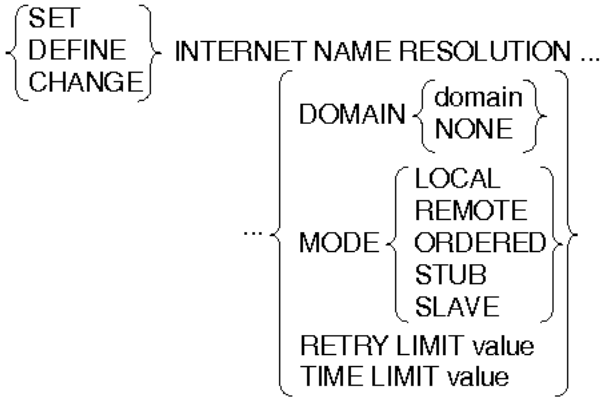
Example: SET/DEFINE/CHANGE INTERNET HOST

```
Local> SET INTERNET HOST BAKER ADDRESS 195.1.1.60
```

This command enters Internet host BAKER into the access server DNS operational database.

INTERNET NAME RESOLUTION (privileged)

Syntax



Description

This privileged command modifies the parameters associated with the Internet domain name system (DNS) function in the access server database.

Keywords

domain

Specifies the access server default name resolution domain.

MODE

Specifies the data retrieval preference. In LOCAL mode, the server queries its own DNS cached database (user-entered data only) for Internet addresses. In REMOTE mode, the server first queries its own cache database (learned data only) and, if it does not find the Internet address there, it queries the name servers.

In ORDERED mode, the server queries its own cached database for the Internet address (learned data first, then user-entered data regardless of whether there is learned data). If there is no learned data in the cache database, the server queries the name servers before checking for user-entered data. The default is ORDERED.

In STUB mode, the access server does not cache any responses from name servers. Any locally defined host addresses are ignored, and the access server does not learn about additional name servers for any domains. All queries are sent to the locally configured name servers. In order to be able to resolve names outside the local domain, the name servers must offer recursive name service.

SLAVE mode incorporates the functions of STUB mode with the added capability of using locally defined host names. However, the access server still performs no caching of learned host or name server information. In SLAVE mode, the name resolver on the access server returns an ordered list of host addresses. Locally defined addresses for the host appear in the list ahead of the addresses returned from the recursive name service.

RETRY LIMIT *value*

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

TIME LIMIT *value*

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

Example: SET/DEFINE/CHANGE INTERNET NAME RESOLUTION

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

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

INTERNET NAMESERVER (privileged)

Syntax

{SET / DEFINE / CHANGE} INTERNET NAMESERVER *name* ADDRESS *inet-address* [ROOT / LOCAL]

Description

This privileged command enters the Internet name server into the access server domain name system (DNS) database.

Keywords

name

Specifies a name for the name server. An absolute domain name is required for a ROOT name server. A relative domain name may be used for a LOCAL name server provided a local domain has been previously set on the access server DNS database.

inet-address

Specifies the Internet address of the name server to be entered in the database. The address must be a valid Internet address of the form *n.n.n.n*, where *n* is a decimal number in the 0 to 255 range.

ROOT

Specifies that a ROOT name server is being defined.

LOCAL

Specifies that a LOCAL name server is being defined. LOCAL is the default.

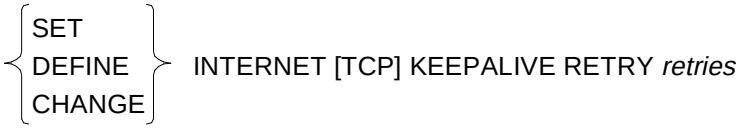
Example: SET/DEFINE/CHANGE INTERNET NAMEserver

```
Local> SET INTERNET NAMEserver FALCON.LKG.DEC.COM ADDRESS
195.1.1.60
```

This command enters the local Internet name server FALCON with the Internet address 195.1.1.60 into the access server DNS operational database.

INTERNET TCP KEEPALIVE RETRY

Syntax



Description

Specifies the maximum number of probes to send to a remote host with a TCP connection. If the remote host does not respond to any of the probes it receives, the access server closes the TCP connection.

Keyword

retries

The total number of probes to send to the remote host after which the access server closes the TCP connection if the remote host does not provide a valid response.

INTERNET TCP KEEPALIVE TIMER

Syntax

Description

This command sets the amount of time in minutes to wait before sending the first TCP keepalive probe to a remote host that has an idle TCP connection.

Keywords

DISABLED

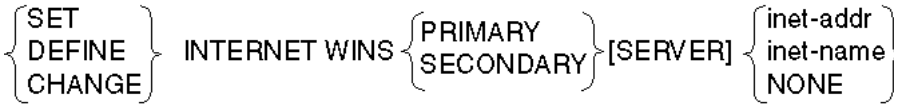
Specifies that the access server sends no TCP keepalive probes to remote hosts with TCP connections.

minutes

The number of minutes, from 1 to 1440 (one day), to wait before sending the first TCP keepalive probe to a remote host.

INTERNET WINS (privileged)

Syntax



Description

This privileged command defines WINS server addresses on the access server. Depending on the client's configuration, these addresses may be given to a PPP dialup client using IP. Use this command if DHCP is disabled on the access server, or if you need to change the WINS server IP addresses provided by DHCP and do not want to re-initialize the access server.

Keywords

PRIMARY/SECONDARY

Specifies which WINS server address will be modified.

inet-addr

The Internet address for the WINS server.

inet-name

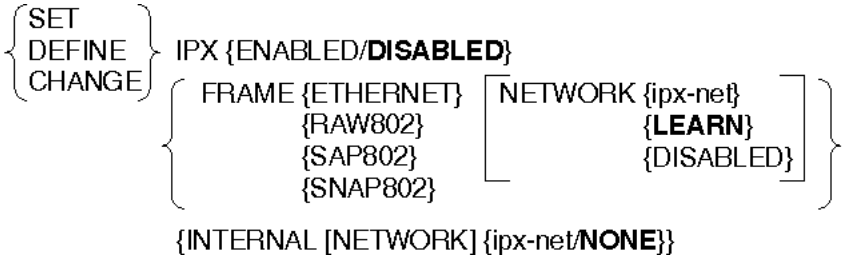
The Internet host name for the WINS server. The maximum length of the *inet_name* is 80 characters.

NONE

Sets the WINS server Internet address to 0.0.0.0.

IPX (privileged)

Syntax



Description

This privileged command enables or alters IPX characteristics.

Keywords

ENABLED

Initializes and enables IPX on the access server.

DISABLED

Use the DEFINE command to disable IPX on the access server and then reboot the access server. IPX will not initialize when the access server is rebooted. If IPX is enabled, you cannot use the SET or CHANGE commands to disable IPX.

FRAME

Specifies which frame-encapsulation type IPX will use, including:

- ETHERNET: Standard Ethernet V2
- RAW802: Novell's 802.3 raw frame type
- SAP802: IEEE 802.2 standard frame type
- SNAP802: IEEE 802.2 subnetwork access (SNAP) SAP

NETWORK

Specifies the network number for the frame type being used. The default value for this is LEARN. Disabling the frame is not allowed for the active server. You cannot configure a frame LEARN or ipx-net for a frame that already has a network number.

ipx-net

A maximum of 8 hexadecimal numbers 1-FFFFFFFE. The number should be the same Novell IPX network number used on the LAN for the FRAME specified.

LEARN

Learn the network number for the FRAME from the network IPX packets. The network number is learned under the following circumstances:

- When the access server sends a SAP Get Nearest Server (GNS) request on the LAN. The network number is learned by monitoring SAP GNS responses. This happens when:
  - The access server is enabled for IPX or a new PPP IPX session is created. Periodic SAP GNS requests are sent for 40 seconds.
  - Any time a SAP GNS request is received from an asynchronous port.
- When the access server receives a RIP broadcast request from the LAN.

DISABLED

IPX is disabled for the specified FRAME.

INTERNAL

Assigns a unique internal IPX network number for the access server. This is used by the asynchronous ports for assigning a common network number when a PC client dials in using PPP/IPXCP. A higher network number explicitly negotiated by a PC client takes precedence over the INTERNAL network number. Use of the INTERNAL network number minimizes network loading. If PC clients require a network number for the PPP/IPXCP link, the internal network number must be configured so that the PC client dial-in succeeds. The internal network number cannot be changed while there is an active IPX port connection.

NONE

There is no IPX address for the internal network.

KERBEROS LIFETIME (privileged)

Syntax

{SET / DEFINE / CHANGE} KERBEROS LIFETIME *seconds*

Description

This defines value for the number of seconds that Kerberos remains active before timeout. Credentials are not implemented in this release.

KERBEROS PASSWORD SERVICE PORT (privileged)

Syntax

{SET / DEFINE / CHANGE} KERBEROS PASSWORD [SERVICE] PORT [*n*]

Description

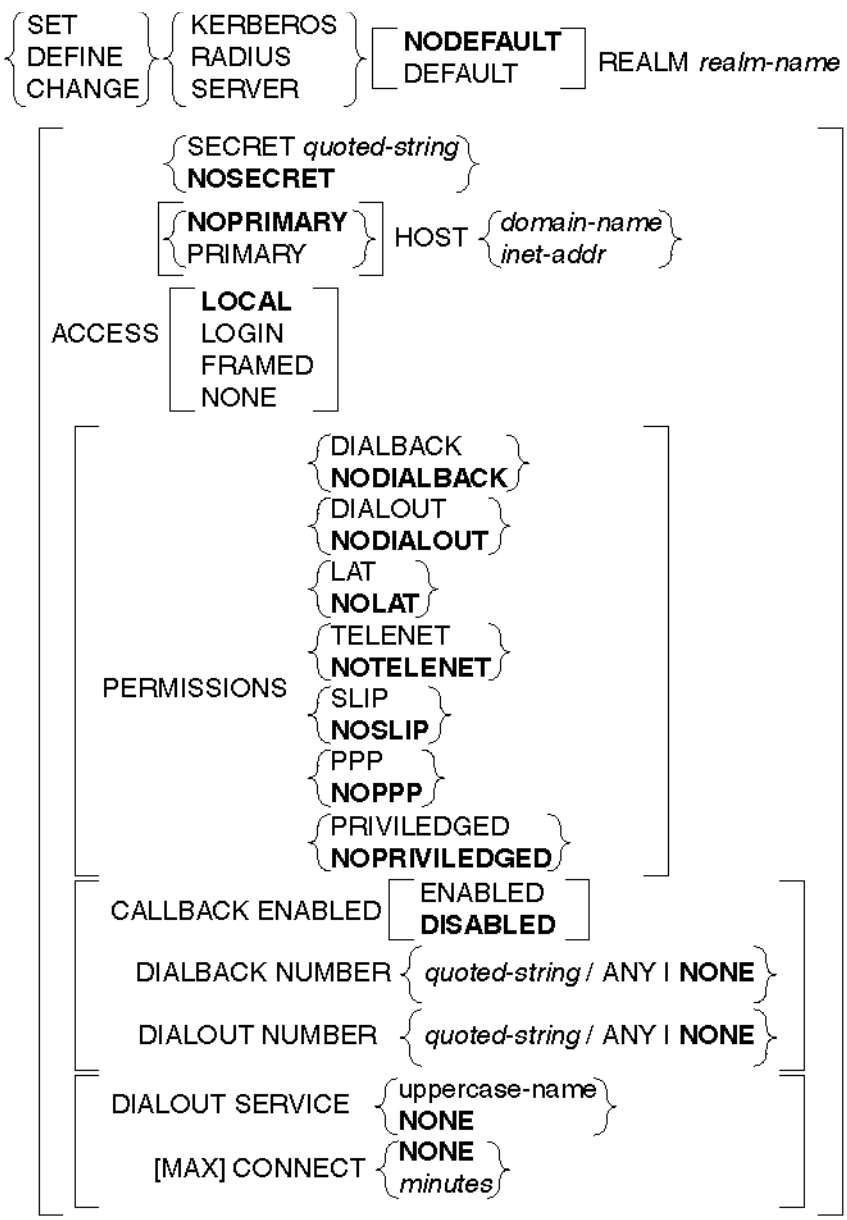
This privileged command specifies the TCP port number to which the access server will send Kerberos messages. Kerberos messages are sent to the master KDC in order to change the user's Kerberos password. The port number can be from 1 to 1024. The default port number is 751.

Note

The default port number 751 may change in the future to allow for standardization. The probable replacement will be 89.

KERBEROS REALM (privileged)

Syntax



Description

The SET/DEFINE/CHANGE REALM command family sets up and tears down the various realms used to identify particular administrative domains. These are privileged commands.

Keywords

SECRET

The SECRET clause is used to specify a secret that the DECserver shares with security servers from the realm. The DECserver software associates no default secret with any realm.

HOST

The HOST clause associates a host with a realm. The DECserver software will use this host to resolve authentication requests. The DECserver software will accept either a domain name or an IP address as a host identifier. The PRIMARY keyword indicates that the DECserver software should give first priority to this host, (that is, it should begin all new authentication requests with this host). The default is NOPRIMARY. A realm can have only one primary host.

INCLUDE/NOINCLUDE

The INCLUDE/NOINCLUDE clause (supported for RADIUS only) indicates whether or not to include the realm name as part of the user ID. The default is NOINCLUDE. This option exists as a convenience to the security administrator.

The clauses ACCESS, PERMISSIONS, CALLBACK, DIALBACK NUMBER, DIALOUT NUMBER, DIALOUT SERVICE, and MAX CONNECT specify the default authorization for users authenticated, but not otherwise authorized, within the realm. The DECserver software provides default values for these categories of information when the authentication service fails to provide them. The NUMBER clause applies to both dialout and dialback (or callback) types of access, and is most meaningful if it is a number mask, (that is, contains an element of wildcarding). Specific, fully qualified telephone numbers do not make sensible realmwide default values.

ACCESS

The ACCESS clause sets the realm's default access mode at connection establishment time. The supported values are:

LOCAL	Interactive access to "Local >" prompt provided
FRAMED	AUTOLINK (PPP or SLIP) access provided
LOGIN	Dedicated connection (Telnet, LAT) to host (only) provided
NONE	Access determined by PORT characteristics

NONE is the default value for this realm characteristic.

CALLBACK

An administrator would specify mandatory callback by configuring an account with CALLBACK ENABLED.

DIALBACK NUMBER, DIALOUT NUMBER

The DIALOUT and DIALBACK NUMBER values have a maximum length of 80 characters, and contain a phone number to be used on dialout/back. It is expected that "normal" modem phone number strings will appear here. You define modem dialing commands in dialer scripts.

The DIALBACK NUMBER is used for Mandatory Dialback as well as for PPP Callback on the same port (where the user is unable to specify a dialback service). The DIALOUT NUMBER clause is used for interactive dial-out commands, the actual number to dial, a number mask (time permitting), and that any number may be used. If the number is not fully specified, and it is not contained in the optional DIALOUT SERVICE definition, the dialer engine will prompt the user for the number. The DIALOUT SERVICE clause specifies a default dialer service to be used when attempting a dialout connection. Refer to the section entitled USERACCOUNT (privileged) for more information on dialback/dialout numbers.

DIALOUT SERVICE

The DIALOUT SERVICE values will be converted to upper-cased and have a maximum length of 16 characters.

MAXCONNECT

The MAXCONNECT clause indicates the maximum number of minutes the user can be logged in before being forcibly logged out. The user interface is the same as USERACCOUNT MAX CONNECT.

Some realms support the following clauses:

Realm	Clause
RADIUS	The PROMPT clause specifies an alternate password prompt to display to interactive users when the entered user-id falls within one of these realms. The maximum prompt length is 16 characters.
SecurID	The ENCODING clause indicates how to encode the user password in authentication requests to the security server. This option is currently valid only for SecurID realms. The supported values are data encryption standard (DES) and PROPRIETARY. The Security Dynamic proprietary encryption is freely exported from the countries outside of the United States, while DES is restricted from foreign export.
Local database	The local database (SERVER REALM) uses the MAX FAILS clause to indicate the number of consecutive authentication failures to permit before deactivating a record. The default is 3; the range is 0 to 100.

KERBEROS TICKET SERVICE PORT (privileged)

Syntax

Description

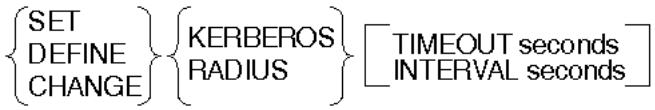
This privileged command specifies the UDP port number to which the access server sends Kerberos messages. Kerberos messages are sent to the key distribution center (KDC) in order to obtain a Kerberos ticket for the user. The port number can be from [1] to [1024]. The default port number is 750.

Note

The default port number 750 may change in the future to allow for standardization. The probable replacement will be 88.

KERBEROS [TIMEOUT] (privileged)

Syntax



Description

This privileged command specifies the number of seconds that a key distribution center (KDC) request can be outstanding before being timed out. The access server will first retransmit an outstanding request after a 1-second retransmit timer, again after a 2-second retransmit timer, doubling each time, then a 4-second retransmit timer, and so forth, until the request is fulfilled either by the KDC or until the KERBEROS TIMEOUT period is reached. If there is more than one KDC for a realm, the retransmit timer is not doubled until the request is retransmitted to all the KDCs for the realm.

Keywords

TIMEOUT *seconds*

The TIMEOUT value specifies the maximum amount of elapsed time the user may wait for the operation to be completed, or to fail with a timeout error message. The allowable range for the TIMEOUT is 1 to 64 seconds; the default value is 2 seconds.

INTERVAL *seconds*

The valid range for INTERVAL is 1 to 20 seconds, with a default of 2 seconds.

KERBEROS USER PASSWORD (KPASSWD) (secure)

Syntax

DEFINE KERBEROS USER [PASSWORD] [principal-name]

Description

This command allows you to change your Kerberos password. If a user name is not specified on the command line, the access server will prompt you for the user name. The principal name can also be used, which is made up of the user name, instance, and realm. A Ctrl/Z will cause the port's user name to be used as the default.

Before a password can be changed, the access server will first prompt you for the old password and the new password. The access server will ask you to verify the new password and will not echo the entered passwords.

Restrictions

- This command affects the master KDCs database. The SET and CHANGE commands are not supported.
- The entered passwords must not exceed 40 characters in length.

Note

Command KPASSWD is equivalent to DEFINE KERBEROS USER [PASSWORD].

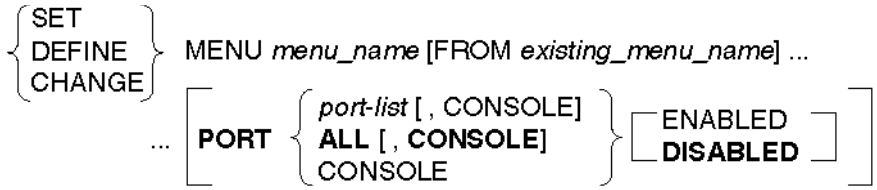
Example: SET/DEFINE/CHANGE KERBEROS USER PASSWORD (KPASSWD)

```
Local> DEFINE KERBEROS USER PASSWORD
Username> J_SMITH
Old Password> SECRET (not echoed)
New Password> DOUBLESECRET (not echoed)
Verification> DOUBLESECRET (not echoed)
Local -468- Attempting to change Kerberos password for user:
J_SMITH@ACME.COM
Local -469- Kerberos password has been changed
```

MENU

MENU (privileged)

Syntax



Description

This privileged command is used to create a menu with an associated name and a port list. It initializes the contents of the menu, either as an empty menu or as a copy of a previous menu. If the menu already exists, this command changes the associated port list.

If a you are a user with privileged access, or if you are logged in to one of the ports in the port list, then you may use the menu from the Local> prompt as the argument of an ENTER MENU command.

Keywords

menu_name

Specifies the name of this menu and will appear as the parameter in an ENTER MENU or DEFINE PORT DEFAULT MENU command. The maximum length of the *menu_name* is 16.

existing_menu_name

Specifies the name of an existing menu, the contents of which will be copied into the newly created menu. If this option is not specified, the menu is initialized as empty.

port-list

Specifies one or more ports that will have access to this menu.

ALL

Specifies all ports. The remote management console port is not included.

CONSOLE

Specifies the remote management console port, available either through Telnet or MOP.

ENABLED/DISABLED

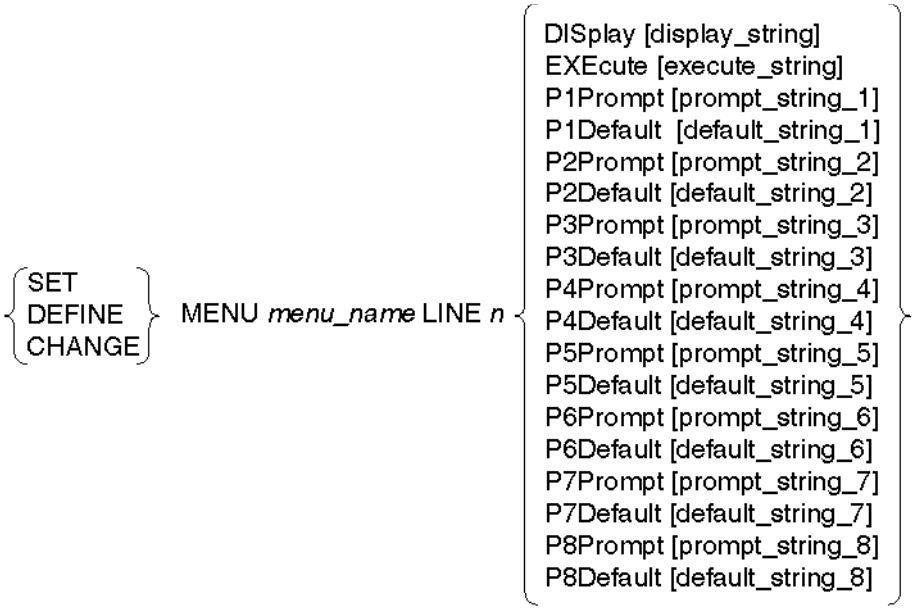
If ENABLED is specified, the ports specified are added to the list of ports allowed to use this menu. If DISABLED is specified, the ports specified are removed from the list of ports allowed to use this menu. If neither DISABLED nor ENABLED is specified, the list of ports specified becomes the list of ports allowed to use the menu.

Note

If a menu is entered through a menu, no privilege checking is done, because the access server manager has already given permission.

MENU LINE (privileged)

Syntax



Description

This privileged command is used to specify the contents of a line in a menu.

Keywords

menu_name

Specifies the name of the menu in which a line is being created or modified. The maximum length of a menu_name is 16.

n

The line number being described. The top line is 1.

Display_string

A display_string is a text string up to 80 characters long displayed on a specified line. If it contains letters that are to remain lowercase or contains spaces, the display_string must be surrounded with quotation marks (" "). If no string is entered, the access server will prompt you for it.

Execute_string

This can be a text string up to 80 characters long. The execute_string will be interpreted as an access server command if you select this text string for execution. If it is a null string, contains letters that are to remain lowercase or contains spaces, the execute_string must be surrounded with quotation marks (" "). If an execute_string is not entered, the access server will prompt you for it. If the string is a DO command, several commands will be executed.

Parameter substitution is indicated wherever a substring of the form "%P*n*" occurs. The *P* following the percent sign may be either upper or lowercase. The *n* may be between 1 and 8 inclusive.

`prompt_string_1 ...`

`prompt_string_8`

These eight text strings can each be up to 80 characters long. If a text string contains letters that are to remain lowercase or contains spaces, the string must be surrounded with quotation marks (" "). The prompt string will be displayed by the server when it is time for you to supply information to be substituted into the execute string. If no string is entered, the access server will prompted you for it.

`default_string_1...`

`default_string_8`

These eight text strings can each be up to 80 characters long. If a text string contains letters that are to remain lowercase or contains spaces, the default_string must be surrounded with quotation marks (" "). The access server will use it as your input, if you respond to the prompt by pressing the Return key. The default string will be displayed in braces following the prompt string. If no string is entered, the access server will prompt you for it.

PORT - PORT AUTOPROMPT

PORT (secure)

Syntax

Description

This command (available to all users) modifies port characteristics. All of the SET/DEFINE/CHANGE port commands accept a port list or ALL as a parameter. The DEFINE PORT command modifies port characteristics in the permanent database. These changes take effect the next time the port is logged in.

The SET PORT command modifies port characteristics in the operational database. Such changes take effect immediately but remain in effect until port logout. Port characteristics revert to the values in the permanent database at the next login.

The CHANGE PORT command modifies port characteristics in both the permanent and operational databases; use the CHANGE PORT command to perform the function of both the DEFINE PORT and SET PORT commands. For all TN3270 usage, refer to the PORT TN3270 command.

Keywords

ALL

A privileged parameter specifying that the defined characteristics apply to all ports.

port-list

A privileged parameter specifying one or more ports to which the defined characteristics apply. The default is your own port. For more information on specifying port-list, refer to Chapter 1.

Restrictions

- Secure users cannot enter the DEFINE PORT or CHANGE PORT command.
- Only privileged users can specify port characteristics for ports other than the port being used.
- Secure and nonprivileged users cannot specify all port characteristics. These restrictions are specified with the applicable characteristics.
- You cannot change any characteristics for the remote management port.

Example: SET/DEFINE/CHANGE PORT

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

In this command, the parameters affect the way port 8 can be used in service mode; these settings remain in effect only until the port is logged out.

PORT ACCESS (privileged)

Syntax

Description

A privileged option that specifies the type of access allowed for the device using the port. This command accepts a port-list or ALL as a parameter.

Caution

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

Keywords

LOCAL

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

REMOTE

Allows access to (1) the port device (typically a line printer) by service node applications or (2) a port device offered as a service or Telnet listener.

DYNAMIC

Allows port to alternate between remote access and local access.

NONE

Allows no access to the port.

Restrictions

- If any of the ports in the port-list are logged in, you cannot use the SET or CHANGE port-list ACCESS REMOTE or NONE command.
- If any port in the port-list is defined REMOTE or NONE, you cannot use the SET or CHANGE port-list ACCESS DYNAMIC or LOCAL command.

PORT ALTERNATE SPEED (privileged)

Syntax

{SET / DEFINE / CHANGE} PORT ALTERNATE [SPEED] {*speed* / **NONE**}

Description

A privileged option that specifies a secondary speed for a multi-speed modem. Permissible values are: 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600, 19200, 38400, 57600, and 115200. NONE (the default) clears a previously specified speed. This command accepts a port-list or ALL as a parameter.

Restriction

ALTERNATE SPEED is not valid on all access servers. For more information, refer to the *Network Access Server Managemen*t manual.

PORT AUTHENTICATION (privileged)

Syntax

DEFINE PORT AUTHENTICATION {ENABLED / DISABLED}

Description

This privileged command determines whether user interactive authentication will be required on the port. The access server manager should decide which ports must authenticate its users at login time. When enabled, AUTHENTICATION will show up in the ENABLED CHARACTERISTICS section of the SHOW PORT CHARACTERISTICS display. This command accepts a port-list or ALL as a parameter.

Restriction

Since the AUTHENTICATION command takes effect only when you log in, the SET and CHANGE commands are not allowed.

Note

Interactive (terminal) users or framed (remote network access) users can use this form of user authentication when a login script is used on the remote client. PPP and AUTOLINK authentication is also available for framed users. See PORT PPP LCP AUTHENTICATION and PORT AUTOLINK AUTHENTICATION for more information.

PORT AUTHORIZED GROUPS (privileged)

Syntax

Description

A privileged option that allows you to authorize groups of LAT service nodes to be available to the port. The default is group 0 ENABLED and all other groups DISABLED. Specify ALL to enable or disable all groups for the port.

Keywords

group-list

One or more decimal codes ranging in value from 0 to 255, each representing a LAT group code. Specify multiple codes by separating individual numbers with commas, by specifying a range of numbers (in ascending order), or a combination of both. For example, the group list 1, 3, 5-8, 14 specifies groups 1, 3, 5, 6, 7, 8, and 14.

ENABLED/DISABLED

Use group-list ENABLED or DISABLED to add groups to or remove groups from the existing list for the port. Specify the group-list value to replace the existing list with a new one.

PORT AUTOBAUD (privileged)

Syntax

Description

A privileged option that specifies whether the access server automatically detects the speed, parity, and character size of the port device on login. This option also sets the access server port characteristics to match the port device (default: ENABLED). The

AUTOBAUD function works only if the port device's CHARACTER SIZE and PARITY characteristics are set to either 8 and NONE or 7 and EVEN. This command accepts a port-list or ALL as a parameter.

Disable AUTOBAUD for ports set to ACCESS REMOTE or ACCESS DYNAMIC. If you enable AUTOBAUD on ports having a preferred or dedicated service, you must press the Return key once more to connect to the service.

Note

Changes to this characteristic become effective on the next port login. You should use the DEFINE or CHANGE command to preserve them after logout.

PORT AUTOCONNECT (nonprivileged)

Syntax

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

Description

A nonprivileged option that specifies whether the access server automatically connects the port to a dedicated service or preferred service at port login and reconnects the port when LAT connection failures occur (default: DISABLED). Also, with AUTOCONNECT ENABLED, the access server will search for a requested LAT service that is not in the access server database, adds that service when it is found, and then establishes the requested connection. This command accepts a port-list or ALL as a parameter.

Restriction

AUTOCONNECT must be DISABLED when using DEFAULT PROTOCOL ANY.

PORT AUTOLINK (privileged)

Syntax

{DEFINE} PORT AUTOLINK { AUTHENTICATION {ENABLED / **DISABLED**} | TIMER [PASS] {ONE / TWO} *number* }

Description

A privileged option that defines AUTOLINK characteristics.

Keywords

AUTHENTICATION

Specifies that the port can support authenticated logins from different types of PPP clients, which may have different LCP capabilities. For SLIP or PPP clients that do not support PAP or CHAP authentication, an interactive or script-based login will be used. With AUTOLINK AUTHENTICATION enabled, only *one* form of authentication will be required during any port login.

TIMER

Specifies the AUTOLINK timers. (See following description.)

PASS

Determines the authentication style and the protocol of a user session. The following table describes each pass of AUTOLINK:

Pass	Description
ONE	If authentication is required, determines the authentication style, otherwise determines the session style. Either PPP authentication or character-cell authentication can be used.
TWO	Used only when there has been an authentication pass to determine the protocol of the user session, which can be SLIP, PPP, or character-cell terminal.

number

Indicates the number of seconds the DECserver waits to sense one of the following:

- A valid PPP frame
- A valid SLIP frame
- A single carriage return character

If the timer expires, AUTOLINK assumes a character cell terminal.

The range for the PASS ONE timer is between 10 and 60 seconds. The range for the PASS TWO timer is between 0 and 60 seconds. The default value is 10 seconds. If you enter 0, character-cell mode is entered immediately in PASS TWO.

Restriction

To use AUTOLINK AUTHENTICATION, you must set the DEFAULT PROTOCOL and the DEDICATED SERVICE for the port to AUTOLINK.

PORT AUTOPROMPT (secure)

Syntax

Description

An option (available to all users) that specifies whether a login sequence is automatically initiated for the port when the port connects to a LAT service (default: ENABLED). This command accepts a port-list or ALL as a parameter.

Note

For this option to work, the LAT service must also support AUTOPROMPT.

Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT BACKWARD SWITCH - PORT DTRWAIT

PORT BACKWARD SWITCH (secure)

Syntax

Description

An option (available to all users) that specifies a switch character that allows you to resume the preceding session in your session list without returning to local mode. You can clear an existing switch by specifying NONE (default). This command accepts a *port-list* or ALL as a parameter.

Note that you can specify control characters by using a two character sequence of the up arrow and a character key. For example, if you enter ^a , the switch character is set to Ctrl/a.

Restrictions

- The BACKWARD switch does not work on a port that has the MULTISESSIONS characteristic ENABLED.
- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.
- You cannot use a parenthesis, (or), as the switch character.
- Using the BACKWARD command within a TN3270 session causes the screen to clear and the 3270 screen to be displayed. The information displayed will be the information that existed prior to the interrupt.

PORT BREAK (secure)

Syntax

Description

An option (available to all users) that specifies how the Break key is handled during a session. This command accepts a *port-list* or ALL as a parameter.

Keywords

LOCAL

Causes the access server to interpret a break signal as a local switch character and to return you to local mode. This is the default. When a TN3270 session is interrupted with the break or the local switch, you are placed in the local mode with the cursor positioned at the last row of the screen.

REMOTE

Causes the access server to ignore LAT session break signals and to pass them to the connected service. This has no affect on Telnet session break signals. This feature is available for Telnet using SET/DEFINE/CHANGE PORT TELNET CLIENT BREAK or SET SESSION TELNET BREAK commands.

DISABLED

Causes break signals to be ignored. When break is DISABLED, the access server recognizes break signals once you return to local mode.

Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT BROADCAST (nonprivileged)

Syntax

Description

A nonprivileged option that specifies whether the port receives messages sent from other ports (default: ENABLED). This command accepts a *port-list* or ALL as a parameter.

PORT CHARACTER SIZE (nonprivileged)

Syntax

Description

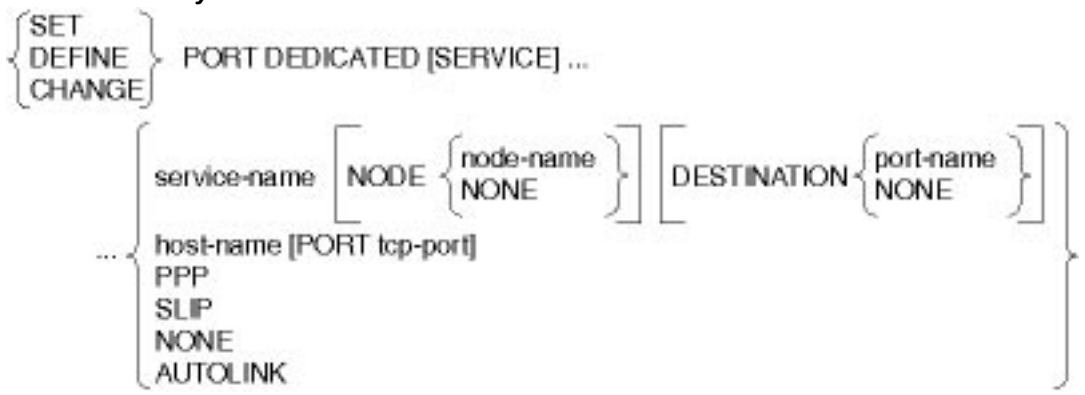
A nonprivileged option that specifies the number of bits in data characters exchanged between the port and the access server (values: 7 or 8 [default]). This command accepts a *port-list* or ALL as a parameter.

Restriction

You cannot modify CHARACTER SIZE for a port that has the AUTOBAUD function enabled.

PORT DEDICATED (privileged)

Syntax



Description

A privileged option that specifies a service to which a local access port is permanently assigned (default: no dedicated service). Entering NONE as the value for *service-name*, NODE, or DESTINATION cancels any previous value entered for that field. Changes to this characteristic become effective on the next port login. AUTOCONNECT is automatically enabled when you specify a dedicated service; at port login, the port is automatically connected to the dedicated service. This command accepts a *port-list* or ALL as a parameter.

Note

If AUTOCONNECT is enabled and AUTOBAUD is disabled on a port that is DEDICATED, the session is started when the access server is initialized. To effectively use PORT DEDICATED, you should change the default protocol to ANY or to the same protocol as the dedicated service.

Keywords

service-name

Specifies the name of the dedicated LAT service. The service name can have a maximum length of 16 characters.

NODE *node-name*

Specifies a LAT service node that offers the dedicated service.

DESTINATION

Specifies a particular port to which you want to connect.

host-name [PORT tcp-port]

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

PPP

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

SLIP

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

AUTOLINK

Specifies that the local access port is permanently assigned to a single PPP or SLIP session, or to an interactive terminal session.

Restrictions

- You cannot use the word TELNET as a service-name or host-name.
- You can specify DEDICATED with the SET PORT command provided the target port is not currently logged in. You cannot enable MULTISESSIONS when you have a dedicated service.

PORT DEFAULT MENU (privileged)

Syntax

DEFINE PORT DEFAULT MENU { NONE | menu_name }

Description

After this privileged command is executed, the user logging in to the port will be automatically put into the specified menu. This command accepts a *port-list* or ALL as a parameter.

Keywords

NONE

Specifies that there is no default menu on the specified port.

menu_name

Specifies the name of the menu that will be the default menu on the specified ports.

PORT DEFAULT PROTOCOL (privileged)

Syntax

Description

An option that defines the default protocol for the port. The factory-set default is LAT. The default protocol is used to resolve ambiguity to commands with no protocol option specified. If a protocol option is specified, it overrides the default protocol. For example, CONNECT PPP *host-name* is not ambiguous, but CONNECT *host-name* is. This command accepts a *port-list* or ALL as a parameter.

Keywords

ANY

Sets the default protocol to ANY. The access server first searches for network resources on the LAT network, then, if unsuccessful, for resources on the TCP/IP network.

AUTOLINK

Sets the default protocol to AUTOLINK. If AUTOLINK is specified, the access server allows a dial-in port to be configured for either SLIP or PPP protocols, or an interactive terminal session.

LAT

Sets the default protocol to LAT protocol. The access server defaults to the LAT protocol if you do not specify a protocol with the CONNECT command.

PPP

Sets the default protocol to the PPP protocol. The access server defaults to the PPP protocol if you do not specify a protocol with the CONNECT command.

SLIP

Sets the default protocol to the SLIP protocol. The access server defaults to the SLIP protocol if you do not specify a protocol with the CONNECT command.

TELNET

Sets the default protocol to the Telnet protocol. The access server defaults to the Telnet protocol if you do not specify a protocol with the CONNECT command.

DIAL

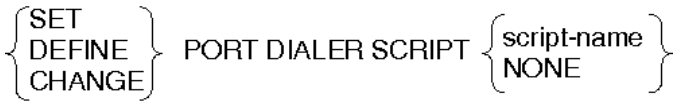
Sets the default protocol to the DIAL protocol. The access server defaults to the DIAL protocol if you do not specify a protocol with the CONNECT command.

Restrictions

- The default protocol is used with the CONNECT and CONNECT PORT commands only. The TELNET and OPEN commands will override the default and assume Internet connections. The DIAL command will override the default and assume a dialer connection.
- The PORT AUTOCONNECT characteristic must be DISABLED when the DEFAULT PROTOCOL is set to ANY.
- The DEFINE and CHANGE commands require a privileged status. The SET command is available to all users.

PORT DIALER SCRIPT (privileged)

Syntax



Description

This privileged command is used to define the type of modem attached to an asynchronous port. The script name specified must exist in the server-wide modem script configuration table, and is used to obtain dial strings for both initializing the attached modem for a dial-out connection as well as resetting the modem after the port has been logged out.

PORT DIALUP (privileged)

Syntax

Description

A privileged option that specifies to the service node that the port is attached to a dial-up line (default: DISABLED). This command accepts a *port-list* or ALL as a parameter.

Note

While the DIALUP option works with most LAT service nodes, there may be some LAT hosts that do not support DIALUP.

PORT DSRLOGOUT (privileged)

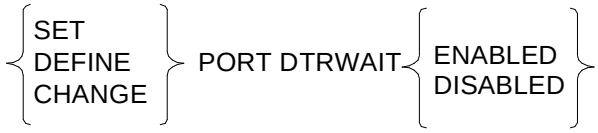
Syntax

Description

A privileged option that specifies whether the access server should log out a port whose attached device is disabled. You can enable DSRLOGOUT only if the port hardware supports DSR signals. DSRLOGOUT does not work if you have DSR flow control enabled. DSRLOGOUT is disabled by default. This command accepts a *port-list* or ALL as a parameter.

PORT DTRWAIT (privileged)

Syntax



Description

A privileged option that specifies whether the access server asserts the Data Terminal Ready (DTR) signal when a modem-controlled port (EIA-232-D) is inactive. DISABLED (the default) causes the access server to assert the DTR signal when it is idle; ENABLED causes it to delay asserting the DTR signal until it detects the RI signal from a modem or until a remote connection is made to the port. This command accepts a *port-list* or ALL as a parameter.

Normally, you should specify ENABLED for remote access ports. You cannot enable DTRWAIT if the device or device cable does not support the DTR signal. Changes to this characteristic become effective on port logout.

Restriction

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

PORT FAILOVER - PORT LOSS NOTIFICATION

PORT FAILOVER (nonprivileged)

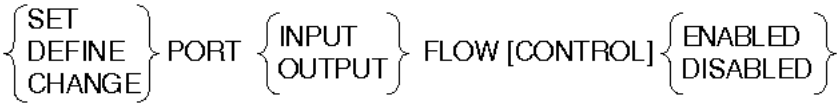
Syntax

Description

A nonprivileged option that specifies whether a port that is disconnected from a LAT service will be automatically connected to another node offering the service. The default is ENABLED. This command accepts a *port-list* or ALL as a parameter.

PORT FLOW CONTROL (nonprivileged)

Syntax



Description

A nonprivileged option that specifies flow control direction. (The default is enabled in both directions.) This command accepts a port-list or ALL as a parameter.

A nonprivileged option that specifies the type of flow control utilized by the access server to control data transfer to and from the port. This command accepts a *port-list* or ALL as a parameter.

Keywords

CTS

Specifies Clear-To-Send/Request-To-Send (CTS/RTS) modem signal flow control (only valid for access servers that support these signals).

DSR

Specifies DTR/DSR signal flow control.

XON

Specifies Transmit On/Transmit Off (XON/XOFF) flow control. XON is the default flow control.

DISABLED

Specifies no flow control.

PORT FORWARD SWITCH (secure)

Syntax

Description

An option (available to all users) that specifies a switch character that allows you to resume the next session in your session list without returning to local mode. You can clear an existing switch by specifying NONE (default). This command accepts a *port-list* or ALL as a parameter.

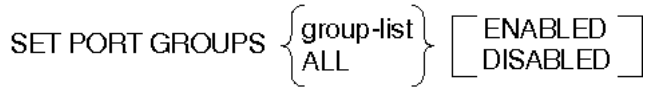
Note that you can specify control characters by using a two character sequence of the up arrow and a character key. For example, if you enter ^a , the switch character is set to Ctrl/a.

Restrictions

- The FORWARD switch does not work on a port that has the MULTISESSIONS characteristic ENABLED.
- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.
- You cannot use a parenthesis, (or), as the switch character.

PORT GROUPS (nonprivileged)

Syntax



Description

A nonprivileged option that specifies which of the groups authorized for the port (refer to the AUTHORIZED GROUPS command) are currently enabled on the port (that is, your current groups). Use GROUPS to select the nodes and services you want to display for the port. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

When you log in to a port, all authorized groups are enabled for the port; therefore, if port characteristics are reset to their defaults, the default for GROUPS matches the default for AUTHORIZED GROUPS (that is, group 0 ENABLED and all other groups DISABLED).

Use the *group-list* format with ENABLED or DISABLED to add or remove groups (within the authorized list). Specify *group-list* without either ENABLED or DISABLED to replace the existing list with a new list. Specify ALL to enable or disable all authorized groups.

Keywords

group-list

One or more decimal codes ranging in value from 0 to 255, each representing a LAT group code. Specify multiple codes by separating individual numbers with commas, by specifying a range of numbers (in ascending order), or a combination of both. For example, the group list 1, 3, 5-8, 14 specifies groups 1, 3, 5, 6, 7, 8, and 14

Restriction

You can specify GROUPS only with the SET PORT command.

PORT INACTIVITY LOGOUT (privileged)

Syntax

{SET / DEFINE / CHANGE} PORT INACTIVITY [LOGOUT] {ENABLED / **DISABLED**}

Description

A privileged option that determines whether the access server automatically logs out a port after a period of inactivity. (The default is DISABLED.) This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

When a port is set to ACCESS LOCAL and the local access user does not use the port, the access server automatically logs out the port after the timeout period. When a port is set to ACCESS REMOTE and there is no activity for a session, the access server automatically disconnects the session and logs out the port after the timeout period. Use the access server characteristic INACTIVITY TIMER to specify the timeout period. For more information, refer to the access server INACTIVITY TIMER command.

PORT INTERRUPTS (privileged)

Syntax

Description

A privileged option that specifies whether a local user can use the Break key to disconnect a remote session at an ACCESS DYNAMIC port in order to log in to the access server. (The default is DISABLED.) This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT LIMITED VIEW (privileged)

Syntax

Description

A privileged option that specifies whether a nonprivileged port is prohibited from showing or listing LAT nodes, LAT services, and various Internet databases (for example, Internet hosts, ARP entries, and gateways. (The default is DISABLED.) This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

An example of the LIMITED VIEW ENABLED command would be the SHOW NODES command. The SHOW NODES command would not be available to ports with the LIMITED VIEW port characteristic enabled.

PORT LOCAL SWITCH (secure)

Syntax

Description

An option (available to all users) that specifies a switch character that you can use to reenter local mode from service mode. The switch character can be a keyboard character; however, you should use a unique, unused character (such as Ctrl/L). You can clear an existing switch by specifying NONE (default). This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT LOCK (privileged)

Syntax

Description

A privileged option that specifies whether a port user can enter the LOCK command. When the LOCK characteristic is ENABLED (the default) on a port and enabled on the access server, the port user can enter the LOCK command to prevent access to the terminal at which the command is entered. The LOCK command prevents any input until a user enters the unlock password at that terminal. DISABLED prevents the use of the LOCK command.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT LONGBREAK LOGOUT (privileged)

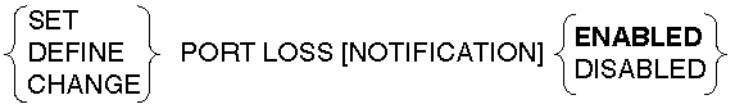
Syntax

Description

A privileged option that, when ENABLED, will log out a port upon receipt of a long break. A long break (a period of 2.5 to 3.5 seconds) is transmitted by some port devices when they are powered down. DISABLED is the default. For more information on this port characteristic, refer to the *Network Access Server Management* manual. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT LOSS NOTIFICATION (nonprivileged)

Syntax



Description

A nonprivileged option that specifies whether you are alerted with a beep when a typed character is lost because of data error or overrun. (The default is ENABLED.) This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

LOSS NOTIFICATION applies only when PORT ACCESS is LOCAL or DYNAMIC.

PORT MESSAGE CODES - PORT PASSWORD

PORT MESSAGE CODES (nonprivileged)

Syntax

Description

A nonprivileged option that specifies whether message codes appear with status and error messages (default: ENABLED). This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT MODEM CONTROL (privileged)

Syntax

Description

A privileged option that specifies whether the access server manipulates modem signals. Specify DISABLED for ports connected to devices or device cables that do not support modem signals. Specify ENABLED for ports connected to devices that support modem signals. (The default is DISABLED.) Changes to this characteristic become effective on the next port login. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- Your access server supports either MODEM CONTROL or SIGNAL CONTROL. For more information on these controls, refer to the *Network Access Server Management* manual.
- Only the DEFINE command can be used with MODEM CONTROL; the SET/CHANGE command is not valid, except for DISABLE.

PORT MULTISESSIONS (secure)

Syntax

Description

An option (available to all users) that specifies whether session management is enabled for the port. (The default is DISABLED.) The port device must be a terminal that supports session management, and the port cannot have a dedicated service. For more information, refer to PORT DEDICATED (privileged). When you disable MULTISESSIONS on an active port, all terminal sessions and their associated service sessions are terminated immediately. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.
- You cannot enable multisessions on a port if a dedicated service exists on the port.

PORT NAME (privileged)

Syntax

Description

A privileged option that defines a port name that is unique on the access server. For more information, refer to the naming conventions in Chapter 1. The access server can send the name you specify with DEFINE/CHANGE PORT NAME to a Telnet server. This is an option when a port user initiates a Telnet connection.

The default is PORT_*n*, where *n* is the port number.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT ON-DEMAND LOADING (nonprivileged)

Syntax

Description

A nonprivileged option that specifies on-demand loading of fonts for those Asian terminals whose fonts are composed of an unusually large number of characters. ON-DEMAND [LOADING] ENABLED affects XON/XOFF flow control processing such that it causes the access server to bypass XOFF (when necessary) to ensure the continuous flow of characters. (The default is DISABLED.) This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

This option is valid only for devices on a LAT network.

PORT PARITY (nonprivileged)

Syntax

Description

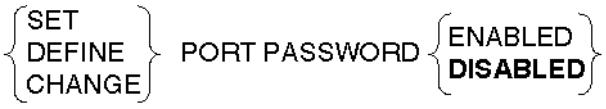
A nonprivileged option that specifies the port parity as EVEN, ODD, MARK, SPACE, or NONE (default). This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

You cannot modify PARITY for a port that is currently in the AUTOBAUD process.

PORT PASSWORD (privileged)

Syntax



Description

A privileged option that specifies whether a password is required for you to log in to the access server (default: DISABLED). You specify the login password by setting the access server characteristic LOGIN PASSWORD. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Note

Changes to this characteristic become effective on the next port login. You should use the DEFINE or CHANGE command to preserve them after logout. For more information on specifying passwords, refer to SERVER PRIVILEGED PASSWORD (privileged).

PORT PPP - PORT PPP IPXCP

PORT PPP (privileged)

Syntax

Description

A privileged command that specifies that a Point-to-Point Protocol (PPP) session may be started on this port. (The default is DISABLED.) If this option is ENABLED, the PPP session startup will prepare for a link startup. Link startup is determined by the LCP ENABLE/DISABLE command and the LCP PASSIVE ENABLE/DISABLE command. PPP and LCP must be ENABLED to bring up a PPP session. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Note

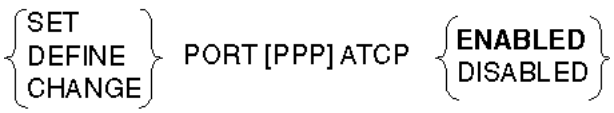
If PPP is DISABLED on a port that is running a PPP session, the session is taken down immediately without notification to the peer. If PPP is enabled on the console port, console messages will not be displayed while a PPP session is active.

Restrictions

- You cannot enable PPP on ports with MULTISESSIONS ENABLED.
- When the port's PPP characteristic is DISABLED, the port prevents a PPP session from starting on the port.
- The attached device on the port must support the PPP protocol to establish a link.

PORT PPP ATCP

Syntax



Description

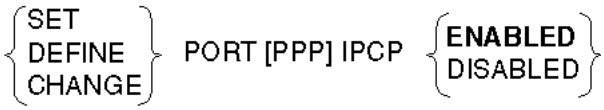
This option controls whether ATCP (AppleTalk Control Protocol) negotiation will be allowed on the link. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP IPCP

Syntax



Description

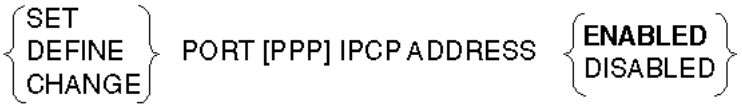
This option controls whether the IPCP (IP Control Protocol) negotiation will be allowed on the link. With this option, a manager can “bounce” the link to pick up new locally configured parameters. This command is often used to debug IPCP setups. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP IPCP ADDRESS

Syntax



Description

Specifies whether the access server should attempt to negotiate the IP address for both ends of this link. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

If enabled, the access server always attempts to negotiate using IPCP option number 3, ADDRESS, first. This is the preferred method. If the attached device does not support option number 3, the access server falls back and attempts to negotiate using option number 1, ADDRESSES.

The access server always proposes the access server IP address as its local address. If the port has an IP address assigned to it, the access server requires that the attached device use that address. If no address has been assigned to the port, the attached device may inform the access server of its IP address via negotiation. If the peer's proposed address is acceptable, (that is, it is part of the access server subnet and not currently held by another port on the access server) the access server allows the peer to use this address. Otherwise, the peer's proposed address is rejected.

If these address negotiations fail, it is possible the link will come up. However, each peer may have inconsistent knowledge about the system with which it is exchanging IP datagrams.

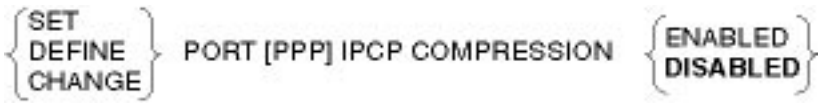
If the link is open, the access server assumes that the peer has the address currently set up on the port. IP datagrams for that IP address will be forwarded. If there is no address associated with the port, the access server does not forward IP datagrams.

Restrictions

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP IPCP COMPRESSION

Syntax



Description

Specifies whether the access server negotiates the use of a compression protocol. The only compression protocol supported is the Van Jacobson Compressed TCP/IP protocol. If it is used, it must be implemented by each peer in both directions. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

When enabled, this option allows the peers to compress the TCP/IP headers. This in turn causes fewer bytes to be sent across the asynchronous line, increasing the line's bandwidth and performance.

Restrictions

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP IPCP COMPRESSION STATES

Syntax

{SET / DEFINE / CHANGE} PORT [PPP] IPCP COMPRESSION STATES number

Description

Specifies the number of TCP connections the access server can decompress from the peer at any given time.The range for the number of TCP connections is between 4 and 16. The default is 16 connections. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP IPCP HOST ADDRESS (nonprivileged)

Syntax

{SET / DEFINE / CHANGE} PORT [PPP] IPCP HOST ADDRESS nn.nn.nn.nn

Description

This option associates a host address with the PPP interface. This option allows the access server to know what IP device is directly attached on the other side of the PPP link. The default for this characteristic is address 0.0.0.0 (no address defined). To remove an existing host address, use the CLEAR/PURGE PORT PPP IPCP HOST ADDRESS command.

Restrictions

- If address negotiations are not used, the IPCP HOST ADDRESS must be configured manually on both sides of the link.
- The DEFINE and CHANGE commands require a nonprivileged status. The SET command has a secure status.
- The command does not support port-list. An address can be associated with only one port.
- The host address specified must reside in the same subnetwork as the access server.

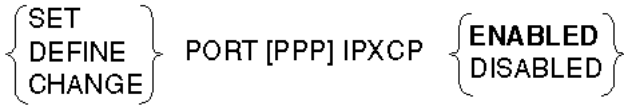
- The host address cannot use the SET or CHANGE command on a port that already has an IP address.
- A port may have only one IP address. Both SLIP and PPP use the same address. This address can be configured either by the SLIP or PPP protocol command.

Note

Address learning (as in SLIP) is not supported by the PPP protocol. PPP uses address negotiation instead.

PORT PPP IPXCP

Syntax



Description

This option controls whether the IPXCP (IPX Control Protocol) negotiation is allowed on the link. With this option, a manager can “bounce” the link to pick up new locally configured parameters. This command is often used to debug IPXCP setups.

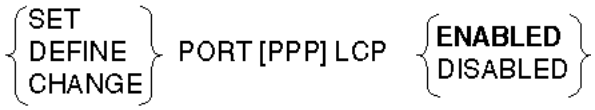
Restrictions

- The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.
- You must be a privileged user to change a port other than your own.

PORT PPP LCP - PORT PPP LCP MRU

PORT PPP LCP

Syntax



Description

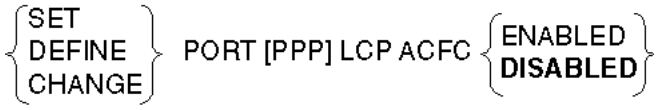
This option controls whether the LCP negotiation is allowed on the link. This can be done by disabling and enabling LCP for a running PPP session. The LCP characteristic will generally be ENABLED, so that LCP starts the link normally. The characteristic value can be changed to force the LCP link to renegotiate using the new locally configured parameters to allow connection to the link without having to first bring the link down.

Restriction

Only a privileged user can enter this command from a port other than the one on which the PPP session is running.

PORT PPP LCP ACFC

Syntax



Description

The keyword ACFC is an abbreviation for “address and control field compression.” This command allows a link to be configured such that this compression is negotiated.

PPP uses unnumbered HDLC frames to encapsulate each packet it sends. HDLC frames include address and control bytes that serve no useful purpose on a PPP link. If the ACFC option is ENABLED, the access server requests that this field be omitted. If DISABLED (default), the address and control field information will be sent.

Restriction

The DEFINE and CHANGE commands require a privileged status. The SET command has a secure status.

PORT PPP LCP AUTHENTICATION (privileged)

Syntax

Description

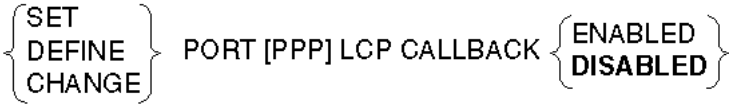
The command specifies whether the access server requires the peer to use the PPP PAP or PPP CHAP protocol to authenticate itself. If NOUSERNAME is specified, the peer must provide the access server with the LOGIN password. If USERNAME is specified, the peer must provide the access server with a user name and password for authentication within the access server's security realms. The user name and password are passed to the authentication host, which the access server's default security realm defines. To use a different realm for authentication, specify a user name using the format "username@realm".

Restrictions

- SET, DEFINE, and CHANGE are all privileged commands.
- The access server does not authenticate itself to the peer.
- The following authentication methods *can* be used with a PPP client using the CHAP protocol: RADIUS and the DECserver's login password.
- The following authentication methods *must* use the PAP protocol with a PPP client using the PPP LCP authentication protocol: Kerberos, SecurID, and the access server's local database of user accounts.

PORT PPP LCP CALLBACK (privileged)

Syntax



Description

This command specifies whether the access server allows the peer to negotiate the use of the PPP callback option. If enabled, the peer is allowed to request the access server to call back the peer. If disabled, the access server will refuse to accept the peer's connection request if the peer requests a callback.

PORT PPP LCP MAP

Syntax

{SET / DEFINE / CHANGE} PORT [PPP] LCP MAP hex-number

Description

This command lets the access server tell the peer which characters require byte-stuffing. Some characters potentially have special meaning to the underlying layers of software or hardware, for example XON/XOFF. Byte-stuffing lets these characters be encapsulated into a two-byte sequence that allows the original character to pass as data. By default, the low 32 ASCII bytes are byte stuffed, which requires additional overhead and consumes bandwidth on a slow serial line. The fewer characters that require byte-stuffing on a given line, the better the performance. This option provides a means to inform the peer of which specific characters require byte-stuffing.

Bits are set in the mask to identify which characters must be stuffed. The bits are ordered right to left, such that the hex character 0x0 (the ASCII character NUL) would need the mask to have the rightmost bit set, that is, 0x00000001. The default of having all characters byte stuffed would use a mask of 0xFFFFFFFF.

Example: PORT PPP LCP MAP

If only XON and XOFF require byte-stuffing, the mask would be set to 0x000A0000. The syntax for the command would be the following:

```
Local> set port lcp map a0000
```

Restriction

The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

PORT PPP LCP MRU

Syntax

{SET / DEFINE / CHANGE} PORT [PPP] LCP MRU number

Description

This option specifies the size in bytes of the maximum receive units (MRU) that the access server wishes to negotiate for the link. This informs the peer what the server wishes to see as an upper limit to packet size. Setting the MRU size allows you to tune

the link performance. The default value for this option is 1500 bytes. The range for this option is 64 to 1500 bytes. The server always accepts packets up to the 1500 byte default, regardless of the negotiated setting.

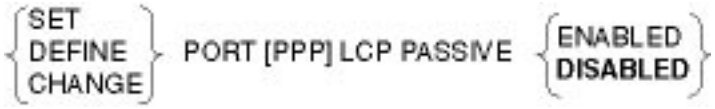
Restriction

The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

PORT PPP LCP PASSIVE - PORT PPP LCP/IPCP/ATCP/ IPXCP RESTART

PORT PPP LCP PASSIVE

Syntax



Description

This option controls whether the LCP will attempt to actively open the LCP link on connection, or whether the LCP will passively await packets from the peer to start the link. If LCP PASSIVE is ENABLED, LCP will wait for the peer to begin negotiations. If LCP PASSIVE is DISABLED, the LCP will actively try to start negotiations as soon as the PPP session is started, depending on the setting of LCP ENABLED/ DISABLED.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Note

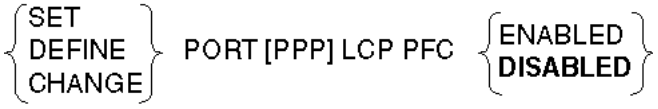
If both the access server and the attached device use PASSIVE, the link will not be negotiated.

Restriction

The DEFINE and CHANGE commands require a privileged status. Only the SET command requires a secure status.

PORT PPP LCP PFC

Syntax



Description

The keyword PFC is an abbreviation for *protocol field compression*. PPP uses a two-character protocol field to identify the type of packet being sent. This field may be compressed into a single byte and still uniquely identify the protocol type. This option lets you conserve bandwidth for slow serial lines.

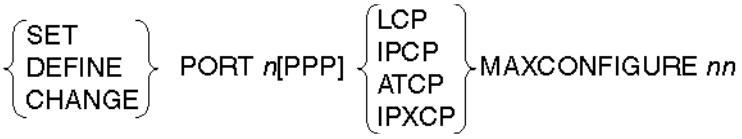
This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

The DEFINE and CHANGE commands require privileged status. The SET command requires secure status.

PORT PPP LCP/IPCP/ATCP/IPXCP MAXCONFIGURE

Syntax



Description

This option determines how many times the LCP, IPCP, ATCP, or IPXCP will send a configure request packet to the peer without receiving a configure acknowledgment signal. Failure of the peer to send an acknowledgment signal after the assigned number of request packets will cause LCP/IPCP/ATCP/IPXCP to assume that the peer cannot respond. The default for this option is 10.

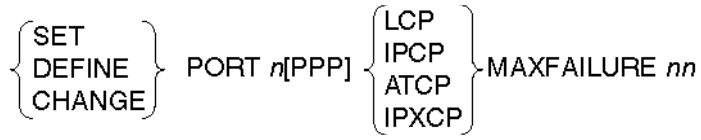
This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP/ATCP/IPXCP MAXFAILURE

Syntax



Description

This option determines how many times LCP, IPCP, ATCP, or IPXCP will send a negative acknowledgment message (NAK) for the peer's proposed options before deciding to start rejecting the problem options (the options whose values the LCP/IPCP/ATCP/IPXCP finds objectionable).

Once LCP/IPCP/ATCP/IPXCP rejects the problem options, the link establishment will either fail or the options must take on the default value. The default value for this characteristic is 10.

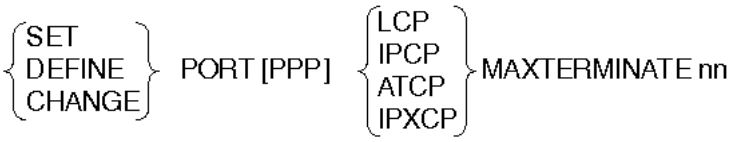
This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP/ATCP/IPXCP MAXTERMINATE

Syntax



Description

This option determines how many times the LCP, IPCP, ATCP, or IPXCP will send a terminate request packet to the peer without receiving a terminate acknowledgment signal. Failure of the peer to send an acknowledgment signal after the assigned number of request packets will result in a take down of the link. The default for this option is 2.

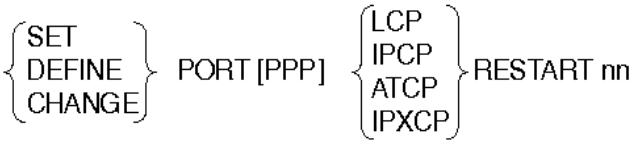
This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PPP LCP/IPCP/ATCP/IPXCP RESTART

Syntax



Description

This option determines how many seconds there will be between a LCP, IPCP, ATCP, or IPXCP configure terminate retransmit while LCP/IPCP/ATCP/IPXCP configuration or link termination is taking place. For example, the LCP will send one configure request packet to the peer, and will wait a period of time for a response. If no response is received within the time limit, another configure request will be sent. Setting the LCP/IPCP/ATCP/IPXCP RESTART option determines the length of this waiting period. The default for this option is 3 seconds. This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

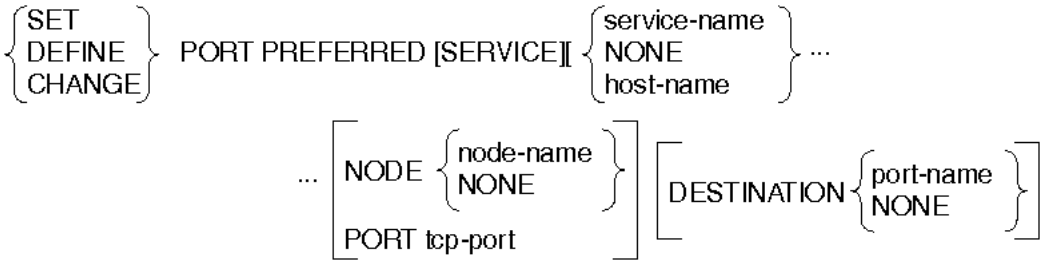
Restriction

The DEFINE and CHANGE commands require a privileged status. The SET command has a nonprivileged status.

PORT PREFERRED - PORT RING

PORT PREFERRED (nonprivileged)

Syntax



Description

A nonprivileged option that specifies a preferred network service when you enter a CONNECT command for the port but do not specify a service name. The default is no preferred service.

If you specify a value for NODE or for DESTINATION, the access server does not attempt automatic failover for LAT sessions. Entering NONE as the value for the preferred service-name, NODE, or DESTINATION cancels any previous value entered for that field.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Keywords

service-name

Specifies the LAT service name to which you want to connect.

host-name

Specifies the Internet host name, or Internet host address to which you want to connect.

NODE *node-name*

Specifies a particular LAT service node to which you want to connect.

tcp-port

Specifies the optional Telnet/TCP port number.

DESTINATION

Specifies a particular port to which you want to connect.

port-name

You must use the DEFINE PORT command to set the port's default protocol to match the protocol (LAT or Telnet) of the preferred service. (The default setting connects you to the first available port that offers the service.)

If your access server supports session management, refer to the *Network Access Server Management* manual for details about using session management when a preferred service is defined.

Restriction

NODE and DESTINATION are valid only if you specify a LAT service as the preferred service.

PORT QUEUING (nonprivileged)

Syntax

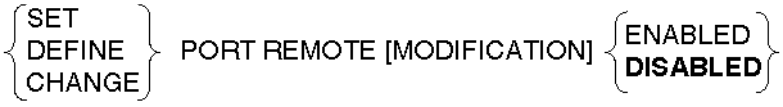
Description

A nonprivileged option that specifies whether queuing of LAT service connection requests is enabled for the port. (The default is DISABLED.) If you disable QUEUING when requests are already queued, those requests remain in the queue until the LAT service becomes available.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT REMOTE MODIFICATION (nonprivileged)

Syntax



Description

A nonprivileged option that specifies whether a suitable LAT service node can remotely modify port characteristics, such as SPEED, CHARACTER SIZE, PARITY, and LOSS NOTIFICATION, to match the port characteristics of a remote device on the access server. (The default is DISABLED.)

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

Enabling this characteristic on a secure port allows the port user to modify the physical port characteristics. To prevent this, do not enable REMOTE MODIFICATION and SECURITY on the same port.

PORT RING (privileged)

Syntax

Description

A privileged option used with certain terminal switches and computers that need to detect a Ring Indicator (RI) signal. The RING characteristic is supported only on those access servers that support the DSRS signal. To use this feature, you need a BC22R or equivalent cable. The default is DISABLED.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

Not all access servers support the DSRS signal.

PORT SECURITY - PORT SIGNAL SELECT

PORT SECURITY (privileged)

Syntax

Description

A privileged option that specifies whether secure status on the port is ENABLED or DISABLED. With security ENABLED, the commands available on the port are restricted to a subset of nonprivileged commands. The default is DISABLED. With security DISABLED, all nonprivileged commands are available to the port.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT SESSION LIMIT (privileged)

Syntax

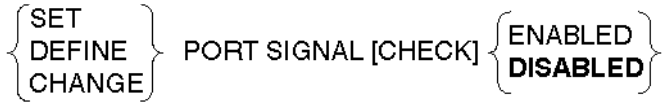
Description

A privileged option that limits the number of permitted sessions (range: 0 to 8; default: 4). Specifying NONE permits the maximum number of sessions allowed on the access server.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT SIGNAL CHECK (privileged)

Syntax



Description

A privileged option that specifies whether the access server checks for incoming signals on a remote access port before allowing a connection. (The default is DISABLED.) The access server rejects an attempted connection if a signal is not present. For more information on this command, refer to the *Network Access Server Management* manual.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

Do not use SIGNAL CHECK for a port using CTS flow control, DSR flow control, SIGNAL CONTROL, or MODEM CONTROL.

PORT SIGNAL CONTROL (privileged)

Syntax

DEFINE PORT SIGNAL CONTROL { ENABLED / DISABLED }

Description

A privileged option that specifies whether the access server manipulates modem signals. Specify DISABLED for ports connected to devices or device cables that do not support modem signals. Changes to this characteristic become effective on the next port login. For more details on using SIGNAL CONTROL, refer to the *Network Access Server Management* manual.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- Your access server supports either MODEM CONTROL or SIGNAL CONTROL. For more information on this command, refer to the *Network Access Server Management* manual.
- Only the DEFINE command can be used with SIGNAL CONTROL. The SET/CHANGE command is not valid.

PORT SIGNAL SELECT (privileged)

Syntax

DEFINE PORT SIGNAL SELECT { CTS-RTS-DSR-DTR / RI-DCD-DSRS-DTR }

Description

A privileged option that specifies which set of modem signals the port uses. The default is CTS-RTS-DSR-DTR (Clear to Send - Request to Send - Data Set Ready - Data Terminal Ready).

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- This command is not available on all access servers; for more information, refer to the *Network Access Server Management* manual.
- Only the DEFINE command can be used with SIGNAL SELECT. The SET and CHANGE commands are not valid.

PORT SLIP - PORT STOP BITS

PORT SLIP (privileged)

Syntax

Description

A nonprivileged option that specifies whether SLIP is enabled for the port. (The default is DISABLED.) To enable SLIP, the attached device on the port must support the SLIP protocol. When you disable SLIP, the SLIP session for the port is disconnected.

Restriction

You cannot enable SLIP on ports with the MULTISESSIONS command or characteristics enabled.

Note

You will receive a warning message if SLIP is enabled on the console port. In session mode, the port will not receive any console messages.

PORT SLIP COMPRESSION (nonprivileged)

Syntax

Description

This command determines whether or not the TCP/IP header compression is used on SLIP/CSLIP. The default for this option is COMPRESSION DISABLED. The three states and requirements for COMPRESSION are:

- ENABLED, compression must be used on the link.
- DISABLED, compression cannot be used on the link.
- AUTOCOMPRESS, SLIP/CSLIP will start out with compression disabled, but if the SLIP receives a compressed packet, compression will started automatically.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

The SET PORT SLIP COMPRESSION command is a secure option.

PORT SLIP COMPRESSION STATES (privileged)

Syntax

Description

This command determines how many compression states will be used on the SLIP datalink. The same number of states are used in each direction. This command accepts a *port-list* or ALL as a parameter for the PORT keyword. The range for the number of compression states is from 4 to 16. The default value is 16.

Restriction

The SET PORT SLIP COMPRESSION command is a secure option.

PORT SLIP HOST ADDRESS (nonprivileged)

Syntax

{SET / DEFINE / CHANGE} PORT SLIP HOST [ADDRESS] *host-id*

Description

A nonprivileged option that assigns the Internet address of the attached device, which is needed to act as a host in the Internet environment. This allows the access server to determine which Internet Protocol (IP) packets it should transmit or receive over the asynchronous line between the IP host and the Internet network.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- A port list is not allowed; the host addresses must be unique.
- The host address must be in the same subnet as the access server Internet address.
- You cannot use the SET or CHANGE command if the port already has a SLIP HOST address. To alter an existing address, you must use the DEFINE command with the new address and log out of the port or clear the port SLIP HOST.
- A port may have only one IP address. Both SLIP and PPP use the same address. This address can be configured either by the SLIP or PPP protocol command (see PORT PPP IPCP HOST ADDRESS (nonprivileged)).

PORT SLIP MTU (nonprivileged)

Syntax

{SET / DEFINE / CHANGE} PORT SLIP MTU *mtu-size*

Description

A nonprivileged option that specifies the Maximum Transmission Unit (MTU) for SLIP packets on the port. The MTU is the largest datagram size (in bytes) that will be accepted on the port (range: 64 to 1500; default: 1006).

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restriction

You cannot change the MTU with an existing SLIP session on the port.

PORT SPEED (INPUT/OUTPUT) (nonprivileged)

Syntax

Description

A nonprivileged option that specifies the port speed in bits per second (bps). Permissible values include: 75, 110, 134, 150, 300, 600, 1200, 1800, 2000, 2400, 4800, 9600 (the default), 19200, 38400, 57600, and 115200.

This option accepts a *port-list* or ALL as a parameter for the PORT keyword.

Note

Some access servers do not accept all speeds. For a list of speeds supported on specific access servers, refer to the chapter entitled Configuring Devices on a Port in the *Network Access Server Management* manual.

You can change the speed in one direction by specifying INPUT SPEED (speed from the device to the access server) or OUTPUT SPEED (speed from the access server to the device).

Restriction

You cannot modify SPEED for a port that is currently in the AUTOBAUD process.

PORT STOP BITS (nonprivileged)

Syntax

Description

A nonprivileged option that tells the access server to use 1 or 2 stop bits when outputting a character. If the port speed is 134 bits per second or less, set STOP BITS to 2. If the port speed is greater than 134 bits per second, set STOP BITS to 1. The default is DYNAMIC. DYNAMIC automatically determines the number of stop bits based on the port's output speed.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET CLIENT - PORT TELNET SERVER NOP INDICATION

PORT TELNET CLIENT (secure)

Syntax

Description

An option (available to all users) that modifies the current Telnet client characteristics for the specified ports in the access server database.

With this option, you can specify the characteristics to be associated with new Telnet connections established from the specified ports. You can specify the following characteristics to the PORT TELNET CLIENT command:

AO [REQUEST]	MESSAGE
AUTOFLUSH	NEWLINE
AUTOSYNCH	PROFILE
AYT [REQUEST]	QUOTE
BINARY	SIGNAL [REQUEST]
BREAK (BRK) [REQUEST]	SWITCH [CHARACTER]
{CHARACTER} [SIZE]	SYNCH [REQUEST]
ECHO	TERMINAL
EOR [REQUEST]	TOGGLE ECHO
INPUT/OUTPUT FLOW CONTROL	VERIFICATION
IP [REQUEST]	

For a detailed description of each of the PORT TELNET CLIENT characteristics, refer to the SET SESSION TELNET command.

Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT TELNET SERVER (privileged)

Syntax

{SET / DEFINE / CHANGE} PORT TELNET SERVER [*characteristics*]

Description

A privileged option that allows you to specify the characteristics to be associated with Telnet connections established to the specified ports. The Telnet access server characteristics are the current user-definable port parameters associated with a Telnet access server connection.

Each of the following characteristics for use with the PORT TELNET SERVER command is described in this section, with syntax and applicable restrictions:

AO [INDICATION]	EOR [INDICATION]
AYT [INDICATION]	IP [INDICATION]
BREAK (BRK) [INDICATION]	NEWLINE FROM HOST
{CHARACTER} [SIZE]	NEWLINE FROM TERMINAL
EC [INDICATION]	NEWLINE TO HOST
ECHO [NEGOTIATION]	NEWLINE TO TERMINAL
EL [INDICATION]	NOP [INDICATION]

PORT TELNET SERVER AO INDICATION (privileged)

Syntax

{SET / DEFINE / CHANGE} PORT TELNET SERVER AO [INDICATION] {*character* / **NONE**}

Description

AO (Abort Output) defines a character that will be sent to the Telnet access server connection's associated access server port when the remote user generates an Abort Output request. There is no character defined by default. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER AYT INDICATION (privileged)

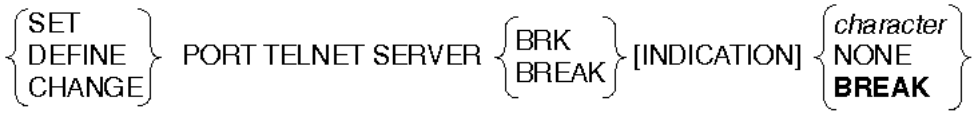
Syntax

Description

AYT (Are-You-There) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an AYT request. There is no character defined by default. This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER BREAK (BRK) INDICATION (privileged)

Syntax



Description

BRK (Break) is a privileged option that defines a character or BREAK signal that will be sent to the Telnet server connection's associated access server port when the remote user generates a Telnet break request. The default is to send a break signal to the access server port. To define the break signal, you must type the individual letters.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER CHARACTER SIZE (privileged)

Syntax

Description

TRANSMIT/RECEIVE CHARACTER SIZE specifies whether the characters sent and received on this connection should be 7-bit or 8-bit. TRANSMIT characters are sent by the access server to the host. RECEIVE characters are received by the access server from the host. The default is 8-bit in both directions.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER EC INDICATION (privileged)

Syntax

Description

EC (Erase previous Character) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an EC request. There is no character defined by default.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER ECHO NEGOTIATION (privileged)

Syntax

Description

ECHO NEGOTIATION is a privileged option that specifies whether the Telnet server should INITIATE ECHO NEGOTIATIONs when the connection is established.

INITIATE means that the access server will offer to perform ECHO by sending the WILL-ECHO Telnet option on behalf of the attach device. The default is INITIATE. Because the Telnet server does not perform echoing, the INITIATE option should be used whenever the attached device is expected to perform echoing.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER EL INDICATION (privileged)

Syntax

Description

EL (Erase previous Line) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an EL request. There is no character defined by default.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER EOR INDICATION (privileged)

Syntax

Description

EOR (End-Of-Record) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an EOR request. There is no character defined by default.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER HOTKEY (privileged)

Syntax

Description

This privileged command enables Telnet listeners (via Telnet hot-key) to start either a dedicated PPP or SLIP connection when you send the specified hot-key character for transmission out the asynchronous port. You can specify the hot-key character like switch characters using the format ^*char* (up arrow followed by a legal hot-key character).

Note that when SLIP or PPP is in use on a port, switch characters are not honored since they are just data to the framed protocol. Therefore, it is legal to define the same character as both a session switch character and a Telnet hot-key character.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER IP INDICATION (privileged)

Syntax

Description

IP (Interrupt Process) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an IP request. There is no character defined by default.

PORT TELNET SERVER NEWLINE FROM HOST (privileged)

Syntax

Description

This characteristic defines a 1- or 2-character sequence that, when received from the local Telnet access server port, is interpreted as newline. The default is <CRLF>.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER NEWLINE FROM TERMINAL (privileged)

Syntax

Description

This characteristic defines a 1- or 2-character sequence that, when received from the remote user, is interpreted as a newline. The default is <CR>.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER NEWLINE TO HOST (privileged)

Syntax

Description

This characteristic defines a 1- or 2-character sequence that will be sent to the local Telnet server access server port whenever a NEWLINE FROM TERMINAL sequence is received from the remote user. The default is <CRLF>.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER NEWLINE TO TERMINAL (privileged)

Syntax

Description

This characteristic defines a 1- or 2-character sequence that will be sent to the remote user whenever a NEWLINE FROM HOST sequence is received from the local Telnet server access server port. The default is <CRLF>.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TELNET SERVER NOP INDICATION (privileged)

Syntax

Description

NOP (No-Operation) defines a character that will be sent to the Telnet server connection's associated access server port when the remote user generates an NOP request. There is no character defined by default.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT TN3270 - PORT TN3270 MODEL

PORT TN3270 (secure)

Syntax

Description

A secure option that modifies the current TN3270 Client characteristics for the specified ports in the access server database. With this option, you can specify the characteristics to be associated with the TN3270 connections established from the specified ports. You can specify the following characteristics to the SET/DEFINE/CHANGE PORT TN3270 command:

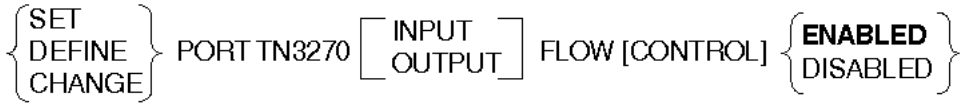
FLOW CONTROL	NULLS
KEYMAP	SWITCH CHARACTER
KEYMAP NVRAM LIMIT	TERMINAL
MODEL	VERIFICATION

Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT TN3270 FLOW CONTROL (secure)

Syntax

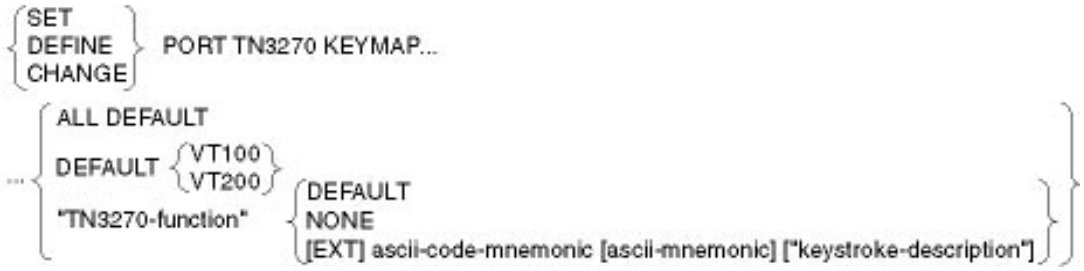


Description

This option changes the flow control. Flow control can be set for both directions: from the access server to the port device (OUTPUT), and from the port device to the access server (INPUT). The default is ENABLED in both directions.

PORT TN3270 KEYMAP (nonprivileged)

Syntax



Description

Customized key mappings are allowed. You can enter a command to declare or remove a keymapping to be in effect for any subsequent sessions on a port.

Keywords

TN3270-function

Refer to Default VT100 and VT220 Keymaps for the IBM TN3270-functions.

ALL DEFAULT

Changes all previously customized key mappings back to the key mappings for the server-based keymap used at the port (see the SHOW TN3270 KEYMAP command). Note that this option differs from the DEFAULT option discussed later in this section.

EXT

The set of ASCII-code-mnemonics is extended with the use of the definable TN3270 EXT key. The EXT key is any one of the ASCII code mnemonics listed in ASCII Code Mnemonics Table. When EXT is redefined, then all TN3270-functions previously specified with EXT will reflect the new EXT definition.

NONE

Assigning a TN3270-function to the keyword NONE means that no key or keys on the keyboard for that port will map to the TN3270-function. This could be useful for a manager who wants to disallow a certain TN3270-function for the users.

DEFAULT

Sets the keymap back to the default definition (VT100/VT220) of the defined TN3270 KEYMAP characteristic. Any customized port KEYMAP definition will be lost.

ascii-code-mnemonic

This is any of the ASCII key code mnemonics in the following table that represent ASCII character sequences. ASCII key code mnemonics should describe the ASCII keyboard keys for terminals VT100 through VT400.

Restrictions

- Only one TN3270-function can be mapped to one Digital key sequence.
- TN3270-functions must have unique Digital key sequences
- A key sequence cannot be specified for a TN3270-function if it is a subset of an existing key sequence.

Note

If a TN3270-function is mapped to a certain Digital key sequence and another command is entered, mapping it to another Digital key sequence, the second Digital key sequence will replace the first.

A warning message will be displayed if a TN3270-function is mapped to a key already in use. The previously mapped TN3270-function will be set to NONE and the new TN3270-function will be assigned.

Example: SET/DEFINE/CHANGE PORT TN3270 KEYMAP

```
Local> DEFINE PORT TN3270 KEYMAP ENTER CTRL/A
(SHOW PORT TN3270 KEYMAP shows ENTER mapped to CTRL/A)
Local> DEFINE PORT TN3270 KEYMAP RESET CTRL/A
Local - 812 DEC sequence already in use. Previous mapping
undone.
(SHOW PORT TN3270 KEYMAP shows ENTER mapped to NONE, RESET
mapped to CTRL/A)
```

ASCII Code Mnemonics Table

The following table shows the ASCII code mnemonics for defining the TN3270-function. Each mnemonic represents an ASCII character sequence.

Mnemonic	Hexadecimal Sequence	ASCII Character Sequence	Comments
CTRL/A	1	SOH	7-bit control characters
CTRL/B	2	STX	7-bit control characters
CTRL/C	3	ETX	7-bit control characters
CTRL/D	4	EOT	7-bit control characters
CTRL/E	5	ENQ	7-bit control characters
CTRL/F	6	ACK	7-bit control characters
CTRL/G	7	BEL	7-bit control characters
CTRL/H or BACKSPACE	8	BS	7-bit control characters
CTRL/I or TAB	9	HT	7-bit control characters
CTRL/J or LINEFEED	A	LF	7-bit control characters
CTRL/K	B	VT	7-bit control characters
CTRL/L	C	FF	7-bit control characters
CTRL/M or RETURN	D	CR	7-bit control characters
CTRL/N	E	SO	7-bit control characters
CTRL/O	F	SI	7-bit control characters
CTRL/P	10	DLE	7-bit control characters
CTRL/Q	11	DCI	7-bit control characters
CTRL/R	12	DC2	7-bit control characters
CTRL/S	13	DC3	7-bit control characters
CTRL/T	14	DC4	7-bit control characters
CTRL/U	15	NAK	7-bit control characters
CTRL/V	16	SYN	7-bit control characters
CTRL/W	17	ETB	7-bit control characters
CTRL/X	18	CAN	7-bit control characters
CTRL/Y	19	EM	7-bit control characters
CTRL/Z	1A	SUB	7-bit control characters
CTRL/3 or ESC	1B	ESC	7-bit control characters
CTRL/4	1C	FS	7-bit control characters
CTRL/5	1D	GS	7-bit control characters

Mnemonic	Hexadecimal Sequence	ASCII Character Sequence	Comments
CTRL/6	1E	RS	7-bit control characters
CTRL/7	1F	US	7-bit control characters
Delete	7F	DEL	7-bit control characters
PF1	1B 4F 50	ESC O P	Numeric-Keypad Keys-Application Mode
PF2	1B 4F 51	ESC O Q	Numeric-Keypad Keys-Application Mode
PF3	1B 4F 52	ESC O R	Numeric-Keypad Keys-Application Mode
PF4	1B 4F 53	ESC O S	Numeric-Keypad Keys-Application Mode
ENTER	1B 4F 4D	ESC O M	Numeric-Keypad Keys-Application Mode
KPCOMMA	1B 4F 6C	ESC O I	Numeric-Keypad Keys-Application Mode
KPMINUS	1B 4F 6D	ESC O m	Numeric-Keypad Keys-Application Mode
KPDOT	1B 4F 6E	ESC O n	Numeric-Keypad Keys-Application Mode
KP0	1B 4F 70	ESC O p	Numeric-Keypad Keys-Application Mode
KP1	1B 4F 71	ESC O q	Numeric-Keypad Keys-Application Mode
KP2	1B 4F 72	ESC O r	Numeric-Keypad Keys-Application Mode
KP3	1B 4F 73	ESC O s	Numeric-Keypad Keys-Application Mode

Mnemonic	Hexadecimal Sequence	ASCII Character Sequence	Comments
KP4	1B 4F 74	ESC O t	Numeric-Keypad Keys-Application Mode
KP5	1B 4F 75	ESC O u	Numeric-Keypad Keys-Application Mode
KP6	1B 4F 76	ESC O v	Numeric-Keypad Keys-Application Mode
KP7	1B 4F 77	ESC O w	Numeric-Keypad Keys-Application Mode
KP8	1B 4F 78	ESC O x	Numeric-Keypad Keys-Application Mode
KP9	1B 4F 79	ESC O y	Numeric-Keypad Keys-Application Mode
UPARROW	1B 5B 41 or 1B 4F 41	ESC [A or ESC O A	Cursor or Application Mode
DOWNARROW	1B 5B 42 or 1B 4F 42	ESC [B or ESC O B	Cursor or Application Mode
RIGHTARROW	1B 5B 43, 1B 4F 43	ESC [C or ESC O C	Cursor or Application Mode
LEFTARROW	1B 5B 44, 1B 4F 44	ESC [D or ESC O D	Cursor or Application Mode
FIND	1B 5B 31 7E	ESC [1 ~	Editing Keys
INSERT	1B 5B 32 7E	ESC [2 ~	Editing Keys
REMOVE	1B 5B 33 7E	ESC [3 ~	Editing Keys
SELECT	1B 5B 34 7E	ESC [4 ~	Editing Keys
PREV	1B 5B 35 7E	ESC [5 ~	Editing Keys
NEXT	1B 5B 36 7E	ESC [6 ~	Editing Keys
F1	1B 5B 31 31 7E	ESC [1 1 ~	Function Keys
F2	1B 5B 31 32 7E	ESC [1 2 ~	Function Keys
F3	1B 5B 31 33 7E	ESC [1 3 ~	Function Keys
F4	1B 5B 31 34 7E	ESC [1 4 ~	Function Keys
F5	1B 5B 31 35 7E	ESC [1 5 ~	Function Keys

Mnemonic	Hexadecimal Sequence	ASCII Character Sequence	Comments
F6	1B 5B 31 37 7E	ESC [1 7 ~	Function Keys
F7	1B 5B 31 38 7E	ESC [1 8 ~	Function Keys
F8	1B 5B 31 39 7E	ESC [1 9 ~	Function Keys
F9	1B 5B 32 30 7E	ESC [2 0 ~	Function Keys
F10	1B 5B 32 31 7E	ESC [2 1 ~	Function Keys
F11	1B 5B 32 33 7E	ESC [2 3 ~	Function Keys
F12	1B 5B 32 34 7E	ESC [2 4 ~	Function Keys
F13	1B 5B 32 35 7E	ESC [2 5 ~	Function Keys
F14	1B 5B 32 36 7E	ESC [2 6 ~	Function Keys
F15 or HELP	1B 5B 32 38 7E	ESC [2 8 ~	Function Keys
F16 or DO	1B 5B 32 39 7E	ESC [2 9 ~	Function Keys
F17	1B 5B 33 31 7E	ESC [3 1 ~	Function Keys
F18	1B 5B 33 32 7E	ESC [3 2 ~	Function Keys
F19	1B 5B 33 33 7E	ESC [3 3 ~	Function Keys
F20	1B 5B 33 34 7E	ESC [3 4 ~	Function Keys

7-bit ASCII Graphic Code Table

Mne-monic	Hex	Mnemonic	Hex	Mnemonic	Hex	Mnemonic	Hex	Mnemonic	Hex
!	21	4	34	G	47	Z	5A	m	6D
QUOTE	22	5	35	H	48	[	5B	n	6E
-	23	6	36	I	49	\	5C	o	6F
$	24	7	37	J	4A	]	5D	p	70
%	25	8	38	K	4B	CARET	5E	q	71
&	26	9	39	L	4C	_	5F	r	72
SQUOTE	27	:	3A	M	4D	'	60	s	73
(	28	;	3B	N	4E	a	61	t	74
)	29	<	3C	O	4F	b	62	u	75
*	2A	=	3D	P	50	c	63	v 76	
+	2B	>	3E	Q	51	d	64	w	77
COMMA	2C	QUESTION	3F	R	52	e	65	x	78
MINUS	2D	@	40	S	53	f	66	y	79
.	2E	A	41	T	54	g	67	z	7A
/	2F	B	42	U	55	h	68	{	7B
0	30	C	43	V	56	I	69	|	7C
1	31	D	44	W	57	j	6A	}	7D
2	32	E	45	X	58	k	6B	~	7E
3	33	F	46	Y	59	l	6C	DEL	7F

The table in the Default VT100 and VT220 Keymaps section lists the keymappings for default VT100 and VT220 keymaps.

Default VT100 and VT220 Keymaps

The following table list the default VT100 and VT220 keymaps:

TN3270 Function	Keys (VT100)	Keys (VT2nn, VT3nn, VT4nn)
BACKTAB	BACKSPACE	F12
CENT	EXT C	EXT C
CLEAR	EXT ENTER	EXT F20
CURSUP	UPARROW	UPARROW
CURSDOWN	DOWNARROW	DOWNARROW
CURSLEFT	LEFTARROW	LEFTARROW

TN3270 Function	Keys (VT100)	Keys (VT2nn, VT3nn, VT4nn)
CURSRIGHT	RIGHTARROW	RIGHTARROW
DELETE	DELETE	DELETE
DUP	EXT *	EXT F12
ENTER	ENTER	ENTER
ERASEEOF	EXT KPCOMMA	F18
ERASEINP	EXT KPMINUS	EXT F18
EXIT	CTRL/Z	CTRL/Z
EXT	KPDOT	KPDOT
FIELDMARK	EXT;	EXT F13
HELP	EXT H	F15 (HELP)
HOME	EXT B	F13
INSERT	EXT PF4	F14
NEWLINE	RETURN	RETURN
NOT	EXT N	EXT N
NUMOVR	EXT J	REMOVE
OR	EXT O	EXT O
PA1	PF4	PF4
PA2	KPMINUS	KPMINUS
PA3	KPCOMMA	KPCOMMA
PF1	PF1	PF1
PF2	PF2	PF2
PF3	PF3	PF3
PF4	KP7	KP7
PF5	KP8	KP8
PF6	KP9	KP9

TN3270 Function	Keys (VT100)	Keys (VT2nn, VT3nn, VT4nn)
PF7	KP4	KP4
PF8	KP5	KP5
PF9	KP6	KP6
PF10	KP1	KP1
PF11	KP2	KP2
PF12	KP3	KP3
PF13	EXT PF1	EXT PF1
PF14	EXT PF2	EXT PF2
PF15	EXT PF3	EXT PF3
PF16	EXT KP7	EXT KP7
PF17	EXT KP8	EXT KP8
PF18	EXT KP9	EXT KP9
PF19	EXT KP4	EXT KP4
PF20	EXT KP5	EXT KP5
PF21	EXT KP6	EXT KP6
PF22	EXT KP1	EXT KP1
PF23	EXT KP2	EXT KP2
PF24	EXT KP3	EXT KP3
REFRESH	CTRL/W	F20
RESET	KP0	KP0
STATUS	EXT S	F17
TAB	TAB	TAB

PORT TN3270 KEYMAP [NVRAM] LIMIT (privileged)

Syntax

{SET / DEFINE / CHANGE} PORT [*port-list*] TN3270 KEYMAP NVRAM LIMIT [*n*]

Description

A privileged option that specifies the number of user-defined keymaps that are allowed per port for specified port(s). The range is 0 to 255 and the default is 0. A limit setting of zero means that no NVRAM definition is allowed.

PORT TN3270 MODEL (nonprivileged)

Syntax

{SET / DEFINE / CHANGE} PORT TN3270 MODEL {2 / NONE}

Description

With this nonprivileged option, you must specify if IBM model 2 information is to be emulated on the ASCII terminal. Entering model 2 enables the server to negotiate IBM TN3270 with the IBM host at connection time using Telnet negotiation. Entering model 2 will also set the screen size up for 24 lines and 80 columns. Model 3, 4, and 5 display stations have screens with more than 24 lines.

If model 2 is entered, both the EXIT and HELP keys will operate as follows:

- The EXIT key aborts and disconnects the TN3270 session.
- The “hot-key” HELP displays a short form of the SHOW PORT SESSION TN3270 KEYMAP display.

Restriction

IBM applications requiring display stations that have screens other than 24x80 are not supported.

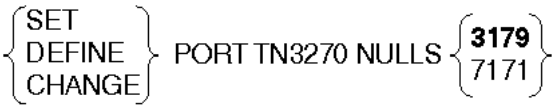
Note

A value of NONE signifies that this port will not be used for TN3270 sessions. NONE is the default.

PORT TN3270 NULLS - PORT TYPE

PORT TN3270 NULLS (nonprivileged)

Syntax



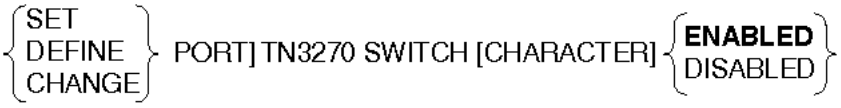
Description

A nonprivileged option that determines how the TN3270 treats null characters for transmission to the host. TN3270 assigns null characters in one of two ways:

- **3179 mode** — Suppresses transmission of nulls. (This is the default.)
- **7171 mode** — Transmits all non-trailing nulls as spaces. INSERT mode operates with both trailing nulls or spaces.

PORT TN3270 SWITCH CHARACTER (secure)

Syntax

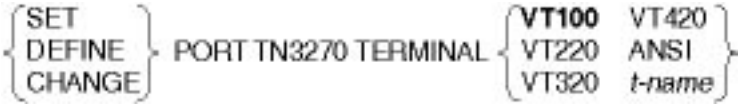


Description

This secure option specifies how the access server handles switch characters for a TN3270 session on the port. If ENABLED, the access server recognizes and responds to FORWARD, BACKWARD, or local SWITCH session characters. If DISABLED, the access server ignores all switch characters on the port. The default is ENABLED.

PORT TN3270 TERMINAL (nonprivileged)

Syntax



Description

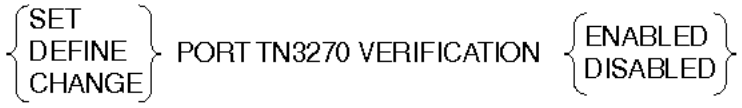
A nonprivileged option that tells the access server which terminal type is connected to each port.

The parameter *t-name* can be a customized name defined in the server's TN3270 TERMINAL LIST. See SHOW TN3270 TERMINAL.

Setting a PORT to a VT100 or ANSI terminal will set the TN3270 KEYMAP to a VT100 KEYMAP. Setting a port to either a VT220, VT320, or VT420 terminal will set the TN3270 KEYMAP to a VT220 KEYMAP. If executing this command selects the same keymap (VT100 or VT200) as the currently selected one, the customized key mappings (if any) are retained. Otherwise, all customized KEYMAPs will be lost. The default is VT100.

PORT TN3270 VERIFICATION (secure)

Syntax



Description

An option that specifies whether the access server sends informational messages to you when you connect, disconnect, or switch sessions (default: ENABLED).

PORT TYPE (secure)

Syntax

Description

An option (available to all users) that specifies the port device type as ANSI (the default), HARDCOPY, or SOFTCOPY. This characteristic affects local mode handling of the delete key and formatting of both the SHOW/LIST and MONITOR displays. HARDCOPY displays deleted characters between backlashes. ANSI clears the screen before each display and causes MONITOR displays to be updated in place, rather than scrolled. Note that port device type ANSI enables command line recall.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

Restrictions

- The access server sends MONITOR displays in ANSI escape sequences regardless of the specified TYPE.
- Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT USERNAME - PRIVILEGED/NOPRIVILEGED

PORT USERNAME (nonprivileged)

Syntax

Description

A nonprivileged option that specifies 1 to 16 ASCII characters (enclosed within quotation marks) as a user name to be associated with the port. The default is no USERNAME.

When you specify user name with the DEFINE PORT command, the USERNAME prompt no longer appears, starting with the next port login. To regain the prompt for subsequent login, enter another DEFINE PORT USERNAME command and specify a quoted null string "?" for the USERNAME characteristics. Quotes are required only if you want to preserve case or if the USERNAME contains embedded blanks.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

PORT VERIFICATION (secure)

Syntax

Description

An option (available to all users) that specifies whether the access server sends informational messages when you connect, disconnect, or switch sessions (default: ENABLED). This command does not affect error and warning messages.

This command accepts a *port-list* or ALL as a parameter for the PORT keyword.

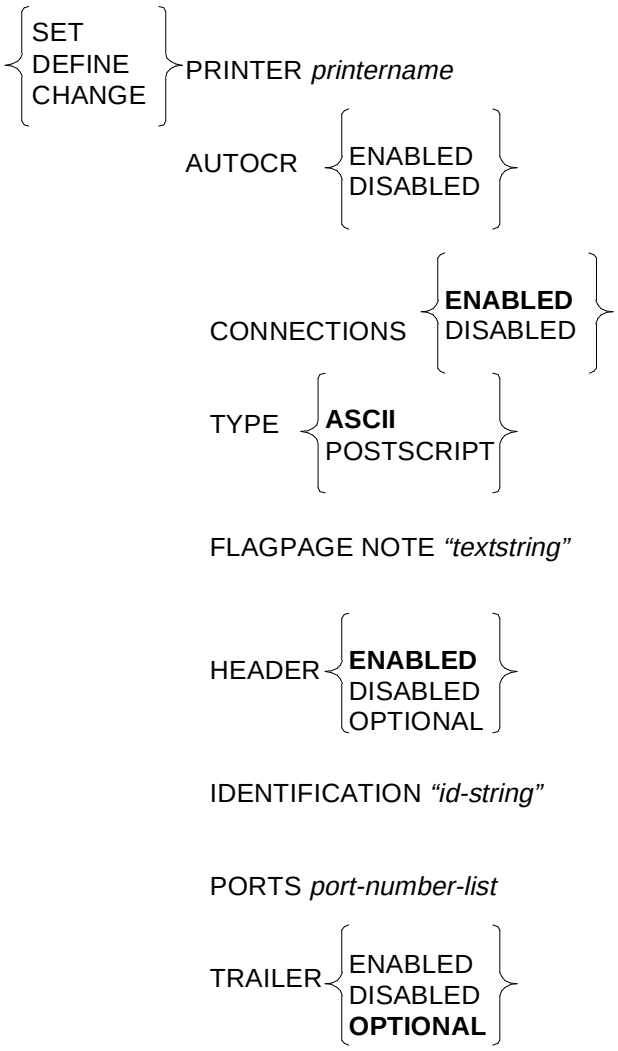
Restriction

Secure users are not allowed to use the DEFINE or CHANGE command with this characteristic.

PORT USERNAME - PRIVILEGED/NOPRIVILEGED

PRINTER (privileged)

Syntax



Description

This command creates a new LPD printer name or modifies the characteristics of an existing LPD printer. LPD is a protocol that UNIX or Windows NT hosts use to send queued print requests to systems and services to which a printer is physically attached.

Keywords

printer-name

The name assigned to the LPD printer associated with the port.

AUTOCR

Automatically inserts a carriage return. When you enable this option, the access server inserts a carriage return after each line feed character if there is no existing carriage return. The AUTOCR option applies only to ASCII text files.

CONNECTIONS

Specifies whether a user can queue a print job to the printer. If disabled, the user cannot access the printer. Disabling the printer temporarily is useful when you need to perform routine maintenance tasks (for example, adding paper or changing a form).

TYPE

Specifies the type of files a printer can print. The default is ASCII. If your printer can print both ASCII and PostScript files, this can be set to either value.

FLAGPAGE [NOTE]

Specifies a message that prints on the generated flag page that precedes output to the printer. The text string can be a maximum of characters.

HEADER

Specifies whether a header page prints before the actual data from the print job. If enabled, the header page always prints. If disabled, the header page never prints. If you specify OPTIONAL, the header page prints only if the access server receives user name information before it starts printing data. Depending on the order in which the access server receives control and data files, it may not know the user name before it starts the print job.

IDENTIFICATION

Specifies a text string that identifies the printer. The text string can be a maximum of 40 characters.

PORTS

Specifies one or more physical ports that can accept LPD print requests for the printer. The access server assumes that printers are connected to the specified ports.

TRAILER

Specifies whether to print a trailer page at the end of the print job. If enabled, a trailer page always prints. If disabled, a trailer page never prints. If you specify OPTIONAL, the trailer page prints only if the access server did not receive user name information at the start of the print job.

PRIVILEGED/NOPRIVILEGED (secure)

Syntax

Description

This secure command enables the port you are using to perform privileged operations. When you enter the command, the access server prompts you for the privileged password. The first time you use your access server, enter the default password SYSTEM. Then use the SET server PRIVILEGED PASSWORD command to immediately set your own password so that unauthorized users cannot enter privileged commands.

When you complete your privileged operations, use the SET NOPRIVILEGED command or log out the port to set the port back to nonprivileged status to prevent unauthorized use.

If you set your port to privileged status when the port characteristic MULTISESSIONS is enabled, the privileged status applies to all your terminal sessions.

Example: DEFINE/SET/CHANGE PRIVILEGED/NOPRIVILEGED

```
Local> SET PRIVILEGED
Password> SYSTEM (not displayed)
Local> SET server PRIVILEGED PASSWORD
Password> PLANET (not displayed)
Verification> PLANET (not displayed)
Local> SET NOPRIVILEGED
```

In this example, the default password SYSTEM is entered at the password prompt. After setting the port to privileged status, the privileged password is changed to PLANET and the port is returned to nonprivileged status. The next time someone attempts to enter privileged status on this port, they must enter the password PLANET. For more information on specifying passwords, refer to Chapter 1.

Port privilege overrides the Limited View characteristic.

RADIUS REALM - SECURITY WARNING INTERVAL

RADIUS REALM (privileged)

The command syntax for RADIUS REALM is identical to that for KERBEROS REALM or SECURID REALM . Please refer to KERBEROS REALM (privileged) or SECURID REALM (privileged) for the complete command description and syntax, being sure to substitute RADIUS for KERBEROS or SECURID in the command line.

RADIUS {ACCOUNTING/AUTHENTICATION} [SERVICE] PORT (privileged)

Syntax

Description

This command allows the UDP (or TCP) port number of the corresponding network server to be specified. This is useful for protocols that do not have well-known port numbers assigned by the Internet Assigned Numbers RFC. Any legal *tcp-port* number can be entered. The default accounting port ID is 1645 and the default authentication port ID is 1646.

RADIUS/KERBEROS/SECURID [TIMEOUT] (privileged)

Syntax

Description

This privileged command specifies the number of seconds that a request can be outstanding before being timed out. The access server will first retransmit an outstanding request after a 1-second retransmit timer, again after a 2-second retransmit timer, doubling (each time), then a 4-second retransmit timer, and so forth, until the request is fulfilled either by the security server or until the TIMEOUT period is reached. If there is more than one security server for a realm, the retransmit timer is not doubled until the request is retransmitted to all the security servers for the realm.

Keywords

TIMEOUT

The TIMEOUT value specifies the maximum amount of elapsed time you may wait for the operation to be completed, or to fail with a timeout error message. The range is 1 to 64 seconds.

INTERVAL

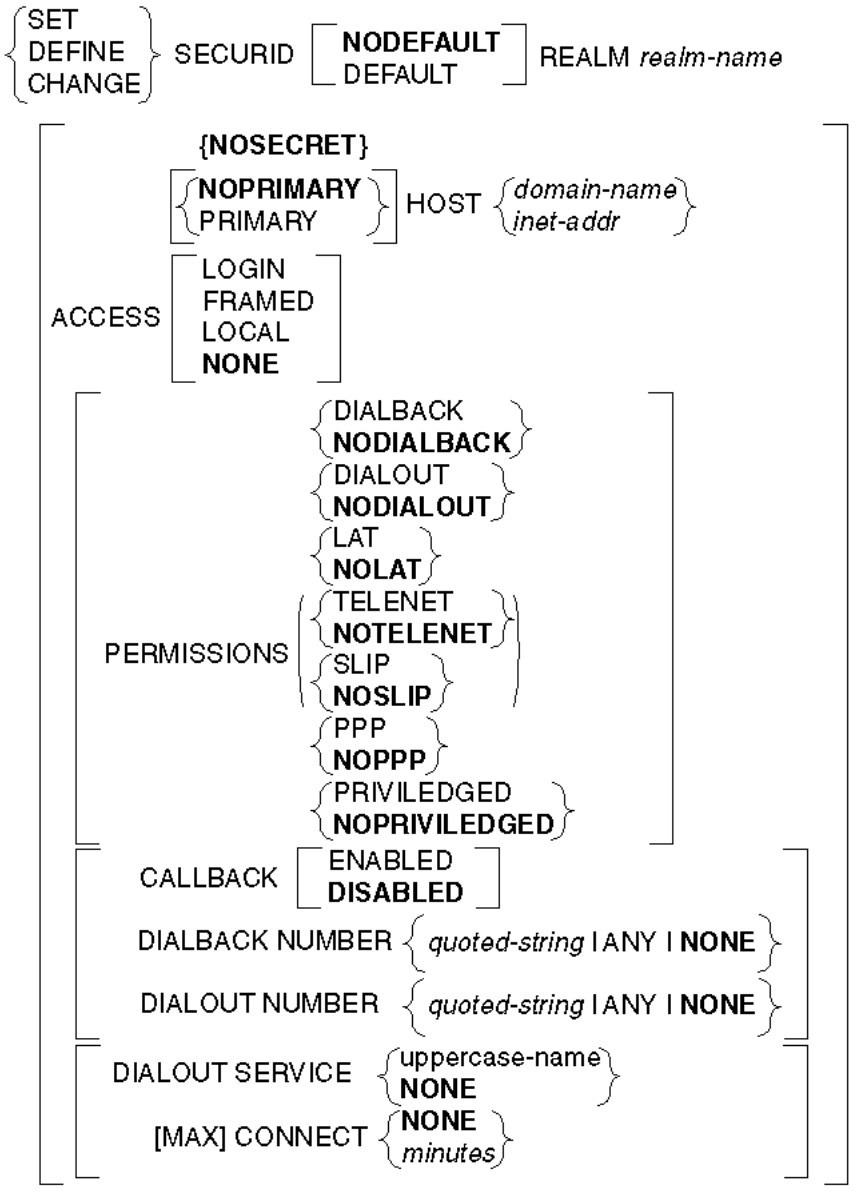
The valid range for INTERVAL is 1 to 20 seconds, with a default of 2 seconds.

Restriction

The allowable range for the TIMEOUT is 1 to 64 seconds, with a default of 2 seconds.

SECURID REALM (privileged)

Syntax



Description

The command syntax for SECURID REALM is nearly identical to that for KERBEROS REALM.

The SET/DEFINE/CHANGE REALM command family sets up and tears down the various realms used to identify particular administrative domains. This is simply an extension of the existing syntax for setting up and tearing down Kerberos. This is a privileged command.

Keywords

SECRET

The SECRET clause is used to specify a secret that the DECserver shares with security servers from the realm. The DECserver software associates no default secret with any realm. SECRET for SecurID realms can be cleared (NOSECRET) but cannot be SET or DEFINED. The SECRET is automatically obtained from the SecurID server.

HOST

The HOST clause associates a host with a realm. The DECserver software will use this host to resolve authentication requests. The DECserver software will accept either a domain name or an IP address as a host identifier. The PRIMARY keyword indicates that the DECserver software should give first priority to this host, (that is, it should begin all new authentication requests with this host). The default is NOPRIMARY. A realm can have only one primary host.

The clauses ACCESS, PERMISSIONS, CALLBACK, DIALBACK NUMBER, DIALOUT NUMBER, DIALOUT SERVICE, and MAX CONNECT specify the default authorization for users authenticated, but not otherwise authorized, within the realm. The DECserver software provides default values for these categories of information when the authentication service fails to provide them. The existing Kerberos commands have been extended to support this clause. The NUMBER clause applies to both dialout and dialback (or callback) types of access, and is most meaningful if it is a number mask, (that is, contains an element of wildcarding). Specific, fully qualified telephone numbers do not make sensible realmwide default values.

ACCESS

The ACCESS clause sets the realm’s default access mode at connection establishment time. The supported values are:

LOCAL	Interactive access allowed
FRAMED	AUTOLINK (PPP or SLIP) access provided
LOGIN	Dedicated connection (Telnet, LAT) to host (only) allowed

NONE	Access determined by PORT characteristics

LOGIN is the default value for this realm characteristic.

CALLBACK

An administrator would specify mandatory callback by configuring the realm with CALLBACK ENABLED.

DIALBACK NUMBER, DIALOUT NUMBER

The DIALOUT and DIALBACK NUMBER values have a maximum length of 80 characters, and contain a phone number to be used on dialout/back.

The DIALBACK NUMBER is used for Mandatory Dialback as well as for PPP Callback on the same port (where the user is unable to specify a dialback service). The DIALOUT NUMBER clause is used for interactive dial-out commands, the actual number to dial, a number mask (time permitting), and that any number may be used. If the number is not fully specified, and it is not contained in the optional DIALOUT SERVICE definition, the dialer engine will prompt you for the number. The DIALOUT SERVICE clause specifies a default dialer service to be used when attempting a dialout connection. Refer to the section entitled USERACCOUNT (privileged) for more information on dialback/dialout numbers.

DIALOUT SERVICE

The DIALOUT SERVICE values will be converted to upper-cased and have a maximum length of 16 characters.

MAXCONNECT

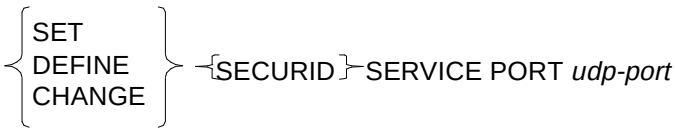
The MAXCONNECT clause indicates the maximum number of minutes you can be logged in before being forcibly logged out. The user interface is the same as USERACCOUNT MAX CONNECT.

Some realms support the following clauses:

Realm	Clause
RADIUS	The PROMPT clause specifies an alternate password prompt to display to interactive users when the entered user-id falls within one of these realms. The maximum prompt length is 16 characters.
SecurID	The ENCODING clause indicates how to encode the user password in authentication requests to the security server. This option is currently valid only for SecurID realms. The supported values are data encryption standard (DES) and PROPRIETARY. The Security Dynamic proprietary encryption is freely exported from the countries outside of the United States, while DES is restricted from foreign export.
Local database	The local database (SERVER REALM) uses the MAX FAILS clause to indicate the number of consecutive authentication failures to permit before deactivating a record. The default is 3; the range is 0 to 100.

SECURID [SERVICE] PORT (privileged)

Syntax



Description

Changes SecurID User Authentication parameters.

This command allows the UDP (or TCP) port number of the corresponding network server to be specified. This is useful for protocols that do not have well-known port numbers assigned by the Internet Assigned Numbers RFC. Any legal *tcp-port* number can be entered. The default SecurID port ID is 755.

SECURITY WARNING [INTERVAL] (privileged)

Syntax

Description

SET SECURITY WARNING is a privileged command that allows the security administrator to specify the interval between and number of warnings the DECserver software will issue before a user's login expires. Expiration is based on the user's maximum connect time, which may be displayed using the SHOW PORT AUTHORIZATION command. The default is an interval of 1 minute, given four times before the user is forcibly logged out. The range is 1 to 20 for INTERVAL and 0 to 30 for TIMES.

SERVER - SERVER MULTICAST TIMER

SERVER (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER characteristic [characteristic]

Description

This privileged command specifies access server characteristics.

Restriction

You cannot change some access server characteristics using a SET command while any sessions are active (or queued) on the access server. Throughout this section, such characteristics are identified with a restriction to that characteristic.

Examples: SET/DEFINE /CHANGE SERVER CHARACTERISTIC

```
Local> DEFINE server IDENTIFICATION "TECHSALES OFC4"
```

This command defines an identification for the access server.

```
Local> SET server CIRCUIT 60 KEEPALIVE 30
```

This command reassigns values for the circuit timer and the keepalive timer. These values revert to the values in the permanent database when the access server is reinitialized.

SERVER ANNOUNCEMENTS (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER ANNOUNCEMENTS {**ENABLED** / DISABLED}

Description

This LAT protocol command specifies whether the access server sends LAT multicast messages over the Ethernet to announce the availability of local services (default: ENABLED). No announcements are sent if no local services are defined.

SERVER BROADCAST (privileged)

Syntax

Description

This privileged command specifies whether the BROADCAST is ENABLED (default) or DISABLED for users on port devices.

SERVER CIRCUIT TIMER (privileged)

Syntax

Description

This privileged LAT protocol command specifies the interval between messages sent from the access server to LAT service nodes. (The range is 20 to 200 milliseconds; the default is 80.)

Restrictions

- You cannot use the SET command with this parameter while any LAT sessions are active.
- This command is valid for LAT protocol only.

SERVER CONSOLE PORT (privileged)

Syntax

Description

This privileged command designates one access server port as the console port. (The default for port is 1.)

SERVER DUMP (privileged)

Syntax

Description

This privileged command specifies whether upline dumping of access server memory is performed when a fatal bug check error occurs. (The default is ENABLED.)

SERVER HEARTBEAT (privileged)

Syntax

Description

This privileged command specifies whether the access server reports errors found by its Ethernet collision detection circuitry. (The default is DISABLED.)

SERVER IDENTIFICATION (privileged)

Syntax

Description

This privileged command specifies a brief description of the access server for access server displays (default: no identification string).

The *id-string* value is a string of 1 to 40 ASCII characters. You must enclose the string in quotation marks ("*id-string*"). To clear an identification string, enter the command with a quoted null string (" "). This string also appears in the welcome banner when a user logs in to the access server.

Restriction

You cannot use the SET command with this parameter while any LAT session is active.

SERVER INACTIVITY TIMER (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER INACTIVITY [TIMER] *minutes*

Description

This privileged command determines the timeout period for ports having the port characteristic INACTIVITY LOGOUT when ENABLED (range: 1 to 120 minutes; default: 30). The timer determines the length of time that a local access port can be logged in without local user input or output. The timer also determines the length of time that a remote access port can be logged in when there is no activity for a session at that port. No timeout occurs if any sessions are active on the port.

SERVER KEEPALIVE TIMER (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER KEEPALIVE [TIMER] *seconds*

Description

This privileged LAT protocol command specifies the interval between messages for LAT circuits on which no data is being transmitted (range: 10 to 180 seconds; default: 20).

Restriction

You cannot use the SET command with this parameter while any LAT sessions are active.

SERVER LOCK (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER LOCK {**ENABLED** / DISABLED}

Description

This privileged command specifies whether interactive port users can use the LOCK command. (The default is ENABLED.)

SERVER LOGIN PASSWORD (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER LOGIN PASSWORD [*"password"*]

Description

This privileged command specifies a password that interactive users must enter when they log in to the access server. You must also set the port characteristic PASSWORD to ENABLED for the password prompt to appear at port login. For more information on specifying passwords, refer to Chapter 1.

You can omit the password value if LOGIN PASSWORD is the only characteristic in the command line. The access server then prompts for the password.

The default password is ACCESS. This default is in effect when the access server is delivered and when you reset the access server characteristics to their default values.

SERVER MAINTENANCE PASSWORD (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER MAINTENANCE PASSWORD *"hex-password"*

Description

This privileged command specifies a password that must be entered by remote operators and by persons using the DECnet NCP CONNECT, TRIGGER, or LOAD commands to downline load the access server. The default is no password checking.

This password can have 1 to 16 hexadecimal characters (values 0 through 9 and A through F only). If you enter 0 or a quoted null string (" ") in the command line, the access server does not check for a password.

You can omit the password value if MAINTENANCE PASSWORD is the only characteristic in the command line. The access server then prompts for the password. Enter the password or 0 in response to the password prompt. For more information on specifying passwords, refer to Chapter 1.

SERVER MULTICAST TIMER (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER MULTICAST [TIMER] *seconds*

Description

This privileged LAT protocol command specifies the time to elapse between transmissions of service announcements. (The range is 10 to 180 seconds; the default is 30.)

SERVER NAME - SERVER SOFTWARE

SERVER NAME (privileged)

Syntax

{SET, DEFINE, CHANGE} SERVER NAME *server-name*

Description

This privileged command specifies a 1- to 16-character name for the access server. The default is LAT_*nnnnnnnnnnn*, where each *n* represents one of the 12 hexadecimal characters in the Ethernet address of the access server.

Reference

You should set the access server name to match the DECnet node name for the access server. For more information, refer to the *Network Access Server Management* manual.

Restriction

You cannot use the SET command with this parameter while sessions are active.

SERVER NODE LIMIT (privileged)

Syntax

{SET, DEFINE, CHANGE} SERVER NODE [LIMIT] {*limit*, NONE}

Description

This privileged LAT protocol command specifies the maximum number of LAT service nodes that the access server maintains in its node database. The range is 1 to 2000. (The default is 200.) NONE implies no limit except the memory constraints of the access server.

SERVER NUMBER (privileged)

Syntax

{SET, DEFINE, CHANGE} SERVER NUMBER [*n*]

Description

This privileged command specifies a number for the access server (range: 0 to 32767; default: 0).

Restriction

You cannot use the SET command with this parameter while sessions are active.

SERVER PASSCHECK (priviledged)

Syntax

{SET / DEFINE / CHANGE} SERVER PASSCHECK {ENABLED / **DISABLED**}

Description

Determines if local service passwords will affect Host Initiated Connect requests.

Keywords

ENABLED

HIC requests must supply a valid password when accessing a password protected LAT service.

DISABLED

HIC requests do not need to supply a valid password when accessing a password protected LAT service.

SERVER PASSWORD LIMIT (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER PASSWORD LIMIT *limit*

Description

This privileged command specifies the number of times a user can try to enter the correct password for any password-protected access server operation. The range is 1 to 10; the default is 3. For more information on specifying passwords, refer to the description in Chapter 1.

SERVER PRIVILEGED PASSWORD (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER PRIVILEGED PASSWORD [*"password"*]

Description

This privileged command specifies the password a user must enter following a SET PRIVILEGED command to use privileged access server commands at the port. You can omit the password value if PRIVILEGED PASSWORD is the only characteristic in the command line. The access server then prompts for the password. For more information on specifying passwords, refer to Chapter 1.

The default password is SYSTEM. This default is in effect when the access server is delivered and when you reset the access server characteristics to their default values.

SERVER PROMPT (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER PROMPT [*"prompt-string"*]

Description

This privileged command specifies a unique string of characters for the prompt-string value that you assign to the access server prompt. This string replaces the default Local> prompt. The *prompt-string* value is a string of 1 to 16 ASCII characters. You must enclose the string in quotation marks (*"prompt-string"*). To set the prompt back to the default (Local>), enter the command with a quoted null string (" ").

SERVER QUEUE LIMIT (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER QUEUE [LIMIT] {*depth* / NONE}

Description

This privileged LAT protocol command specifies the maximum number of queued connection requests for remote access to access server ports. This number is called the depth of the queue. (The range is 0 to 200; the default is 100.) A value of 0 disables the queue, and NONE is equivalent to the maximum number of allowable queued connection requests.

SERVER REALM (privileged)

The command syntax for SERVER REALM is identical to that for KERBEROS REALM or SECURID REALM. Refer to KERBEROS REALM (privileged) or SECURID REALM (privileged) for the complete command description and syntax, being sure to substitute SERVER for KERBEROS or SECURID in the command line.

SERVER REMOTE PASSWORD (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER REMOTE PASSWORD ["*password*"]

Description

This privileged command specifies a password that remote users must enter when they log in to the access server. You must also set the port characteristic REMOTE PASSWORD to ENABLED for the password prompt to appear at port login. For more information on specifying passwords, refer to Chapter 1.

You can omit the password value if REMOTE PASSWORD is the only characteristic in the command line. The access server then prompts for the password.

The default password is ACCESS. This default is in effect when the access server is delivered and when you reset the access server characteristics to their default values.

SERVER RESPONDER (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER RESPONDER {ENABLED / DISABLED}

Description

This privileged command enables or disables the RESPONDER characteristic.

Keywords

RESPONDER

RESPONDER enables or disables the access servers ability to respond to solicit information requests on behalf of other nodes.

ENABLED

In addition to responding to solicit information requests targeted to itself, the access server may also respond to information requests on behalf of other nodes. The access server will act as an agent for another node only if the local database contains information about the specified service and node, and the access codes of the requesting node intersect the access codes of the targeted node.

DISABLED

The access server will respond only to solicit information datagrams requesting local node and service information. DISABLED is the default.

Note

Setting or clearing the access servers RESPONDER characteristic does not affect its ability to respond with local service/node information when it receives a Solicited Information request targeted to itself.

Restriction

This characteristic is used by the LAT protocol only.

SERVER RETRANSMIT LIMIT (privileged)

Syntax

{SET / DEFINE / CHANGE} SERVER RETRANSMIT [LIMIT] *limit*

Description

This privileged command specifies the number of times a LAT message is retransmitted to a service node when the access server does not receive any acknowledgment messages. (The range is 4 to 120; the default is 8.)

Restrictions

- You cannot use the SET command with this parameter while a LAT sessions is active.
- This command is valid for a LAT protocol only.

SERVER SERVICE GROUPS (privileged)

Syntax

Description

This privileged command specifies which groups are assigned to all locally defined services and are enabled for the access server when it functions as a service node (the default is 0 ENABLED, 1-255 DISABLED). Use the *group-list* format with ENABLED or DISABLED to add groups to or remove groups from the existing list. Specifying a value for *group-list* without the keywords ENABLED or DISABLED will replace the existing list with a new one. Specify ALL to enable or to disable all service groups.

Keywords

group-list

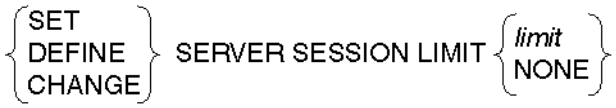
One or more decimal codes ranging in value from 0 to 255, each representing a LAT group code. Specify multiple codes by separating individual numbers with commas, by specifying a range of numbers (in ascending order), or a combination of both. For example, the group list 1, 4-7, 9 specifies groups 1, 4, 5, 6, 7, and 9.

Restriction

This characteristic is used by the LAT protocol only.

SERVER SESSION LIMIT (privileged)

Syntax



Description

This privileged command specifies the maximum number of active sessions that the access server allows at one time. The range is 0 to 128; the default is default 64. NONE means that the limit is equivalent to the maximum number of sessions allowed on the access server.

SERVER SOFTWARE (privileged)

Syntax

Description

This privileged command specifies the filename (1 to 9 characters) of the access server software load image. If you enclose the filename in quotes, you can use both uppercase and lowercase letters in the filename. You can specify a quoted null string (" ") to have no name for the software image (useful for downline loading with some protocols).

Reference

For more information, refer to the *Network Access Server Management* manual.

SERVICE - SERVICE QUEUE

SERVICE (privileged)

Syntax

{SET, DEFINE, CHANGE} SERVICE *service-name* [characteristic [characteristic(s)]]

Description

This privileged command specifies local LAT services and their characteristics.

Keywords

service-name

This privileged command specifies the name of the LAT service you wish to define. You can have a maximum of 20l LAT services defined at one time.

Example: SET SERVER PORT

```
Local> SET SERVICE BOSTON PORTS 1,3,6-8 ENABLED QUEUE
DISABLED
```

If the LAT service BOSTON does not exist, this command creates this service on ports 1, 3, 6, 7, and 8 with queuing disabled. If BOSTON does exist, this command adds these ports to the existing port list and disables queuing for the service.

Summary of SERVICE Characteristics

The following lists all characteristics to the SERVICE command. The syntax for each characteristic is provided in this section, along with descriptions, defaults, and restrictions.

CONNECTIONS

IDENTIFICATION

PASSWORD

PORTS

QUEUE

Defaults are shown in **BOLD** type.

SERVICE CONNECTIONS (privileged)

Syntax

Description

This privileged command specifies whether the access server can accept new connections to the specified LAT service. (The default is ENABLED.) Current sessions are unaffected.

SERVICE IDENTIFICATION (privileged)

Syntax

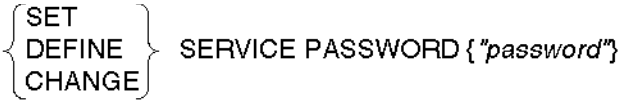
Description

This privileged command specifies a brief description of the LAT service for the access server to transmit in multicast messages to advertise the service (default: no description is sent).

The id-string value is a string from 1 to 40 ASCII characters. To clear an identification string, enter the command with a quoted null string (" ").

SERVICE PASSWORD (privileged)

Syntax



Description

This privileged command specifies a LAT service access password that a user must supply in order to establish a session with the LAT service. (The default is set to no password required.)

You can omit the password value when PASSWORD is the only characteristic in the command line. The access server then prompts you for the password. If no value is entered for the password, pressing the carriage return (only) will clear the password. To clear an existing password, enter the command line with a quoted null string (" "). For more information on specifying passwords, refer to Chapter 1.

SERVICE PORTS (privileged)

Syntax

Description

This privileged command specifies ports that offer the LAT service (default: ALL DISABLED). Specify *port-list* with ENABLED or with DISABLED to add or remove ports from the existing port list. Specify *port-list* without keywords ENABLED or DISABLED to replace the existing list with a new one. Specify ALL to enable or disable use of the LAT service by all ports.

Keywords

port-list

Specifies one or more ports to which the defined characteristics apply. The default is your own port. For more information on specifying *port-list*, refer to Chapter 1.

SERVICE QUEUE (privileged)

Syntax

Description

This privileged command specifies whether the access server places requests for a local LAT service into the access server connection queue when the service is unavailable. (The default is ENABLED.) Disabling queuing does not affect existing queues.

SESSION LAT - SESSION TELNET IP REQUEST

SESSION LAT (secure)

Syntax

SET SESSION [LAT] { **INTERACTIVE** | PASTHRU | PASSALL }

Description

This secure command (available to all users) specifies characteristics for your current LAT session (the last LAT session you entered in service mode).

Keywords

INTERACTIVE

Enables special switch characters and messages at the access server port. This is the default.

PASTHRU

Disables all switch characters and access server messages at the access server port while you are using the affected session. Use this option for ASCII file transfers.

PASSALL

Disables all switch characters, access server messages, and XON/XOFF flow control at the access server port while you are using the affected session. Use this option for binary file transfers.

Restriction

If you SET SESSION to PASSALL or PASTHRU mode, messages broadcast to your port are ignored while you are using the affected session.

Example: SET SESSION LAT PASSALL

```
Local> SET SESSION LAT PASSALL
```

This command disables all switch characters, flow control characters, and access server messages at the port while you are using the affected LAT session.

SESSION TELNET (secure)

Syntax

SET SESSION TELNET [CLIENT] {Characteristics}

Description

This secure command (available to all users) modifies the Telnet client characteristics for the current Telnet session.

Type SHOW PORT SESSION to view Telnet session characteristics. You must resume a suspended Telnet session before characteristics altered by SET SESSION TELNET commands go into effect.

```
Local> SET SESSION TELNET CLIENT AUTOSYNCH AO ENABLED
```

This command specifies that an Automatic Synch character occurs whenever the keyboard character defined as AO is entered.

SESSION TELNET AO REQUEST (secure)

Syntax

SET SESSION TELNET AO [REQUEST] { character (Default: Ctrl/O) | <DEL> | NONE }

Description

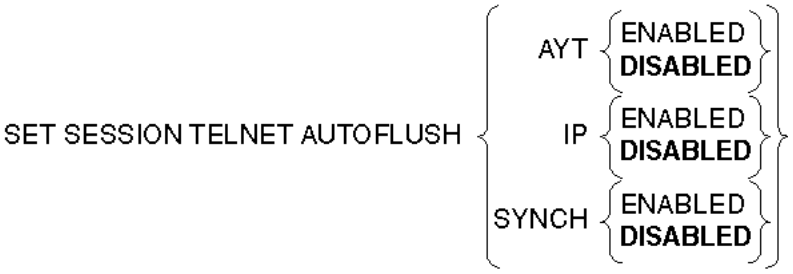
The abort output (AO) request defines a keyboard character that, when entered, invokes the Telnet Abort Output function. This function causes any output currently on its way to the user's terminal to be aborted. The default character is Ctrl/O. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default. For more information, refer to the description of the SESSION TELNET SIGNAL REQUEST (secure).

SESSION TELNET AUTOFLUSH (secure)

Syntax



Description

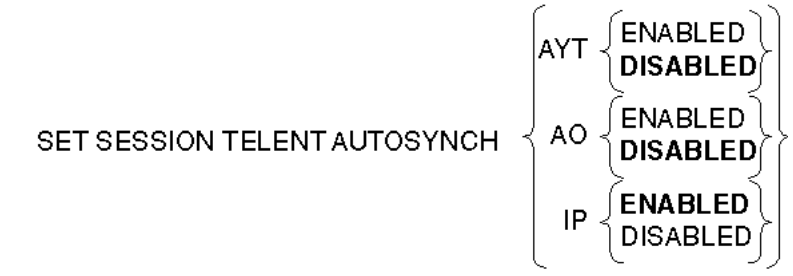
Automatic Flush specifies that an Automatic Flush of output (same as Abort Output) should occur whenever the keyboard characters defined as IP, SYNCH, or AYT are entered. AUTOFLUSH causes any output currently on its way to the user's terminal to be aborted. The default is DISABLED for IP, SYNC, and AYT.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET AUTOSYNCH (secure)

Syntax



Description

Automatic Synch specifies that an Automatic Synch should occur whenever the keyboard character defined as AO, IP, or AYT is entered. AUTOSYNCH causes all input currently on its way to the remote process to be dropped. (Defaults: The AO and AYT default are DISABLED. The IP default is ENABLED.)

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET AYT REQUEST (secure)

Syntax

SET SESSION TELNET AYT [REQUEST] { character (Default: Ctrl/T) | <DEL> | NONE }

Description

Are-You-There (AYT) request defines a keyboard character that, when entered, invokes the Telnet AYT function. This function causes the remote host to send back a message indicating that it is still up and running. The default character is Ctrl/T. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET BINARY (secure)

Syntax

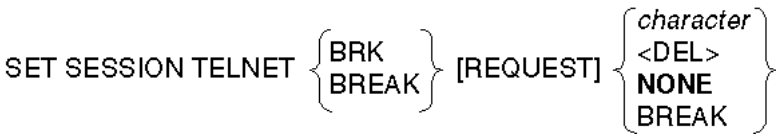
SET SESSION TELNET BINARY { **DISABLED** | DUPLEX | RECEIVE | TRANSMIT }

Description

Binary transmission transmits and receives binary data on this Telnet connection. It can be enabled or disabled in each direction independently. The default is DISABLED in both directions (duplex).

SESSION TELNET BREAK (BRK) REQUEST (secure)

Syntax



Description

The secure BRK or BREAK request defines a keyboard character that, when entered, causes the Telnet Break command to be sent to the remote host. There is no default BRK character. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows. To define the Break key, you must type the individual letters.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET CHARACTER SIZE (secure)

Syntax

Description

The secure transmit and receive character size specifies whether the characters sent and received on this connection should be 7-bit or 8-bit. The default is 8-bit in both directions.

SESSION TELNET ECHO (secure)

Syntax

Description

The secure Echo (ECHO) option specifies whether input on this connection should be echoed locally (by the access server) or remotely (by the remote host). The default is REMOTE.

Restriction

When ECHO is set to LOCAL, input can be suppressed locally by either of two methods: by setting the PROFILE characteristic to BINARY or by typing the defined TOGGLE ECHO character to suppress local echoing. For more information, refer to the SESSION TELNET TOGGLE ECHO (secure).

SESSION TELNET EOR REQUEST (secure)

Syntax

Description

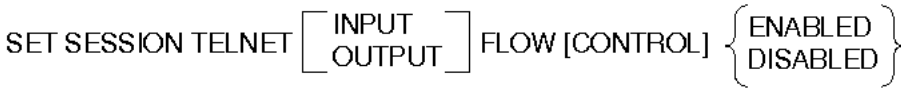
The secure End-Of-Record (EOR) request defines a keyboard character that, when entered, invokes the Telnet End-Of-Record function. This function indicates to the remote host that this is the end of the current input record. There is no character defined as EOR by default. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default. Additionally, the EOR option must be currently enabled through negotiation with the Telnet peer.

SESSION TELNET FLOW CONTROL (secure)

Syntax



Description

This secure command specifies how the access server handles flow control for data transfer between the access server and the port device. Flow control can be set for both directions: from the access server to the port device (OUTPUT), and from the port device to the access server (INPUT). The default is ENABLED in both directions.

SESSION TELNET IP REQUEST (secure)

Syntax

Description

The interrupt process (IP) request defines a keyboard character that, when entered, invokes the Telnet Interrupt Process function. This function causes the remote host to interrupt or abort the remote process. The default character is Ctrl/Y. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET NEWLINE FROM HOST - SESSION TELNET VERIFICATION

SESSION TELNET NEWLINE FROM HOST (secure)

Syntax

Description

The SET SESSION TELNET NEWLINE FROM HOST command defines a 1- or 2-character sequence that, when received by the access server from the remote host, is interpreted as newline, translated into the NEWLINE TO TERMINAL character sequence, and sent to the terminal. The default is <CRLF>. To define <CRLF> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

This function will not work if either the SET SESSION TELNET BINARY option is set to something other than DISABLED or the SET SESSION TELNET PROFILE option is set to BINARY.

SESSION TELNET NEWLINE FROM TERMINAL (secure)

Syntax

Description

The secure command defines a 1- or 2-character sequence that, when received by the access server from the terminal, is interpreted as newline, translated into the NEWLINE TO HOST character sequence, and sent to the remote host. The default is <CR>. To define <CR> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

Same restriction as NEWLINE FROM HOST.

SESSION TELNET NEWLINE TO HOST (secure)

Syntax

Description

This secure command defines a 1- or 2-character sequence that the access server sends to the remote host whenever a NEWLINE FROM TERMINAL character sequence is received from the terminal. The default is <CRLF>. To define <CRLF> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

Same restriction as NEWLINE FROM HOST.

SESSION TELNET NEWLINE TO TERMINAL (secure)

Syntax

Description

This secure command defines a 1- or 2-character sequence that the access server sends to the user's terminal whenever a NEWLINE FROM HOST character sequence is received from the remote host. The default is <CRLF>. To define <CRLF> as the keyboard character, you must enter the individual characters, including the left and right arrows.

Restriction

Same restriction as NEWLINE FROM HOST.

SESSION TELNET PROFILE (secure)

Syntax

SET SESSION TELNET PROFILE { **CHARACTER** | BINARY }

Description

This secure command selects a set of characteristics for a Telnet connection. This characteristic is intended to prevent you from having to set all of the individual characteristics in just the right way to produce a desired behavior on a Telnet connection.

There are two predefined sets of characteristics: CHARACTER and BINARY. The default is CHARACTER. In character mode, user data is forwarded immediately to the remote host, one character at a time, and is echoed by the remote host. Binary mode sends and receives binary data over the Telnet connection.

SESSION TELNET QUOTE (secure)

Syntax

SET SESSION TELNET QUOTE { *character* | **NONE** }

Description

This secure command defines a keyboard character that, when entered, causes the next character entered to be treated as ordinary user data. Keys that are mapped to Telnet functions (for example, Ctrl/T to AYT, Ctrl/O to AO, and so on) can be entered as ordinary data by preceding them with the QUOTE character. There is no QUOTE character by default.

Restriction

For this function to work, the SET SESSION TELNET SIGNAL REQUEST characteristic must be ENABLED, which is the default.

SESSION TELNET SIGNAL REQUEST (secure)

Syntax

SET SESSION TELNET SIGNAL REQUEST { ENABLED | DISABLED }

Description

This secure command enables or disables predefined keyboard characters that are mapped to Telnet functions, such as AO, AYT, BRK, EOR, IP, QUOTE, SYNCH, and TOGGLE ECHO. When disabled, these characters are interpreted as ordinary user data. When enabled, they cause the corresponding Telnet function to be invoked. The default is ENABLED.

SESSION TELNET SWITCH CHARACTER (secure)

Syntax

SET SESSION TELNET SWITCH [CHARACTER] { ENABLED | DISABLED }

Description

This secure command specifies how the access server handles switch characters for Telnet sessions on the port. If enabled, the access server recognizes and responds to any switch characters defined on the port. If disabled, the access server ignores all switch characters on the port. The default is ENABLED.

SESSION TELNET SYNCH REQUEST (secure)

Syntax

SET SESSION TELNET SYNCH [REQUEST] { character (Default: Ctrl/X) | <DEL> | NONE }

Description

This secure command defines a keyboard character that, when entered, invokes the Telnet Synch function. This function causes all input currently on its way to the remote process to be dropped (that is, it clears the path to the remote process). The default is Ctrl/X. To define <DEL> as the keyboard character, you must enter the individual characters, including the left and right arrows.

SESSION TELNET TERMINAL (privileged)

Syntax

SET SESSION TELNET TERMINAL { VTXXX | ANSI | UNKNOWN }

Description

This privileged command allows you to specify the terminal type during Telnet client sessions.

Keywords

VTXXX

Denotes numerically any member of the DIGITAL VT family of terminals from VT10 through VT999.

ANSI

Non-DIGITAL VT terminals that support ANSI.

UNKNOWN

All other terminal types.

SESSION TELNET TOGGLE ECHO (secure)

Syntax

SET SESSION TELNET TOGGLE ECHO { character (Default: Ctrl/E) | NONE }

Description

This secure command defines a keyboard character that, when entered, enables or suppresses echoing on this connection. For example, you might toggle echo OFF while entering a password. The default character is Ctrl/E.

Restriction

Entering the TOGGLE ECHO character works only when input is being echoed locally by the access server. For more information, refer to the ECHO command.

SESSION TELNET VERIFICATION (secure)

Syntax

SET SESSION TELNET VERIFICATION { **ENABLED** / DISABLED }

Description

This secure command specifies the display of information messages by the access server when an existing Telnet client session is started, stopped, or resumed. If you enable verification, the access server displays the session number and the name of the Telnet host. If you disable verification, no session information is displayed. The default is ENABLED.

SESSION TN3270 FLOW CONTROL - SYSTEM

SESSION TN3270 FLOW CONTROL (secure)

Syntax

SET SESSION TN3270 [INPUT / OUTPUT] FLOW CONTROL {**ENABLED** / DISABLED}

Description

This secure command option changes the current TN3270 session. Flow control can be set for both directions for the session: from the access server to the port device (OUTPUT), and from the port device to the access server (INPUT). The default is ENABLED in both directions.

SESSION TN3270 SWITCH CHARACTER (secure)

Syntax

SET SESSION TN3270 SWITCH [CHARACTER] {**ENABLED** / DISABLED}

Description

This secure option changes the current session. The command determines whether FORWARD, BACKWARD, or local SWITCH port characters are recognized at the port. If ENABLED, the access server recognizes and responds to FORWARD, BACKWARD, or local SWITCH characters. If DISABLED, the access server ignores all switch characters on the port. The default is ENABLED.

SESSION TN3270 VERIFICATION (secure)

Syntax

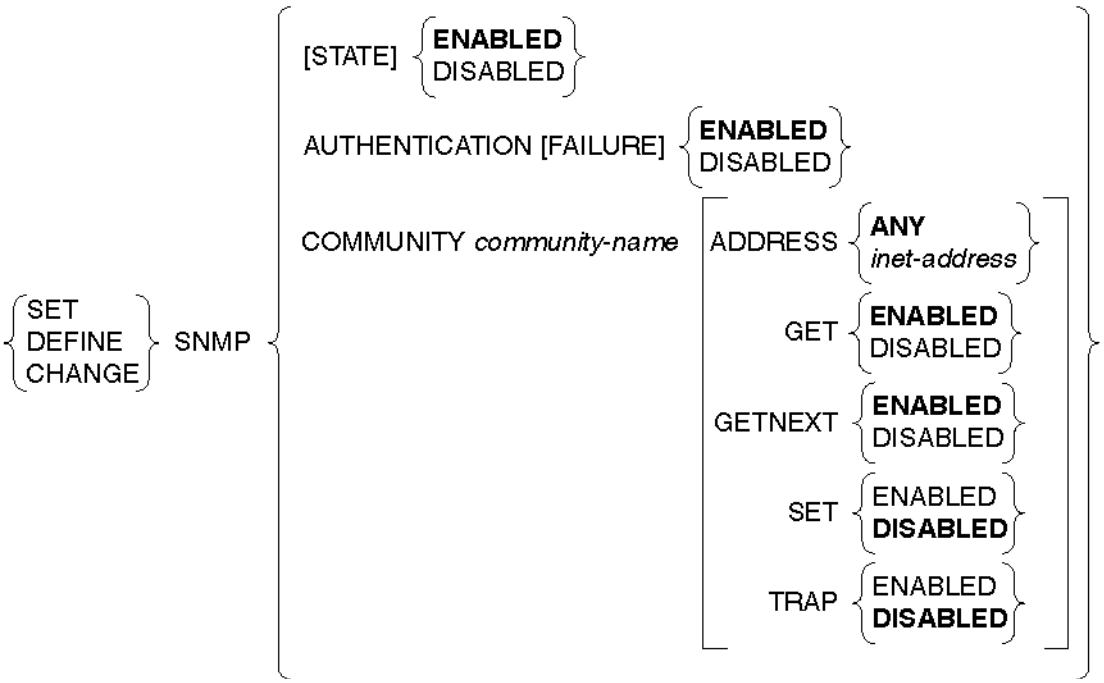
SET SESSION TN3270 VERIFICATION {**ENABLED** / DISABLED}

Description

A secure option that changes the current session. This command determines whether the access server sends user messages on connect, disconnect, or switch sessions. The default is ENABLED.

SNMP (privileged)

Syntax



Description

This privileged command configures the Simple Network Management Protocol (SNMP) agent for access from SNMP Network Management Stations (NMSs). Community names are used to verify access from NMSs.

The members of the SNMP community can access the variables as defined in the access server Management Information Bases (MIBs). For each community, the SNMP GET, GETNEXT, SET, and TRAP operation can individually be enabled or disabled.

Keywords

[STATE]

When enabled, the access server can respond to GET, GETNEXT, and SET requests through SNMP and can generate authentication traps to these hosts when necessary. When disabled, all SNMP requests are ignored and traps are not generated by the access server. The default is ENABLED.

AUTHENTICATION [FAILURE]

When enabled, the access server can emit authentication failure traps. These traps are sent when an unauthorized host attempts to access the access server or when a host uses an unauthorized SNMP request. The traps are sent to all communities in the access server SNMP database for which TRAP is ENABLED. When disabled, the access server does not emit authentication failure traps. The default is ENABLED.

COMMUNITY

Used to add a community name or specify a community's characteristics in the access server community database. A default community named PUBLIC is preset in the community database; the default characteristics of the community database are ADDRESS ANY, GET ENABLED, GETNEXT ENABLED, SET DISABLED, and TRAP DISABLED.

community-name

An ASCII string, maximum length 32 printable characters per *community-name*, enclosed in double quotes (" "). If the number of characters for any one name exceeds 32 characters, the name will be truncated to 32 characters. Each *community-name* will be associated with either ADDRESS ANY or with one particular *inet-address*. The default is ANY.

ADDRESS

inet-address

The Internet address of the remote host, in the form *nnn.nnn.nnn.nnn*. If the correct form is provided, both the community name and address are checked before the access server allows access to its databases. An error message appears if the *inet-address* is not in the correct form. Assigning an *inet-address* to a community name increases the number of overhead characters (requires from 2 characters to 6 characters to store the information). For more information, refer to the *community-name*.

ANY

Specify ANY to configure the server to accept SNMP messages from any *inet-address* associated with that community. You can also specify ANY to dissociate the community from any specific *inet-address*. This will delete a previously specified *inet-address*.

Note

TRAP must be disabled before setting ADDRESS to ANY.

GET

When enabled, allows members of the community to read values from the server management information base (MIB). The default is ENABLED.

GETNEXT

When enabled, allows members of the community to read values sequentially from the server supported MIBs. The default is ENABLED.

SET

When enabled, allows members of the community to modify values sequentially from the server supported MIBs. The default is DISABLED.

TRAP

When enabled, identifies the Internet address as a location that receives traps. The default is DISABLED.

Restrictions

- The access server must have an Internet address assigned to enable the SNMP agent.
- Due to memory constraints, only 80 characters are available for all community names. That is, the total number of characters of all defined community names, including 2 overhead characters for each name, cannot exceed 80 characters. If you define a specific Internet address for a community name, the overhead for that community name increases by 4 characters (to store the Internet address) for a total of 6 characters. If you exceed the 80-character maximum, you cannot define any more community names.

For example, if you need to specify 8 community names, each with an Internet address, you would have to restrict the character length of each name to an average of 4 characters (32 characters total). When this is added to the overhead sum of 6 characters per community name (48 total characters of overhead), the 80-character maximum is reached.

For example, if you need to specify 8 community names, each with an Internet address, you would have to restrict the character length of each name to an average of 4 characters (32 characters total). When this is added to the overhead sum of 6 characters per community name (48 total characters of overhead), the 80-character maximum is reached.

Although the maximum length of any one community name is 32 characters, using fewer characters per name allows you to define more community names.

Examples: DEFINE SNMP COMMUNITY

The following command creates SNMP community name “MONTY”, which can be accessed only by the Internet host with a 195.1.1.60 address:

```
Local> DEFINE SNMP COMMUNITY "MONTY" ADDRESS 195.1.1.60
```

The following command enables Internet hosts that can access the community "MONTY" to use SNMP GET messages to obtain value information from the access server supported MIBs:

```
Local> SET SNMP COMMUNITY "MONTY" GET ENABLED
```

SYSTEM (privileged)

Syntax

Description

This privileged command specifies system-related information, such as the name of the person managing the access server or the location of the access server.

Keywords

CONTACT *contact-name*

Displays the name of the person managing the access server. The *contact-name* is an ASCII string, maximum length 32 printable characters, enclosed in double quotes. The name entered is truncated to 32 characters if it exceeds this limit.

LOCATION *location-name*

Displays the physical location of the access server. The *location-name* is an ASCII string, maximum length 32 printable characters, enclosed in double quotes. The name entered is truncated to 32 characters if it exceeds this limit.

Example: Assigning System Contact

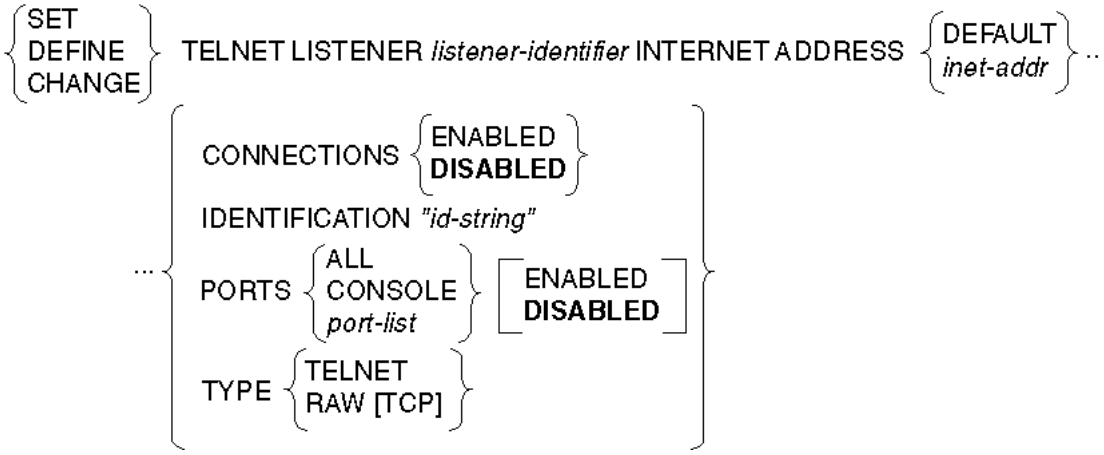
```
Local> SET SYSTEM CONTACT “Larry Koslowski X-5277”
```

This command assigns Larry Koslowski and his phone extension as the system contact.

TELNET LISTENER - USERACCOUNT

TELNET LISTENER (privileged)

Syntax



Description

This privileged command specifies a Telnet listener or Telnet remote console port on the access server. The listener may be associated with one or more physical access server ports or with the remote console virtual port. You can also assign an Internet address to the Telnet listener. The access server can accept connections that specify the TCP port or listener-identifier as a destination.

Keywords

listener-identifier

Identifies the Telnet listener that remote users specify in their connect request. The valid values are 23 (for all access servers), 2001 to 2008 (for an 8-port access server), 2001 to 2016 (for a 16-port server), and 2001 to 2032 (for a 32-port access server). If you do not assign an IP address to the Telnet listener, the value of the *listener-identifier* determines the Telnet listener's port.

inet-addr

Specifies an Internet address in dotted-decimal notation. When you assign an Internet address to the Telnet listener, it accepts connection requests addressed only to TCP port 23 of the specified IP address. If you do not assign an IP address to the Telnet listener, it accepts requests addressed to the access server's IP address. The value of the *listener-identifier* determines the Telnet listener's TCP port.

DEFAULT

Causes the Telnet listener to revert to using the access server's IP address and a TCP port equal to the value of the *listener-identifier*.

CONNECTIONS

Specifies whether the listener is ENABLED or DISABLED to receive connections. Default is DISABLED.

IDENTIFICATION *"id-string"*

A descriptive text string that is associated with the listener for SHOW displays. The default is no *id-string.*

PORTS

Specifies the access server physical ports or the remote console virtual port with which a Telnet listener will be associated. Enabled associates the port(s) with the listener. Disabled dissociates them. The default is DISABLED.

The above defaults apply to *tcp-ports* 2001 and above only. *Tcp-port* 23 has the following defaults:

Identification:	Telnet Console
Console Ports:	Console
Connections:	Enabled

ALL

Associates the listener with all the access server ports.

CONSOLE

Specifies the Telnet remote console port.

port-list

Specifies the access server port number or numbers. For more information on specifying port-list, refer to Chapter 1.

TYPE

Specifies whether the SERVER will be spawned running the Telnet protocol or the TCP RAW protocol.

Restrictions

- CONNECTIONS must be DISABLED before you can SET or CHANGE PORTS.
- You cannot disable Telnet listener ports with active sessions.
- You cannot enable connections to a Telnet listener if the listener is not associated with any access server ports, or if the Internet address has not been set on the access server.
- You cannot specify CONSOLE and physical ports together for a Telnet listener.
- If CONSOLE is already ENABLED when ALL or a port-list is ENABLED, the CONSOLE will be DISABLED.
- When the CONSOLE is enabled, any currently defined physical ports will be DISABLED.

Examples: SET/DEFINE/CHANGE TELNET LISTENER

```
Local> SET TELNET LISTENER 23 CONSOLE ENABLED

Local> SET TELNET LISTENER 23 CONNECTIONS ENABLED
```

These commands enable Telnet listener 23 on the Telnet remote console port. These commands affect the access server operational database.

```
Local> DEFINE TELNET LISTENER 2001 PORTS 1,2

Local> DEFINE TELNET LISTENER 2001 CONNECTIONS ENABLED
```

These commands enable Telnet listener 2001 on access server ports 1 and 2. These commands affect the access server permanent database.

TN3270 ATOE (privileged)

Syntax

{SET / DEFINE / CHANGE} TN3270 ATOE ascii-code {ebcdic-code / DEFAULT}

Description

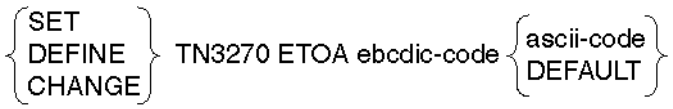
This privileged command allows you to change an ASCII to EBCDIC translation. An ASCII to EBCDIC translation can be reset to the default value using DEFAULT. Codes listed in the following table are the defaults in hexadecimal:

Least Significant Hex Digit (ASCII) Table

Most Significant Hex Digit (ASCII)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	02	03	37	2D	2E	2F	16	05	25	0B	0C	0D	0E	0F
1	10	11	12	13	3C	3D	32	26	18	19	3F	27	1C	1D	1E	1F
2	40	5A	7F	7B	5B	6C	50	7D	4D	5D	5C	4E	6B	60	4B	61
3	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	7A	5E	4C	7E	6E	6F
4	7C	C1	C2	C3	C4	C5	C6	C7	C8	C9	D1	D2	D3	D4	D5	D6
5	D7	D8	D9	E2	E3	E4	E5	E6	E7	E8	E9	3F	E0	3F	5F	6D
6	79	81	82	83	84	85	86	87	88	89	91	92	93	94	95	96
7	97	98	99	A2	A3	A4	A5	A6	A7	A8	A9	C0	4F	D0	A1	07
8	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
9	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
A	3F	6A	4A	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
B	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
C	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
D	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
E	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F
F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	3F	FF

TN3270 ETOA (privileged)

Syntax



Description

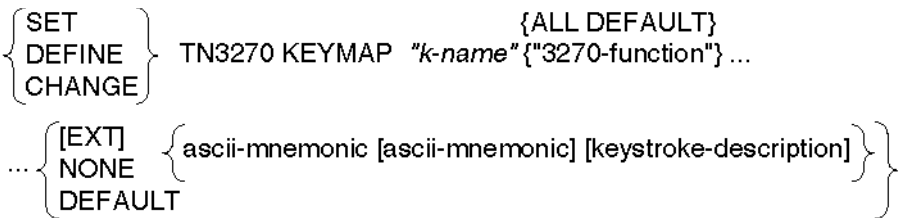
This privileged command allows you to change an EBCDIC to ASCII translation. An EBCDIC to ASCII translation can be reset to the default value using DEFAULT. Codes listed in the following table are the defaults in hexadecimal:

Least Significant Hex Digit (EBCDIC) Table

Most Significant Hex Digit (EBCDIC)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	02	03	26	09	26	7F	26	26	26	0B	0C	0D	0E	0F
1	10	11	12	13	26	0A	08	26	18	19	26	26	1C	1D	1E	1F
2	26	26	26	26	26	0A	17	1B	26	26	26	26	26	05	06	07
3	26	26	16	26	26	26	26	04	26	26	26	26	14	15	26	1A
4	20	26	26	26	26	26	26	26	26	26	A2	2E	3C	28	2B	7C
5	26	26	26	26	26	26	26	26	26	26	21	24	2A	29	3B	5E
6	2D	2F	26	26	26	26	26	26	26	26	A1	2C	25	5F	3E	3F
7	26	26	26	26	26	26	26	26	26	60	3A	23	40	27	3D	22
8	26	61	62	63	64	65	66	67	68	69	26	26	26	26	26	26
9	26	6A	6B	6C	6D	6E	6F	70	71	72	26	26	26	26	26	26
A	26	7E	73	74	75	76	77	78	79	7A	26	26	26	26	26	26
B	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26	26
C	7B	41	42	43	44	45	46	47	48	49	26	26	26	26	26	26
D	7D	4A	4B	4C	4D	4E	4F	50	51	52	26	26	26	26	26	26
E	5C	26	53	54	55	56	57	58	59	5A	26	26	26	26	26	26
F	30	31	32	33	34	35	36	37	38	39	26	26	26	26	26	FF

TN3270 KEYMAP (privileged)

Syntax



Description

This privileged command allows you to redefine a TN3270 function for a customized server keymap. An error will occur if the keymap is predefined. Predefined keymaps are VT100 and VT220.

TN3270-function

Refer to ASCII Code Mnemonics Table for the IBM TN3270-functions.

Keywords

k-name

An existing customized server keymap.

ALL DEFAULT

Changes all previously customized key mappings back to the key mappings for the server-based keymap used at the port (see the SHOW TN3270 KEYMAP command). Note that this option differs from the DEFAULT option discussed below.

EXT

Extends the set of ASCII-code-mnemonics with the use of the definable TN3270 EXT key. Using the EXT key with an ASCII-mnemonic key sequence is similar to using the Shift key with another key on a standard keyboard. The EXT key is any one of the ASCII code mnemonics listed in ASCII Code Mnemonics Table, except 7-Bit ASCII Graphic Codes 21-7E. When EXT is redefined, then all TN3270 functions previously specified with EXT will reflect the new EXT definition.

ascii-code-mnemonic

Any of the ASCII key code mnemonics described in the ASCII Code Mnemonics Table, which represents ASCII character sequences. ASCII key code mnemonics should describe the ASCII keyboard keys for terminal servers VT100 through VT400.

keystroke-description

An optional text description for purposes of describing the keyboard keystrokes on the user's ASCII keyboard. The network access server emulator will then translate the sequence into a TN3270 function.

NONE

Stops any key or keys on the keyboard for that port from mapping to the TN3270 function specified in the command. This could be useful for a manager who wants to disallow a certain TN3270 function for the users.

DEFAULT

Sets the keymap back to the default definition (VT100/VT220) of the defined TN3270 KEYMAP characteristic. Any customized port KEYMAP definitions will be lost.

Restrictions

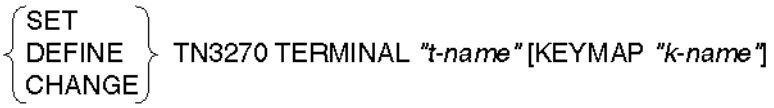
- Only one TN3270 function can be mapped to one Digital key sequence.
- TN3270 functions must have unique Digital key sequences.
- A key sequence cannot be specified for a TN3270 function if it is a subset of an existing key sequence.

Note

If a previously mapped TN3270 function is mapped to another Digital key sequence, the second Digital key sequence replaces the first. A warning message appears if a TN3270 function is mapped to a key already in use. The previously mapped TN3270 function is set to NONE and the new TN3270 function is assigned.

TN3270 TERMINAL (privileged)

Syntax



Description

This privileged command creates a customized TN3270 TERMINAL device in the server-wide database or changes the keymap associated with an existing TN3270 terminal. The TN3270 TERMINAL device is available to any port to be used with the SET PORT TN3270 TERMINAL command.

Keywords

t-name/k-name

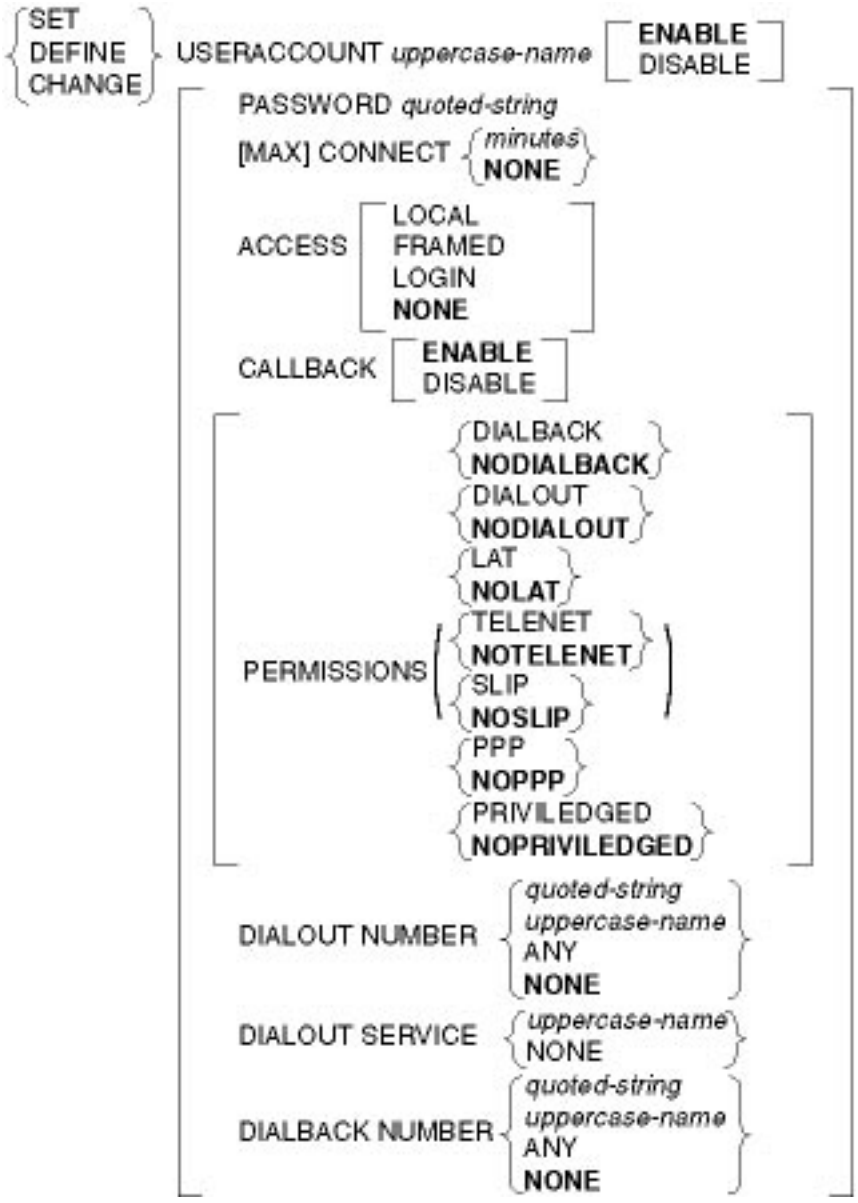
The names of a terminal type and its associated keyboard map (keymap). The names must be unique in the server-wide database. If you do not specify a k-name, the default is VT100. The following are predefined terminal types and cannot be used as customized TERMINAL names: ANSI, VT100, VT220, VT320, and VT420. Both t-name and k-name can be up to 12 characters.

KEYMAP Guidelines:

- VT100 and VT220 are predefined keymaps. If you enter either of these for k-name, the keymap is defined using VT100 or VT220 default keymap definitions.
- When you specify a unique name for k-name to create a new keymap, the keymap is initially defined using the VT100 default keymap definitions. Thereafter, you can customize the new keymap with the SET/DEFINE/CHANGE TN3270 KEYMAP command.
- If an existing customized keymap name is used, the keymap is defined using the functions defined by the keymap specified.
- To modify a VT100 or VT220 default keymap specified for a given TERMINAL, the keymap name must be changed to a customized k-name. VT100 and VT220 cannot be used as keymap names.

USERACCOUNT (privileged)

Syntax



Description

This privileged command allows the security manager to manage a small local database to be used for authentication and authorization. While technically required to prevent lockout of the security manager, it can also be used to support a small office.

The SET/DEFINE/CHANGE command permits entry addition and modification. Individual accounts can be enabled and disabled using the ENABLE or DISABLE keywords.

Multiple characteristics can be entered on the command line.

Keywords

PASSWORD

The PASSWORD clause allows modification of the password field for the specified entry. The maximum length is 40 characters. This field may be case sensitive, depending on which authentication service (protocol) is used. It is case insensitive for the local DECserver user database. To clear the PASSWORD, enter PASSWORD NONE.

ACCOUNT

The ACCOUNT user name has a maximum length of 40 characters.

DIALOUT and DIALBACK

The DIALOUT and DIALBACK NUMBER values have a maximum length of 80 characters, and contain a phone number to be used on dial-back/out. Quotation marks are required. It is expected that “normal” modem-dialing strings will appear here.

DIALOUT SERVICE

The DIALOUT SERVICE is an string with a maximum length of 16 characters that is entered in the command line without quotation marks. It is converted to uppercase.

MAX CONNECT

The MAX CONNECT clause indicates the maximum number of minutes the user can be logged in before being forcibly logged out. The default is no limit, which is indicated by “0” on the display. The range is 0 to 10000. This clause accepts NONE as the keyword, which is equivalent to “0”.

ACCESS

The ACCESS clause specifies the default access mode this user is granted. The supported values are:

LOCAL	Interactive access provided
FRAMED	AUTOLINK (PPP, SLIP) access (only) provided
LOGIN	Dedicated connection (Telnet, LAT) to host (only) provided
NONE	Access determined by realm defaults or port characteristics

PERMISSIONS

The PERMISSIONS clause specifies additional services that the user will be admitted to, typically from the interactive login command language. The supported values are:

DIALBACK	Callback may be invoked, voluntarily, from the current session
DIALOUT	Dialout may be initiated from the current session
LAT	Interactive LAT connection may be initiated
TELNET	Interactive Telnet connection may be initiated
SLIP	Framed SLIP session may be initiated
PPP	Framed PPP session may be initiated
PRIVILEGED	Minimum privilege level will be PRIVILEGED

Parentheses enclose and separate the PERMISSIONS clause from the rest of the command line.

Examples: SET/DEFINE/CHANGE USERACCOUNT

```
Local> SET USERACCOUNT W_JASON PERMISSIONS (LAT TELNET)
```

To disable a permission, add the prefix NO to the keyword.

```
Local> SET USERACCOUNT W_JASON PERMISSIONS (NOLAT)
```

Permissions keywords may be abbreviated; however, if the last keyword in the list is abbreviated, there must be a space between it and the closing parenthesis.

CALLBACK

The CALLBACK clause specifies if mandatory callback is required for this user. The supported values are:

ENABLED	The user must be called back. (If no callback information is available, the user will be denied access.)
DISABLED	The user will not be called back at login time.

An administrator would specify mandatory callback by configuring an account with CALLBACK ENABLED.

DIALBACK NUMBER

The DIALBACK NUMBER is used for Mandatory Dialback as well as for PPP Callback on the same port (where the user is unable to specify a dialback service).

DIALOUT NUMBER

The DIALOUT NUMBER clause, used in interactive dialout commands, specifies the actual number to dial. The keyword ANY specifies that any number may be used. If the DIALOUT number is not fully specified, and it is not contained in the optional DIALOUT SERVICE definition, the dialer engine will prompt the user for the number.

The DIALOUT SERVICE clause specifies a default dialer service to be used when attempting a dial-out connection. The standard rules for service-names apply.

The two NUMBER clauses set default phone numbers, which can be used by any user in the realm. Because the set of permissible characters in phone numbers varies from country to country, the User Interface allows almost all printable characters to be entered on the command line. It is the responsibility of the administrator to configure only meaningful phone numbers. The default is NONE.

There is no requirement for the security administrator to associate every possible field with each local database entry. This feature permits the administrator to configure fewer or more local database records for a given NVRAM allocation.

Chapter 5

SHOW/MONITOR/LIST Commands

Overview

Introduction

This chapter describes the SHOW, MONITOR, and LIST commands.

The **SHOW** command displays current status or information about various options from the access server operational database.

The **MONITOR** command displays continuously updated access server information on various options. Type any character to stop a monitor display. The MONITOR command displays have the same format as the corresponding SHOW command displays, but requires privileged.

The **LIST** command displays information about various options from the permanent database.

Reference

For more information about the commands used in this chapter, refer to the *Network Access Server Management* manual.

Note

To get help at any time with commands, enter a question mark (?) at the prompt or within a command. A list of all the legal keywords or data types you can use at that point in the command will appear.

ACCOUNTING - APPLETALK

ACCOUNTING (secure)

Syntax

Description

This secure command displays the values of the Accounting characteristics.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

ACCOUNTING LOG (privileged)

Syntax

Description

This privileged command displays the accounting log.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

APPLETALK (secure)

Syntax

Description

This secure command displays operational information pertinent to AppleTalk.

Keywords

ARP ENTRY

Displays information for every entry in the operational AppleTalk ARP table.

COUNTERS

Displays all pertinent AppleTalk counters.

ROUTES

Displays each entry in the operational AppleTalk routing table.

STATUS

Displays AppleTalk status information, including the acquired AppleTalk address and NBP name.

Restriction

When you use the MONITOR command, your port type characteristic should be set to ANSI. If the port type characteristic is not set to ANSI, the displayed information scrolls off the screen.

Note

Some displays are longer than one screen and the information may scroll off the screen even if the port type characteristic is set to ANSI.

APPLETALK (secure)

Syntax

{LIST} APPLETALK [CHARACTERISTICS]

Description

This secure command displays the values of the permanent AppleTalk characteristics.

COMMAND GROUP - DIALER SERVICE

COMMAND GROUP

Syntax

Description

This command displays the names of the command groups in the access server database or to display the contents and characteristics of those command groups.

If this command is entered by a privileged user, then all command groups are available for display. Otherwise, only the command groups enabled for the port entering the command are available.

Keywords

cg_name

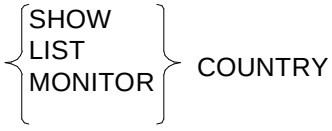
Specifies the name of the command group whose contents are to be displayed. If this parameter is omitted, the access server displays a list of command groups.

ALL

This command option displays the characteristics for all command groups.

COUNTRY

Syntax

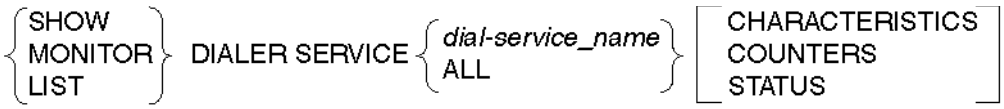


Description

This command displays all of the supported country codes and the current or NVRAM country code setting for the modems in a DECserver 900MC access server.

DIALER SERVICE (nonprivileged)

Syntax



Description

This nonprivileged command produces a display of one or all dialer services. A user on a port with SECURITY enabled would not have access to the STATUS display because it might provide access to unlisted or sensitive phone numbers and other information received from the modem. In the second example below, port 10 is currently available; the last phone number it dialed was found to be busy. Ports 9 and 11 are presently in use. Port 13 is actually dialing a phone number, while port 14 is waiting for a response from the modem. When the dialer port is initialized prior to making a phone call, the Last Connection Status field is cleared.

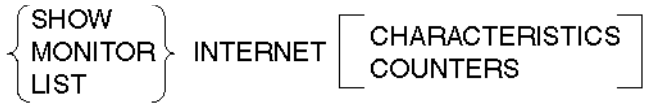
Examples: SHOW/MONITOR/LIST DIALER SERVICE

```
Local> SHOW DIALER AT_TRADESHOW CHAR
Dial Service:       AT_TRADESHOW
Identification:     Dial-back from tradeshow
Connections:        Enabled
Ports:              1,2,9-14
Phone Number:       8-1-508-555-1234
Delay(seconds):     30          Mode:                   PPP
Username:           Smith       Password:              None

Local> SHOW DIALER AT_TRADESHOW STATUS
Dial Service: AT_TRADESHOW - Available

Port      User                Status        Last Connection Status

9          (remote)            Connected       CONNECTED 14400/LAPM
10        Available        BUSY
11          Janice Decserver   Connected             CONNECTED 9600
12                             Available                  NO ANSWER
13         Jim                Dialing                         N
14        Elle Presidente    Waiting

Local> SHOW DIALER AT_TRADESHOW COUNTERS
Dial Service:                    AT_TRADESHOW
Seconds Since Zeroed:  1989692   Failures:                17
Connections Attempted: 113       Busy:                    10
Connections Completed: 96        No Answer:                0
                                 No Response:              0
                                 Authentication:           7
```

INTERNET - INTERNET HOST

INTERNET (secure)

Syntax



Description

This command (available to all users) displays information in the access server Internet database.

Keywords

CHARACTERISTICS

Displays the current settings of the user-definable parameters associated with the Internet protocol, for example, Internet address. This display also shares the current status of DHCP and TCP keepalive features. This is the default display.

COUNTERS

Displays the current values of the different counters associated with the Internet protocol.

Restrictions

- MONITOR is a privileged command.
- COUNTERS is invalid with the LIST command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Examples: SHOW/MONITOR/LIST INTERNET

```
Local> SHOW INTERNET COUNTERS
```

This command displays current values of the different counters associated with the Internet protocol in the operational database.

```
Local> SHOW INTERNET CHARACTERISTICS
```

This command displays current settings of the user-definable parameters associated with Internet protocol in the operational database.

INTERNET ARP ENTRY (secure)

Syntax

Description

This command (available to all users) displays ARP entries in the access server ARP database.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Example: SHOW/MONITOR/LIST INTERNET ARP ENTRY

```
Local> SHOW INTERNET ARP ENTRY
```

This command displays all Internet ARP entries in the operational database.

INTERNET GATEWAY (secure)

Syntax

Description

This command (available to all users) displays the Internet gateways known to the access server and the networks and hosts that the user can access.

Restrictions

- You cannot use INTERNET GATEWAY if the PORT LIMITED VIEW characteristic is ENABLED.
- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

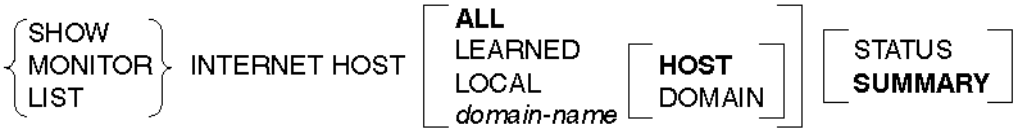
Example: SHOW/MONITOR/LIST INTERNET GATEWAY

```
Local> SHOW INTERNET GATEWAY
```

This command displays all current gateways in the operational database, along with the corresponding networks, associated subnet masks, and hosts that the user can access.

INTERNET HOST (secure)

Syntax



Description

This command (available to all users) displays information about the access server Internet domain name system (DNS) database entries.

Keywords

ALL

Specifies that all hosts in the DNS cache will be shown. This is the default.

LEARNED

Specifies that only hosts that the access server has learned about will be shown.

LOCAL

Specifies that only hosts defined locally at the access server will be shown.

domain-name

Specifies the domain name of a host or of a domain.

HOST

Identifies the *domain-name* as a domain name for the host. The domain name for a host can be an absolute or a relative name. If a relative name is specified, the default local domain will be automatically appended to the host name. If the HOST option is specified, only the specified host will be displayed. This is the default. This option is valid only when specifying a *domain-name.*

DOMAIN

Identifies the *domain-name* as a specific domain name for a particular domain. The domain name for a domain must be an absolute name. If the DOMAIN option is specified, all the hosts with the specified domain and its subdomains will be displayed. This option is valid only when specifying a *domain-name*.

STATUS

Specifies the time-to-live (TTL) numbers for each host shown.

SUMMARY

Displays a summary of information about the host. This is the default.

Restrictions

- MONITOR is a privileged command.
- LEARNED and STATUS are not valid with the LIST command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Examples: SHOW/MONITOR/LIST INTERNET HOST

```
Local> SHOW INTERNET HOST LOCAL
```

This command displays all current hosts defined locally in the access server operational database.

```
Local> LIST INTERNET HOST ALL
```

This command displays all hosts defined in the access server permanent database.

INTERNET NAME RESOLUTION - MEMORY

INTERNET NAME RESOLUTION (secure)

Syntax

Description

This command (available to all users) displays the information in the access server WINS (Windows Internet Naming Service) and DNS (domain name system) databases.

When you enter this command, the access server displays its WINS servers and the name servers (both locally configured and learned) that serve the current default domain of the access server. If you change the value of the default domain, the SHOW INTERNET NAME RESOLUTION command will display different DNS name servers. Note that the WINS server information remains the same.

Keywords

CHARACTERISTICS

Displays the current settings of the parameters associated with the access server DNS module, including domain name, query time limit, resolution timeout, host limit, and name servers. The display also indicates if a DHCP server provided the WINS servers and domain name information, and the Internet address of the DHCP server. This is the default.

COUNTERS

Displays the current values of the different counters associated with the access server DNS module.

Restrictions

- MONITOR is a privileged command.
- COUNTERS is invalid for the LIST command.
- Secure users cannot execute the LIST command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

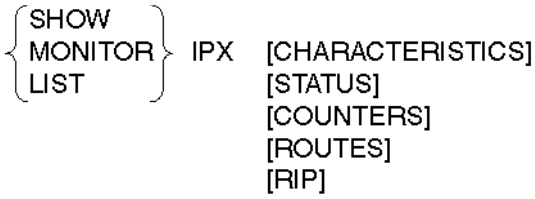
Example: SHOW/MONITOR/LIST INTERNET NAME RESOLUTION

```
Local> LIST INTERNET NAME RESOLUTION
```

This command displays current values of the user-definable parameters in the permanent database associated with the access server DNS module.

IPX (secure)

Syntax



Description

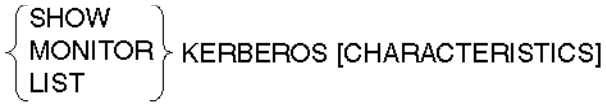
LIST CHARACTERISTICS displays IPX data from the permanent database. All other IPX commands display current IPX values and status.

If the optional parameters (CHARACTERISTICS, STATUS, COUNTERS, and ROUTES) are not specified, only CHARACTERISTICS and STATUS are displayed.

RIP shows all unique Netware networks currently known by the server. ROUTES shows all the routes to network addresses on the serial lines and LAN currently known by the server.

KERBEROS CHARACTERISTICS (nonprivileged)

Syntax



Description

This nonprivileged command shows all the current settings for Kerberos.

Note

If a realm has no explicitly specified domain, the realm name itself will be used as an implied domain.

Restriction

LIMITED VIEW ENABLED ports will be prohibited from this display.

Example: SHOW/MONITOR/LIST KERBEROS CHARACTERISTICS

The following command displays all current Kerberos characteristics defined locally in the access server operational database:

```
Local> SHOW KERBEROS CHAR
```

MENU

Syntax

Description

If this command is entered by a privileged user, then all menus are available for display. Otherwise, only the menus enabled for the port entering the command are available.

In response to this command, the server will either display the names of all of the menus that have been defined or it will display the definition of the specified menus.

Keywords

ALL

This command option will display the characteristics for all menus.

MEMORY (secure)

Syntax

Description

This secure command displays information about the access server memory.

Keywords

CONFIGURATION

Displays the size of memory installed on the access server and the functional status of Flash RAM. CONFIGURATION is the default.

STATUS

Displays the amount of memory available and the percentage of memory in use.

Example: SHOW/MONITOR MEMORY

```
Local> SHOW MEMORY CONFIGURATION
```

This command displays the size of memory and the functional status of Flash RAM.

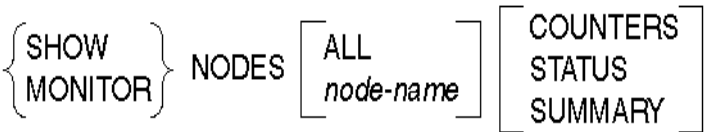
Note

If Flash RAM is installed, but its boot block is invalid, then the total memory size will be displayed as zero.

NODES - PORT AUTHORIZATION [STATUS]

NODES (secure)

Syntax



Description

This command displays information about LAT service nodes known to the access server.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

For nonprivileged users, the access server displays only those nodes that have at least one of the groups currently selected on the port (as defined by the GROUPS port characteristic). Privileged users can specify ALL to display all nodes in the access server database or a specified node regardless of whether the nodes are included in the port's current group selection. Nodes have Reachable or Unreachable status, depending on whether or not they currently accept connections from access server ports.

For users with Limited View, nothing is displayed.

Keywords

ALL

Displays information for all authorized service nodes currently selected on the port that have the status Reachable, Unknown, or Unreachable. If you do not specify ALL, the default display includes only currently selected nodes that are Reachable or Unknown.

node-name

Specifies a service node for which information is displayed.

COUNTERS

Displays current counter values for the specified node(s).

STATUS

Displays full information about the specified node(s), including name, address, identification string, enabled group codes, and services. This is the default display when you specify a node name.

SUMMARY

Displays a one-line summary of information for the specified node(s), including node name, status, and identification string. This is the default display when you do not specify a node name.

Restrictions

- MONITOR is a privileged command.
- The SHOW NODES command is not available to ports if the LIMITED VIEW port characteristic is enabled and if the port is not privileged.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Examples: SHOW/LIST NODES

```
Local> SHOW NODES ALL
```

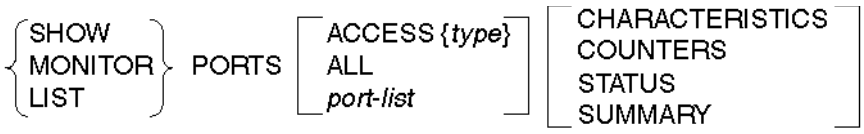
This command produces a one-line summary of information from the operational database about each service node that has the status Reachable, Unreachable, or Unknown.

```
Local> SHOW NODE SALES_1
```

This command generates a display of status information from the operational database for node SALES_1.

PORTS (secure)

Syntax



Description

This command (available to all users) displays information about access server ports. This information includes the characteristics that you assign with the SET/DEFINE/CHANGE PORT commands.

Reference

For a detailed description of the displays, refer the to *Network Access Server Management* manual.

Keywords

ACCESS {*type*}

Specifies that information is displayed for those ports only with ACCESS set to the type you choose (LOCAL, REMOTE, DYNAMIC, NONE). ACCESS is a port characteristic specified with the SET/DEFINE/CHANGE PORT command.

ALL

Specifies that information for all ports is displayed.

port-list

Specifies one or more ports for which information is displayed (default: the port you are using). For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

CHARACTERISTICS

Displays characteristics that can be set for the specified port. This is the default when you specify no port, one port, or a port list.

COUNTERS

Displays current counter values for the specified port.

STATUS

Displays current port status for the specified port.

SUMMARY

Displays a one-line summary of information for the specified port, including port number, accessibility, status, and local services. This is the default when you specify ALL or ACCESS.

Restrictions

- MONITOR is a privileged command.
- Users on secure ports cannot include port designations (*port-list*, ALL, and ACCESS) in these commands.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Examples: SHOW/LIST/MONITOR PORTS

```
Local> SHOW PORT ACCESS REMOTE SUMMARY
```

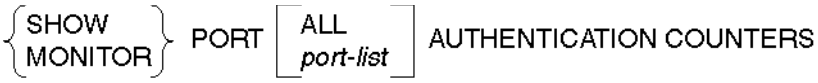
This command displays a one-line summary of information for each access server port that has its ACCESS characteristic set to REMOTE.

```
Local> SHOW PORTS ALL
```

This command displays a summary, from the operational database, for all the ports on the access server.

PORT AUTHENTICATION COUNTERS (nonprivileged)

Syntax



Description

This privileged command shows all the current and cumulative port counters for Kerberos authentication events.

Restrictions

- The LIST command is disallowed for counters.
- Secure users may show counters for their own port only.

Example: SHOW/MONITOR PORT AUTHENTICATION COUNTERS

```
Local> SHOW PORT 1 AUTHENTICATION COUNTERS
```

PORT AUTHORIZATION [STATUS] (nonprivileged)

Syntax

Description

This command shows the user profile being used for the specified ports. This command displays information only when the port is already logged in.

The following example shows the port authorization status display.

Restrictions

Nonprivileged users may show authorization status for their own port only.

Example: SHOW/MONITOR PORT AUTHORIZATION [STATUS]

```
Local> SHOW PORT AUTHORIZATION STATUS
Port 7:               d_jones           Server:              DECSERVER1

  Username:             d_jones@finance.acme.com
  Access:               INTERACTIVE      Forced CallBack:        DISABLED
  Max Connect Time:     00 08:00:00      Dialout Service:       DIAL14400
  Remaining Time:       00 00:33:24      Framed IP Address:   16.22.33.44
  Login IP Host:        16.20.22.33      Login LAT Service:    LATSERVICE
  Login Service Type:   LAT Login        Port:                         15
  Authenticated By:     16.129.42.15     Authentication Type:      RADIUS
  Login LAT Node:       MONEY
  DialBack Number:      1-802-767-8345
  DialOut Number:       (Any)
  Login LAT Groups:     2,5,66-68,133,135,139,172,206,230-250
  Permissions:          LAT, TELNET, SLIP, PPP,
                        DIALACK, DIALOUT,NONPRIVILEGED
```

PORT PPP - PORT SECURITY COUNTERS

PORT PPP (secure)

Syntax

SHOW PORT PPP [ALL | *port-list*] [COUNTERS | STATUS]

Description

These commands display the PPP counters and status.

Keywords

ALL

Specifies that information for all ports is displayed.

port-list

Specifies one or more ports for which information is displayed (default: the port you are using). For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

COUNTERS

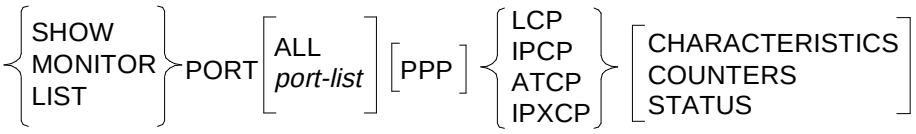
Displays information about all the COUNTERS relevant to the PPP protocol operation.

STATUS

Displays information about the state of the PPP implementation in the access server.

PORT PPP LCP/IPCP/ATCP/IPXCP (secure)

Syntax



Description

These secure commands display information associated with PPP LCP, IPCP, ATCP, or IPXCP ports from the access server database.

Keywords

ALL

Specifies that information for all ports is displayed.

port-list

Specifies one or more ports for which information is displayed (default: the port you are using). For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

CHARACTERISTICS

Displays current values for port PPP LCP, IPCP, ATCP, or IPXCP characteristics. The command displays characteristics for the specified port, which may include name, identification string, restart timer time, maximum transmissions failure, charter mask, as well as additional characteristics. The information displayed includes the latest values configured by the SET PORT *n* PPP LCP/IPCP/ATCP/IPXCP command. Use the SHOW/MONITOR PORT *n* PPP LCP/IPCP/ATCP/IPXCP STATUS command to see the values actually being used by the link.

COUNTERS

Displays information about all the COUNTERS relevant to the LCP, IPCP, ATCP, or IPXCP protocol operation. The command is normally used as a diagnostic aid. The CONNECT and DISCONNECT commands zero each of these counters.

STATUS

Displays information about the state of the LCP, IPCP, ATCP, or IPXCP implementation in the access server. Because of the nature of PPP negotiations, this can be different than the configured characteristics shown with the SHOW PORT *n* PPP LCP/IPCP/ATCP/IPXCP CHARACTERISTICS display. The command will display information in two field categories. The first category is general link status and the second is status of each of the LCP, IPCP, ATCP, or IPXCP options.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.
- Secure users can specify their own port only.

PORT SECURITY COUNTERS (nonprivileged)

Syntax

Description

This command displays all port-related security counters. The display is very similar to the one that results from the existing SHOW PORT AUTHENTICATION COUNT command. The existing display will also be updated to include port authorization counters.

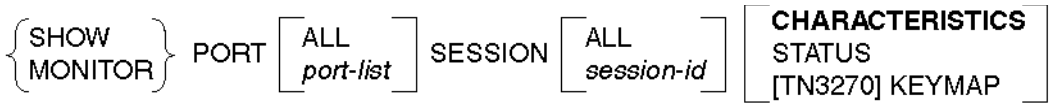
Example: SHOW/MONITOR PORT SECURITY COUNTERS

```
Local> SHOW PORT SECURITY COUNTERS

Port 1: admiral_nelson    Server:                    DECSERVER1

                         Cur login    Cur login    Total       Total
                       attempts:    failures:    attempts:   Failures:

User authentication:        1234         1234         1234         0

RADIUS Silent Discards:                      0
SecurID Silent Discards:                     0
                      Total auth    Total auth      Current      Total
                    received:     defaults:      failures:    failures:
User authorization:   1234          34567          567890       567890
Time since last user authentication success:                    never
Time since last user authentication failure:                    never
Time since last user authorization failure:                     never
Time since counters last zeroed:                          37 01:59:31
```

PORT SESSION - PORT SESSION TN3270 KEYMAP

PORT SESSION (secure)

Syntax



Description

This command (available to all users) displays information from the operational database for one or all sessions on the access server. Unlike the SHOW/MONITOR SESSIONS command that displays all sessions only, this command can display one session at a time.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Keywords

PORT ALL

Displays sessions for all ports on the access server.

PORT *port-list*

Displays sessions for the specified port. The default displays sessions for your current port.

SESSION ALL

Displays all sessions for the specified ports.

SESSION *session-id*

Identifies the session number to be displayed for the specified port. The current session is the default if none is specified.

CHARACTERISTICS

Displays the current settings for session characteristics. This is the default.

STATUS

Displays the current session status.

For the SHOW PORT SESSION command, the field will display the port setting read from dynamic memory at the time the Telnet connection was initiated. This may or may not be the same as the final terminal type negotiated between the host and the client. The SHOW PORT SESSION STATUS command shows the results of the negotiation.

TN3270 KEYMAP

Allows the user to display a current TN3270 session keymap. Refer to the PORT SESSION TN3270 KEYMAP (secure) command for more information.

Restrictions

- MONITOR is a privileged command.
- Secure users cannot specify SESSION ALL or reference a port other than their own.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.

Example: SHOW/MONITOR PORT SESSION

```
Local> SHOW PORT 1 SESSION ALL STATUS

Port 1, session 1, Protocol Ping
(no status information available for PING sessions)

Port 1, session 2, Protocol TELNET
Do-Binary                                          Disabled
Will-Binary                                        Disabled
Do-Echo                                            Disabled
Will-Echo                                           Enabled
Do-SGA                                             Disabled
Will-SGA                                            Enabled
Do-Status                                           Enabled
Will-Status                                        Disabled
Do-End of Record                                   Disabled
Will-End of Record                                 Disabled
Do-Remote Flow Control                             Disabled
Will-Remote Flow Control                           Disabled
Will-Terminal Type             Enabled               UNKNOWN

Port 1, session 3, Protocol LAT
(no status information available for LAT sessions)

Port 1, session 4, Protocol TN3270
Do-Binary                                          Disabled
Will-Binary                                        Disabled
Do-Echo                                            Disabled
Will-Echo                                           Enabled
Do-SGA                                             Disabled
Will-SGA                                            Enabled
Do-Status                                           Enabled
Will-Status                                        Disabled
Do-End of Record                                   Disabled
Will-End of Record                                 Disabled
Do-Remote Flow Control                             Disabled
Will-Remote Flow Control                           Disabled
Will-Terminal Type             Enabled           IBM-3278-2
```

```
Local> SHOW PORT SESSION STATUS

Remote Console, Session 1, Protocol TELNET
Do-Binary                                          Disabled
Will-Binary                                        Disabled
Do-Echo                                             Enabled
Will-Echo                                          Disabled
Do-SGA                                             Enabled
Will-SGA                                            Enabled
Do-Status                                          Disabled
Will-Status                                        Disabled
Do-End of Record                                   Disabled
Will-End of Record                                 Disabled
Do-Remote Flow Control                             Disabled
Will-Remote Flow Control                           Disabled
Will-Terminal Type         Enabled                DEC-VT100

Local>
```

In this example, the command displays the status of all the current sessions on port 1.

Reference

Refer to the SHOW PORT SESSIONS command in the *Network Access Server Management* manual for more information.

Note

The terminal type displayed in the Will-Terminal Type field is different than the type displayed via the SHOW PORT SESSION command. This is the result of having negotiated for a mutually acceptable terminal.

PORT SESSION TN3270 KEYMAP (secure)

Syntax

Description

This command (available to all users) allows you to display a current TN3270 session keymap.

Note

Changes to a port's keymappings do not affect an established session's keymappings.

Keywords

PORT ALL

Specifies that the information for all ports session keymap be displayed.

PORT *port-list*

Displays sessions for the specified port (default: displays sessions for your current port).

SESSION *session-id*

Identifies the session number to be displayed for the specified port. The current session is the default if none is specified.

SESSION ALL

Displays all sessions for the specified ports.

The display is similar to the SHOW PORT TN3270 KEYMAP display except that the EXTend ASCII mnemonic definition represented by EXT is displayed in the session keymap display, not as EXT but as the ASCII mnemonic it represents. If model 2 is entered using the SET PORT TN3270 MODEL command, both the EXIT and HELP keys will operate as follows:

- The EXIT key aborts and disconnects the TN3270 session.
- The “hot-key” HELP displays a short form of the SHOW PORT SESSION TN3270 KEYMAP display.

Refer to the IBM 3270 documentation for an explanation of the IBM function keys.

Example: SHOW PORT SESSION TN3270 KEYMAP

```
Local> SHOW PORT 1 SESSION 1 TN3270 KEYMAP

PORT 1, SESSION 1, Protocol TN3270 KEYMAP
```

TN3270 Function	ASCII Mnemonic	Keystroke Description
BACKTAB	F12	" "
CENT	KPDOTC	" "
CLEAR	KPDOT F20	" "
CURSUP	UPARROW	" "
CURSDOWN	DOWNARROW	" "
CURSLEFT	LEFTARROW	" "

PORT SESSION - PORT SESSION TN3270 KEYMAP

TN3270 Function	ASCII Mnemonic	Keystroke Description
CURSRIGHT	RIGHTARROW	" "
DELETE	DELETE	" "
DUP	KPDOT F12	" "
ENTER	ENTER	" "
ERASEEOF	F18	" "
ERASEINP	KPDOT F18	" "
EXIT	CTRL/Z KP	" "
EXT	DOT	" "
FIELDMARK	KPDOT F13	" "
HELP	F15 (HELP)	" "
HOME	F13	" "
INSERT	F14	" "
NEWLINE	RETURN	" "
NOT	KPDOT N	" "
NUMOVR	REMOVE	" "
OR	KPDOT O	" "
PA1	PF4	" "
PA2	KPMINUS	" "
PA3	KPCOMMA	" "
PF1	PF1	" "
PF2	PF2	" "
PF3	PF3	" "
PF4	KP7	" "
PF5	KP8	" "
PF6	KP9	" "

TN3270 Function	ASCII Mnemonic	Keystroke Description
PF7	KP4	" "
PF8	KP5	" "
PF9	KP6	" "
PF10	KP1	" "
PF11	KP2	" "
PF12	KP3	" "
PF13	KPDOT PF1	" "
PF14	KPDOT PF2	" "
PF15	KPDOT PF3	" "
PF16	KPDOT KP7	" "
PF17	KPDOT KP8	" "
PF18	KPDOT KP9	" "
PF19	KPDOT KP4	" "
PF20	KPDOT KP5	" "
PF21	KPDOT KP6	" "
PF22	KPDOT KP1	" "
PF23	KPDOT KP2	" "
PF24	KPDOT KP3	" "

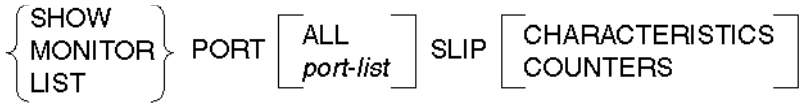
Restrictions

- Entering this command for a non-TN3270 session results in an error message.
- This command does not support LIST commands.
- User needs privileged status to show keymaps for other ports.
- For undefined keymaps, the ASCII mnemonic column will be blank.
- IBM applications requiring display stations that have screens other than 24x80 are not supported.

PORT SLIP - PORT TN3270 KEYMAP

PORT SLIP (secure)

Syntax



Description

These commands display information associated with SLIP ports from the access server database. This information includes the characteristics that you assign with the SET/DEFINE/CHANGE PORT SLIP command. For a detailed description of the displays, refer to the Network Access Server Management manual.

Specifying ALL or *port-list* may require privilege.

Keywords

ALL

Specifies that information for all ports is displayed.

port-list

Specifies one or more ports for which information is displayed (default: the port you are using). For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

CHARACTERISTICS

Displays current values for port SLIP characteristics. This is the default.

COUNTERS

Displays current counter values for the specified port.

Restrictions

- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, the displayed information will scroll off the screen.
- Secure users can specify their own port only.

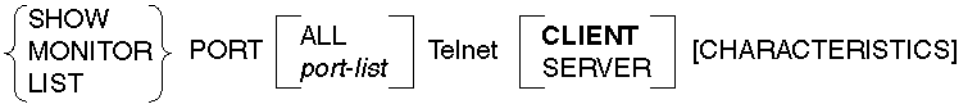
Example: SHOW/LIST/MONITOR PORT SLIP

```
Local> SHOW PORTS ALL SLIP
```

This command displays all characteristics of SLIP-specific ports in the operational database.

PORT TELNET (secure)

Syntax



Description

This command (available to all users) displays information associated with Telnet ports from the access server database.

Keywords

ALL

Displays the Telnet database for all access server ports.

port-list

Specifies which access server port number will be displayed for the Telnet database. The default is the port you are using. For more information on specifying *port-list*, refer to Chapter 1 for examples and conventions.

TELNET

Displays only the Telnet characteristics of the access server port database.

CLIENT

Displays Telnet client characteristics. This is the default.

For the SHOW PORT TELNET CLIENT command, this field will display the current port setting as read from dynamic memory. For the LIST PORT TELNET CLIENT command, the field will display the value stored in NVRAM.

This change also adds a new field to the {SHOW | LIST} PORT TELNET CLIENT and SHOW PORT SESSION commands. The new display looks like:

```
Profile: Character
Echo:             Remote      Newline From Term:     <CR>
Toggle Echo:       ^E         Newline From Host:   <CRLF>
Binary:           Disabled     Newline To Term:    <CRLF>
Xmit Char Size:    8           Newline To Host:    <CRLF>
Rcv Char Size:     8          Input Flow Control:  Enabled
Signal Req:       Enabled     Output Flow Control: Enabled
IP:               +s +f ^Y     Verification:       Enabled
SYNCH:            +s -f ^X    Switch Character:    Enabled
AYT:               -s -f ^T     Quote:                None
AO:               -s +f ^O     Terminal Type:        VT110
EOR:                -s -f None
BRK:                -s -f None
```

The user's selected terminal type is displayed in the Terminal Type field.

SERVER

Displays Telnet server characteristics.

CHARACTERISTICS

Displays the current port parameters associated with Telnet.

Restrictions

- The port-list characteristic is available on privileged ports only.
- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

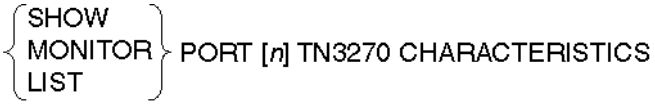
Example: SHOW/MONITOR/LIST PORT TELNET

```
Local> SHOW PORT ALL TELNET
```

This command displays Telnet client characteristics for all access server Telnet ports.

PORT TN3270 CHARACTERISTICS (secure)

Syntax



Description

This command displays current values for TN3270 port characteristics. This includes the characteristics that you assign with the SET/DEFINE/CHANGE PORT TN3270 command.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

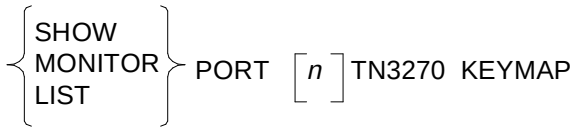
Example: SHOW/MONITOR/LIST PORT TN3270 CHARACTERISTICS

```
Local> SHOW PORT 1 TN3270 CHARACTERISTICS
```

This command displays the port characteristics for port 1 on the access server.

PORT TN3270 KEYMAP (secure)

Syntax



Description

This command displays to the user the ASCII character sequences and keystroke descriptions used for 3270 functions.

The following command displays the default keymap. The ASCII code mnemonic represents the ASCII character sequence expected to be received at the port that represents the 3270 function. The keystroke description is an optional text description of the user's keyboard key(s) to be used to produce the ASCII character sequence.

Restriction

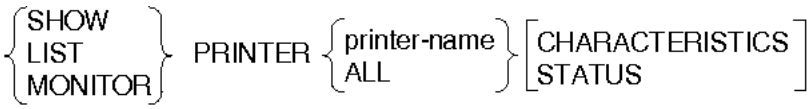
Only a privileged user can view the keymap for another port.

Example: SHOW/MONITOR/LIST PORT TN3270 KEYMAP

```
Local> SHOW PORT 1 TN3270 KEYMAP
```

PRINTER

Syntax



Description

This command displays characteristics of a specific printer or all printers configured on the access server.

Keywords

printer-name

Displays characteristics for the specified printer.

ALL

Displays characteristics for all configured printers.

Example: SHOW/MONITOR/LIST PRINTER

```
Local> SHOW PRINTER ALL
Printer:             LPS32_PS         Header Page:      Enabled
Connections:         Enabled       Trailer Page:       Optional
Flag Page Type:      Postscript         Auto C/R:      Disabled
Identification:      The PostScript Printer
Flag Page Note:      LPS32_PS - For PostScript Files Only
Ports:               6, 7

Printer              LPS32_ASCII       Header Page:      Enabled
Connections:         Enabled          Trailer Page:     Disabled
Flag Page Type:      Postscript           Auto C/R:     Disabled
Identification:      The Text Printer
Flag Page Note:      LPS32_ASCII - For Text Files Only
Ports:               8

Local>
```

QUEUE - SECURITY SUMMARY

QUEUE (nonprivileged)

Syntax

Description

This nonprivileged command displays information about entries in the LAT access server queue. The MONITOR command provides a continuous display that is updated as changes are made.

Reference

For a detailed description of the displays, refer to the Network Access Server Management manual.

Keywords

ALL

Displays information for all LAT queue entries on the access server. ALL is the default display selection.

NODE *node-name*

Displays information for all LAT queue entries requested by the specified LAT node.

PORT *port-number*

Displays information for all LAT queue entries that could be served by the specified port.

SERVICE *service-name*

Displays information for all LAT queue service-name entries for the specified service.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

Example: SHOW/MONITOR QUEUE

```
Local> SHOW QUEUE NODE NELSON
```

RADIUS/SERVER REALM/KERBEROS CHARACTERISTICS (nonprivileged)

Syntax

Description

This command shows the various realms of the specified type that are configured for the access server; it is a privileged command.

Note

The Server Realm is the realm for User Accounts. You must enter the keyword REALM because SHOW SERVER is an entirely different command.

Example: SHOW RADIUS

```
Local> SHOW RADIUS
Retransmit Interval:      0:00:01        Retransmit TimeOut:     00:00:20
Ticket Service Port:      1645           Service Port:               1646

Realm:                    XXX.YYY.XXX.COM
  Realm Inclusion:        NOINCLUDE
  Prompt:                 (None)
  Secret:                 (Entered)
  Authentication Host:    16.20.55.66
  Accounting Host:        radius.host.somewhere
  Authorization Defaults:
    Access:           (None)             Forced Callback:        DISABLED
    Max Connect:      00 08:00:00        Dialout Service:       DIAL14400
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT, TELNET, DIALBACK
```

Example: SHOW SECURID

```
Local> SHOW SECURID
Retransmit Interval:  00:00:02    Retransmit TimeOut:  00:00:20
                                  Service Port:             755

Realm:                AAA.BBB.CCC.COM
  Realm Inclusion:    NOINCLUDE   Encoding Format:          DES
  Prompt:             Enter Passcode>
    Secret:           Entered)
    Primary Host:     16.20.55.66
    Authorization Defaults:
    Access:           LOGIN        Forced Callback:    DISABLED
    Max Connect:      00 08:00:00  DialOut Service:   DIAL28800
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT, TELNET, SLIP, PPP
```

Example: SHOW SERVER REALM

```
Local> SHOW SERVER REALM

Realm:                local.NAS
  Max Fails:          3
  Authorization Defaults:
    Access:           LOGIN       Forced Callback:    DISABLED
    Max Connect:      00 08:00:00 DialOut Service:    DIAL9600
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT
```

Example: SHOW KERBEROS

```
Local> SHOW KERBEROS

Retransmit Interval:  00:00:01    Retransmit TimeOut:  00:00:20
Ticket service port:       750    Service Port:             751

Default Realm:        33H.LKG.DEC.COM
 Secret:              (None)
 Primary Host:        prowlr.lkg.dec.com
 Master Host:         ds900.lkg.dec.com
 Host:                foo.bar.dec.com
 Authorization Defaults:
    Access:           LOGIN        Forced Callback:    DISABLED
    Max Connect:      00 08:00:00  DialOut Service:   DIAL14400
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT, TELNET, SLIP, PPP, DIALBACK, DIALOUT

Realm:                kerberos.realm.somewhere
 Secret:              (Entered)
 Host:                foo.bar.dec.com
 Authorization Defaults:
    Access:           INTERACTIVE  Forced CallBack:    DISABLED
    Max Connect:      00 08:00:00  DialOut Service:    DIAL9600
    DialBack Number:  555-1234
    DialOut Number:   (Any)
    Permissions:      LAT, TELNET, SLIP, PPP, DIALBACK
```

SECURITY CHARACTERISTICS (nonprivileged)

Syntax

Description

The SHOW SECURITY command will display all configured realms, plus the number of free logout warnings and the warning interval for users who are assigned a MAX Connect Time, as well as any pertinent configuration parameters. This command is privileged. This will show the various authentication servers that are configured for each realm as well as the Kerberos KDCs. It will also show the existing local server security database.

SECURITY COUNTERS (nonprivileged)

Syntax

Description

This command will cause the access server to display the counters for all realms (server, RADIUS, KERBEROS). The existing SHOW AUTHENTICATION COUNTERS command will also show this new display. This is a nonprivileged command.

Example: SHOW SECURITY COUNTERS

```
Local> SHOW SECURITY COUNTERS
                                    Total         Total       Total
                                    attempts      failures    Errors
User authentication (all realms):     11            3           0

                                    Total         Valid       Error
                                    Packets       Packets     Packets
                                    Sent          Received    Received
Realm: 33H.LKG.DEC.COM                 0             0           0
Realm: XXX.YYY.XXX.COM                 1             1           0
Realm: AAA.BBB.CCC.COM                10             9           1
Realm: kerberos.realm.somewhere        0             0           0
Realm: local.NAS                       0             0           0
Time since counters last zeroed:                          37 01:57:45
```

SECURITY SUMMARY (privileged)

Syntax

Description

This command displays the logout warning parameters and the names of all the currently configured security realms, but does not show any details. It is privileged.

Example: SHOW SECURITY SUMMARY

```
Local> SHOW SECURITY SUMMARY
Logout Warning ------------------------------------------------
Interval:             2
Times:               30
Kerberos ------------------------------------------------------
Default Realm: 33H.LKG.DEC.COM   Realm: Kerberos.realm.somewhere
RADIUS --------------------------------------------------------
Realm:         XXX.YYY.XXX.COM
SecurID-------------------------------------------------------
Realm:         XXX.YYY.XXX.COM
Server --------------------------------------------------------
Realm:         local.NAS
```

SERVER - SESSIONS

SERVER (nonprivileged)

Syntax

Description

This nonprivileged command displays service information about the access server. For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Keywords

CHARACTERISTICS

Displays definable characteristics for the access server, including a list of LAT group codes groups offered by the access server (as specified by the SET/DEFINE/CHANGE server SERVICE GROUPS command). This is the default display type.

COUNTERS

Displays current Ethernet data link protocol and LAT protocol counter values for the access server.

STATUS

Displays status information for the access server.

SUMMARY

Displays a summary of information for the access server, including name, address, identification string, and a summary of all groups currently selected by all ports on the access server.

Restrictions

- MONITOR is a privileged command.
- COUNTERS and STATUS are not valid with the LIST command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

Example: SHOW SERVER COUNTERS

```
Local> SHOW SERVER COUNTERS
```

This command displays the access server counters from the operational database.

SERVER AUTHENTICATION COUNTERS (nonprivileged)

Syntax

Description

This command shows all the current access server counters for the security features.

Restrictions

- The LIST command is not allowed for counters.
- LIMITED VIEW ENABLED ports will be prohibited from this display.

Example: SHOW SERVER AUTHENTICATION COUNTERS

```
Local> SHO SERVER AUTHEN COUNT
```

SERVICES (secure)

Syntax

Description

This command (available to all users) displays information about LAT services that you can connect to.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Keywords

ALL

Displays information for all LAT services (whether available or unavailable) in the database that match your current group codes. Privileged users refer to all LAT services in the database. ALL is the default selection displayed on SHOW commands. However, if you do not specify ALL in the command, the access server displays only the available LAT services.

LOCAL

Displays information for all LAT services (whether available or unavailable) offered by the local access server that match your current group codes. LOCAL is functional only in SHOW and MONITOR commands because LIST commands display only local node LAT services.

service-name

Displays information for the specified services, provided they are included in your current group codes. If you do not specify a service name or LOCAL, the access server displays all LAT services that match your current group codes.

CHARACTERISTICS

Displays definable characteristics for the specified local services, including name, identification string, and ports. For remote LAT services, only the name and identification string are displayed.

STATUS

Displays information about the specified services, including node names and status, rating, and identification string. This is the default when you specify a service name.

SUMMARY

Displays a one-line summary of information for the specified services, including name, status, and identification. This is the default when you do not specify a service name.

Restrictions

- MONITOR is a privileged command.
- The SHOW SERVICES command is not available if the LIMITED VIEW port characteristic is enabled.
- ALL, STATUS, and SUMMARY are not valid for the LIST SERVICES command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

Examples: SHOW SERVICE

```
Local> SHOW SERVICE DEVELOP
```

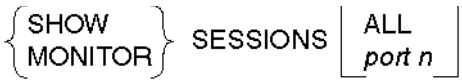
This command displays status information about service DEVELOP, including all service nodes offering the service.

```
Local> SHOW SERVICES LOCAL
```

This command displays summary for all local services from the operational database.

SESSIONS (secure)

Syntax



Description

This command (available to all users) displays session information from the operational database for one or all ports on the access server. Unlike the SHOW/ MONITOR PORT SESSIONS command that displays session characteristics for one session at a time, this command displays all sessions.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Keywords

ALL

Displays sessions for all ports on the access server. (ALL is not accepted on secure ports.)

PORT *n*

Displays sessions for the specified port (default: displays sessions for your current port).

Restrictions

- Only a privileged user can view these characteristics for another port.
- MONITOR is a privileged command.
- Secure users cannot specify PORT and ALL.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

SNMP - TELNET LISTENER

SNMP

Syntax

Description

These commands display SNMP-related information, such as SNMP characteristics, error and access counters, and operational status.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Keywords

CHARACTERISTICS

Displays current values for SNMP community names and Internet addresses. Also displays “enabled” or “disabled” for SNMP characteristics GET, GETNEXT, SET, and TRAP.

COUNTERS

Displays current SNMP error and access counters.

STATUS

Displays whether SNMP is running or not running.

Restrictions

- SNMP CHARACTERISTICS is a privileged command. SHOW SNMP COUNTERS and SHOW SNMP STATUS are available to all users.
- The LIST command is invalid for SNMP COUNTERS or SNMP STATUS.
- MONITOR is a privileged command.

Examples: SHOW SNMP

```
Local> SHOW SNMP STATUS
```

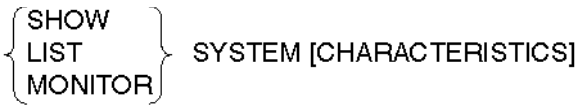
This command displays whether the SNMP protocol is running or not running.

```
Local> LIST SNMP CHARACTERISTICS
```

This command displays SNMP community names, Internet addresses, and whether SNMP characteristics GET, GETNEXT, SET, and TRAP are enabled or disabled.

SYSTEM CHARACTERISTICS (secure)

Syntax



Description

This command (available to all users) displays access server characteristics such as the system location and the system contact person.

Keywords

CHARACTERISTICS

Displays (in ASCII format) system information such as the name of the system contact person (system manager) and the system location.

Restriction

MONITOR is a privileged command.

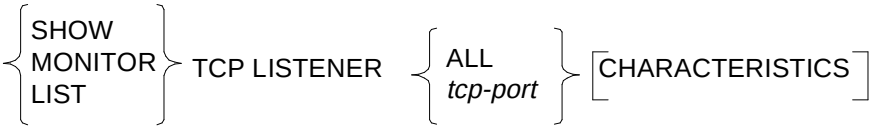
Example: SHOW SYSTEM

```
Local> SHOW SYSTEM
```

The above command displays system-group characteristics as recorded in the access server operational database.

TCP LISTENER (secure)

Syntax



Description

This command (available to all users) displays information about TCP listeners on the access server.

Keywords

ALL

Specifies that all TCP listeners are to be displayed.

tcp-port

Specifies that information only about the TCP listener associated with the specified TCP port is to be displayed.

CHARACTERISTICS

Specifies that the characteristics of the TCP listener(s) are to be displayed.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.
- Telnet listener is not available to ports if the LIMITED VIEW port characteristic is enabled.

Example: SHOW TCP LISTENER

Local> **SHOW TCP LISTENER 2001**

This command shows the characteristics of the TCP listener on TCP port 2001.

TELNET LISTENER (secure)

Syntax

{SHOW / MONITOR / LIST} Telnet LISTENER {ALL / *tcp-port*} [CHARACTERISTICS]

Description

This command (available to all users) displays information about Telnet listeners on the access server.

Keywords

ALL

Specifies that all Telnet listeners are to be displayed.

tcp-port

Specifies that information only about the Telnet listener associated with the specified TCP port is to be displayed.

CHARACTERISTICS

Specifies that the characteristics of the Telnet listener(s) are to be displayed.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.
- Telnet listener is not available to ports if the LIMITED VIEW port characteristic is enabled.

Example: SHOW TELNET LISTENER

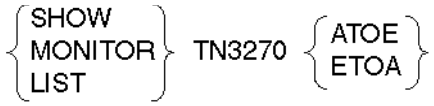
Local> **SHOW TELNET LISTENER 2001**

This command shows the characteristics of the Telnet listener on TCP port 2001.

TN3270 ATOE/ETOA - USERS

TN3270 ATOE/ETOA (secure)

Syntax



Description

This command allows you to display the current translation table. Codes are in hexadecimal. Refer to the TN3270 ATOE/ETOA commands for more information.

Keywords

ATOE

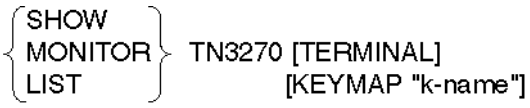
The ATOE option allows you to display the ASCII to EBCDIC translation table for ASCII codes. These translations are used to translate user data from ASCII based terminals to EBCDIC data sent to the host. All customized translations will have an asterisk displayed next to them on the display screen.

ETOA

The ETOA option allows you to display the EBCDIC to ASCII translation table for EBCDIC codes. These translations are used to output ASCII data to ASCII based terminals from EBCDIC received from the IBM host. All customized translations will have an asterisk displayed next to them on the display screen.

TN3270 TERMINAL (secure)

Syntax



Keywords

TERMINAL

This command shows the TN3270 terminal types and their associated keymaps (keyboard maps) in a two column display. The first five terminal types listed are the predefined terminal types. Newly defined or customized terminal types and their keymaps appear below the predefined types. The default is TERMINAL.

KEYMAP

This command shows the current mapping of IBM functions to DEC key sequences for the specified *k-name*.

USERACCOUNT (privileged)

Syntax

Description

SHOW USERACCOUNT is a privileged command, and will allow the security administrator to view the local database. The password field value will *not* be displayed for any database entry.

Keywords

username

Designates an individual account name that the security manager wishes to view.

Note

An account name does not necessarily have to be the user's name. It can be any string of characters chosen by the system administrator to designate an account name. See the Example: SHOW USERACCOUNT below.

ALL

The command ALL will show a list of all user accounts. See the Example: SHOW USERACCOUNT below for a sample of this display.

Example: SHOW USERACCOUNT

```
Local> SHOW USERACCOUNT ALL
Server Realm:         NAS700.LKG.DEC.COM
Username:             Betterman
Password:             (Entered)       User Status:         ENABLED
Access:               LOCAL           Forced CallBack:    DISABLED
Max Connect Time:     00 08:00:00     DialOut Service:   DIAL14400
DialBack Number:      9=*70=1-212-555-1234
DialOut Number:       (Any)
Permissions:          LAT, TELNET, SLIP, PPP, DIALBACK, DIALOUT

Username:             BOB_SMITH
Password:             (None)          User Status:         ENABLED
Access:               FRAMED          Forced CallBack:     ENABLED
Max Connect Time:     00 08:00:00     DialOut Service:      (None)
DialBack Number:      555-1234        DialOut Number:       (None)
Permissions:          SLIP, PPP

Username:             Manager
Password:             (Entered)       User Status:         ENABLED
Access:               LOCAL           Forced CallBack:    DISABLED
Max Connect Time:     (None)          DialOut Service:   DIAL28000
DialBack Number:      555-2222
DialOut Number:       (Any)
Permissions:          LAT, TELNET, SLIP, PPP, DIALBACK, DIALOUT
                      PRIVILEGED
```

USERS (nonprivileged)

Syntax

{SHOW / MONITOR} USERS

Description

This nonprivileged command displays information about port users.

Reference

For a detailed description of the displays, refer to the *Network Access Server Management* manual.

Restrictions

- MONITOR is a privileged command.
- When using the MONITOR command, your port type characteristic should be set to ANSI; otherwise, displayed information will scroll off the screen.

Example: SHOW USERS

```
Local> SHOW USERS
```

This command displays user names affiliated with ports that have permanent user names.