LANReach
Remote Access Server

User Manual

Document No.DUMNLR15010200G

HCL PERIPHERALS
(A Unit of HCL Infosystems Ltd.,)
#299, Arcot Road, Vadapalani,
Chennai – 600 026.
Phone : 91 44 4800156/91 44 4844304
Fax: 91 44 4834563

NOTICE

The information contained in this document is subject to change without notice.

HCL Peripherals Limited makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, HCL Peripherals Limited shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited.

Use of this manual and media supplied for this pack is restricted to this product only. Additional copies of the programs can be made for security and back-up purposes only. Resale of programs in their present form or with alterations, is prohibited.

Trademark Acknowledgment.

Brand and product names mentioned in this document are trademarks or registered trademarks of their respective holders. **LANReach** is a trademark of **HCL Peripherals Limited**.

HCL PERIPHERALS
(A Unit of HCL Infosystems Ltd.,)
#299, Arcot Road, Vadapalani,
Chennai – 600 026.
Phone : 91 44 4800156/91 44 4844304
Fax: 91 44 4834563
URL: http://www.hclperipherals.com/

CONTENTS

1 ___ 9

PRODUCT OVERVIEW ___ 9

Remote access server Features ___ 10

- Single board solution ___ 10
- Memory ___ 10
- Connectivity ___ 10
- Multiple booting options ___ 10
- Ease of configuring ___ 11
- Friendly and secured administration ___ 11
- Online modification to configuration ___ 11
- Remote Administration Facility ___ 11
- Facility to restrict access at host level ___ 11
- Fixed port connection ___ 11
- Implicit connection to host ___ 11
- Network protocol and applications ___ 12
- Multiple sessions ___ 12
- Routing ___ 12
- Subnetting ___ 12
- Reverse Telnet ___ 12
- SNMP Support ___ 13
- Domain Name System ___ 13
- Secondary boot servers ___ 13
- Dynamic switching ___ 14
- Separate console port ___ 14
- Friendly user interface ___ 14
- Protocol filters ___ 14
- Web management ___ 14
- UDP configuration support ___ 15
- Auditlog feature ___ 15
- Network Address Translation (NAT) ___ 15

Functional Overview ___ 16

Models and Configurations ___ 18

Terminologies ___ 18

2 ___ 21

INSTALLATION OF THE REMOTE ACCESS SERVER ___ 21

Hardware Installation ___ 22

Select Location ___ 24

Software Installation ___ 27

Configuring the Boot Options ___ 28

3 ___ 33

COMMAND SET ___ 33

Introduction ___ 33

GENERAL USER COMMANDS 34
Identifying the hosts 35
Verifying the host 37
Creating a Session 39
Exiting out of a Session 40
Suspending a Session 41
Defining a Escape Sequence 41
Naming a Session 43
List the Existing Sessions 44
Resuming a suspended session 45
Closing a Session 46
Setting Port Parameters 47
Display and Modify Characteristics 49
Set Baudrate 49
Set Transmit Character Size 50
Set the Parity Type 50
Enable and Disable Parity Check 51
Set Number of Stop Bits 51
Controlling Software Flow Control 51
Break Signal 52
Modem Control 52
Enable DSR signal sensing 53
Enable DTR signal togglling 53
Define Control Characters 53
Define Character for Session Switching 54
Telnet 55

Status Display Commands 57
Display Version Details 59
Display Diagnostics Information 59
Display Status of Hosts on the Network 60
Display Process Status 61
Display Server Activity Statistics 62
Display Dial-On-Demand statistics 64
Display ARP Table Contents 64
Identifying the hosts 65
Verifying the host 67
Query the DNS Name Server 68
Quit 69

ADMINISTRATIVE COMMANDS 70
Activity 74
Configure 75
Date 78
Closing Down a Session 79
Reset to Factory Default 80
getconfig 80

gethost 81
Configure boot parameters 81
gethost 82
Help 83
Save Configuration Information 83
Configure boot parameters 84
Configure UDP port parameters 85
Route 87
Set Port Parameters 92
Configure SNMP Parameters 96
Set Port Characteristics 99
Display Message on all Ports 102
Display Message on given Terminal 103
ifconfig 103
Reset a port 105
Protocol filter commands 106
  Help 106
  Display Filter entries 106
  Add a filter entry 107
  Modify a filter entry 108
  Insert a filter entry 108
  Delete a filter entry 108
  Clear the filter information database 109
  Quit 109
Dial on Demand commands 109
Help 109
Adding and Deleting a DOD entry 110
Display DOD entries 110
Clear the DOD route table entries 111
Quit 111
Staticroute commands 111
Help 112
Adding and Deleting a static route entry 112
Display route entries 114
Quit 114
Access statistics commands from Admin Mode 114
Exit from Administrative Mode 115
Access and Modify Host Database information 115
Webserver commands 117
  help 117
  Display web server parameters 117
  Modify webserver parameters 118
  Download webserver files into flash memory 118
  Exit from Webserver Directroy 118
Point to Point Link commands 119
help 119
Commands To Manipulate Path Database 120
Commands To Manipulate User Database 124

Auditlog directory 128
Commands To Manipulate Modemchat Database 132
Commands To Manipulate Logchat Database 135
Start a path 138
Stop a path 139
Security Access Server Commands 139
Add a port to an active path 142
Delete a port from an active path 143
List the active paths 144
Exit from ppl menu 144

TELNET COMMANDS 145
Telnet Command Menu 145
Display 148
Mode 149
Send 150
Local Character Recognition 151
Set 152
Debug 153
Resume 154

4 155

SETUP CONFIGURATION 155
Introduction 155
Setup Configuration Commands 156
Configure 156
Factory 159
getconfig 159
Help 160
Save Setup Configuration Information on Host 160
Set Port Parameters 161
Configure SNMP Parameters 165
Set Port Characteristics 167
Quit 171
Setup Procedures 172
Switched Port 172
Implicit Port 173
Fixed Port 174
Reverse Telnet Port 176
Connecting Printer to Implicit Port 177
Connecting Printer to Fixed Port 179
Modifying the configuration 181

5 182

ERROR MESSAGES 182
Diagnostic Error messages 183
Run time Error Messages 186

6 _______________________________ *195*

TROUBLESHOOTING THE REMOTE ACCESS SERVER _______ **195**

System Panic Messages _______ 195

Fixed Pty Messages _______ 196

7 _______________________________ *199*

web management of remote access server _______ **199**

A _______________________________ *204*

CABLE CONNECTION DETAILS _______ **204**

Serial Port to Terminal Cable Connection - 3 Wire _______ 205

Serial Port to Terminal Cable Connection - 4 Wire _______ 206

Serial Port to Terminal Cable Connection - 8 Wire _______ 207

Cable for Compatibility with Exterm 1600 _______ 208

Serial Port to Modem Cable Connection _______ 209

Parallel Printer Port Pin-outs _______ 211

AUI Port (D-15) Pin-outs _______ 212

Twisted Pair Port Cabling _______ 213

B _______________________________ *214*

CLASSIFICATION OF REMOTE ACCESS SERVER PORTS _______ **214**

C _______________________________ *216*

PHYSICAL AND ELECTRICAL PARAMETERS _______ **216**

Physical _______ 216

Electrical Power _______ 216

Environmental _______ 216

D _______________________________ *217*

HARDWARE FLOW CONTROL _______ **217**

E _______________________________ *218*

ERROR REPORTING _______ **218**

Checklist of Inputs _______ 218

F _______________________________ *220*

INSTALLING AND Configuring REMOTE ACCESS SERVER IN VARIOUS UNIX MACHINES _______ **220**

FOR DIGITAL UNIX SERVER _______ 221

FOR IBM AIX4 SERVER _______ 228

FOR SCO 5 SERVER _______ 233

FOR SCO Unixware SERVER _______ 239

FOR SUN SOLARIS 5.6 SERVER _______ 246

FOR SVR4.2 SERVER _______ 253

G ____ *259*

PPP DOCUMENTATION ______________________________ **259**

H ____ *276*

remote access server - models ______________________ **276**

I ____ *277*

sync port - details ______________________________ **277**

LANReach 1600S ______________________________ 277

V.35 Cable Details ______________________________ 277

V.35 Interface with Sync Card ______________________ 278

Configuration Details ______________________________ 278

1

PRODUCT OVERVIEW

The ***LANReach*** remote access server is a versatile, high performance system that provides upto sixteen asynchronous RS232-C compatible ports, one console port and one centronics compatible parallel port and enables connection to TCP/IP host systems over twisted pair network. It provides the users access to any host system on the TCP/IP Internet network and enables users on the host to remotely access devices such as serial printers, parallel printer and modem links, which are connected to the remote access server. The remote access server thus provides the user

- Optimal cabling
- Ability to share resources across multiple hosts
- Ability to overcome serial interface distance limitations
- Optimize utilisation of host processing power by reducing the serial i/o processing overheads.

The remote access server enables the user to remote login to systems, using **rlogin** and **telnet TCP/IP** applications.

Remote access server Features

- **Single board solution**

  The remote access server hardware is implemented on a single board thereby increasing the reliability and robustness of the system. The hardware fits in a sleek cabinet ensuring easy and comfortable handling during installation and subsequent maintenance.

- **Memory**

  The remote access server hardware includes:

  - On board memory (16MB) from where the server software is executed
  - 128KB of battery backed Non Volatile Random Access Memory, which maintains the configuration information of the server, across powerdowns.
  - **Optionally**, a flash memory (2MB), where the server software is stored so that downloading the server software during boot time is avoided.

- **Connectivity**

  The remote access server provides connectivity to **sixteen** RS232-C compatible serial devices like,

  - Dumb terminals
  - Modems
  - Serial printers
  - Other RS232-C compatible devices, say a PC

  and **one** Centronics compatible parallel printer interface for connecting parallel printer. The serial ports support different baud rates from 75 to 460800.

- **Multiple booting options**

  The remote access server, once switched on runs a self test and executes a boot program from the Flash, which loads the remote access server software and then passes control to it, to proceed with the boot process further. Different mechanisms are provided for loading the software, which the administrator can select while configuring.

  - boot from flash memory, if flash memory is present and contains the server software
  - download the software from a specified host over network into on-board RAM and boot
  - download the software from any host that contains the software over network into the on-board RAM and boot

- **Ease of configuring**

  The remote access server provides a simple command line interface to configure the server after booting. Facility to save the configuration information in the Non Volatile memory and on a host for backup are provided, so that subsequently, the configuration information is available to the server without user interaction.

- **Friendly and secured administration**

  A simple Unix like command line interface is available, using which the administrator may configure the server facilities and the port parameters. Online help facility is also available. The administrative command access is secured by a password, so that the server is secure against misuse either intentional or inadvertent.

- **Online modification to configuration**

  The configuration of server facilities and port parameters may be modified while the server is running. The administrator will be able to do these dynamic modifications for any ports while the user will be able to do it for his port alone.

- **Remote Administration Facility**

  The configuration of server facilities and maintenance activities can be performed from any host system on the network by doing a remote login to the remote access server. The administrator need not be using the terminals connected to the console or other ports of the remote access server for performing these functions.

- **Facility to restrict access at host level**

  The administrator, while configuring, may restrict or permit access to specific hosts from individual ports.

- **Fixed port connection**

  Facility to configure a port as a **fixed port** is available, wherein when the terminal connected to the port is switched on, the login prompt of a specified host to which the port has a fixed (nailed) connection, appears on the screen. With this facility, a controlled environment can be provided for novice users.

- **Implicit connection to host**

  An implicit port of a remote access server provides a permanent login session with a specific user name and a specific host.

  Implicit connection feature, provides a similar facility like fixed connection, except for the difference that there is no permanent tty device name associated with.

- **Network protocol and applications**

The remote access server implements the TCP/IP protocol stack. TCP/IP, which stands for Transmission Control Protocol/Internet Protocol is a set of protocols, defined by Department of Defence (DoD), USA for use in Internet networks. The TCP/IP implementation of the server is as per standard requirements of the corresponding RFCs (Request For Comments).

Host systems in an Internet network are identified by an Internet address and a corresponding symbolic name. The Internet address consists of

- a network identification part and
- a host identification part.

The address is represented in dot decimal notation like 196.1.68.53.

The standard TCP/IP applications, **rlogin** and **telnet** are implemented to enable users on the server to connect to remote hosts using the transport services provided by TCP/IP.

Rlogin provides a remote login facility to establish connection to TCP/IP hosts.

Telnet is a standard terminal package, which allows users access to TCP/IP hosts and initiate a terminal session with them.

- **Multiple sessions**

User may establish multiple sessions to one or more hosts from a single port. Facility to escape from a session to the server, through a user defined escape sequence and to resume any session, extend lot of flexibility to the user.

- **Routing**

When two Internet networks are interconnected through a gateway system, which connects to both the networks using two network interfaces, the traffic across the network will be routed by the gateway system. The Routing Information Protocol RIP is implemented on the server to enable routing.

- **Subnetting**

Normally organisations subscribe for a Internet network address for their local network. Within the organisation this Internet network may be subdivided into multiple logical networks called **subnets**. The **subnet** is defined by specifying a **subnet mask**. Communication between subnets can be done through a gateway node. The remote access server supports subnetting.

- **Reverse Telnet**

A remote access server port can be defined to be of type reverse telnet and devices connected to this port can be shared by users on the other hosts.

Typical applications using reverse telnet may be :

- A printer can be connected to a port of the remote access server which is defined as a reverse telnet port enabling users from different host systems to share this printers, by a command like

```
cat filename | telnet TSname TCPport
```

- Modems can be connected to the port of the remote access server defined as reverse telnet port. Subsequently, users from different host systems on the network can do telnet into this port and reach a remote system through the modem and leased lines.

- **SNMP Support**

Simple Network Management Protocol (SNMP) is part of Internet protocol suite. It provides a mechanism for a Network Management Station (NMS) to obtain information about and control other nodes in the TCP/IP network. Typically, a SNMP **agent** will be running on the monitored nodes and respond to requests from a SNMP **manager** running on the NMS. The manager issues requests to the agent requesting for information about the node and issues commands to the agent to modify parameters. SNMP defines the communication between the manager and the agent.

The structure in which information is exchanged between the manager and the agent is defined by means of a database called **Management Information Base (MIB).** The MIB is divided into groups and these groups consist of **objects**. **SNMP** also allows users to add their own objects under a separate group, called enterprise.

The remote access server implements an SNMP agent with standard MIB-II objects.

- **Domain Name System**

Normally, the remote access server downloads the hostname/address information in */etc/hosts* file from the boot server. This is a static database, as any changes to the database must be manually done. Mapping of host name and address using this static database is **static binding**.

Domain Name System is part of Internet protocol Suite. It enables a dynamic mapping of host names and addresses by maintaining a distributed database of hosts present in the domain.

DNS implementation consists of name servers and name resolvers. The remote access server with DNS configured provides a name resolver. The Domain Name resolver dynamically establishes a database by making DNS query requests to the name server and establishes a dynamic name/address map called **DNS cache**. This mapping is called **dynamic binding**.

- **Secondary boot servers**

The remote access server provides the facility to define a secondary boot server to boot from, in case the primary server is not available.

- **Dynamic switching**

  When a host to which an implicit or fixed port connection is established, goes down, the terminal session gets disconnected. In order to enable mission critical application to achieve minimal downtime, the remote access server provides the facility to configure implicit/fixed ports with a set of host names, instead of a single host. When a host does not respond, the remote access server times out and tries to establish the connection with the available host.

- **Separate console port**

  A separate port for console is available for Administration purposes. Debug messages will be displayed on this port. The Administrator, subsequently take actions depending on the Debug messages.

- **Friendly user interface**

  The remote access server provides a simple Unix like, command line user interface. The general user commands which help in establishing connection to host, switching between sessions etc are provided at the main prompt. Advanced commands and administrative commands are provided in independent different modes. This division of commands makes the usage easy for a novice user.

  Online help indicating the list of commands available at different command modes (general user, advanced user and administrator) are provided with provision to get detailed information of individual commands.

  A command history is maintained for each port, to enable the user to recall previous few commands and reissue. Also, facility is provided to edit the recalled commands to make changes and reissue. The name of the command is matched even if it is partial as long as the part of the command typed is unambiguous and unique. These features reduce the typing burden on the user.

- **Protocol filters**

  LANReach can selectively filter specific packets based upon their Ethernet protocol type using Protocol Filters. Protocol Filters are useful in preventing protocols used in one segment of a network from being bridged to other subnets that do not use those protocols. This increases the amount of bandwidth available on the network.

- **Web management**

  Configuration of LANReach can be done from a remote system on the global or local internet. This type of Web Management is easier to use and more intuitive than the console/text base configuration.

- **UDP configuration support**

  The remote access server provides UDP packet forwarding feature. With this feature, the administrator can enable/disable the broadcasting of UDP packets on a particular port.

- **Auditlog feature**

  This feature provide the system administrator with information about the usage of the LANReach such as the frequency with which users dial in, status of their calls etc.

- **Network Address Translation (NAT)**

  With this feature, multiple computers can be connected to the internet using one IP address. NAT implemented in RAS creates a firewall between your internal nework and outside networks or the internet.

Functional Overview

Figure 1.1 illustrates a typical installation environment where a remote access server is connected in an internet network with multiple hosts.

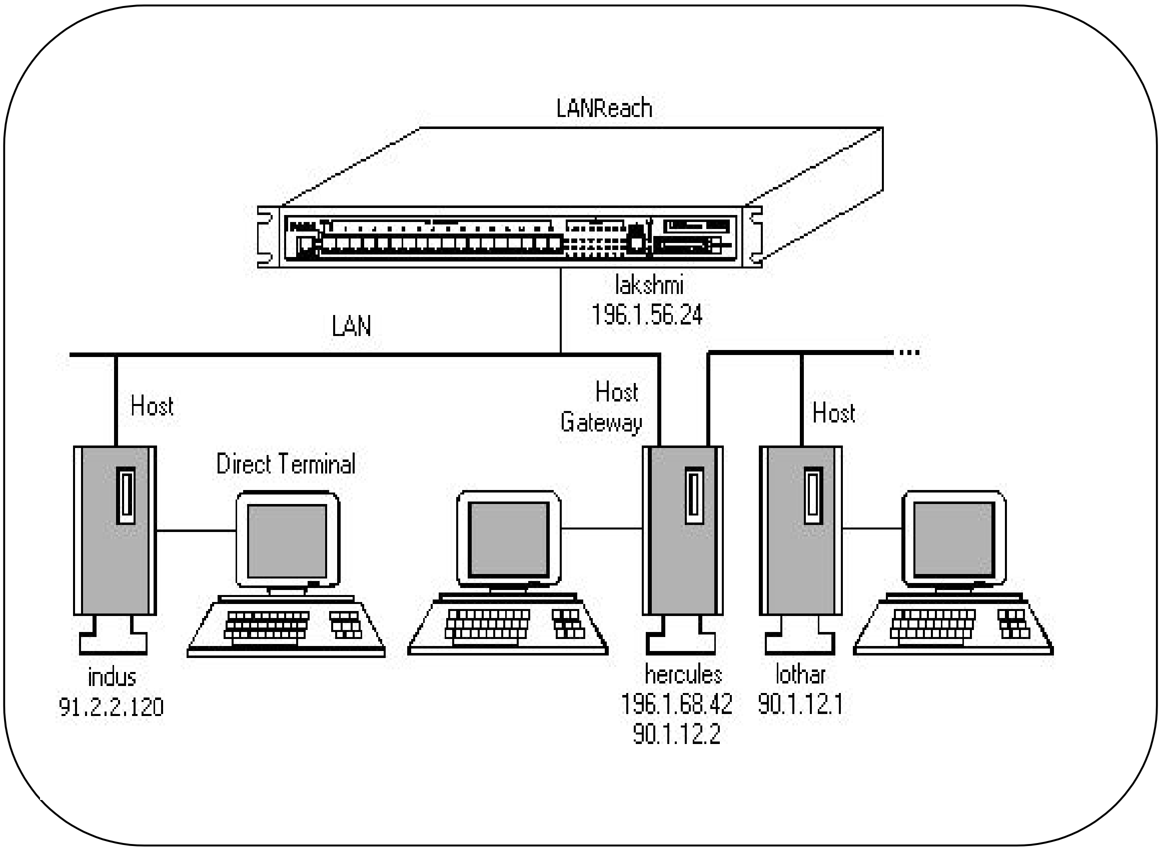


Figure 1.1

Typically in this environment,

- user can login to any host, from the terminals connected to the serial ports of the server, using **rlogin** or **telnet**

- user on any host can share the resources available on the server. Resources like, serial printer, parallel printer, modem connection etc, can be connected to the Remote access server as shown in Figure 1.2.

- user can have an implicit connection to any host

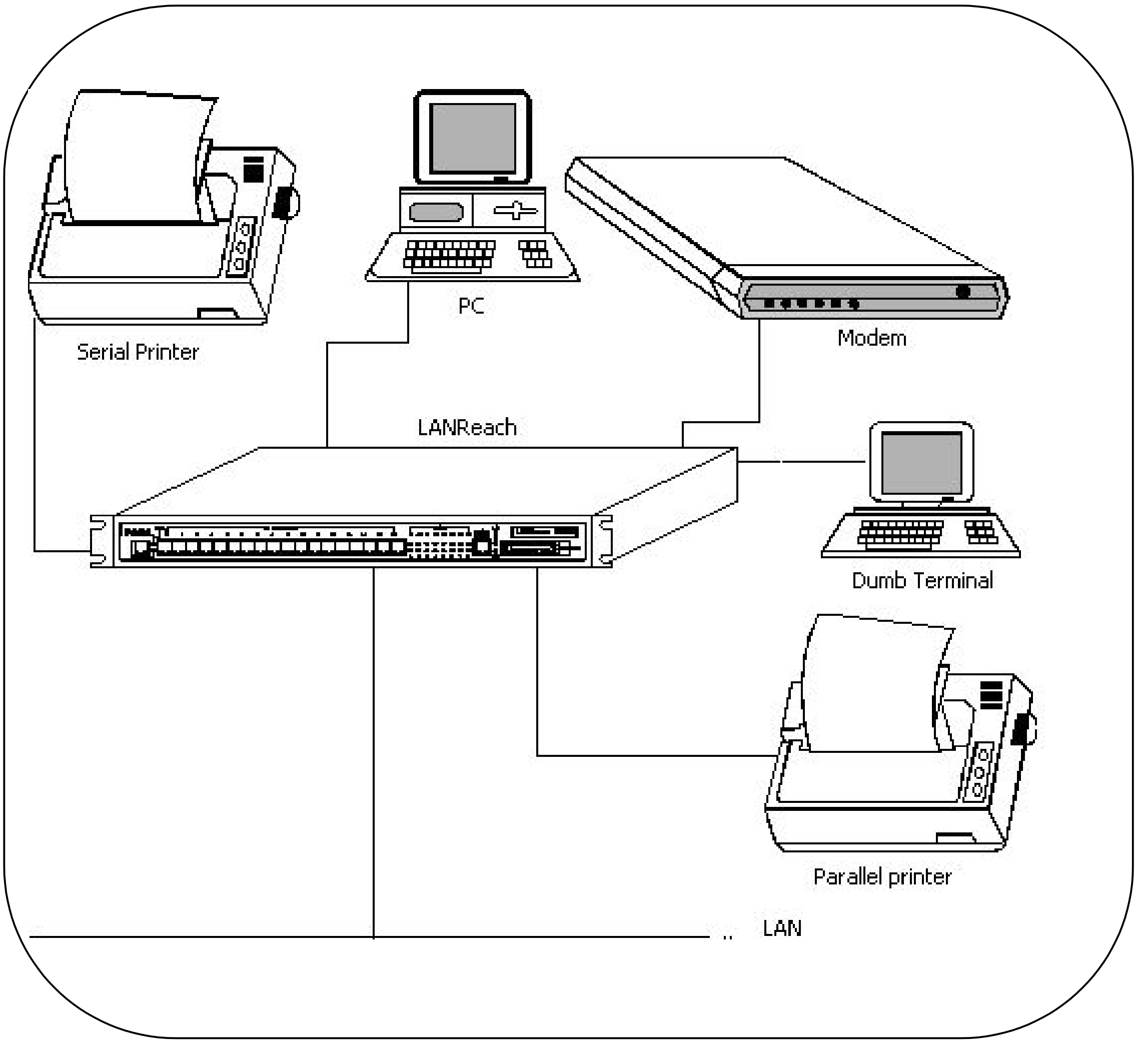


Figure 1.2

- user may have a fixed port connection with any host that provides the corresponding fixed port login service program.

- user on any host may login to the remote access server and do administrative functions provided he has the privilege.

Models and Configurations

The *LANReach* remote access server is available in different models. The table below describes the model numbers and the configurations of these models.

Table 1.1 : Model Numbers and Configuration

LANReach Model Number	Configuration
800 – V4	*LANReach* RAS with **8 serial ports, one console port and one parallel port**
1600 - V4	*LANReach* RAS with **16 serial ports, one console port and one parallel port**
1600S	*LANReach* RAS with **16 serial ports, one console port, one parallel port and one Sync port**

The following chapters of this guide explain the installation, command set, configuration and administration of the server facilities and provide guidelines on troubleshooting.

Terminologies

The remote access server is present in a Local Area Network with multiple systems. These systems are called **nodes** of a network.

Each node has, associated with it, an **internet network address** which looks like 196.1.68.58. They can also be referred by symbolic names called **nodename**.

A node which is present in two networks and enables the user to access the hosts across the two network is referred to as a **gateway** node. The process of sending information from one network to the other network is referred to as **routing**.

The system to which the user establishes connection from his remote access server port is called the **host system** or **host**.

The connection established between the remote access server port and a host is called a session. Each session from a port is identified uniquely by a **session-id**, which may be, a unique number assigned to the session by the remote access server, called **session number**

a unique name assigned to the session by user, called **session name**

name of the host with which the session is connected in case where there is only one
session with the host.

A **current active session** is the most recently used session on the terminal. It is represented by the character *.

A **previous active session** is the session used just before the current active session. It is represented by the character #.

The serial asynchronous RS232-C compatible connections and the parallel printer connections that the remote access server provides are called **ports**. The console port is named S0.The sixteen serial ports are named S1, S2 and so on upto S15. The parallel port is named P0.

The ***LANReach*** provides three types of terminal access on its asynchronous ports. The remote access server administrator can configure a port to be one of the three types.

The three types of accesses are:

- Fixed port
- Implicit port
- Switched port

Fixed type of connection to a remote access server port is one on which user gets a login prompt of the host system to which the port is attached always. This type of connectivity, prevents the user of the terminal connected to such a port, from assessing multiple hosts at will, and is meant for novice users. In the case of fixed port terminals, user will get the login prompt of the host, directly and hence the user will not notice any difference from direct terminals connected to the host. The device name of the terminal on such ports, will be the configured pseudo terminal name. The fixed port sessions are managed by **fixed manager**.

Implicit type of connection is one on which a session is established to a specified host and logged in as a specified user. Optionally, a null user name may be specified, in which case, the login prompt will appear as in the case of fixed ports. The difference in the case of implicit port is that the terminal device name on these ports will vary as any available pseudo device will be used. The implicit port sessions are managed by **implicit manager**.

Switched type of connection is one on which when a terminal is switched on, the remote access server prompt will appear. On a port configured as switched port, **line manager** gets executed, which provides a command line interface to the user. The switched port sessions are managed by the **line manager**.

Generally, the remote access server maintains a database of hostname, internet address, and alias names downloaded from the /etc/hosts file in the host server. This is called the **static host**

database. Mapping and binding of hostnames and addresses using the static host database is called **static host binding**.

Such a static binding is a limitation in a dynamic LAN domain. **Domain Name System (DNS)**, which is a part of Internet protocol suite, provides a flexible way of mapping host names and addresses by maintaining a distributed database of hosts present in a domain.

A DNS implementation consists of servers called **Name Servers** and clients called **Name resolvers**. The dynamic database of host names, addresses and alias names collected by the **Name resolver** by making DNS query requests to the **Name Server** is called **DNS cache**. Mapping and binding achieved using DNS mechanism is called **dynamic binding**. DNS is said to be unusable under the following conditions:

- domain name not set
- name servers not defined
- no name server is up/running
- network is down
- unrecoverable internal failures

Even if DNS is unusable, it is possible to examine the DNS cache and analyse problems by using appropriate commands.

2

INSTALLATION OF THE REMOTE ACCESS SERVER

The ***LANReach*** remote access server must be installed and configured appropriately before putting the server to use at the installation. This chapter describes the procedures for

- installing the hardware, connecting the network and connecting other serial devices and parallel printer
- installing the software
- Configuring the server boot options.

The command set details of the remote access server is described in Chapter 3.

Note

For detailed information about Installation and configuration of the remote access server with various Unix machines, refer Appendix F

HARDWARE INSTALLATION

The remote access server provides

- Eight or Sixteen RS232-C serial ports
- One console port
- One Parallel port (Centronics interface)
- and Twisted Pair interface (10base T).

Serial port (S0) is the console port. All diagnostic and software error messages will appear on the terminal connected to this port.

The serial port connectivity is provided through RJ-45 connectors. The parallel printer port connectivity is through female D-25 connector. The Network interface connection is through RJ-45 connector.

After receiving the remote access server at your installation, unpack the contents and check whether all items are included.

The front and rear views of the remote access server cabinet are shown below indicating the various parts of the remote access server.

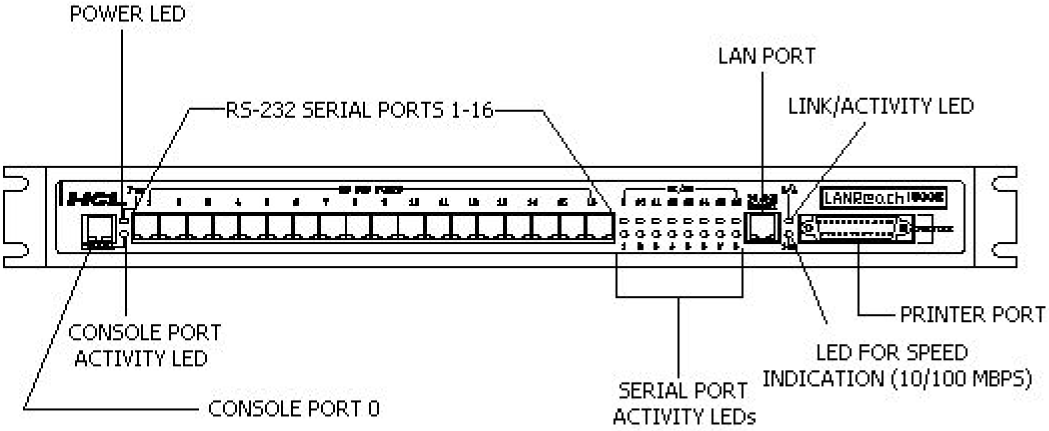


Figure 2.1 LANReach Front View

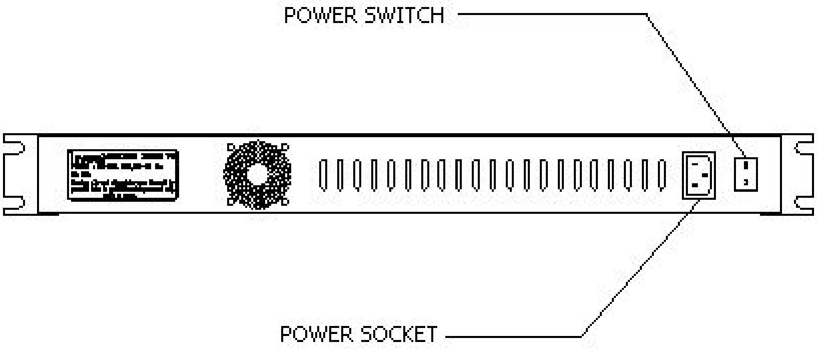


Figure 2.2 LANReach Rear View

The power LED marked as **Pwr** indicates the Power-On condition.

The console port LED marked as **Console** indicates the transmit and receive activity of the console port.

The Serial Port Activity LEDs marked from **1 to 16** indicate both the transmit and receive activity of the corresponding serial ports, S1 to S16 respectively.

The LAN port LED marked as **L/A** on the panel indicates the Link/Activity status of the LAN network.

The LAN port LED marked **100** indicates the speed of the operation of the LAN network. The speed of operation may be either 10 Mbps or 100 Mbps. Glow of LED indicates 100 Mbps operation. Otherwise, it is 10 Mbps operation.

Select Location

Installation of the remote access server should be done at a proper location. The following guidelines may be followed for selecting a location to install the remote access server.

- All serial port cables must terminate at the chosen location.
- Maximum cable lengths between devices and ports should not exceed the limits defined by RS232-C standards. Typically, it should not exceed 50 ft. for devices operating at 19200 baud.
- All serial cable lengths must be optimum.
- The power plug should be of minimum 5 Amps with properly grounded earth pin.
- Preferable to have UPS (Uninterruptible Power Supply).

Cabling

The steps below indicate the procedure for installing the remote access server at the location chosen. Refer to Appendix A for cable connection details.

Step 1 Connect the power cable into the 3-pin power socket located on the back of the cabinet.

Step 2 Connect a terminal to the Console Port with a cable terminated on one side with RJ-45 jack and the other side with standard RS232-C male D-25 connector.

Step 3 Connect the remaining 16 serial ports with suitable cables depending on the requirements.

Step 4 Connect the parallel printer to the parallel port using standard centronics printer cable.

Step 5 Connect the remote access server to the network using RJ-45 cable.

Note

RJ-45 type of connectors is provided for both serial RS232-C ports and LAN twisted-Pair interface. So care should be taken while plugging in serial port cables and LAN Twisted-Pair cable. Never interchange these cables.

Startup

Before powering up the remote access server, the following points must be checked :

- Verify that the power cable, console cable and network cable are connected properly.
- The default characteristics of the console port are 8 bit, no parity and 1 stop bit. Therefore, the terminal connected to this port should be at these settings.

Once powered-on the remote access server runs self-tests and subsequently the boot message appears on the console. If nothing appears on the console after 10 seconds, the following things need to be verified :

- Check whether Power LED (Pwr) is on. If not, check the power cable and power switch.
- Check the screen. If it is blank, check terminal power and console cable.
- If garbled message appears on the screen, check the console cable and terminal settings.

On successful completion of the self tests, the boot message

```
Self-Test Routine
Memory Test - Passed
Serial Controller Test
ACE Internal Loop back Test Passed for Port - 0
ACE Internal Loop back Test Passed for Port - 1
ACE Internal Loop back Test Passed for Port - 2
ACE Internal Loop back Test Passed for Port - 3
ACE Internal Loop back Test Passed for Port - 4
ACE Internal Loop back Test Passed for Port - 5
ACE Internal Loop back Test Passed for Port - 6
ACE Internal Loop back Test Passed for Port - 7
ACE Internal Loop back Test Passed for Port - 8
ACE Internal Loop back Test Passed for Port - 9
ACE Internal Loop back Test Passed for Port - 10
ACE Internal Loop back Test Passed for Port - 11
ACE Internal Loop back Test Passed for Port - 12
ACE Internal Loop back Test Passed for Port - 13
ACE Internal Loop back Test Passed for Port - 14
ACE Internal Loop back Test Passed for Port - 15
NVRAM present
FLASH1-AMD 29F080B
FLASH1-AMD 29F080B

Available Memory = 16MB

 Do you want to change the boot parameters ?
```

will appear on the console.

Software Installation

The remote access server software is usually installed on one of the host systems in the network. The software will normally get downloaded when the server is booted in to the local memory of the server and then executed.

Optionally, the server may have a flash memory on to which the software may be downloaded and saved. In this case the server will load the software from the flash memory into the local memory and then execute.

Options for Booting

The remote access server provides three options to execute the software :

- Execute from the Flash memory, if available on the server
- Download from a specified host in the network and execute
- Download from any host in the network that contains the remote access server software and execute

In the first option, the remote access server software resides in the flash memory of the server and the server boot program in the boot Flash will download the contents of the flash memory into the RAM and pass control to it.

The second and third options for booting, may be used when there is no flash memory present in the server or if the contents of the flash memory are not valid or it is not desired to use the software in flash memory. In both these options, the server software may reside on one or more of the host systems connected in network with the remote access server. The server boot program in the boot Flash, using the Trivial File Transfer Protocol (TFTP), downloads the software from the host system into the on-board local memory over the network, and then passes control to it.

If a specific host address is specified for downloading the software, then the boot program sends appropriate TFTP requests to that host to download the software. This option would be highly helpful when different host systems hold different versions of the server software and the user wants to use a specific version of software. The host identified by the given host address is called the **preferred boot server**.

It is also possible to specify a secondary server to boot from in case the primary boot server is not up.

If no specific host address is specified, then the TFTP requests for downloading the software, is broadcast over the network and the software is downloaded from any host that responds first to the request. In this case, a broadcast address of 0.0.0.0 should be specified as the **primary** or **secondary Boot Server.**

After downloading the software from the host, the user may save the same in the flash memory, so that subsequent boot and execution may be from the flash memory instead of from the host.

Configuring the Boot Options

When the remote access server is booted the first time, the NVRAM contents will not be valid and hence the message

```
Available Memory = 16MB
Warning!! Check sum is bad
Restoring Factory Defaults

Do you want to change the boot parameters ?n
```

will be displayed on the console. If the administrator responds with y, then the Boot configuration menu will be displayed.

```
                      BOOT PARAMETERS

  1.   Interface Internet Address ... : Not Defined
  2.   Interface Subnet mask ........ : Not Defined
  3.   Primary Boot Server .......... : Not Defined
  4.   Secondary Boot Server ........ : Not Defined
  5.   Boot Filename ................ : /etc/ts/LANReach
  6.   Boot From FLASH Memory ....... : No  (Empty)
  7.   Update FLASH Memory after boot : No
  8.   Ethernet Interface Select .... : 10M / (100M) / (AUTO)
  9.   Take system setup from NVRAM . : No
  A.   System Setup Filename ........ : /etc/ts/ts.conf
  B.   Hosts Filename ............... : /etc/hosts
  G.   Default Gateway .............. : Not Defined
  F.   Set to factory defaults
  S.   Save
  E.   Exit
```

If the administrator responds with n, then the Boot configuration menu will be displayed along with the following message.

```
The Interface address is not set properly. Please try again
```

When the contents of the NVRAM are valid on booting, the prompt,

Available Memory = 16MB

Do you want to change the boot paramters ?n

will be displayed. If the administrator responds with y, then the boot configuration menu above will be displayed. If the administrator does not respond in 20 seconds, or responds with n, then the remote access server will continue the boot process as per the options configured in the NVRAM.

When the Flash Memory contains a valid server software, then the version number of the software will be indicated along with the option 6 in the boot configuration menu, like :

6. Boot From FLASH Memory .... : No (Ver 7.01)

On choosing an option by typing a number between 1 and 9, the option is redisplayed with the current value. For instance, if option 1 is chosen, then,

1. Interface Internet Address ….... : 80.0.0.64

is displayed.

Note The boot program will automatically fill up The Interface Subnet mask, once a valid internet address is given. It can be modified, if desired.

If an invalid internet address is typed after selecting option 1, then the message,

```
Illegal Internet Address. Try Again
```

will be displayed and the boot configuration menu will appear again with the old value.

The internet address must be given in dot notation, like, 200.100.150.1

By selecting option 3, the administrator may specify the primary boot server. The primary boot server may be specified to be a preferred boot server by giving the internet address of the host on the network. If no preferred boot server is required, the broadcast address of the subnet may be specified so that any host that responds to the TFTP request may be used as a download host. Specifying **0.0.0.0** also is sufficient for booting from any host.

By selecting option 4, the administrator may specify a secondary boot server which may be used for booting in case the primary boot server is not up. It is possible to specify a broadcast address as secondary boot server as in the case of primary boot server.

The default boot file to be downloaded from the host is */etc/ts/LANReach.mem*. The administrator may specify a full pathname in case the software is installed in a different directory or so. The maximum number of characters for the full pathname should not exceed 25 characters.

Note The path of the Boot Filename will be relative to the TFTPD server directory of the host system from which the boot file is downloaded. This is host operating system dependent. Refer to appropriate host manual.

If the flash memory is present in the server, normally, choosing yes as the option for updating flash memory will save the software. The option 6 can be set to yes to boot from flash memory, after the server software has been saved in flash.

The option 8, Ethernet Interface Select, provides an option to select the speed of the operation of the network whether it is 10 Mbps/100 Mbps. If the user selects the option AUTO, then the server will automatically find out the speed of the network by AUTO Negotiation.

The option A, Take Setup from NVRAM is used to specify whether the system setup information has to be read from Nonvolatile memory or from a file in a host. When this option is set to no, the setup information is read from the filename specified in System Setup File name option.

The option B, Hosts file name is used to download host database from the specified path of the Boot server. The factory default path is /etc/hosts.

The option F may be used to set boot parameters to factory defaults.

The option G, Default Gateway is used, if the boot server is not in the same network, the Remote access server will try to reach it through the default gateway. This parameter specifies the IP address of the default gateway. For example, let the IP address of the Remote access server is 200.200.200.100 and the IP address of the boot server is 201.201.201.100 which is in a different network. Assume we can reach the boot server using a gateway 200.200.200.1 from the Remote access server. This option has to specify the IP address of default gateway, which is 200.200.200.1

After configuring the boot options as described and desired, the boot configuration options can be saved in NVRAM using the save option S of the boot configuration menu.

On exiting from the boot configuration menu using the Exit option E, the server proceeds with the boot, wherein, the server software will be downloaded from the host specified (or from flash memory, if present and valid and the option is to boot from flash) in to the local memory. If the software is downloaded from the host and the flash memory update option is set to **yes**, then the prompt,

```
Do you want to continue ?
```

will appear. On typing **y** to the above prompt, the software will be saved in the flash memory and the following messages will be displayed.

```
Erasing..done
Writing............done
```

Also, while the saving is in progress, a series of dots will appear in the screen till completion of saving in the Flash Memory. After the software is saved in the Flash Memory, by choosing the option to Boot From Flash Memory to be **yes**, the server will boot from the flash memory on subsequent boots.

Installation of Download Software on the Host

The remote access server software available in the release media may be extracted to a temporary directory on the host system. The installation script *tsinstall*, which is part of the release, may be executed for installing the software. After installing the software on the host, the host address and the filename may be specified as the boot server address and boot filename in the boot configuration menu of the remote access server. Subsequently, while booting, the remote access server will download the software from the host.

The procedure for installing the download software on a host and details of the release media are described in the release note. Refer to the ***LANReach*** *Remote access server Release Note.*

Software Update

Subsequent to the first time installation of the server, the updates of server software may be downloaded from the host to the flash memory at the site itself.

The steps given below are to be followed for upgrading the server software in the flash memory to another version.

Step 1 Install the required version of download software on the host from which it should be downloaded to the remote access server, as explained above.

Step 2 Switch on the remote access server.

Step 3 Enter boot configuration menu.

Step 4 Set option 6 to **no** so that remote access server does not boot from Flash memory; instead downloads the software from host.

Step 5 Set option 7 to **yes** so that after downloading the software from the host, the flash memory is updated.

Step 6 Set option 3 to the internet address of the host where the software was installed in step 1.

Step 7 Set option 5 to the full pathname of where the installation is done in step 1.

Step 8 Save the boot configuration option.

Step 9 Exit from boot configuration menu.

Step 10 After downloading the software from the specified host, before updating the flash memory, the prompt,

Do you want to continue ?

will be displayed. Respond with **y**.

The flash memory will be updated and the following messages and series of dots will appear.

```
Erasing..done
Writing............done
```

If the Setup configuration information in the NVRAM is valid, the prompt,

```
    Do you want to setup the system?
```

will appear. If **n** is typed or if no response is given for 5 seconds, the remote access server will enter multi-user mode and the STATUS prompt will appear.

Note

Since the console port is separate and specifically meant for administration purpose, after the remote access server boot up, STATUS prompt will appear instead of RAS prompt.

Whenever, FLASH Memory is attempted to be written, the following warning message appears on the console :

```
WARNING    Flash is an expensive device in the system. It should
           be reprogrammed only for software upgradation.
```

Note

The FLASH Memory is an expensive device in the server. In order to have a longer life for the FLASH Memory, the user is advised not to do frequent writes onto flash memory. Preferably the user is required to write the flash memory, at the first time installation and subsequently only for software updating.

FLASH Memory is an optional component in the remote access server. If your remote access server does not contain one, installing the upgraded version of the download software on the boot server alone is sufficient. Subsequent, power-on of the remote access server will download the update from the boot server host.

3

COMMAND SET

Introduction

The remote access server consist of a powerful command set which can be subdivided into three categories, depending on their usage.

- General *user commands* which are available at the RAS prompt called the **main prompt.**

- Status *display commands* which are available after entering into the tsadmin mode by typing **tsadmin** from the prompt.

- *Administrative commands* which are privileged commands available only to the administrator who may enter into the administrative mode from tsadmin mode by typing either **admin** or **nvram** and entering the password.

  The administrative commands that enable the administrator to set/change configuration parameters permanently are available under **nvram** mode.

  The administrative commands that enable the administrator to set/change configuration parameters dynamically for the current boot and other general maintenance commands are available under **admin** mode.

Note

Since the console port is separate and specifically meant for administration purpose, after the remote access server boot up, STATUS prompt will appear. From the STATUS prompt, the administrator can switch to ADMIN or NVRAM mode by typing admin or nvram respectively.

GENERAL USER COMMANDS

Using General User Commands, the remote access server user may,

- Identify the hosts that are connected in network with the remote access server and verify whether they are alive
- create a session with any of the hosts
- suspend and resume these sessions
- list and name these sessions.

The following table 3.1 gives a list of general user commands.

Table 3.1 : General User Commands

No.	Command	Functions
1.	hosts	To get the names and internet addresses of hosts in the network and known to the server
2.	ping	To verify whether a host is active
3.	rlogin	To create a rlogin session with specified host.
4.	escape	To define an escape sequence which may be used to suspend the current session, or to disable the facility to suspend.
5.	Namesession	To name a session
6.	List	To display the list of sessions from a port to all/specified host(s)
7.	resume	To resume a suspended session
8.	detach	To close a session from a port
9.	stty	To display/set/modify port characteristics
10.	set	To display/set/modify port parameters
11.	telnet	To create a telnet session with a specified host
12.	tsadmin	To enter tsadmin mode

Identifying the hosts

To establish connection with a host system from a remote access server port, the user may have to know the list of hosts that are available in the network with the server and known to the server.

The command **hosts** displays the names of hosts known to the server and their internet network address.

Example

```
RAS>hosts
Internet address(es) /alias(es)           official host name(s)

127.0.0.1                                  localhost
196.1.68.50                                pallavi
196.1.68.49                                padmini
196.1.68.41                                indus
196.1.68.42                                hercules
```

If the names of one or more hosts are given with the command, the Internet addresses and names of the specified hosts are displayed.

Example

```
hosts pallavi

Internet address(es) /alias(es)           official host name(s)

196.1.68.50                                pallavi

hosts pallavi padmini
```

Given the network address of one or more hosts the command displays the names of the hosts.

Example

```
hosts 196.1.68.50 196.1.68.49

Internet address(es) /alias(es)    official host name(s)

196.1.68.50                        pallavi
196.1.68.49                        padmini
```

When it is required to use explicitly the static host database or dynamic database (DNS cache), **-s** or **-d** option must be used respectively, with the **hosts** command.

Example

```
hosts  -s sco

Entries shown from the static host database
official hostname         Internet address(es) /alias(es)
SCO                       220.0.0.1

hosts  -d sco

Entries shown from DNS cache
official hostname         Internet address(es) /alias(es)
SCO                       220.0.0.1
```

When a comparison between the static database and DNS cache is required -c option may be used.

Example

```
hosts  -c sco
```

When DNS cache is empty/unusable the **hosts** command with **-d** option displays an error message.

Example

```
hosts  -d sco

hosts: dns cache is empty.dns is not configured.
And dns is not usable
```

Verifying the host

On knowing the names of the hosts, the user may want to verify whether the host to which the user wants to connect is alive and active on the network. The command **ping**, displays the status of the host.

Example

```
ping indus
```

where **indus** is the host name, displays

```
indus is alive
```

if the host **indus** is active and

```
no answer from indus
```

if the host is not active.

The **ping** command transmits a packet of specified number of bytes to the host and based on whether the packet is received back or not identifies the host status. The default packet size is 64 bytes.

ping command with -s option displays packet transmit/receive status in detail.

It estimates the roundtrip time for the packet to reach the host across the network and return. This test is continued until the interrupt character is typed.

Note

The default interrupt character of the remote access server is CTRL-C. Refer to **stty** command for procedure to set the interrupt character.

Example

```
ping -s indus
```

```
64 bytes from indus (196.1.68.41) : icmp_seq=0. time = 0. ms
64 bytes from indus (196.1.68.41) : icmp_seq=1. time = 0. ms
64 bytes from indus (196.1.68.41) : icmp_seq=2. time = 0. ms
64 bytes from indus (196.1.68.41) : icmp_seq=3. time = 0. ms
64 bytes from indus (196.1.68.41) : icmp_seq=4. time = 0. ms
64 bytes from indus (196.1.68.41) : icmp_seq=5. time = 0. ms

---------indus PING statistics------------------
6 packets transmitted, 5 packets received, 16% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

The default packet size is 64. This may be changed by specifying the packet size in the command. Also, an iteration count may be specified.

Example

```
ping -s indus 100 10
```

will transmit and receive packets of 100 bytes each and this will be repeated for 10 iterations.

If the iteration count is not specified or specified as zero, then the test will be repeated till the interrupt character is typed.

Note

Ping uses the ICMP protocol. Some hosts may not support this protocol, in which case no answer from <host> will be printed.

Creating a Session

A session is created by typing the **rlogin** command.

Example

```
rlogin indus
```

On entering the command, the login prompt of the host appears on the terminal.

Optionally, the user trying to create the session may also give his login name by specifying the **-l** option in the **rlogin** command.

Example

```
rlogin indus     -l user1
```

On entering the command above, the prompt for typing the password appears on the terminal if the user has a password or logs into the system.

Optionally, the remote access server facilitates the user to name a session, to enable easy identification of the session at a later point of time. This is achieved by the **-n** option of the **rlogin** command.

Example

```
rlogin indus     -l user1     -n mysession
```

This command will result in a session to the host *indus* to be created, login as the user *user1* on the host and also name this session as *mysession*. On entering the command, the password prompt of the host will appear on the terminal.

Optionally, the user may create a rlogin session with 8-bit data transfer mode by specifying **-8** option.

Example

```
rlogin indus     -l user1     -n mysession       -8
```

This command will result in a session with 8-bit data transfer mode.

Note

1. The user may have multiple sessions to one or more hosts from a port.

2. The maximum number of sessions that may be connected from a port is limited to 8.

3. The administrator may reduce the maximum number of sessions from any port.

4. The user should ensure that **rlogin** service is enabled and active in the host.

Exiting out of a Session

After a login session is complete, when the user exits using the exit command of the host (or by typing CTRL -D), the session gets closed automatically and the RAS prompt reappears on the terminal.

Suspending a Session

The remote access server allows the user to suspend the session which he is currently in, by typing the escape sequence.

The remote access server by default recognizes ^T. (CTRL-T and DOT) as the escape sequence using which the user can suspend the session he is currently in. When the user suspends a session, the remote access server displays the RAS prompt on the terminal screen. The user may give any remote access server command at this prompt again.

Defining a Escape Sequence

The user may define a different escape sequence to suspend a session, using the command **escape**. The escape sequence, may have a maximum of four characters.

Example

```
escape ABCD
```

will define the escape character sequence to be ABCD. After this command, whenever the sequence ABCD is typed on the terminal, the session is suspended and the remote access server prompt is displayed.

When control characters are to be specified while defining the escape sequence, user may either type ^(caret) followed by the character or specify the equivalent octal value in the format ‘\xxx’ where ‘xxx’ is the three digit octal value.

Example

```
escape ^K
escape     \013
```

The user may also set the escape sequence back to the default value.

Example

```
escape default
```

The user may also want to turn off the facility to suspend and resume sessions by turning off the facility to escape from a session.

Example

```
escape disable
```

Subsequently, the user will not be able to suspend a session by typing the escape sequence.

The **escape** command without any arguments, displayed the current escape sequence.

Example

```
escape

current escape sequence is ^T
```

After suspending a session using the escape sequence, the user may execute any of the remote access server commands.

Naming a Session

A session may be named at the time of its creation using the **-n** option of the **rlogin** and **telnet** commands. Also, a session may be named subsequent to its creation, using **namesession** command. The **namesession** command may be used to name a session, modify the name of a session or unset the name of a session.

Example

```
namesession    8 mysess
```

will name the session whose session number is 8, as mysess. After this command, the session with session number 8 may be referred to by the name **mysess** in the other commands.

```
namesession    8
```

will unset the current name of the session whose number is 8. After giving this command, the session with number 8 can no longer be referred by its name.

It is also possible to use the * and # identifiers instead of the session number in the **namesession** command to name the current active or previous active sessions.

Example

```
namesession    * mysess
```

will result in the current active session being named as *mysess.*

```
namesession    # mysess
```

will result in the previous active session being named as *mysess*.

List the Existing Sessions

To get a list of the existing sessions from a port, the command **list** may be used.

The **list** command displays on the terminal,

- the session number
- type of connection (rlogin, telnet)
- number of data bytes waiting to be output on the terminal from this session
- session name
- the destination host to which the session establishes connection.

The **list** command may be used, to display the details for

- a given session, by specifying the session-id
- a list of given sessions, by specifying their session-ids.
- all sessions to a given host by specifying the host name
- for the current or previous active session by specifying * or #.

Example

1. list indus

   will list details about all sessions connected to the host indus.

2. list 8 15

   will list details about sessions whose numbers are 8 and 15.

3. list

   on a port on which there are no sessions, will display the following:

```
Upto 8 sessions are allowed from the port S0
No sessions open from this port
```

4. Without any arguments, the command displays details of all sessions from the port.

```
Upto 8 sessions are allowed from this port S2.

Session-no.  (type)    data   name   destination
0 *          (telnet)  2560   --     hclhpmas
4 #          (rlogin)  0      --     hercules
5            (rlogin)  0      --     hclhpmas
6            (rlogin)  0      --     indus
```

Resuming a suspended session

A session that has been previously suspended, may be continued again by giving the resume command.

The session may be resumed by specifying

- the session number or
- the session name or
- the host name of the host to which the session is created. The host name can be used to resume a session only if there is exactly one session to the host from the port.

Example

```
resume 8
resume mysess
resume indus
```

The current active or previous active sessions may be resumed by

```
resume *
```

and

```
resume #
```

respectively.

The command **resume** without any arguments resumes the current active session.

Closing a Session

The session with the host, may be closed down using the **detach** command.

The session to be closed, may be specified by the session number or the name of the session if the session has a name, or the host name with which the session is created.

Example

```
detach 8
```

will close the session with session number 8.

```
detach mysess
```

will close the session whose name has been set as **mysess**.

```
detach indus
```

will close the session with the host **indus**, if only one session exists with **indus**.

It is also possible to close the current active session by the command

```
detach *
```

The command

```
detach #
```

may be used to close the previous active session.

Multiple session-ids or session names can be specified in the **detach** command.

```
detach 8 15
detach mysess1 mysess2
```

All sessions can be closed by using **-a** option.

```
detach –a
```

Setting Port Parameters

The **set** command permits the user to specify,

- a termname for the terminal
- prompt to be displayed by the remote access server
- input hardware flow control option
- output hardware flow control option.

The user may restrict changes to his port by **port_modify** option of **set** command. This option can be changed only in Admin mode. The user can able to change the options of **set** command, only if port_modify option is set to permitted mode. If the user attempts to change the options of set command, when port_modify is in denied mode, then the following message will appear

set: Permission denied

The **set** command will also display

- maximum number of possible sessions from the port
- list of hosts to which this port is permitted/denied access
- type of this port connection.

The command,

```
set term=vt100
```

sets the TERM environment variable to vt100.

The command,

```
set prompt=LANREACH>
```

changes the prompt displayed by the server from

```
RAS>
```

into

```
LANREACH>
```

The prompt may be a string of maximum of 10 characters.

The command,

```
set inflow=<option>
```

sets the input hardware flow control to use the specified option for input side hardware flow control.

The command,

```
set ohwflow=<option>
```

sets the output side flow control to use the specified option.

The following table gives the **<option>** available and the meaning:

Option	Meaning
Rts	Use RTS signal for flow control. This can be used only with input hardware flow control.
Rts	Use CTS signal for flow control. This can be used only with output flow control.
None	Use no hardware flow control. This can be used with both input and output hardware flow control.

Display and Modify Characteristics

The **stty** command enables the user to display and modify characteristics of a port.

The characteristics that can be manipulated by this command are:

- baud rate
- transmission character size 7 or 8 bit
- odd or even parity
- enable or disable checking of parity
- one or two stop bits
- enable or disable input flow control (software flow control)
- enable or disable output flow control (software flow control)
- modem control or no modem control
- DSR signal sensing
- DTR signal toggling
- erase character
- interrupt character
- start character
- stop character
- escape sequence

The characteristics of a port can be changed only if **port_modify** option of **set** command is in permitted mode. If the user attempts to change the **characteristics** of **stty** command, when **port_modify** is in **denied** mode, then the following message will appear

stty: Permission denied

The **stty** command without any arguments displays current characteristics of the port.

Example

```
stty S1
+ixon -ixoff +ignbrk 9600 cs8 +parodd -parenb -cstopb +clocal intr=^C
erase=^H start=^Q stop=^S escape=^T
```

Set Baudrate

```
stty S1 9600
```

sets the baud rate of the port S1 to 9600.

The possible baudrates to which the port may be set are:

```
50, 75, 100, 150, 200, 300, 600, 1200, 1800, 2400,3600,
4800, 7200, 9600, 19200, 38400, 14400, 57600, 76800, 115200,
230400, 460800
```

However, the terminal on the port must be capable of supporting the baud rate specified in the **stty** command. The appropriate terminal reference manual may be referred to get the details on supported baud rates.

Set Transmit Character Size

The command,

```
stty S1 cs7
```

sets the transmit character size to 7 bits.

The command,

```
stty S1 cs8
```

sets the transmit character size to 8 bits.

Set the Parity Type

The command,

```
stty S1 parodd
```

or

```
stty S1 +parodd
```

sets the parity to odd and the command

```
stty S1 -parodd
```

sets the same to even.

Enable and Disable Parity Check

The command,

```
stty S1 parenb
```

or

```
stty S1 +parenb
```

enables the parity checking and the command

```
stty S1 -parenb
```

disables checking of parity.

Set Number of Stop Bits

The command,

```
stty S1 cstopb
```

or

```
stty S1 +cstopb
```

sets number of stop bits to 2, whereas

```
stty S1 -cstopb
```

sets the number of stop bits to 1.

Controlling Software Flow Control

To enable output flow control, the command

```
stty S1 ixon
```

or

```
stty S1 +ixon
```

may be used.

```
stty S1 -ixon
```

will disable the output flow control.

Similarly, the commands,

```
stty S1 ixoff
```

or

```
stty S1 +ixoff
```

and

```
stty S 1 -ixoff
```

will enable and disable input flow control respectively.

Break Signal

The **stty** command displays the break signal option also. This is a non-modifiable option.

Modem Control

```
stty S1 clocal
```

or

```
stty S1 +clocal
```

disables modem control.

```
stty S1 -clocal
```

enables modem control.

Enable DSR signal sensing

```
stty S1 dsr
```

or

```
stty S1 +dsr
```

enables DSR signal sensing i.e. the connection will be established only when DSR signal is active (the device is present). If the DSR signal is not active, the connection will not be established. This option can be enabled to avoid data loss by transferring data only if the device is present. By default, this option will be disabled.

```
stty S1 -dsr
```

disables DSR signal sensing feature. If the option is disabled, the connection will be established irrespective of DSR signal status.

Enable DTR signal togglling

```
stty S1 dtr
```

or

```
stty S1 +dtr
```

enables DTR signal toggling feature. If this option is enabled, the DTR signal will be acive only when the connection is alive. If this option is disabled, the DTR signal will be active always.

```
stty S1 -dtr
```

disables DTR signal toggling feature.

Define Control Characters

```
stty S1 erase=A
```

will set the erase character to A. Subsequently, typing **A** will result in erasing of the character last typed.

```
stty S1 intr=A
```

will set the interrupt character to A. After this setting, typing the character **A** will result in the process getting interrupted.

```
sttySIstop=^S
```

will set the stop character to ^S. After this command, typing the character **^S** will cause the output flow control to be effected, the display to be stopped.

```
sttySIstart=^Q
```

will set the start character to ^Q. After this command, typing the character **^Q** will cause the display stopped earlier due to the stop_character to be resumed.

```
sttySIescape=^T
```

will set the escape sequence character to ^T. Note that this is same as **escape ^T** command.

When control characters are to be specified while defining the escape sequence, user may either type ^(caret) followed by the character or specify the equivalent octal value in the format '\xxx' where 'xxx' is the three digit octal value. It is recommended that the octal value format is used rather than ^(caret) format.

Example

```
sttySIescape=^K
sttySIescape=      \013
```

Define Character for Session Switching

```
sttySIswitch=^B
```

will set the session switching character to ^B. Subsequently, typing ^B will result in switching of the sessions sequentially incase of two or more sessions. Suppose, if there are five sessions are active as shown below.

```
session-no  (type)   data   name    destination
0          (telnet)   0              10.10.30.2
1 #        (telnet)   0              10.10.30.2
2 *        (telnet)   0              10.10.30.2
3          (telnet)   0              10.10.30.2
5          (telnet)   0              10.10.30.2
```

Let the user is currently in session 0. Pressing ^B will take the user to session 1. Pressing ^B again will take the user to session 2. The default character is ^K.

Telnet

The **telnet** command like **rlogin** command, establishes connection with a specified host.

Example

```
telnet everest
```

On establishing connection with the host *everest* the login prompt of the host will appear on the terminal. Like in **rlogin** command, it is possible to name a session, optionally, using the **-n** option.

Example

```
telnet everest -n mysession
```

Optionally, user may specify a network service port number in the **telnet** command, so that connection with the specified service port on the given host is established instead of **login** service.

Example

```
telnet indus 19
```

This command establishes connection with network service port 19 of the host indus.

Note

For details of the network ports and the services provided by the host, refer to **services** database and the manual page on **services** on the required host. Also ensure that the required services are enabled and active on the host.

Optionally, a telnet session may be initiated with **-d** option, in which case debug messages indicating the flow of operations will be displayed.

Example

```
telnet -d everest

received DO TTYPE
received WILL SGA
received SB, TTYPE, SEND
sent SB, TTYPE, SEND
```

```
received DO 1
sent WONT 1
login: received DONT 1
```

After connecting to the host, using the telnet command, when the user types the telnet escape character, the prompt,

```
telnet>
```

appears on the terminal.

The default telnet escape character is CTRL-]. When telnet session is invoked from RAS prompt, the current escape character is displayed.

```
RAS> telnet hercules
Trying ...
Connected to hercules.
Escape character is '^]'.
login:
```

At the telnet prompt, typing help or ? displays a menu of telnet commands.

```
telnet> help
```

For description of **telnet** commands refer to *Telnet Commands*.

STATUS DISPLAY COMMANDS

LANReach Remote access server includes commands using which, user may

- see remote access server name, server software version, processor type etc.
- display diagnostic messages on the server
- obtain the status of different systems on the network with the server
- display the status of the various server processes
- display statistics on the server activities
- display process stack
- display ARP table contents
- Identify the hosts on the network
- Verify availability of hosts
- Query the DNS name server

Table 1.2 gives the list of status display Commands.

Table 3.2 : Status Display Commands

No.	Command	Functions
1.	kmesg	To display system boot and diagnostics messages
2.	uname	To display server details
3.	ruptime	To display status of hosts on the network
4.	netstat	To display network activity statistics
5.	ps	To display details of processes running on the server
6.	dod	To display Dial on Demand path statistics
7.	arp	To display ARP table contents
8.	ping	To verify whether a host is alive
9.	hosts	To get the names and internet address of hosts in the network and known to the remote access server through static host database or through name resolver.
10.	dnsquery	To query the name server and display the results.
11.	quit	To quit from RAS admin mode to RAS prompt or logout from remote access server.
12.	admin	To enter admin mode
13.	nvram	To enter NVRAM mode.

These commands, which help the user achieve the above facilities, are normally used by advanced users and remote access server administrators, to collect details about the server for maintenance and trouble shooting.

Typing admin at the `Stat>` prompt takes the user to the admin command mode. The user is prompted to type the password. On entering the correct password the prompt:

```
Admin>>
```

appears on the terminal.

Typing nvram at the `stat>` prompt takes the user to the nvram command mode. The user is prompted to type the password. On entering the correct password the prompt

```
Nvram>>
```

appears on the terminal.

Display Version Details

The **uname** command displays :

- remote access server product name
- node name of the server
- Version number of the server software
- Model number

Example

```
Stat>uname
LANReach LANReach Version - 7.07 1600F
```

Display Diagnostics Information

The command **kmesg** displays all the diagnostic information about the server.

Example

```
kmesg
```

When **-p** option is used, the **kmesg** command displays the panic message stored in the non volatile memory.

```
kmesg -p
```

When **-c** option is used, the **kmesg** command clears the panic message stored in the non volatile memory.

```
kmesg -c
```

Display Status of Hosts on the Network

The command **ruptime** displays the status of each **host** on the network.

The status displayed for each host includes.

- host name
- whether up or down
- duration for which the host is up or down in the form

  number of days + number of hours : number of minutes
- number of users on the host
- load on the system

The command display is similar to the **ruptime** command on UNIX systems.

Note

- **ruptime** command uses **rwhod** protocol. This protocol queries the state of the system on the network to update status messages and will be enabled only when the **rwhod_send** is set to **send** in the **Admin** mode. This can be done using **configuration** command.
- The number of users and load displayed for the remote access servers will be 0 always.

Example

```
ruptime

LANReach  up  0:30,  0 users, load 0.00, 0.00, 0.00
 rasunix   up  5:49,  6 users, load 2.12, 1.96, 1.92
```

Display Process Status

The **ps** command displays the following details indicating the status of the processes on the remote access server.

- process id
- state of the process, sleep, delay, current priority of the process
- channel on which the process is waiting/sleeping
- control terminal
- cumulative execution time
- signal
- process flags
- stack pointer address
- name of the process

The **ps** command is provided for better problem analysis in case user encounters a problem. The **ps** command output should be enclosed while reporting problems.

Example

```
      ps

PID STATE   PRIO   WCHAN   TTY  TIME  SIGNAL  FLAGS  STACK  COMMAND

  0  sleep   20  1437540   ?    0:05    0      1  16df80c init
  1  sleep   20  14c8dbc   ?    0:27    0      1  16e280c STREAMER
  2  sleep   20  1438bbc   ?    4:07    0      1  16e580c watchdog
  3  delay   20        0   ?    0:24    0      0  16e880c KEEP
  4  delay   20        0   ?    0:00    0      0  16eb80c persd
  5  delay   20        0   ?    0:00    0      0  16ee80c rwhod
  6  delay   20        0   ?    0:00    0      0  16f180c namsd
  7  sleep   20  17ce9ac   ?    0:00    0      1  16f480c dhcpd

      .
      .
```

Display Server Activity Statistics

The remote access server maintains statistical information regarding the interfaces, protocols and STREAMS usage to help in trouble shooting. The **netstat** command displays the network statistics in detail.

These details will help in analyzing the status and reliability of the network and will help in diagnosing and trouble shooting. While reporting problems, it is recommended that these statistics are also enclosed.

Example

1. netstat

   will display the network statistics as follows :

```
Active Internet connections

Proto Recv-Q Send-Q  Local      Foreign (state)   channel
                     Address    Address
tcp    0      0    *.login       *.*     LISTEN(  5)  0
tcp    0      0    *.telnet      *.*     LISTEN(  5)  1
udp    0      0    *.echo        *.*     IDLE
udp    0      0    *.discard     *.*     IDLE
udp    0      0    *.who         *.*     IDLE
udp    0      0    *.68          *.*     IDLE
udp    0      0    *.route       *.*     IDLE
udp    0      0    *.1026        *.*     IDLE
udp    0      0    *.snmp        *.*     IDLE
```

2. netstat -n

   will display the statistics with host addresses instead of names

```
Active Internet connections

proto Send-Q  Local Address     Foreign Address   (State)
tcp   0       196.1.68.53.1004  196.1.68.42.513   ESTABLISHED
tcp   0       196.1.68.53.1028  196.1.68.38.19    ESTABLISHED
tcp   0       196.1.68.53.987   196.1.68.38.513   ESTABLISHED
tcp   0       196.1.68.53.986   196.1.68.41.513   ESTABLISHED
```

3 netstat -r

will display the routing table information

Routing tables

```
Destination    Gateway  Flags   Refs  use       Metric  Interface
196.1.68.32    bargavi    U      7    1139932   0        amd0
```

4 netstat -m

will display the STREAMS block usage statistics

5 netstat -l

will display the status of all network interfaces.

```
Name   Mtu    Network       Address   Ipkts    Ierrs    Opkts  Oerrs  Coll
amd0   1500   196.1.68.32   bargavi   543071   1        842398 0      495
```

6 netstat -lamd0

will display status of amd0 interface.

7. netstat -sip
netstat -sudp
netstat -stcp
netstat -sdns

will display the statistics about the protocol specified. The protocols for which the statistics can be obtained are: ip, udp, tcp, dns.

8 netstat -h

will display usage of memory heap.

9 netstat -c3

displays statistics about TCP channel number 3.

The user may want to observe the network activities for continued duration by repeatedly sampling the statistics at regular time intervals. The '-t' option enables this. When a time interval is specified, the activities will be repeatedly displayed after sampling for those many seconds each time. The sampling can be stopped by typing the interrupt character.

Example

```
netstat -sip -t10
```

Display Dial-On-Demand statistics

The **dod** command displays statistics on dial-on-demand path. It displays the dial-on-demand path name, start time of the path and end time of the path.

Display ARP Table Contents

The remote access server maintains the Address Resolution Protocol table (ARP table) which provides the mapping between the Internet address of the host system and the Ethernet address of the network interface. The command **arp** displays the contents of the ARP table. It displays

- Node name
- Internet address
- Ethernet Address
- Status of the entry, which has internal information about the usage of the entry.

Example

```
arp
nodename     Internet Address    Ethernet Address       Status

indus          196.1.68.41       0.128.72.128.126.133   05
hercules       196.1.68.42       0.0.112.0.0.149        05
hclhpmas       196.1.68.38       8.0.9.24.141.147       05
```

Identifying the hosts

To establish connection with a host system from a remote access server port, the user may have to know the list of hosts that are available in the network with the server and known to the server.

The command **hosts** displays the names of hosts known to the server and their internet network address

Example

```
RAS>hosts

internet address(es) /alias(es)   official host name(s)
127.0.0.1                         localhost
196.1.68.50                       pallavi
196.1.68.49                       padmini
196.1.68.41                       indus
196.1.68.42                       hercules
```

If the names of one or more hosts are given with the command, the Internet addresses and names of the specified hosts are displayed.

Example

```
hosts pallavi

Internet address(es) /alias(es)       official host name(s)
196.1.68.50                           pallavi
hosts pallavi padmini
```

Given the network address of one or more hosts the command displays the names of the hosts.

Example

```
hosts 196.1.68.50          196.1.68.49

Internet address(es) /alias(es)   official host name(s)
196.1.68.50                        pallavi
196.1.68.49                        padmini
```

When it is required to use explicitly the static host database or dynamic database (DNS cache), **-s** or **-d** option must be used respectively, with the **hosts** command.

Example

```
hosts -s sco

Entries shown from the static host database
official hostname       Internet address(es)/alias(es)
SCO                     220.0.0.1

hosts -d sco

Entries shown from DNS cache
official hostname       Internet address(es)/alias(es)
SCO                     220.0.0.1
```

When a comparison between the static database and DNS cache is required -c option may be used.

Example

```
hosts -c sco
```

When DNS cache is empty/unusable the **hosts** command with **-d** option displays an error message.

Example

```
hosts -d sco

hosts : dns cache is empty.dns is not configured.
                 And dns is not usable
```

Verifying the host

On knowing the names of the hosts, the user may want to verify whether the host to which the user wants to connect is alive and active on the network. The command **ping**, displays the status of the host.

Example

```
ping indus
```

where **indus** is the host name, displays

```
indus is alive
```

if the host **indus** is active and

```
no answer from indus
```

if the host is not active

The **ping** command transmits a packet of specified number of bytes to the host and based on whether the packet is received back or not identifies the host status. The default packet size is 64 bytes.

ping command with **-s** option displays packet transmit/receive status in detail.

It estimates the roundtrip time for the packet to reach the host across the network and return. This test is continued until the interrupt character is typed.

Note

The default interrupt character of the remote access server is CTRL-C. Refer to **stty** command for procedure to set the interrupt character.

Example

```
ping   -s indus
```

```
64 bytes from indus (196.1.68.41):  icmp_seq=0.  time = 0. ms
64 bytes from indus (196.1.68.41):  icmp_seq=1   time = 0. ms
64 bytes from indus (196.1.68.41):  icmp_seq=2.  time = 0. ms
64 bytes from indus (196.1.68.41):  icmp_seq=3.  time = 0. ms
64 bytes from indus (196.1.68.41):  icmp_seq=4.  time = 0. ms
64 bytes from indus (196.1.68.41):  icmp_seq=5.  time = 0. ms

 ------ indus PING statistics ---------------
 6 packets transmitted, 5 packets received, 16% packet loss
 round-trip (ms) min/avg/max = 0/0/0
```

The default packet size is 64. This may be changed by specifying the packet size in the command. Also, an iteration count may be specified.

Example

```
ping   -s indus 100 10
```

will transmit and receive packets of 100 bytes each and this will be repeated for 10 iterations.

If the iteration count is not specified or specified as zero, then the test will be repeated till the interrupt character is typed.

Note

Ping uses the ICMP protocol. Some hosts may not support this protocol, in which case `no answer from <host>` will be printed.

Query the DNS Name Server

The remote access server implements a name resolver component of the Domain Name Service. Configuring the DNS to run and setting up a domain name and defining the host to be used as name server are done by the administrator. The **dnsquery** command causes the remote access server to send a DNS query to the name server and display the results.

The **dnsquery** command will help in identifying problems with DNS and analyse them.

Example

```
dnsquery indus
```

examines the status of host **indus** by querying the defined name server and displays the result of the query.

A specific domain name to be used for the current query can be specified using **-n** option.

```
dnsquery -n hclhprnd.uunet.in indus
```

Instead of the defined name server, a specific host to be preferred as name server can be specified using **-s** option.

```
dnsquery -s calculus indus
dnsquery -s calculus -n hclhprnd.uunet.in indus
```

The host and name server can be specified by name, alias or internet address.

To get more detailed display **-d** option may be used

```
dnsquery -d10 indus
```

Specifying a higher number gives more details.

Quit

The user may enter tsadmin mode from the RAS prompt or by using rlogin to the remote access server. This facility known as Remote Administration Facility enables administration of the remote access server from other systems apart from terminals connected to the remote access server.

The **quit** command causes the user to go back to the RAS prompt if he has entered tsadmin from there or logs him out to the system from where he rlogged in to the remote access server.

Example

```
1.    stat> quit
      RAS>
2.    stat> quit
      hercules#
```

ADMINISTRATIVE COMMANDS

LANReach technical server administrator may, on a terminal connected to the remote access server port, type tsadmin command at the RAS> prompt which will display the `Stat>` prompt. From the `Stat>` prompt, administrative mode may be entered. In this case, when the administrator type quit, the RAS> prompt is displayed.

The administrator may also remote login to the remote access server from any host using `rlogin` command available on the host, which will directly enter into **tsadmin** mode and display the `Stat>` prompt. From the `Stat>` prompt administrative mode may be entered. In this case, when the administrator types quit the remote login session from the host closes down.

LANReach remote access server administrator may, go into the administrative mode from the `Stat>` prompt. For changing configuration parameters dynamically for the current boot of the server, the administrator may type admin from the `Stat>` prompt of TSadmin mode. The changes done at the admin mode take immediate effect and will be in effect only until the remote access server is shutdown.

The administrator may make permanent changes to configuration at the setup configuration mode (single user mode) as defined previously or may type nvram at the `Stat>` prompt. The difference between the setup configuration changes and nvram mode changes are that the setup configuration changes take effect when the RAS goes to multiuser mode. Whereas nvram mode changes take effect only after rebooting the remote access server, subsequent to the changes. In both these cases the changes are saved in non-volatile memory and are permanent.

From the `Stat>` prompt when the admin or nvram command is typed, the prompt for the administrative password will be displayed on the terminal. The password will not be echoed on the terminal. After validating the password the administrative prompt is displayed on the terminal as

either

```
        Admin>>
```

or

```
        nvram>>
```

depending on the command type. Once the administrative mode is entered by giving a correct password, all prompt are displayed with two > symbols instead of >. This is to indicate that the user is in privileged mode and should not leave the terminal unattended in that mode. Even if the administrator changes to stat mode from the administrative mode, the prompt will be `Stat>>`.

Only after a quit is typed, the user exits from the privileged mode.

Note

The remote access server is delivered with the default administrative password of HCLPD

If the administrator password of the remote access server is forgotten, contact the Support team for recovery.

Table below lists down the administrative commands, a brief explanation about their function and their availability under admin, nvram modes.

Table 3.3 : Administrative Commands

No	Command	Function	Availability
1.	activity	Display port activities	Only under admin mode
2.	configure	Configure server parameters	Under both admin and nvram mode
3.	date	Display/Set date on the server	Only under admin mode
4.	detach	Close down a session	Only under admin mode
5.	factory	Reset to factory default	Only under nvram mode
6.	getconfig	Get configuration information from specified host	Only under nvram mode
7.	bootconfig	Configure boot parameters	Only under nvram mode
8.	gethost	Get host database from the specified host	Only under admin mode
9.	help	Display help	Under both admin and nvram mode
10.	putconfig	Save the configurations on a host	Under both admin and nvram mode
11.	reboot	Reboot the remote access server	Only under admin mode
12.	route	Add/Modify/Delete/Display routing table information	Only under admin mode
13.	set	Set port parameters	Under both admin and nvram mode
14.	snmpconfig	Set SNMP parameters	Under both admin and nvram mode
15.	stty	Set port characteristics	Under both admin and nvram mode
16.	wall	Write administrative message to all ports.	Only under admin mode

17.	write	Write administrative message to specified ports.	Under both admin and nvram mode
18.	ifconfig	To show/modify interface configuration	Only under admin mode
19.	reset	To reset a port	Only under admin mode
20.	filter	To enter into protocol filter menu	Only under admin mode
21.	dod	To enter into Dial On Demand mode	Only under admin mode
22.	staticroute	To enter into staticroute menu	Only under admin mode
23.	statistics	To enter into RAS prompt menu	Only under admin mode
24.	http	To enter into Web server directory	Only under nvram mode
25.	ppl	To enter into ppl menu	Only under admin mode
26.	quit	Exit from administrative mode	Under both admin and nvram mode

After completing the administrative tasks, the administrator may go back to the general user command mode, by typing the command quit; or to the status display command mode by typing **statistics**.

Note

Any changes made in the configuration using administrative commands under admin mode will be effective immediately. The changes cannot be saved permanently and will be lost on powerdown. To make permanent changes, the changes should be done in either setup configuration at boot or under nvram mode.

Activity

The activity command displays the information regarding the port activity. The information displayed are:

- Name of the port
- Type of port configuration (Fixed/Implicit/Printer)
- Terminal name
- Maximum number of sessions configured on the port
- Number of characters transmitted
- Number of characters received
- Number of characters overrun
- Number of errors
- Number of characters lost.

After this, for each of the ports, the following session details are displayed:

- Session number
- Command used (rlogin)
- Session name
- Host to which session establishes connection

The syntax of the command is:

activity *portname* [, *port name* ...]

When no *port name* is specified, details about all ports are displayed by the command.

This command is available only under nvram mode.

Example

```
activity S2
```

will display

```
Port   Type   Traffic:  Xmt       Recv   Overrun  Errors  Lost
S3     line             686985    20911   0         0       0

Sessions from port S2 are:

1      (rlogin)         I      indus.hclhprnd.uunet.in
8      (rlogin)         ch     cheetah.hclhprnd.uunet.in
```

```
activity
```

Configure

The configure command is used for setting the system wide parameters of the server. The parameters that may be set by the **configure** command are:

- Name of the server
- Port number for the Fixed pty server
- Whether ARP trace is to be enabled or not
- Mode in which rwhod must function (quiet or send)
- Mode in which the routed daemon must function (quiet or send)
- Whether IP packets are to be forwarded if not intended for this server.
- Whether the TCP acknowledgment should be delayed or immediate.
- Administrative password
- Domain Name System to be configured or not
- Domain Name Servers
- sName of the domain
- Reverse Telnet pool distribution mode

The configure command is available under both **admin** and **nvram** modes.

The syntax of the command is:

```
configure [ <option> [= <value>] ]
```

The configure command without any options will display the current configuration information.

The options that may be configured and the possible values are explained below.

name

Name of the server. The server name should be set from the Setup Configuration Menu. It cannot be changed here.

fptyport

Fixed pty port number. This should be set from the Setup Configuration Menu. It cannot be changed here.

arp_trace=on|off

The Address Resolution Protocol resolves the host name to address mappings. If the ARP trace is **on**, then a trace of all ARP packets sent or received by the server is displayed on the console.

If the trace is set to **off**, this information is not displayed.

rwhod_send=quiet|send

The daemon **rwhod** services the **ruptime** command by sending packets of information. This will be done only when this option is set to **send**.

routed_send=quiet|send

The daemon **routed** implements the RIP protocol used for routing. This option controls whether the server should transmit RIP information. Normally, RIP information should be transmitted only by nodes acting as a gateway. When this option is set to send the RIP information is transmitted.

ip_forward=on|off

When multiple network controllers are present in the remote access server hardware, the server can act as a gateway between two networks. To get this functionality, the configuration should define ip_forward=on so that all internet packets from one network will be forwarded to the other network, if they are meant for the other network. If forwarding is disabled by configuring ip_forward=off, then the functionality of a gateway will not be there. IP forwarding can also be done with a single network controller. In this situation, packets not meant for the server will be forwarded to the right node.

tcpnodelack=on|off

The server generates acknowledgment packets in response to incoming TCP data. These ACK packets can be delayed for performance reasons to reduce network traffic. This parameter controls whether TCP acknowledgment should be delayed or immediate. TCP acknowledgment will be delayed if **off** is specified and will be immediate if **on** is specified.

dns=on|off

The domain name system on the remote access server may be configured by setting **dns** to **on**. Once this is done dynamic DNS name to address binding to take effect. The dynamic mapping can be removed by specifying **off**.

nameservers=*internet address, internet address* ...

The *internet* address of the host which functions as the name server for DNS, is specified by this option. More than one name server may be specified by giving a list of internet addresses separated by comma. A maximum of 4 servers can be specified. When more than one name server is available, a query is sent to the first available server in the list. Only in case of problems with the first, the next server is referred. If no nameserver is specified, DNS will be unusable.

domain=*domain name*

The name of the domain can be specified in this option. If domain name is not specified, DNS will be unusable.

pool_distr=round-robin|linear

When multiple ports are configured reverse telnet type, with one TCP channel, they constitute a pool. If the user wants to distribute the usage of ports in a round-robin manner, round-robin may be specified. If the user wants to use the first available port, the option should be set to linear.

password

When this option is specified in the **config** command the prompt,

```
Enter old Password:
```

will appear. On typing the current administrator password, the prompt,

```
Enter new Password:
```

will appear. The new password may be typed now. On entering the new password, the prompt for reconfirming the password will appear as:

```
Reenter new Password:
```

The new password should be typed again to reconfirm. The default admin password is HCLPD. The maximum number of characters for the password is 16.

Date

The **date** command is used to

- display the current date and time
- modify the date and time, set on the server

The **date** command is available only under **admin** mode.

The command syntax:

```
date [mmddhhmmss[yyyy]]
```

The **date** command without any argument displays the date and time currently set on the server.

When the **date** command is followed by an argument, the argument is interpreted as follows:

• 2 digit month number	- 01 means January and 12 means December
• 2 digit date	- 01 to 31
• 2 digit hour	- 00 to 23
• 2 digit minutes	- 00 to 59
• 2 digit seconds	- 00 to 59
• optionally 4 digit year	- 2000 to 2199

If the year is not specified, it is taken to be 2000.

Example

```
date 11091236082001
```

will set the date and time to Nov 9, 2001 and 12:36:08 Hrs. respectively.

Example

```
date 12141827002020
```

will set the date and time to Dec 14, 2020 and 18:27:00 Hrs. respectively.

Closing Down a Session

The administrator may close down a session of any user. The **detach** command may be used for this function. This command is available only under **admin** mode.

The syntax of the command is:

```
detach session-number [,session-number ...]
```

where *session-number* is the session identifier.

Example

```
detach 8
```

Note

Only the administrator may forcibly close down sessions of other users through **detach** command. This **detach** command does not accept session name and host name as parameters.

Reset to Factory Default

All the remote access server configuration parameters saved in the non-volatile memory may be reset to factory default values by the administrators in order to resolve critical situations. The command **factory** resets the parameters in the non-volatile memory to factory default values.

This command is available only under **nvram** mode.

Example

```
factory
```

getconfig

The **getconfig** command, present only under **nvram** mode is used to download the configuration information from a specified file in a specified host.

The command syntax is

```
getconfig [host]:[file]
```

The specified *file* containing the configuration information is downloaded through TFTP requests, from the *host*. The default host is the boot server specified in boot configuration. The default file is */etc/hosts*.

gethost

The **gethost** command available only under **admin** mode, is used to download the host database file from the specified host.

The command syntax is

gethost [*host*]:[*file*]

The specified *file* containing the host **database** information will be downloaded from the given *host.*

The default host is the boot server specified in boot configuration. The default file is */etc/hosts*.

Configure boot parameters

The administrator can configure the boot parameters of the **LANReach** using **bootconfig** command. The syntax of the **bootconfig** command is

bootconfig [*modify* | *show*]

modify

with this option, the administrator can modify the boot parameters

show

with this option, the administrator can view the boot parameters.

If no options are given, current boot parameters will be displayed.

Example

bootconfig

will display the current boot parameters.

```
                  BOOT PARAMETERS

     1.   Interface Internet Address ... : 80.0.0.62
     2.   Interface Subnet mask ........ : 255.0.0.0
     3.   Primary Boot Server .......... : 80.0.0.20
     4.   Secondary Boot Server ........ : Not Defined
     5.   Boot Filename ................ : /tstsyncn.mem
     6.   Boot From FLASH Memory ....... : Yes (Ver 7.01)
     7.   Update FLASH Memory after boot : Not Applicable
```

```
8.    Ethernet Interface Select .... : AUTO/(100M)/(10M)
9.    Take system setup from NVRAM . : Yes
A.    System Setup Filename ........ : /etc/ts/ts.conf
B.    Hosts Filename ............... : /etc/hosts
G.    Default Gateway .............. : Not Defined
```

gethost

The **gethost** command available only under **admin** mode, is used to download the host database file from the specified host.

The command syntax is

gethost [*host*]:[*file*]

The specified *file* containing the host **database** information will be downloaded from the given *host.*

The default host is the boot server specified in boot configuration. The default file is */etc/hosts*.

Help

The **help** command gives a list of commands available at the **admin** or **nvram** mode of the server depending on under what mode the user is presently in. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command.

Example:

```
help configure
```

will display details like syntax, description and explanation for the arguments of the command configure.

The **?** command and **help** command may be used interchangeably.

Save Configuration Information

The administrator may save the current server configuration information on any of the hosts in the same network as the server on a given file name. The syntax of the **putconfig** command which does this function is:

```
putconfig <host>:<file>
```

This command results in the current server configuration to be transferred to the host <*host*> as a file <*file*>, using the trivial file transfer protocol tftp. This file may later be used for reconfiguring the server in the event of a loss of local configuration information.

This command is available under both **admin** and **nvram** mode.

Example:

```
putconfig indus:/etc/ts/bargavi.conf
```

Note

putconfig command will work properly only if the TFTP write service is enabled properly on the host. Refer appropriate host documentation for details.

Configure boot parameters

The administrator can configure the boot parameters of the lanreach using **bootconfig** command. The syntax of the **bootconfig** command is

bootconfig [*modify* | *show*]

modify

with this option, the administrator can modify the boot parameters

show

with this option, the administrator can view the boot parameters.

If no options are given, current boot parameters will be displayed.

Example

bootconfig

will display the current boot parameters.

```
                    BOOT PARAMETERS

1.   Interface Internet Address ... : 80.0.0.62
2.   Interface Subnet mask ........ : 255.0.0.0
3.   Primary Boot Server .......... : 80.0.0.20
4.   Secondary Boot Server ........ : Not Defined
5.   Boot Filename ................ : /tstsyncn.mem
6.   Boot From FLASH Memory ....... : Yes (Ver 7.01)
7.   Update FLASH Memory after boot : Not Applicable
8.   Ethernet Interface Select .... : AUTO/(100M)/(10M)
9.   Take system setup from NVRAM . : Yes
A.   System Setup Filename ........ : /etc/ts/ts.conf
B.   Hosts Filename ............... : /etc/hosts
G.   Default Gateway .............. : Not Defined
```

Configure UDP port parameters

The administrator can enable the broadcasting of UDP packets on a particular port using commands available under **udp** menu. This menu is available under **nvram** menu and has the following commands.

No.	Command	Function
1.	Help	Display help
2.	Modify	Modify status and UDP ports configuration
3.	Show	Display the current UDP ports configuration
4.	Quit	Exit from UDP menu

1. nvram/udp/help

The **help** command gives a list of commands available in the *udp* menu. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *path* menu commands.

Example:

```
help modify
```

will display details like syntax, description and explanation for the arguments of the command modify.

The **?** command and **help** command may be used interchangeably.

2. nvram/udp/modify

Using **modify** command, the administrator may enable/disable the UDP packet forwarding feature. Ports that are to be enabled for forwarding can be configured using this command. The configurable UDP port range is 0 to 9999. The command syntax is

```
modify
```

Example:

modify

```
-----------------------------------------------------------------
Parameter                                   Current Value
-----------------------------------------------------------------
UDP Forwarding                              enabled
Listening Port #1                           4100
Broadcast Port #1                           4104
Listening Port #2                           4108
Broadcast Port #2                           4112
```

will allow the administrator to modify the UDP parameters shown in the above table.

3. nvram/udp/show

The **show** command displays the current configuration of the UDP ports. The command syntax is

show

Example:

Show

will show the parameter and its current value as shown in the below table.

```
-----------------------------------------------------------------
Parameter                                   Current Value
-----------------------------------------------------------------
UDP Forwarding                              disabled
Listening Port #1                           4100
Broadcast Port #1                           4104
Listening Port #2                           4108
Broadcast Port #2                           4112
```

4. nvram/udp/quit

The **quit** command is used to exit form the UDP menu and return to **nvram** menu. The syntax of the command is

quit

Route

The **route** command, present only in **admin** mode, may be used by the administrator to

- display the current routing information present in the route table
- add new route information
- delete a route entry

The command enables the administrators to manipulate the routing table. The command syntax is:

```
route [-f] [-n] [show | add |delete ] [net | host] <dstn> <gw> [metric]
```

route [-f] [-n] [add | delete | show] [net | host] *destination gateway* [*metric*]

The following three options of the **route** command indicate the operation to be done on the route table.

add

add a new entry to the table. If the route already exists, the message

```
add: Route already exists
```

is displayed and no change is effected.

Note

When the route table is full, adding more entries to the table using the add option results in the message,

```
add: Route table Overflow
```

is displayed.

When trying to add a route if the gateway cannot be reached with the available routing information then the error message,

```
add: Gateway cannot be reached
```

is displayed.

delete

delete a route entry in the table. If the route is not available in the table then the message,

```
delete: Route not found
```

is displayed.

show display the routing table entries.

The following two options indicate the type of destination address that follows, whether it is a host address or a network address.

net indicates that the destination address that follows is the network address and not a specific host.

host indicates that the destination address that follows is a specific host address.

Note

If the destination type (**net** or **host**) is not specified, the Internet address associated with the destination is interpreted and if it has a local address part of INADDR_ANY then the address is assumed to be a specific host address; otherwise, it is assumed to be a route to the network.

The following three options specify the route table entry to be added or deleted. These are not to be specified for the show option.

destination

destination host system where the packets will be routed. *destination* can be

- a host name
- a network name
- an Internet address in dot notation

  or
- the keyword default, which signifies the wildcard gateway route.

gateway

The gateway through which the destination is reached. *gateway* can be

- a host name

  or
- an Internet address in dot notation.

metric An integer that indicates whether the gateway is a remote host or the local host. If the route leads to a destination via a remote gateway, *metric* should be a number greater than 0. If the route leads to destination and the gateway is the local host, *metric* should be 0. The default for *metric* is 0. The result is not defined if *metric* is negative.

The **-f** and **-n** option are used as follows:

-f Flushes all route table entries for which the gateway is a remote host. If **-f** is specified with other commands (**add**, **delete** or **show**), then the entries are flushed at first and then the command **add**, **delete** or **show** is acted on.

-n This option indicates that the host addresses be displayed symbolically by names. In case, the name is not known, then the address will be displayed.

if **-n** option is not specified, by default the host addresses will be displayed as Internet addresses.

Example

1. route show

will display the routing table entries as show below:

```
Routing tables
Destination   Gateway   Flags   Refs   Use   Metric Interface
196.1.68.67   hclhpmas  UGH       1     1         1      amd0
196.1.68.32   bargavi   U        11    149154    0      amd0
```

2. route -n show

will display Internet address of the gateway instead of the name.

```
Routing tables
Destination  Gateway      Flags Refs  Use     Metric Interface
196.1.68.67  196.1.68.38  UGH    1     1         1      amd0
196.1.68.32  196.1.68.53  U      11   149154     0      amd0
```

3. route add 196.1.67.00 196.1.68.38

will add a new route table entry to reach the network 196.1.67 through the gateway 196.1.68.38 and will display,

```
add: host 196.1.67.0: gateway 196.1.68.38, flags 1
```

After adding this entry,

```
route show
```

will display,

```
Routing tables
Destination   Gateway   Flags  Refs  Use    Metric  Interface
196.1.68.67   hclhpmas   UGH     1     1       1         amd0
196.1.67.0    hclhpmas   UG      0     0       0         amd0
196.1.68.32   bargavi    U       11   149154   0         amd0
```

4. route add 196.1.67.38 hclhpmas

   will add the route entry and display,

   ```
   add: host 196.1.67.38: gateway hclhpmas, flags 5
   ```

   After adding this entry, the command,

   ```
   route show
   ```

   will display

   ```
   Routing tables
   Destination    Gateway  Flags  Refs  Use      Metric   Interface
   196.1.68.67    hclhpmas UGH     1     1          1          amd0
   196.1.67.38    hclhpmas UGH     0     0          0          amd0
   196.1.67.0     hclhpmas UG      0     0          0          amd0
   196.1.68.32    bargavi  U       11   149154      0          amd0
   ```

5. route delete 196.1.67.38 hclhpmas

   will delete the route entry to the destination host 196.1.67.38 through the gateway hclhpmas and display.

   ```
   delete: host 196.1.67.38: gateway hclhpmas, flags 5
   ```

6. route -f

   will flush the route table entries for which the gateway is a remote host, and display

   ```
   Flushing route tables:
   196.1.68.67      hclhpmas    done
   196.1.67.0       hclhpmas    done
   ```

7. route show

   will display the route table entries.

   ```
   Routing tables
   Destination   Gateway   Flags  Refs  Use     Metric Interface
   196.1.68.32   bargavi   U      10    150279  0           amd0
   ```

8. route add net 196.1.65.4 hclhpmas

will add the route entry and display,

```
add: net 196.1.65.4: gateway hclhpmas, flags 3
```

9. route add host 196.1.65.0 hclhpmas

will add the route entry and display,

```
add: host 196.1.65.0: gateway hclhpmas, flags 7
```

The flags in the route table entries displayed by the show command may be interpreted using the following table.

Table 3.4: Route Table Flags

Destination Type	Flags	Route Type
network	1=U	route to a network via a gateway which is the local host itself
network	3=UG	route to a network via a gateway which is a remote host
Host	5=UH	route to a host via a gateway which is the local host itself
Host	7=UGH	route to a host via a gateway which is a remote host
Default	1=U	wildcard route via the local host
Default	3=UG	wildcard route via a remote gateway

Note

For the route table manipulation commands to be effective in the cases of virtual circuit connections or bidirectional datagram transfers, appropriate route commands must be executed on

- the local host
- the destination host and
- all the intermediate hosts

Only after the reciprocal commands are executed on all relevant host systems, the route table manipulation will be complete.

Normally, the route table is maintained by the **routed** daemon on the server, exchanging information with other hosts/gateways on the network using the RIP (Routing Information Protocol). Manual administration is required only if the gateways are not able to exchange information with the remote access server due to some reason.

Set Port Parameters

The **set** command is used to display or define port parameters and is available under both **nvram** and **admin** modes. The syntax of the command is:

```
set [portname] [ option[=value] ...]
```

The **set** command without any argument, displays the server parameters for all the ports.

The port name can be specified as a single port (S3), or a list of ports (S1, S3, S5) or a range of ports (S7-S10).

If *portname* is specified in the command, the intended action is only for the specified port(s). If *portname* is not specified, then the **set** is for all the ports of the server. If no *option* and *value* are specified, the parameters are displayed. If *option* is specified, then the parameter is set to the *value* specified.

The following table gives the options and their meaning. The values that may be specified is also indicated.

Table 3.5: Port Parameter Options

Option	Meaning	Possible Values
term	The name of the terminal connected to the port	name of the terminal eg. vt100, vt220
prompt	The prompt displayed by the server on the user terminal. This is meaningful only in case of **switched port** terminals.	eg. RAS>

Table 3.5: Port Parameter Options (Contd.)

Option	Meaning	Possible Values
maxsession	Maximum number of sessions that can be simultaneously open from the port. The default value is 8. The administrator may reduce the same.	Number less than or equal to 8.

	This is not meaningful for implicit and fixed port connections.		
inhwflow	Input side hardware flow control	none rts	no hardware flow control use RTS signal
outhwflow	Output side hardware flow control	none cts	no hardware flow control use CTS signal
user	Login name to be used for logging in a **implicit port** terminal.	Any valid login name. If no **value** is specified i.e. (user=) the host login prompt will appear.	
hosts	The list of host names separated by comma and prepended by a + represents the hosts to which access is allowed. In the case of switched ports, the list specifies that sessions can be established only with these hosts. In the case of implicit and fixed ports, the list specifies that implicit or fixed connection can be established with the first available host in the list. That is, if the first host is up connection is established with it. If the first one is down, then the connection is established with the next available one in the list.	eg. hosts=+indus, everest	

Table 3.6: Port Parameter Options (Contd.)

Option	Meaning	Possible Values
	The list of host names separated by comma and prepended by a -, represents the hosts to which access is restricted (not permitted). This is	eg. hosts=-cheetah, hclhpmas

	applicable only for switched ports.	
type	Type of the port, switched/implicit/fixed/rtelnet	The administrator can specify • line for switched port • implicit for implicit port • fixed for fixed port • rtelnet for Reverse Telnet • off for unused port
port_modify	Whether access to this port must be allowed or denied to any user.	Permitted/Denied
tcpport	The TCP port to be used for Reverse Telnet	Default is 2000
cdetect	Whether carrier detection in Sync port is to be performed or not	on/off
authen	Whether authentication for Reverse Telnet is required.	on/off on – user and password required. off – no authentication is required.
allowsecond	Whether to allow second reverse telnet connection for a port by closing the previous one.	yes/no

Example

```
set S2 type=line term=vt100 prompt=LANS2>
```

The **set** command for a switched port will display like,

```
S1 inhwflow=none outhwflow=none  type=line  term=vt100
prompt=RAS> hosts=indus  maxsession=8
```

Note

In a switched port parameter display, the **hosts** option may or may not be present.

The **set** command for a implicit port will display like,

```
S2  inhwflow=none  outhwflow=none  type=implicit  term=vt220
hosts=indus  user=myname
```

Note

In an implicit port parameter display,

1. The **hosts** option will be present always and will have only one host name to which implicit connection is established.

2. The **user** option will be present in **implicit** port definitions. If no user name is specified, **set** will display **user=<null>.**

The **set** command for a fixed port will display like,

```
S3  inhwflow=none  outhwflow=none  type=fixed  term=vt100
hosts=hclhpmas
```

Note

In a fixed port parameter display, the **hosts** option will be present and will have only one host name to which fixed port connection is established.

The **set** command for a reverse telnet port will display like,

```
      S4 inhwflow=none  outhwflow=none  type=rtelnet  tcpport=2000
authen=off allowsecond=no
```

For a unused port, the **set** command will display the type as **off**.

Configure SNMP Parameters

The administrator may view or modify SNMP options on the remote access server by using the **snmpconfig** command.

The command syntax is

```
snmpconfig [option=[value]...]
```

If no option is specified, the command will display all options and their current values.

Example

```
snmpconfig

sysLocation=Delhi  sysContact=NWManager  authTraps=enabled
trapdests=host:public  community=public:RO
```

The following tables gives the options, their meanings and the possible/default values.

Table 3.7: SNMP Options

Option	Meaning	Possible Values
sysLocation	Physical location of the remote access server. This option can be set by a SNMP SET request from a SNMP manager.	A string upto a maximum length of 31 Factory default is a null string. If no *value* is specified, it is set to null.
sysContact	Name of the person incharge of the remote access server. This also can be set by a SNMP SET request from a SNMP manager.	String of upto 31 characters. Factory default is null. If no *value* is specified, the option is set to null.

Table 3.7: SNMP Options (Contd.)

Option	Meaning	Possible Values
authTraps	Control enabling or disabling of authentication traps.	enabled or disabled. Factory default is disabled. If no value

		is specified, error is displayed.
trapdests	The host name and its community to which traps are to be sent. To add a pair the *value* must be preceded by +. To delete a pair the *value* must be preceded by -.	*hostname:community* or *internet address:community* Community string can be a maximum of 15 characters and refers to valid community name for the SNMP manager. Multiple pairs can be added/deleted by giving a comma separated list. All pairs can be deleted by specifying no value. The command, snmpconfig *trapdests=host:community* will delete all existing destinations and add this host as a new destination.
Community	Add or delete the community: permissions pair which are to be used to validate incoming SNMP requests. To add a pair the value must be preceded by +. To delete a pair the *value* must be preceded by-.	*+community name:permission* will add a pair *-community name:permission* *or* *-community name* will delete a pair. *community name* can be upto 15 characters. Multiple pairs can be added or deleted, by giving a comma separated list.

Table 3.7: SNMP Options (Contd.)

Option	Meaning	Possible Values
	When a SNMP request is received, its community name is checked. If the name matches one of the	All pairs can be deleted by specifying no value. The command

	configured name, its permissions for the requests are checked. If the permissions do not allow the request then a No Ack is sent to the manager indicating that the received request is not available to the community. If community itself does not match any of the configured community names, the request is dropped. If community and permission match, then the request is allowed.	snmpconfig *community=communityname:permission* deletes all existing pairs and adds this pair. The permissions and their meanings are defined in the table below.

The community permissions and their meanings are described in the table below:

Table 3.8: SNMP Community Permissions

Permission	Meaning
RO	The SNMP request from a SNMP manager belonging to the corresponding community can only be to GET information and not to SET.
RW	The SNMP request from the SNMP manager belonging to the corresponding community can do both GET and SET.
WO	The SNMP request from the SNMP manager belonging to the corresponding community can only SET.
NA	The SNMP request from the SNMP manager belonging to the corresponding community can neither GET nor SET information.

Set Port Characteristics

The administrator may view or modify the characteristics of any or all ports of the server using the **stty** command, present in both **admin** and **nvram** modes.

The command syntax is:

```
stty [portname] [option[=value]...]
```

The command without any parameters displays the port setting of all ports of the server. When a *option* and its *value* is specified, the *option* is set to that *value*.

If a *portname* is specified, the parameters of the specified port is displayed or set. If *portname* is not specified, then the parameters of all the ports are displayed or set as specified.

The table below gives the list of parameters and meaning of the parameter. Wherever applicable, the values possible are specified.

Table 3.9 : Port Characteristics

Parameter	Syntax	Meaning
Speed of the terminal	*<baudrate>*	Specify a number indicating the baudrate. The possible baudrates are 50 75 100 150 200 300 600 1200 1800 2400 3600 4800 7200 9600 19200 38400 14400 57600 76800 115200 230400 460800
Number of bits per character	cs7	set 7 bits per character
	cs8	set 8 bits per character
Odd or Even parity	+parodd	Set odd parity
	-parodd	Set even parity
Enable or disable parity checking	+parenb	Enable parity checking
	-parenb	Disable parity checking

Table 3.9 : Port Characteristics (Contd.)

Parameter	Syntax	Meaning
Number of stop bits per character	+cstopb	2 stop bits per character

	-cstopb	1 Stop bit per character
Software output flow control	+ixon	Enable software output flow control (Control-S, Control-Q will be the default start and stop characters)
	-ixon	Disable software output flow control
Software Input flow control	+ixoff	Enable software input flow control
	-ixoff	Disable software input flow control
Modem control	-clocal	Modem control required on the port
	+clocal	No modem control required on the port (default)
Break character	+ignbrk	Ignore break character This option cannot be changed.
DSR signal sensing	-dsr	Connection will be established irrespective of DSR signal status
	+dsr	Connection will not be established if DSR is not active
DTR signal toggling	+dtr	DTR will be active only if the connection is alive
	-dtr	DTR signal will be present always
Set erase character	erase=<*char*>	The erase character is set to the character specified.
Set start character	start=<*char*>	Start character is set to the character specified.
Set stop character	stop=<*char*>	Stop character is set to the character specified. The start and stop characters are used for software (input/output) flow control, ixoff/ixon.

Table 3.9 : Port Characteristics (Contd.)

Parameter	Syntax	Meaning
Set Interrupt character	intr=<*char*>	The character specified is defined to be the interrupt character. This is used by line manager to enable the user to abort the currently executing remote access server command, like, **ping.**
Set DSR signal sensing	+dsr	DSR signal sensing is enabled
	- dsr	DSR signal sensing is disabled
Set escape sequence for the remote access server to escape from sessions	escape=<*sequence*>	The sequence for escaping from server sessions is set to the sequence specified. The sequence can be upto four characters. The default escape sequence is ^T. (CTRL-T DOT)

Example

```
stty S2 9600 cs7 +ixon +parodd escape=^T
```

Note

When control characters are to be specified while defining the escape sequence, user may either type ^(caret) followed by the character or specify the equivalent octal value in the format '\xxx' where 'xxx' is the three digit octal value. It is recommended that the octal value format is used rather than ^(caret) format.

When modem control is enabled, the remote access server provides processing of DTR signals. The manager running on the port will wait for DCD (Carrier Detect) signal before proceeding. All sessions initiated from the port will be terminated when the carrier is lost.

Display Message on all Ports

The administrator may send an administrative message to all the terminals on the server using the write-all command wall. The message may contain a maximum of 66 characters. The **wall** command is available only under **admin** mode.

Example

```
wall The server is going down. Logoff
```

Display Message on given Terminal

The administrator may send a message to a user of one or more ports of the server using the **write** command. The **write** command is available only under the admin mode.

The syntax of the command is:

```
write portname [,portname ...] message
```

Example

```
write S2 Please Exit from the application you are using.
```

Note

The message will appear immediately on the port. If the port is in the midst of an application, the screen display may be garbled.

ifconfig

The **ifconfig** command available only under **admin** mode, is used to view or modify the network interface configuration.

The command syntax is

```
ifconfig    [-n] [<interface> [<prot>:down]]
```

The **ifconfig** command without any argument displays the network interface configuration on the server.

-n

If this option is specified, then the network addresses will be indicated as numbers

[<interface> [<prot>:down]]

With this option, it is possible to bring down the interface for protocols which can be ip, ipx or nb

Examples

1. ifconfig

   will display

```
net0 10/100Mbps Ethernet Controller
  IP: flags=c3 <UP,RUNNING,BROADCAST,ARP>
    inet testpc5 netmask 255.0.0.0 destination
80.0.0.0


lo0  Software Loopback
  IP: flags=49 <UP,RUNNING,LOOPBACK>
    inet localhost netmask 255.0.0.0 destination
localhost
```

   where net0 and lo0 are network interfaces.

2. ifconfig -n

   will display

```
net0 10/100Mbps Ethernet Controller
  IP: flags=c3 <UP,RUNNING,BROADCAST,ARP>
    inet 80.0.0.64 netmask 255.0.0.0 destination 80.0.0.0

lo0  Software Loopback
  IP: flags=49 <UP,RUNNING,LOOPBACK>
```

```
inet 127.0.0.1 netmask 255.0.0.0 destination 127.0.0.1
```

3. ifconfig –n net0 ip:down

   will bring down the interface net0 for ip protocol and the following will be displayed

   ```
   net0: ip shut down
   ```

Reset a port

The administrator may reset any of the sixteen ports (S1 – S16) using **reset** command. When this command is invoked, all the sessions will be disconnected and reinitialised.

The command syntax is

```
reset   <port name>
```

where <port name> is S1,S2,S3 etc.

Example

Suppose if two sessions are currently opened on port S1, the following command

```
reset S1
```

will disconnect the two sessions and reinitialise the port displaying the following message

```
Resetting port S1
Session 0 to rasunix closed
Session 1 to rasunix closed

init: starting 'line: S1
```

Protocol filter commands

Protocol Filters help regulate the different protocol traffic flowing in and out of the remote access server. The administrator by typing **filter** can switch from **admin** mode to Filter menu. From Filter menu, the administrator can access the filter commands. The Filter commands are listed below.

No	Command	Function
1.	Help	Display help
2.	Show	Show the filter information database
3.	Add	Add a new filter
4.	Modify	Modify filter parameters
5.	Insert	Insert a new filter
6.	Delete	Delete an existing filter
7.	Clear	Clear the filter information database
6.	Quit	Exit form filter menu

Help

The help command display a list of commands available in the filter menu. The administrator may get detailed information about any particular command available by giving the command name as the argument to the help command.

Example

help show

will display details like syntax, description and explanation for the arguments of the command show.

The **?** command and **help** can be used interchangeably.

Display Filter entries

The administrator may view the filter entries using **show** command. The syntax is

show <filtername>

<filtername>

Name of the existing filter entry

If the filter name is given, the command shows the settings of the specified entry. Otherwise, it shows the summary of the filter information database.

Example

show mac

```
------------------------------------------------------------
                             PROTOCOL FILTERS
------------------------------------------------------------
         Parameter                         Current Value
------------------------------------------------------------
Status (Enabled/Disabled)                      Enabled
Interface Type(Lan/Wan)                        lan
Direction (Inward/Outword/Both)                Inward
Protocol Type(IP)                              ip
Source IP Address                              80.0.0.23
Source IP Address mask                         255.0.0.0
Destination IP Address                         80.0.0.65
Destination IP Address mask                    255.0.0.0
Packet Type(in hex)                            *
Source Socket Number (in hex)                  *
Destination Socket Number(in hex)              *
Access (Deny/Permit)                           permit
```

will display the details of the filter named mac as shown above.

show

```
---------------------------------------------------------------
                             PROTOCOL FILTERS
Filter Name        Interface            Status          Access
Rule
---------------------------------------------------------------

  mac                 LAN               Enabled          Permit
  mac2                LAN               Enabled          Deny
---------------------------------------------------------------
```

will display the entire filter entries.

Add a filter entry

The administrator can add a new filter entry using **add** command. If the filter database is empty, it will be added at the beginning. Otherwise, it will be added at the end of the filter database. The command syntax for **add** is

```
add   <filtername>
```

<filtername>

Name of the filter entry to be added. The name should be unique.

Modify a filter entry

The administrator may modify the parameters of a specific filter entry available in the filter information database using **modify** command. The command syntax for **modify** is

```
modify   <filtername>
```

<filtername>

Name of the filter entry to be modified.

Insert a filter entry

The administrator can insert a filter entry using **insert** command. The name of the filter to be inserted should be unique. The command syntax for **insert** is

```
insert   <new filter name> <filter name>
```

<new filter name>

Name of the new filter to be inserted.

<filter name>

Name of the existing filter.

Delete a filter entry

The administrator can delete a specific filter entry available in the filter information database using **delete** command. The command syntax for **delete** is

```
delete   <filtername>
```

<filtername>

Name of the existing filter entry to be deleted.

Clear the filter information database

The administrator may clear the entire filter information database using **clear** command. The syntax is

```
Clear
```

Quit

Exit from the Filter menu.

Dial on Demand commands

The administrator by typing **dod** can switch from **admin** mode to DOD menu. From DOD menu, the administrator can access the DOD commands. When a path is configured in dial on demand mode, a destination entry should be made and the path will be invoked if there is any demand for that destination. The commands available in the dod menu are listed below.

No	Command	Function
1.	Help	Display help
2.	Show	Show the DOD table entries
3.	Add	Add a DOD entry
4.	Delete	Delete a DOD entry
5.	Clear	Clear all the entry in the table
6.	Quit	Exit form DOD menu

Help

The help command display a list of commands available in the DOD menu. The administrator may get detailed information about any particular command available by giving the command name as the argument to the help command.

Example

help show

will display details like syntax, description and explanation for the arguments of the command show.

The **?** command and **help** can be used interchangeably.

Adding and Deleting a DOD entry

The administrator can make a DOD entry using **add** command. The administrator may delete a DOD entry using delete **command**. The command syntax for **add** is

```
add        <dstn> <mask> <pathname>
```

The command syntax for **delete** is

```
delete    <dstn> <mask> <pathname>
```

The following three options specify the route table entry to be added or deleted.

desn

Destination host or network to which the route leads.

mask

Mask for the destination address. Mask depends on the subnetting or class of the destination network.

pathname

Name of the path used for routing the packets with the destination address.

Display DOD entries

The administrator may view the DOD table entries using **show** command. The syntax is show -n

-n

With this option, the network addresses will be displayed as numbers

Example

show

```
 ------------------------------------------------------
            Dial  on Demand  Routing Table For IP
     Destination        Mask              Path Name
 ------------------------------------------------------
        rasunix          255.0.0.0         path1
        testpc           255.0.0.0         path2
 ------------------------------------------------------
```

will display the configured route entries.

show –n

```
 ------------------------------------------------------
            Dial  on Demand  Routing Table For IP
     Destination        Mask              Path Name
 ------------------------------------------------------
         80.0.0.20         255.0.0.0         path1
         80.0.0.23         255.0.0.0         path2
 ------------------------------------------------------
```

will display the network addresses of the route table entries as numbers.

Clear the DOD route table entries

The administrator may clear the entire DOD route table entries using **clear** command. The syntax is

clear

Quit

Exit from the DOD menu.

Staticroute commands

When the administrator types **staticroute** form **admin** prompt , the **staticroute** prompt will be displayed. From this prompt, the administrator can access the **staticroute** commands. The static route entries will be stored in NVRAM memory and hence permanently available. The static route commands are listed in the following table.

Table 3.10 : Staticroute commands

No	Command	Function
27.	Help	Display help
28.	Add	Add static gateway
29.	Delete	Delete static gateway configured
30.	Show	Show static gateways configured
31.	Quit	Exit from staticroute menu

Help

The help command display a list of commands available in the **staticroute** menu. The administrator may get detailed information about any particular command available by giving the command name as the argument to the help command.

Example

help show

will display details like syntax, description and explanation for the arguments of the command show.

The **?** command and help can be used interchangeably.

Adding and Deleting a static route entry

The administrator can make a permanent route entry in the route table using **add** command. The administrator may delete a static entry from the route table using delete **command**. The command syntax for **add** is

```
add [net|host] <destination> <gateway> [metric]
```

The command syntax for **delete** is

```
delete [net|host] <destination> <gateway> [metric]
```

The following two options indicate the type of destination address that follows, whether it is a host address or a network address.

net indicates that the destination address that follows is the network address and not a specific host.

host indicates that the destination address that follows is a specific host address.

Note

If the destination type (**net** or **host**) is not specified, the Internet address associated with the destination is interpreted and if it has a local address part of INADDR_ANY then the address is assumed to be a specific host address; otherwise, it is assumed to be a route to the network.

The following three options specify the route table entry to be added or deleted. These are not to be specified for the show option.

destination

destination host system where the packets will be routed. *destination* can be

- a host name
- a network name
- an Internet address in dot notation

or

- the keyword default, which signifies the wildcard gateway route.

gateway

The gateway through which the destination is reached. *gateway* can be

- a host name

or

- an Internet address in dot notation.

metric An integer that indicates whether the gateway is a remote host or the local host. If the route leads to a destination via a remote gateway, *metric* should be a number greater than 0. If the route leads to destination and the gateway is the local host, *metric* should be 0. The default for *metric* is 0. The result is not defined if *metric* is negative.

Display route entries

The administrator may view the static route entries of the route table using **show** command. This command has no arguments. The syntax is

```
show
```

Example

The command **show** will display the route entries.

```
-------------------------------------------------------
Destination      Gateway          TYPE            METRIC
-------------------------------------------------------
90.0.0.0         80.0.0.44     Network              0
90.0.0.1         80.0.0.55     Network              0
-------------------------------------------------------
```

Quit

This command is used to exit from the **staticroute** facility.

Access statistics commands from Admin Mode

The administrator may access commands available in the statistics menu by typing **statistics** from the admin menu. After accessing statistics commands, the administrator can return to **admin** mode by typing admin from the **stat** prompt.

The difference between **exit** and **statistics** command is, once if exit from admin mode, the administrator has to enter password again to enter into admin mode. But it is not necessary incase of **statistics** command.

Exit from Administrative Mode

The administrator may exit from the privileged modes of (**admin** and **nvram**) administrative operations, by typing **quit**. Subsequently, all prompts will be with > character instead of >> characters.

Example

```
nvram >>quit
RAS>
```

If user has remote logged in from a host, then the rlogin session will close and the host prompt will appear.

Access and Modify Host Database information

The administrator can access and modify host database information using **hosts** command available in the **admin** mode. The command syntax for **hosts** is hosts <add | delete | modify | show>

add

Adds a host to the host database

delete

Deletes a host to the host database

modify

Modifies a host entry in the host database

show

Shows database information by host name or host address. Return will show all the host entries

Example

1. hosts add

will allow the administrator to add the host name and its IP address as shown below.

```
------------------------------------------------------------
Parameter               Current Value               New value
------------------------------------------------------------
 Hostname                                            armnet
 Host IP address              -                      80.0.0.23
```

The host entry added will be permanently available in the host database information.

2. hosts delete

will allow the administrator to delete a host entry from the host database. After entering the above command, the administrator has to specify the host entry to be deleted.

```
 Hostname                                              armnet
```

This will delete the host entry armnet from the host information database.

3. hosts modify

will allow the administrator to modify the parameters of a host entry. The administrator has to specify the host entry to be modified.

4. hosts show

will prompt for

```
Hostname                                              armnet
```

will display the details of the host entry armnet. If hostname is not specified, all the host entries of the host database information will be displayed.

Webserver commands

The administrator can enter into Web server directory by typing **http** from **nvram** mode. The Web server directory has the following commands.

No.	Command	Function
1.	Help	Display help
2.	Show	Show web server parameters
3.	Modify	Modify web server parameters
4.	Download	Download files required for web management into the flash memory
5.	Quit	Exit from Web server directory

help

The **help** command gives a list of commands available in the *http* menu. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command.

Example:

```
help download
```

will display details like syntax, description and explanation for the arguments of the command download.

The **?** command and **help** command may be used interchangeably.

Display web server parameters

The **show** command displays the configured web server parameters. Webserver parameters include HTTP port, Fetch files from flash, TFTP server and TFTP directory.

Example

```
show
```

will display the webserver parameters as given below.

```
-----------------------------------------------------------------
Parameter                                  Current Value
-----------------------------------------------------------------
HTTP Port                                  80
Fetch files from flash                     (enable/disable)disable
TFTP Server                                80.0.0.20
TFTP Directory                             /etc/lanrmgr
```

Modify webserver parameters

The **modify** command allows the administrator to change the web server parameters.

Download webserver files into flash memory

The **download** command allows the administrator to download all the files needed for web management into the flash memory. The syntax of the **download** command is,

```
download    [ host :] [ registry ]
```

host — indicates the TFTP server from where web files are to be downloaded. If it is not specified, the TFTP server specified in the webserver configuration will be selected

registry — indicates the name of the registry file with its absolute path. This file contains a list of file names that are to be downloaded. If it is not specified, the TFTP directory specified in the webserver configuration is assumed for fetching the registry file

Exit from Webserver Directroy

The **quit** command allows the administrator to exit from webserver directory and return to **nvram** mode.

Point to Point Link commands

LANReach provides support for SLIP and PPP. These protocols enable connectivity using serial lines and modems in place of network cables, though at lesser speeds.

All the commands used for configuring and using the point to point links through SLIP and PPP protocols are available under menu *ppl*. This menu is available under the *admin* menu. Invoking the ppl command from the admin menu enters the ppl menu. The *ppl* menu has the following commands.

No.	Command	Function
13.	Help	Display help
14.	Path	Enter into path menu
15.	User	Enter into user menu
16.	Modemchat	Enter into modemchat menu
17.	Logcat	Enter into logchat menu
18.	Start	Start a path
19.	Stop	Stop the active path
20.	Sas	Enter into SAS menu
21.	Addport	Add a port to an active path
22.	Delport	Delete a port from an active path
23.	List	List the active paths
24.	Quit	Quit from ppl menu

help

The **help** command gives a list of commands available in the *ppl* menu. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command.

Example:

```
help addport
```

will display details like syntax, description and explanation for the arguments of the command configure.

The **?** command and **help** command may be used interchangeably.

Commands To Manipulate Path Database

Administrator can configure paths on the remote access server to enable users to establish connectivity through a **path**. The path database configuration is done through commands available in *path* menu. The administrator has to type **path** from *ppl* menu to enter into *path* menu. The *path* menu commands are listed below.

No.	Command	Function
14.	Help	Display help
15.	Show	Show the destination information database
16.	Add	Add a path to the destination table
17.	Delete	Delete a path from the destination table
18.	Modify	Modify a path in the destination table
19.	Upload	Upload path configuration to the specified file
20.	Download	Download path configuration from the specified file
21.	Quit	Exit from path menu and return to ppl menu

1. ppl/path/help

The **help** command gives a list of commands available in the *path* menu. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *path* menu commands.

Example:

```
help modify
```

will display details like syntax, description and explanation for the arguments of the command configure.

The **?** command and **help** command may be used interchangeably.

2. ppl/path/show

The **show** command displays the destination information database. If a path is specified, the command shows the specified entry. Otherwise, the commands show the summary of path database. The syntax of the **show** command is

```
show        [<path>]
```

[<path>] indicates path name for which information is desired.

Example:

```
show
```

```
-----------------------------------------------------------------
Pathname            Protocol  Connection Type    ULPs Enabled
-----------------------------------------------------------------
test                PPP       Demand             IP
test1               PPP       Demand
test2               PPP       Demand
-----------------------------------------------------------------
```

3. ppl/path/add

The **add** command is used to add a path in the destination table. The path should be unique. The syntax of the command is

add *<path>*

<path> indicates pathname to be added.

Example:

add test

will show the parameter and its current value as shown in the below table. The user may choose the new value according to the required settings.

```
-----------------------------------------------------------------
Parameter                                    Current Value
New value
-----------------------------------------------------------------
Status (Enabled/Disabled)                    Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)      Demand
Destination Type (Host/Gateway)              Host
.
.
.
```

4. ppl/path/delete

The **delete** command is used to a delete from the destination table. The syntax of the command is

delete *<path>*

<path> indicates the pathname to be deleted.

Example:

delete test

will delete the test path from the destination table

5. ppl/path/modify

The modify command is used to change the path parameters. The syntax of the command is

```
modify      <path>
```

<path> specifies the pathname to be modified.

Example:

```
modify test
```

will allow the user to change all the parameters of the path test.

6. ppl/path/upload

The **upload** command can be used to upload the path configuration to the specified file on the indicated host. The syntax of the command is

```
upload      [host:]<filename>
```

host

Indicates the remote host to upload. If it is not specified, the boot server will be selected

filename

Filename for uploading

Example:

```
Upload 80.0.0.20:/etc/ts/path.ts
```

will upload the path information database to the specified file on the host 80.0.0.20

7. ppl/path/download

The **download** command can be used to download the path configuration from the specified file on the indicated host. The syntax of the command is

```
download      [host:]<filename>
```

host

Indicates the remote host from where to be downloaded. If it is not specified, the boot server will be selected

filename

Filename for downloading

Example:

```
download 80.0.0.20:/etc/ts/path.ts
```

will download the path information database from the specified file on the host 80.0.0.20

8. ppl/path/quit

The **quit** command is used to exit from *path* menu and return to *ppl* menu. The syntax of the command is

```
quit
```

Example:

```
quit
```

After invoking the above command, the remote access server will exit from *path* menu and enter into *ppl* menu.

Commands To Manipulate User Database

Administrator can configure user or accesscode database information on the remote access server through commands available in the *user* menu. The administrator has to type **user** from ppl menu to enter into *user* menu. The *user* menu commands are listed below.

No.	Command	Function
1.	Help	Display help
2.	Show	Display the accesscode information database
3.	Add	Add an accesscode to the information database

4.	Delete	Delete an accesscode from the information database
5.	Modify	Modify an accesscode in the information database
6.	Clear	Clear the accesscode information database
7.	Upload	Upload user configuration to the specified file
8.	Download	Download user configuration from the specified file
9.	Quit	Exit from path menu and return to ppl menu

1. ppl/user/help

The **help** command gives a list of commands available in the *user* menu. The administrator may get detailed information about a specific command. by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *path* menu commands.

Example:

```
help modify
```

will display details like syntax, description and explanation for the arguments of the command configure.

The **?** command and **help** command may be used interchangeably.

2. ppl/user/show

The **show** command displays the accesscode information database. If an accesscode is specified, the command shows the specified entry. Otherwise, the command shows the summary of accesscode database. The syntax of the **show** command is

```
show        [<accesscoder>]
```

accesscode

indicates accesscode whose details are to be shown

Example:

```
show
```

```
----------------------------------------------------------------
AccessCode      User ID         Authentication   Login-Session
```

```
-----------------------------------------------------------------
test            test            PT              Path
test1           test1           PT              Path
```

3. ppl/user/add

The **add** command is used to add an accesscode to the database. The syntax of the command is

add   *<accesscode>*

accesscode

indicates pathname to be added.

Example:

add user

will show the parameter and its current value as shown in the below table.

```
-----------------------------------------------------------------
Parameter                                     Current Value
-----------------------------------------------------------------
User ID                                       test
Start time (hhmmss)                           0
Stop time (hhmmss)                            0
Session(Shell/Path/Rtelnet)                   Path
path name                                     test
password                                      ****
```

4. ppl/user/delete

The **delete** command is used to delete an accesscode from the destination table. The syntax of the command is

delete   *<accesscode>*

<accesscode>
indicates the accesscode to be deleted.

Example:

delete test

will delete the accesscode test from the destination table

5. ppl/user/modify

The **modify** command is used to change the accesscode parameters. The syntax of the command is

```
modify      <accesscode>
```

<accesscode>

specifies the pathname to be modified.

Example:

```
modify test
```

will allow the user to change all the parameters of the accesscode test.

6. ppl/user/clear

The **clear** command is used to clear the accesscode database information. The syntax of the command is

```
clear
```

Example:

```
clear
```

will clear the entire accesscode database information.

7. ppl/user/upload

The **upload** command can be used to upload the accesscode configuration to the specified file on the indicated host. The syntax of the command is

```
upload      [host:]<filename>
```

host

Indicates the remote host to upload. If it is not specified, the boot server will be selected

filename

Filename for uploading

Example:

```
Upload 80.0.0.20:/etc/ts/user.ts
```

will upload the accesscode information database to the specified file on the host 80.0.0.20

8. ppl/user/download

The **download** command can be used to download the accesscode configuration from the specified file on the indicated host. The syntax of the command is

```
download      [host:]<filename>
```

host

Indicates the remote host from where to be downloaded. If it is not specified, the boot server will be selected

filename

Filename for downloading

Example:

```
download 80.0.0.20:/etc/ts/user.ts
```

will download the accesscode information database from the specified file on the host 80.0.0.20

9. ppl/path/quit

The **quit** command is used to exit from *user* menu and return to *ppl* menu. The syntax of the command is

```
quit
```

Example:

```
quit
```

After invoking the above command, the remote access server will exit from *path* menu and enter into *ppl* menu.

Auditlog directory

The commands under this directory provide the system administrator with information about the usage of the LANReach such as the frequency with which users dial in, status of their calls, etc.

The audit records are displayed in a spreadsheet style format with each record displayed in a separate row. The event fields stand for the following:

Login - User logging into the LANReach
Logout - User logging out of the LANReach
UsrAdd - Admin has added a new user entry
UsrDel - Admin has deleted a deleted a user entry
UsrMod – Admin has modified a user entry
UsrUpl – Admin has uploaded the user database

UsrDow – Admin has downloaded the user database
UsrClr – Admin has cleared the user database from the NVRAM
PathSt – A path has been started
PathSp – Path has been stopped
PaliSt – Line of a path has been brought up
PaliSp – Line of a path has been brought down
Unknown – Unknown event

The status type is interpreted as follows:
FAC – False Access Code , NPWD – Password error, NRSP – No response form the LANReach, AB – Process Aborted, IU – User Already in, PT – Pass Through User

The auditlog commands available under admin/ppl/user/audit menu are listed below.

No.	Command	Function
1.	Help	Display help
2.	Show	Display the audit trail database
3.	Flush	Flush the audit trail database
4.	Print	Configure audit trail print on a port
5.	Upload	Upload audit trail on a host
6.	Quit	Exit from auditlog directory

1. admin/ppl/user/audit/help

The **help** command gives a list of commands available in the *audit* menu. The administrator may get detailed information about a specific command by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *path* menu commands.
Example:

```
help upload
```

will display details like syntax, description and explanation for the arguments of the command upload.

2. admin/ppl/user/audit/show

The **show** command displays the audit trail database. The syntax of the command is

```
show
```

Example:

```
show
```

```
----------------------------------------------------------------
Identifier     Port Event  Start Time             End Time
Status
----------------------------------------------------------------
ra              -   UsrAdd Oct 26, 2001 20:12:38 -,-
-
rb              -   UsrAdd Oct 26, 2001 20:12:44 -,-
-
rb              -   UsrMod Oct 26, 2001 20:13:08 -,-
-
----------------------------------------------------------------
```

will display the log entries and their parameters.

3. admin/ppl/user/audit/flush

This command flush all audit records from the audit trail database. The syntax of the command is

flush

Example:

flush

will display,

```
This command will clear the whole Audit Trail database.
Proceed(y/n)(n)? y

flushing audit trail database
```

The flush command can be used to verify that the audit trail database is cleared.

4. admin/ppl/user/audit/print

This command prints the audit trail on the port specified. The syntax of the command is

print *[<Port name> | disable]*

Port name

Name of the port where the printer is connected

disable

Printing is disabled

Example:

print P0

will enable the audit trail printing on the port P0 and will display the message

```
Audit Trail Printing Enabled on P0
```

If no argument is given, the current status will be displayed.

```
print
```

```
Audit Trail Printing : P0
```

```
Print disable
```

will disable the printing and display the following message

```
Audit Trail Printing Disabled
```

5. admin/ppl/user/audit/upload

This command uploads the audit records to the specified path on the indicated host. The syntax of the command is

upload [[host:] *<filename>* | *disable*]

host:

Indicates the remote host to upload. If it is not specified, the boot server will be selected.

<filename>

Pilename for uploading

disable

Disables uploading to host

Example:

```
upload 80.0.0.23:/auditlog
```

will enable the audit trail uploading and will display the message.

```
Audit Trail Uploading to Host Enabled
```

If no argument is given, the current status will be displayed.

```
upload
```

```
Audit Trail Uploading to Host : 80.0.0.23:/auditlog
```

upload disable

will disable the uploading and will display the following message

```
Audit Trail Uploading to Host Disabled.
```

5. admin/ppl/user/audit/quit

This command is used to exit from the auditlog directory and return to *user* menu. The syntax of the command is

```
quit
```

Commands To Manipulate Modemchat Database

Administrator can manipulate modemchat database information using **modemchat** commands. The administrator has to type **modemchat** from *ppl* menu to enter into *modemchat* menu. The modemchat commands are listed below.

No.	Command	Function
1.	Help	Display help
2.	Show	Display the modemchat database
3.	Delete	Delete a modemchat entry from the modemchat database
4.	Clear	Clear the modemchat database entry
5.	Download	Download modemchat information
6.	Quit	Exit from modemchat menu and enter into ppl menu

1. ppl/modemchat/help

The **help** command gives a list of commands available in the *modemchat* menu. The administrator may get detailed information about a specific command by giving the command name as the argument to the **help** command. The syntax of the command is

help *[<any command>]*

The <*any command*> may be any one of the *path* menu commands.

Example:

```
help show
```

will display details like syntax, description and explanation for the arguments of the command configure.

2. ppl/modemchat/show

The **show** command displays the modemchat database information. If chat name is specified, the command shows the specified entry. Otherwise, the command shows the summary of modemchat database. The syntax of the **show** command is

show *[<chat_name>]*

chat_name

indicates chat name whose details are to be shown

Example:

```
Show Hayes
```

```
Hayes                  / AT&F\r / \dOK / AT&D2\r / \dOK / AT&C1\r
/ \dOK / ATS0=0\r / \dOK / AT\r / \dOK / ATDT$t\r / CONNECT
```

3. ppl/modemchat/delete

The **delete** command is used to delete a chat entry from the modemchat database. The syntax of the command is

delete *<chat_name>*

<chat_name>

indicates the chat name to be deleted.

Example:

```
delete Hayes
```

will delete the chat entry Hayes from the destination table

4. ppl/modemchat/clear

The **clear** command is used to clear the modemchat database information. The syntax of the command is

```
clear
```

Example:

```
clear
```

will clear the entire modemchat database information.

5. ppl/modemchat/download

The **download** command can be used to download the modemchat configuration from the specified file on the indicated host. The syntax of the command is

```
download      [host:]<filename>
```

host

Indicates the remote host from where to be downloaded. If it is not specified, the boot server will be selected

filename

Filename for downloading

Example:

```
download 80.0.0.20:/etc/ras/mod.scr
```

will download the modemchat information database from the specified file on the host 80.0.0.20

9. ppl/modemchat/quit

The **quit** command is used to exit from *modemchat* menu and return to *ppl* menu. The syntax of the command is

```
quit
```

Example:

```
quit
```

After invoking the above command, the remote access server will exit from *modemchat* menu and enter into *ppl* menu.

Commands To Manipulate Logchat Database

Administrator can manipulate logchat database information using **logchat** commands. The administrator has to type **logchat** from *ppl* menu to enter into l*ogchat* menu. The logchat commands are listed below.

No.	Command	Function
1.	Help	Display help
2.	Show	Display the modemchat database
3.	Delete	Delete a modemchat entry from the modemchat database
4.	Clear	Clear the modemchat database entry
5.	Download	Download modemchat information
6.	Quit	Exit from modemchat menu and enter into ppl menu

1. ppl/logchat/help

The **help** command gives a list of commands available in the *logchat* menu. The administrator may get detailed information about a specific command by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *path* menu commands.

Example:

```
help show
```

will display details like syntax, description and explanation for the arguments of the command configure.

2. ppl/logchat/show

The **show** command displays the logchat database information. If chat name is specified, the command shows the specified entry. Otherwise, the command shows the summary of logchat database. The syntax of the **show** command is

```
show        [<chat_name>]
```

chat_name

indicates chat name whose details are to be shown

Example:

```
Show pclogin
```

```
pclogin                \r / Username: / $u / Password: / $p /
Login\ Successful\r\n
```

3. ppl/logchat/delete

The **delete** command is used to delete a logchat entry from the logchat data base.. The syntax of the command is

```
delete      <chat_name>
```

<chat_name>

indicates the chat name to be deleted.

Example:

```
delete raslogin
```

will delete the logchat entry raslogin from the destination table

4. ppl/logchat/clear

The **clear** command is used to clear the logchat database information. The syntax of the command is

```
clear
```

Example:

```
clear
```

will clear the entire logchat database information.

5. ppl/logchat/download

The **download** command can be used to download the logchat configuration from the specified file on the indicated host. The syntax of the command is

```
download    [host:]<filename>
```

host

Indicates the remote host from where to be downloaded. If it is not specified, the boot server will be selected

filename

Filename for downloading

Example:

```
download 80.0.0.20:/etc/ras/logchat.scr
```

will download the logchat information database from the specified file on the host 80.0.0.20

6. ppl/logchat/quit

The **quit** command is used to exit from *logchat* menu and return to *ppl* menu. The syntax of the command is

```
quit
```

Example:

```
quit
```

After invoking the above command, the remote access server will exit from *logchat* menu and enter into *ppl* menu.

Start a path

Administrator can start a path to the specified destination using **start** command. By invoking the **start** command, dialout is initiated to the phone number specified in the path and after successful connection establishment, starts SLIP or PPP as specified in the path configuration.

The syntax of the **start** command is

```
start      [-v <level>] <pathname>
```

-v <level>

level of debug information required when the dialout occurs. The possible range of values is : 0-100. A higher value results in display of more debug information. The default value of level is 0.

Example:

```
start –v 70 test1
```

will start the path test1 with verbose level 70.

Stop a path

Administrator can stop an active path using **stop** command. The syntax of the **stop** is

```
stop
```

Example:

```
Stop test1
```

will stop the path test1.

Security Access Server Commands

Security Authentication Servers can be configured which support RADIUS. When a remote user tries to login to the remote access server, it consults the RADIUS sever for authenticating the user and getting parameters for establishing connection with the client. The commands under **SAS** menu are used to configure security authentication servers. The **SAS** menu commands are listed in the below table.

No.	Command	Function
1.	Help	Display help
2.	Show	Show all the SAS entries
3.	Add	Add a SAS entry
4.	Delete	Delete a SAS entry
5.	Modify	Modify a SAS entry
6.	Clear	Clear all the SAS entries
7.	Quit	Exit from SAS menu and return to ppl menu

1. ppl/sas/help

The **help** command gives a list of commands available in the *sas* menu. The administrator may get detailed information about a specific command by giving the command name as the argument to the **help** command. The syntax of the command is

```
help        [ <any command> ]
```

The <*any command*> may be any one of the *sas* menu commands.

Example:

```
help add
```

will display details like syntax, description and explanation for the arguments of the command configure.

2. ppl/sas/show

The **show** command displays the sas entries. If a particular sas entry is given, the command shows the specified entry. Otherwise, the command shows all the entries. The syntax of the **show** command is

```
show        [<sast_entry>]
```

chat_name

indicates sas entry whose details are to be shown

Example:

```
show
```

will show all the configured entries as given below.

```
-----------------------------------------
    SAS Name                  Protocol
-----------------------------------------
     80.0.0.20                  RADIUS
-----------------------------------------
     80.0.0.21                  RADIUS
-----------------------------------------
```

3. ppl/sas/add

The **add** command is used to add a new SAS entry. The syntax of the command is

```
add <IP Address>
```

<IP Address>

IP address of the RADIUS server

Example:

add 80.0.0.66

will the table as given below. The user can provide the new values according to the required settings.

```
-----------------------------------------------------------------
Parameter                                    Current Value    New
value
-----------------------------------------------------------------
Shared Secret                                -
.
.
.
```

4. ppl/sas/delete

The **delete** command is used to delete a SAS entry. The syntax of the command is

delete *<IP Address>*

<IP Address>

IP address of the RADIUS server

Example:

delete 80.0.0.23

will delete the SAS entry with the IP address 80.0.0.23.

5. ppl/sas/modify

The **modify** command is used to change the SAS entry parameters. The syntax of the command is

modify *<IP Address>*

<IP Address>

IP address of the RADIUS server whose parameters are to be changed.

Example:

modify 80.0.0.23

will allow the user to change all the parameters of the RADIUS server whose IP is 80.0.0.23

6. ppl/sas/clear

The **clear** command is used to clear the SAS database information. The syntax of the command is

```
clear
```

Example:

```
clear
```

will clear all the SAS entries.

7. ppl/logchat/quit

The **quit** command is used to exit from *sas* menu and return to *ppl* menu. The syntax of the command is

```
quit
```

Example:

```
quit
```

After invoking the above command, the remote access server will exit from *sas* menu and enter into *ppl* menu.

Add a port to an active path

Additional ports to an active path can be added using **addport** command. This will increase the throughput. One added, the Bandwidth on Demand functionality won't delete it from the path unless its is deleted through delport command. The syntax of the command is

```
addport  [-v <level>]  <pathname>  <port> [<pid>]
```

pathname

name of the active path on which additional port to be added

port

name of the port to be added

Example:

```
addport demo S1
```

will add the port S1 to the active path demo.

Delete a port from an active path

A port from an active path can be deleted using **delport** command. Once deleted, the Bandwidth on Demand functionality won't add it to the path unless it is added through the addport command. The syntax of the command is

```
delport     <pathname>  <port> [<pid>]
```

pathname

name of the active path from which port to be added

port

name of the port to be deleted

Example:

```
delport demo S1
```

will delete the port S1 to the active path demo.

Note

The **addport** and **delport** commands should be used only with the paths with MLPPP protocol

List the active paths

The **list** command is used to list the active paths. The syntax of the command is

```
list
```

Example:

```
list
```

will list the active paths

```
hari.pid = 25, ppp0 - S1
```

Exit from ppl menu

The **quit** command is used to exit from *ppl* and return to *admin* menu. The syntax of the command is quit

Example:

quit

After invoking the command, the remote access server will exit from *ppl* menu and return to *admin* menu.

TELNET COMMANDS

Telnet Command Menu

From an active telnet session, established using telnet command, when user types the escape character sequence of the server port, the prompt.

```
telnet>
```

is displayed on the terminal.

At this prompt, user may

- invoke the telnet commands
- resume the telnet session from which the telnet command mode was entered.
- enter the general user command menu

The on line help facility is available at the telnet prompt. Typing.

help

at the **telnet** prompt displays the telnet commands as follows :

```
Valid commands are:
      help              [<any command>]
      display
      mode              <c|1|?>
      send              <ao|ayt|brk|ec|el|ga|ip|nop|?>
      localchar
      debug
      set               <Parameter> <value>|<?>
      resume
```

The following sections describe the telnet commands in detail.

Note

The command history facility, partial command matching facility and the command editing features are available at the telnet command menu also.

Help

Typing **help** at the telnet prompt, displays the telnet commands and their function as shown above.

As in the case of other server menus, the **?** character may be used, in place of the **help** command.

Typing **help** followed by a specific telnet command, displays more details about the telnet command.

Example

```
help display
```

Display

The **display** command, displays the current operating parameters of the presently active telnet session from the port. The parameters that will be displayed are :

- host to which the session connects to
- current mode (line or character)
- whether local character recognition of certain special characters is on or off
- value of these special characters

After displaying the parameters, the telnet prompt is redisplayed.

Example

```
telnet> display
Connected to hercules
Mode is character mode
```

```
Local characters is off
echo                          [^E]
escape                        [^]]
The following need 'localchar' to be toggled true
erase                         [^H]
kill                          [@]
interrupt                     [^?]
abort_output                  [^C]
break                         [^\]

telnet>
```

Mode

The **mode** command may be used to define how the characters typed are transmitted to the host.

In a character mode of operation, the character is transmitted to the host as soon as the character is typed.

In a line mode of operation, the characters are buffered till a carriage return is typed and then transmitted to the host.

Example

```
mode c
```

will set the mode to character mode.

```
mode l
```

will set the mode to line mode.

Note

The line-by-line mode of operation is not available in server version 1.00 Hence, on typing the command mode l will cause the message

```
Line mode not supported now
```

to be displayed.

Specifying **mode** without any argument or an argument other than **c** or **l** will display the usage.

Example

```
telnet> mode
format is <mode Mode> where Mode is one of:
c character-at-a-time mode
1 line-by-line mode

telnet>
```

Send

The **send** command may be used to transmit certain special character sequences to the host to which this telnet session has established connection.

The following table gives the arguments that may be specified with the send command.

Table 3.9 : Port Characteristics

Argument	Meaning
ao	The Telnet AO (abort output) sequence is sent, which causes the host to flush all output to the user terminal.
ayt	The Telnet AYT (Are You There) sequence is sent, to which the remote host may or may not respond.
brk	The Telnet Break sequence is sent to the host.
ec	The Telnet EC (Erase Character) sequence is sent, so that the remote system erases the last character entered.
el	The Telnet EL (Erase Line) sequence is sent, which should

	cause the remote host to erase the current line.
ga	The Telnet GA (Go Ahead) sequence is sent, which is unlikely to have any significance at the host.
ip	The Telnet IP (Interrupt Process) sequence is sent, which should cause the remote host to abort the currently running process.
nop	The Telnet NOP (No Operation) sequence is sent.
?	Prints the argument that may be given with **'send'** command.

Typing **send** without any arguments, displays :

```
need at least one argument for 'send' command
'send ?' for help
```

Typing **send** with a wrong argument displays

```
Invalid argument
'send ?' for help
```

After successful execution of the **send** command, the active telnet session from which the user entered the telnet menu, will be resumed.

Local Character Recognition

Initially, when the **telnet** is in character-at-a-time mode, the special characters are not recognized locally by the telnet.

The local character recognition may be toggled using the **localchar** command. On toggling the option from ‘off’ to ‘on’, the special characters are recognized by telnet locally, and transformed into corresponding TELNET Sequences.

Example

```
telnet> localchar
localchars is toggled on
telnet> localchar
localchars is toggled off
telnet>
```

Set

The **set** command in telnet defines the special character sequences for

- echo
- escape
- erase
- kill
- interrupt
- abort
- break

When the local character recognition is set to on, if the user types the sequence defined by the **set** command, then the telnet interprets them locally and transforms them to corresponding TELNET sequences and send to the host.

The sequences other than echo and escape, set by the **set** command does not have any effect when the local character recognition is set to off.

The meaning of these sequences and their default initial values are given in the table.

Argument	Meaning and Operation	Initial Value
echo	Character to toggle local echoing on/off	CTRL-E
escape	Character to escape back to telnet command mode	CTRL-]
erase	TELNET EC Sequence is sent to the host	CTRL-H
kill	TELNET EL Sequence is sent to the host	@
abort	TELNET AO sequence is sent to the host	CTRL-C
break	TELNET BRK sequence is sent to the host	^\

After the **set** command, the telnet prompt is displayed on the terminal.

Example

```
telnet> set erase ^F
telnet> set kill ^C
```

The above commands set the erase sequence to ^F and kill sequence to ^c. Subsequently, when the user types these characters from the telnet session, the corresponding telnet sequence (say, EC sequence if ^F is typed and EL sequence if ^c is typed) will be sent to the host.

Debug

The **debug** command toggles the debug flag of the telnet command. If the status of the flag is on, the telnet option management will be displayed.

Example

```
telnet> debug
debug flag is toggled on
telnet> debug
debug flag is toggled off
telnet>
```

Resume

User may resume a current telnet session from the telnet> prompt. It is not possible to resume other sessions from this prompt. The other options of **resume** command are also not available.

Example

```
telnet>re
```

After **resume** command, the current telnet session is resumed.

4

SETUP CONFIGURATION

Introduction

When the remote access server software (downloaded from host or from flash memory) starts executing, the contents of the NVRAM are verified for setup configuration information. If the setup configuration information is not present in the NVRAM or if it is invalid the server displays the prompt.

```
        Enter Password to setup the system
        Password:
```

When the correct password is typed, the setup configuration prompt.

```
        Nvram>
```

is displayed.

Even if the NVRAM contains valid setup configuration information, the server software, after verifying, displays the prompt:

```
        Do you want to change system setup?
```

and waits for 5 seconds. If **n** is typed or no response is given in 5 seconds the server proceeds further and enters multiuser mode. The administrator may type y if the setup configuration needs to be changed. The prompt:

```
        Password:
```

will be displayed. On entering the correct password, the configuration prompt is displayed as:

```
        Nvram>
```

Only the console will be active when the user is in this mode.

Note

The remote access server is delivered with the default administrative password as HCLPD
If the administrator password of the remote access server is forgotten, contact the Support team for recovery.

The setup configuration commands, procedures for setting up different configurations like implicit connection etc are explained in the following sections.

Setup Configuration Commands

The commands available at the setup configuration prompt are given in the Table 4.1.

Table 4.1 : Setup Configuration Commands

No.	Command	Function
1.	configure	Configure server parameters
2.	factory	Restore all configurable parameters to factory default values.
3.	getconfig	Get configuration information from specified host
4.	help	Display help information for administrative commands
5.	putconfig	Save the configurations on a host file
6.	set	Set port parameters
7.	snmpconfig	Configure SNMP parameters
8.	stty	Set port characteristics
9.	quit	Exit from the setup menu and enter multiuser mode

After completing the setup configuration, the setup information is saved in the NVRAM automatically. When the administrator invokes the **quit** command to quit from setup configuration prompt, the server enters the multiuser mode. The setup configuration done so far is effective only when entering the multiuser mode.

The following sections describe the commands and their options in detail and explain how the administrator can configure the remote access server to utilise various features.

Configure

The configure command is used for setting the system wide parameters of the server. The parameters that may be set by the **configure** command are:

- Name of the server
- Port number for the Fixed port pseudo-terminal
- Whether ARP trace is to be enabled or not

- Mode in which rwhod must function (quiet or send)
- Mode in which the routed daemon must function (quiet or send)
- Whether IP packets are to be forwarded, if not intended for this server
- Whether the TCP acknowledgment be delayed or immediate
- Administrative password
- Domain Name System to be configured or not
- Domain Name Servers
- Name of the domain
- Reverse Telnet pool distribution mode.

The syntax of the command is:

```
configure [ <options> [ = <value> ] ]
```

The **configure** command without any options will display the current configuration information as below:

name=LANReach fptyport=8065 arp_trace=off rwhod_send=quiet routed_send=send ip_forward=on tcpnodelack=off dns=off domain= nameservers= pool_distr=linear tcpkeepalive=on

The options that may be configured and the possible values are explained below.

name=<*host name*>

The name of the server is defined as <*host name*> by this option. The name should not exceed 16 characters. The default name is LANReach. A proper name must be given using this command.

fptyport=*fixed pty port number*

The network port number for providing fixed-port service is defined by this parameter. The administrator may specify any port number here and configure the same port for Fixed Pty service on the required host, in ARPA services database, */etc/services*.

arp_trace=on/off

The Address Resolution Protocol resolves the host name to address mappings. If the ARP trace is **on**, then a trace of all ARP packets sent or received by the server is displayed on the console. If the trace is set to **off**, this information is not displayed.

rwhod_send=quiet/send

The daemon **rwhod** services the **ruptime** command by sending packets of information. This will be done when this option is set to **send**.

routed_send=quiet/send

The daemon **routed** implements the RIP protocol used for routing. This option controls whether the server should transmit RIP information. Normally, RIP information should be transmitted only by nodes acting as a gateway. When this option is set to **send** the RIP information is transmitted.

ip_forward=on/off

When multiple network controllers are present in the remote access server hardware, the server can act as a gateway between two networks. To get this functionality, the configuration should define ip_forward=on so that all internet packets from one network will be forwarded to the other network, if they are meant for the other network. If forwarding is disabled by configuring ip_forward=off, then the functionality of a gateway will not be there. IP forwarding can also be done with a single network controller. In this situation, packets not meant for the server will be forwarded to the right node.

tcpnodelack=on/off

The remote access server generates acknowledgment packets in response to incoming TCP data. These ACK packets can be delayed for performance reasons to reduce network traffic. This option controls whether TCP acknowledgment should be delayed or immediate. TCP acknowledgment will be delayed if **off** is specified and will be immediate if **on** is specified.

dns=on/off

The domain name system on the remote access server may be configured by setting **dns** to **on**. Once this is done dynamic DNS name to address binding takes effect. The dynamic mapping can be removed by specifying **off**.

ameservers=*internet address, internet address.*

The *internet address* of the host which functions as the name server for DNS, is specified by this option. More than one name server may be specified by giving a list of internet addresses separated by comma. A maximum of 4 servers can be specified. When more than one name server is available, a query is sent to the first available server in the list. Only in case of problems with the first, the next server is referred. If no nameserver is specified, DNS will be unusable.

domain=*domain name*

The name of the domain can be specified in this option. If domain name is not specified, DNS will be unusable.

pool_distr=round-robin/linear

When multiple ports are configured as reverse telnet type, with one TCP channel, they constitute a pool. If the user wants to distribute the usage of ports in a round-robin manner, round-robin may be specified. If the user wants to use the first available port, the option should be set to linear.

password

When **configure** command is invoked with this option, the prompt,

```
Enter old Password:
```

will appear. On typing the current administrator password, the prompt,

```
Enter new Password:
```

will appear. The new password may be typed now. On entering the new password, the prompt for reconfirming the password will appear as:

```
Reenter new Password:
```

The new password should be typed again to reconfirm. The default admin password is HCLPD. The maximum number of characters for the password is 15.

Factory

The administrator may restore the configuration parameters to factory default values to resolve any problems, using the command.

```
factory
```

in the setup configuration prompt.

getconfig

The **getconfig** command, present only under **nvram** mode is used to download the configuration information from a specified file in a specified host.

The command syntax is

```
getconfig [host]:[file]
```

The specified *file* containing the configuration information is downloaded through TFTP requests, from the *host*. The default host is the boot server specified in boot configuration. The default file is */etc/hosts*.

Help

The **help** command gives a list of commands available at the setup configuration menu of the server. The administrator may get detailed information about a specific command, by giving the command name as the argument to the **help** command.

Example

```
help configure
```

will display details like syntax, description and explanation for the arguments of the command **configure.**

The **?** command and **help** command may be used interchangeably.

Save Setup Configuration Information on Host

The administrator may save the current server configuration information on any of the hosts in the same network as the server on a given file name. The syntax of the **putconfig** command which does this function is:

```
putconfig <host>:<file>
```

This command results in the current server configuration to be transferred to the host <*host*> as a file <*file*>, using the trivial file transfer protocol tftp. This file may later be used for reconfiguring the server in the event of a loss of local configuration information.

Example:

```
putconfig indus:/etc/ts/bargavi.conf
```

Note

putconfig command will work properly only if the TFTP write service is enabled properly on the host. Refer appropriate host documentation for details.

Set Port Parameters

The **set** command is used to display or define port parameters. The syntax of the command is:

```
set [portname] [ option[=value] ...]
```

The **set** command without any argument, displays the server parameters for all the ports.

The port name can be specified as a single port (S3), or a list of ports (S1, S3, S5) or a range of ports (S7-S10).

If *portname* is specified in the command, the intended action is only for the specified port(s). If *portname* is not specified, then the **set** is for all the ports of the server. If no *option* and *value* are specified, the parameters are displayed. If *option* is specified, then the parameter is set to the *value* specified.

The following table gives the options and their meaning. The values that may be specified is also indicated.

Table 4.2 : Port Parameter Options

Option	Meaning	Possible values
term	The name of the terminal connected to the port	name of the terminal eg. vt100, vt220
prompt	The prompt displayed by the server on the user terminal. This is meaningful only in case of switched port terminals.	eg. RAS>

Table 4.2 : Port Parameter Options (Contd.)

Option	Meaning	Possible values
maxsession	Maximum number of sessions that can be simultaneously open from the port.The default value is 8. The administrator may reduce the same.This is not meaningful for implicit and fixed port connections.	Number less than or equal to 8.
Inhwflow	Input side hardware flow control	none -no hardware flow control rts -use RTS signal
Outhwflow	Output side hardware flow control	none -no hardware flow control cts -use CTS signal
user	Login name to be used for logging **implicit port** terminal.	Any valid login name. If no value is specified i.e. (user=) the host login prompt will appear.
Hosts	The list of host names separated by comma and prepended by a + represents the hosts to which access is allowed. In the case of switched ports, the list specifies that sessions can be established only with these hosts. In the case of implicit and fixed ports, the list specifies that implicit or fixed connection can be established with the first available host in the list. That is, if the first host is up connection is established with it. If the first one is down, then the connection is established with the next available one in the list.	eg. hosts=+indus, everest

Table 4.2 : Port Parameter Options (Contd.)

Option	Meaning	Possible values
	The list of host names separated by comma and prepended by a -, represents the hosts to which access is restricted (not permitted). This is applicable only for switched ports	eg. hosts=-cheetah, hclhpmas
type	Type of the port, switched /implicit /fixed /rtelnet.	The administrator can specify • line for switched port • implicit for implicit port • fixed for fixed port • rtelnet for Reverse Telnet Port • off for unused port
port_modify	Whether access to this port must be allowed or denied to any user.	Permitted/Denied.
tcpport	The TCP port to be used for Reverse Telnet.	Default is 2000
cdetect	Whether carrier detection in Sync port is to be performed or not.	on/off
authen	Whether authentication for Reverse Telnet is required.	on/off on – user name and password required. off – no authentication is required.
allowsecond	Whether to allow second reverse telnet connection for a port by closing the previous one.	yes/no

Example

```
set S2 type=line term=vt100 prompt=LANS2>
```

The **set** command for a switched port will display like,

```
S1 inhwflow=none outhwflow=none type=line term=vt100 prompt=RAS>
hosts=indus maxsession=8
```

Note

In a switched port parameter display, the **hosts** option may or may not be present.

The **set** command for a implicit port will display like,

```
S2  inhwflow=none  outhwflow=none  type=implicit  term=vt220
hosts=Indus user=myname
```

Note

In an implicit port parameter display,

1. The **hosts** option will be present always and will have only one host name to which implicit connection is established.

2. The **user** option will be present in **implicit** port definitions. If no user name is specified, **set** will display **user=<null>**.

The **set** command for a fixed port will display like,

```
S3  inhwflow=none  outhwflow=none  type=fixed  term=vt100
hosts=hclhpmas
```

Note

In a fixed port parameter display,the **hosts** option will be present and will have only one host name to which fixed port connection is established.

The **set** command for a reverse telnet port will display like,

```
     S4 inhwflow=none  outhwflow=none  type=rtelnet  tcpport=2000
authen=off allowsecond=no
```

For a unused port, the **set** command will display the type as **off.**

Configure SNMP Parameters

The administrator may view or modify SNMP options on the remote access server by using the **snmpconfig** command.

The command syntax is

snmpconfig [*option*=[*value*]...]

If no option is specified, the command will display all options and their current values.

Example

```
snmpconfig

sysLocation=Delhi  sysContact=NWManager  authTraps=enabled
trapdests=host:public  community=public:RO
```

The following tables gives the options, their meanings and the possible/default values.

Table 4.3 : SNMP Options

Option	Meaning	Possible values
sysLocation	Physical location of the remote access server. This option can be set by a SNMP SET request from a SNMP manager.	A string upto a maximum length of 31. Factory defa ult is a null string. If no *value* is specified, it is set to null.
SysContact	Name of the person incharge of the remote access server. This also can be set by a SNMP SET request from a SNMP manager.	String of upto 31 characters. Factory default is null. If no *value* is specified, the option is set to null.

Table 4.3 : SNMP Options (Contd.)

Option	Meaning	Possible values
authTraps	Control enabling or disabling of authentication traps.	enabled or disabled. Factory default is disabled. If no value specified,error is displayed.
trapdests	The host name and its community to which traps are to be sent. To add a pair the *value* must be preceded by +. To delete a pair the *value* must be preceded by -.	*hostname:community* or *internet address:community* Community string can be a maximum of 15 characters and refers to valid community name for the SNMP manager. Multiple pairs can be added / deleted by giving a comma separated list. All pairs can be deleted by specifying no *value.* The command snmpconfig trapdests=host:community will delete all existing destinations and add this host as a new destination.
Community	Add or delete the community: permissions pair which are to be used to validate incoming SNMP requests. To add a pair the *value* must be preceded by +. To delete a pair the *value* must be preceded by -.	+*community name:permission* will add a pair -*community name:permission* or -*community name* will delete a pair *community name* can be upto 15 characters. Multiple pairs can be added or deleted, by giving a comma separated list.

Table 4.3: SNMP Options (Contd.)

Option	Meaning	Possible values
	When a SNMP request is received, its community name is checked. If the name matches one of the configured name, its permissions for the requests are checked. If the permissions do not allow the request then a No Ack is sent to the manager available to the community If community itself does not match any of the configured community names, the request is dropped. If the community and permission match, then the request is allowed.	All pairs can be deleted by specifying no *value* The command snmpconfig community=*community name : permission* deletes all existing pairs and adds this pair. The permissions and their meanings are defined in the table

The community permissions and their meanings are described in the table below:

Table 4.4: SNMP Community Permissions

Permission	Meaning
RO	The SNMP request from a SNMP manager belonging to the corresponding community can only be to GET information and not to SET.
RW	The SNMP request from the SNMP manager belonging to the corresponding community can do both GET and SET.
WO	The SNMP request from the SNMP manager belonging to the corresponding community can only SET.
NA	The SNMP request from the SNMP manager belonging to the corresponding community can neither GET nor SET information.

Set Port Characteristics

The administrator may view or modify the characteristics of any or all ports of the server using the **stty** command.

The command syntax is:

```
stty [portname] [option[=value]...]
```

The command without any parameters displays the port setting of all ports of the server. When a option and its value are specified, the option is set to that value.

The portname can be specified as a single port (S3) or a list of ports (S3, S5, S7) or a range of ports (S3-S7).

If *portname* is specified, the parameters of the specified port(s) are displayed or set. If *portname* is not specified, then the parameters of all the ports are displayed or set as specified.

The table below gives the list of parameters and meaning of the parameter. Wherever applicable, the values possible are specified.

Table 4.5 : Port Characteristics

Parameter	Syntax	Meaning
Speed of the terminal	<baudrate>	Specify a number indicating the baudrate. The possible baudrates are 75, 110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 7200, 14400, 57600, 76800, 115200
Number of bits per character	cs7	set 7 bits per character
	cs8	set 8 bits per character
Odd or Even parity	+parodd	set odd parity
	-parodd	set even parity

Table 4.5 : Port Characteristics (Contd.)

Parameter	Syntax	Meaning
Enable or disable parity Checking	+parenb	Enable parity checking
	-parenb	Disable parity checking
Number of stop bits per character	+cstopb	2 Stop bits per character
	-cstopb	1 stop bit per character
Software output flow control	+ixon	Enable software output flow control (Control-S, Control-Q will be the default start and stop characters)
	-ixon	Disable software output flow control
Software Input flow control	+ixoff	Enable software input flow control
	-ixoff	Disable software input flow control
Modem control	-clocal	Modem control required on the port
	+clocal	No modem control required on the port. (default)
DSR signal sensing	-dsr	Connection will be established irrespective of DSR signal status
	+dsr	Connection will not be established if DSR is not active
DTR signal toggling	+dtr	DTR will be active only if the connection is alive
	-dtr	DTR signal will be present always
Break character	+ignbrk	Ignore break character This option cannot be changed.
Set erase character	erase=*<char>*	The erase character is set to the character specified.
Set start character	start=*<char>*	Start character is set to the character specified

Table 4.5 : **Port Characteristics (Contd.)**

Parameter	Syntax	Meaning
Set stop character	stop=*<char>*	Stop character is set to the character specified The start and stop character are used for software (input/output) flow control, ixoff/ixon.
Set Interrupt character	intr=*<char>*	The character specified is defined to be the interrupt character This is used by line manager to enable users to abort the currently executing remote access server command like, **ping.**
Set escape sequence for the remote access server to escape from sessions	escape=*<sequence>*	The sequence for escaping from server sessions is set to the sequence specified. The sequence can be upto four characters. The default escape sequence is ^T. (CTRL-T DOT)

Example

```
stty S2 9600 cs7 +ixon +parodd escape=^T
```

Note

When control characters are to be specified while defining the escape sequence, user may either type ^(caret) followed by the character or specify the equivalent octal value in the format '\xxx' where 'xxx' is the three digit octal value. It is recommended that the octal value format is used rather than ^(caret) format.

When modem control is enabled, the remote access server provides processing of DTR signal. The manager running on the port on which modem control is required, will wait for DCD (Carrier Detect) signal before proceeding. All sessions initiated from this port will be terminated when carrier is lost.

Quit

The quit command automatically saves the configuration in the NVRAM enables the administrator to quit from the setup configuration menu and enter the multiuser mode. All configuration setup done during the setup phase will be in effect when entering the multiuser mode.

Setup Procedures

The details of how to configure the ports for

- Switched port usage
- Implicit port usage
- Fixed port usage
- Reverse Telnet port usage
- Connecting a printer on Implicit port
- Connecting a printer on Fixed port

are given below.

Switched Port

For configuring a server port as a switched port, the following command should be given at the setup configuration prompt.

```
set portnumber type=line
```

where *portnumber* is the port which is being setup.

In this configuration, the following options also may be specified.

- prompt
- term
- maxsession
- hosts or -hosts

Example

```
set S2 type=line prompt=S2:rb> term=hp
```

Note

For detailed information about Intallation and Cofiguration of the remote access server with various Unix maching, refer Appendix-F

Implicit Port

For configuring a server port as an implicit port, the following set command should be given.

```
set portnumber type=implicit hosts=hostname user=username
```

where *portnumber* is the port which is being setup, the *hostname* is the name of the host to which implicit connection is to be established and *username* is the name of the user to be logged in. As mentioned earlier the *username* need not be specified.

Example

```
set S3 type=implicit hosts=hclhpmas user=rb
```

This will configure port S3 as an implicit port. On entering multiuser mode a login connection will be established with the host **hclhpmas** and with the username as **rb**.

If no user name is specified in the implicit port setup, a login prompt will be displayed by the remote access server indicating the host name to which logging in will be attempted. After the user enters the login name a rlogin session will be established with that host for the user name.

Example

```
rlogin to indus as: rb
```

If the host name is not specified, when the remote access server enters multiuser mode, an error message will be displayed, like

```
implicit: port S3, host is not set
```

If the implicit connection fails, the remote access server will retry for the connection after **timeout** seconds specified in the **set** command. The default value of **timeout** is 60.

Fixed Port

For configuring a server port as a fixed port, both the remote access server and the host to which fixed port is required, are to be configured accordingly.

Configuring the fixed port at the remote access server side

set *portnumber* type=fixed hosts=*hostname*

will configure the port *portnumber* as a fixed port with the host *hostname.*

Example

```
set S4 type=fixed hosts=hclhpmas
```

will configure port S4 as a fixed port to hclhpmas

Configuration for the fixed port, at the host side

Step 1 In the ARPA services database on the host, an entry for **fpty** service may be present. If it is not present, a default fixed-pty service port number of 8065 is assumed.

Step 2 For each port specified as fixed port in the remote access server(s), an entry should be added in the */etc/fptyd.conf file* so that the ptys can be reserved and allocated for fixed ports.

Format of an entry in the file is:

```
Ptyname     Internet Address             Portnumber
                    or
            Remote access server name
```

Example

1. /dev/pty/ttyp3   196.1.68.34   S10

   This will make */dev/pty/ttyp3* fixed to the port S10 of the server having internet address 196.1.68.34

2. It is also possible to specify the server name in place of the internet address.

   /dev/pty/ttyq3   bargavi   S2

3. For parallel port, the port number should be specified as P0.

   /dev/pty/ttyq5   90.3.4.5   P0

   This will make */dev/pty/ttyq5* fixed to the parallel port P0 of the server having internet address 90.3.4.5.

Step 3 In the */etc/inittab file*, an entry must be made for the pseudo-tty name, to respawn */etc/getty*. This is required only if this port is to be used for login purposes.

For instance, if the pseudo-tty name for a fixed port is, */dev/pty/ttyp3*, the corresponding */etc/inittab* entry should be like:

ttyp3:2:respawn:/etc/getty -h */dev/pty/ttyp3* vt100

This is only an indicative example and the actual format of the inittab entry depends on the host system.

Step 4 After making entries in the */etc/fptyd.conf file* and in */etc/inittab file*, the host must be rebooted, for the changes to take effect.

Note

Make sure that the chosen pty devices are valid, and configured in the kernel. For the procedure to be used for configuring the ptys on the host, refer to the respective host system administrator's manuals. For example, the kernel parameters **nfile** and **npty** are to be configured appropriately on HP systems running HP-UX.

Reverse Telnet Port

For configuring a remote access server port as an reverse telnet port, the following **set** command can be given:

```
        set <portnumber> type=rtelnet tcpport=tcpport hosts=[+|-]hostname authen=on/off
allowsecond=yes/no
```

Where *portnumber* can be one or more port numbers specified as a list or range to be set as the rtelnet port, *tcpport* specifies the TCP channel number on which Reverse Telnet Service is available and *hostname* specifies the list of permitted/restricted hosts. authen can be used for providing authentication for reverse telnet.a*llowsecond* can be used for allowing a second reverse telnet connection to a port by closing the previous one, if the option is enabled.

A maximum of four hosts only can be specified in the list. **The type of a port can not be changed dynamically.**

Example

```
        set S4 type=rtelnet     tcpport=2000     hosts=+indus, calculus authen=on
allowsecond=yes
```

While setting the port type, to reverse telnet the user may form a pool of ports, by specifying multiple port numbers with a single TCP channel (tcpport). After constituting a pool of rtelnet ports, the distribution of usage of these ports may be defined as **round-robin** or **linear** in the **pool-distr** option of **configure** command.

Example

```
        configure pool_distr=round-robin
```

After configuring the reverse telnet port when the remote access server comes up, a printer may be connected to the port and shared by all hosts in the network. Users from any host may use the printer by using a command such as

```
        cat filename | telnet TSname tcpport
```

Example

```
        cat myfile | telnet bargavi 2000
```

Connecting Printer to Implicit Port

To configure for connecting a printer to an implicit port of the remote access server, the port should be setup as an implicit port using the **set** command in the setup configuration.

```
set portnumber type=implicit hosts=hostname user=printername
```

This will configure the port *portnumber* of the remote access server to establish an implicit connection to the host *hostname* and login as *printername*.

The **portnumber** must be specified as S1, S2 ...., S16 for serial port 1, 2, ..., 16 respectively and must be specified as P0 for parallel port.

When more than one printer is configured through implicit ports of same or different remote access servers, to a single host, the *printername* specified, must be unique.

Note

If the printer is connected to a serial port, then the baud rate, parity and software flow control (ixon/ixoff) settings on the printer and at the remote access server port should be identical. Normally, on the serial printer this is set using switches. On the remote access server this should be set through **stty** command. For printer switch settings refer to the printer manuals.

If a parallel printer is to be connected to the parallel port of the remote access server, then the parallel port P0 must be configured as either implicit or fixed port.

The following steps are to be done on the host to which implicit connection is required.

Step 1 Logins are to be created for the printer with login id as the *printername*. No password is to be assigned for this login. This login should have permissions, owner and group identical to that of the line printer system **lp** on the host. This login account should execute the *etc/ts/lp/tsprof* in the TFTP home directory, in place of the login shell.

Note

For the procedure to be followed to define a login-id without an associated password on secure host systems, refer to the appropriate host manuals.

Step 2 The printer should be configured using the procedure below.

- Stop the lpscheduler with **/usr/lib/lpshut**
- Use the lpadmin command to add the printer to the system

```
lpadmin -pprintername -v/dev/null –mtsmodel
```

- Make the printer interface accept lp requests by using **accept** command
- Start the lpscheduler by running **lpsched**
- Enable the printers by **enable** command.

Note

1. **tsmodel** is a interface program supplied with the package.

2. Printer errors, such as Out of Paper etc will be indicated on the remote access server by using the **activity** command only; the host system will not be able to detect these.

Example

To connect a printer with name **tspr0** on implicit port 3 of remote access server, set the printer port as implicit with host indus and user tspr0. This example assumes that the RAS software is installed in */usr/tftpdir* on the host. This may vary between host systems.

```
set S3 type=implicit hosts=indus user=tspr0
```

Similarly, if the printer is to be connected to the parallel port then it should be configured like,

```
set P0 type=implicit hosts=indus user=tspr0
```

Do the following on host indus.

1. Add a login with id **tspr0**, with permissions same as login id **lp** and login script as *etc/ts/lp/tsprof,* using the system administration procedure of the host. After configuring, the */etc/passwd file* will contain an entry like,

```
tspr0:x:71:2:printer:/usr/tspr0:/usr/tftpdir/etc/ts/lp/tsprof
```

2. Configure printer as follows:

```
lpshut
lpadmin -ptspr0 -v/dev/null -mtsmodel
accept tspr0
lpsched
enable tspr0
```

Connecting Printer to Fixed Port

For connecting printer to a fixed port of the remote access server, both the remote access server and the host to which fixed port is required, are to be configured accordingly.

Configuring the fixed port at the remote access server side

set *portnumber* type=fixed hosts=*hostname*

will configure the port *portnumber* as a fixed port with the host *hostname* and will use the fixed pseudo-tty port *ptyname* for connection.

The **portnumber** must be specified as S1, S2 ....., S16 for serial port 1,2,...., 16 respectively and must be specified as P0 for parallel port.

Note

If the printer is connected to a serial port, then the baud rate, parity and software flow control (xon/xoff) settings on the printer and at the remote access server port should be identical. Normally, on the serial printer this is set using switches. On the remote access server this should be set through **stty** command. For printer switch settings refer to the printer manuals.

If a parallel printer is to be connected to the parallel port of the remote access server, then the port P0 must be configured as implicit or fixed.

Configuration for connecting the printer to the fixed port, at the host side

Step 1 In the ARPA services database on the host, an entry for **fpty** service may be present. If it is not present, a default fixed-pty service port number of 8065 is assumed.

Step 2 For each port specified as fixed port in the remote access server(s), an entry should be added in the */etc/fptyd.conf* file so that the ptys can be reserved and allocated for fixed ports. For details of the */etc/fptyd.conf* file format refer to Fixed port configuration above.

Step 3 In the */etc/inittab* file, an entry must be made for the pseudo-tty name, as shown below:

```
ttyp3:2:off:/etc/getty -h /dev/pty/ttyp3 vt100
```

Note that the **action** field in the **inittab** entry is **off** in case of printer.

Step 4 The printer should be configured using the procedure below.

- Stop the lpscheduler with **/usr/lib/lpshut**
- Use the lpadmin command to add the printer to the system

```
lpadmin -pprintername -v/dev/pty/ttyp3 - mdumb
```

- Make the printer interface accept lp requests by using **accept** command
- Start the lpscheduler by running **lpsched**
- Enable the printers by **enable** command.

Note

1. the interface program, **dumb** or any other suitable one, provided by the system should be used for the fixed printer.

2. the **tsmodel** interface should **NOT** be used with fixed printer.

3. Printer errors, such as Out of Paper etc will be indicated on the remote access server by using the **activity** command only; the host system will not be able to detect these.

Step 5 After making entries in the */etc/fptyd.conf* file and in */etc/inittab* file, the host must be rebooted, for the changes to take effect.

Modifying the configuration

After configuring the remote access server, the user may exit from the setup configuration menu and enter multiuser mode. Subsequently, if it is required to modify any parameters, administrative commands may be used in the **admin** menu. These changes will be applicable only for the current run of the remote access server. For changing the configuration parameters permanently, the user will have to do the changes at the remote access server setup configuration at boot time and save the changes in the Non-volatile memory or use the administrative commands in nvram menu.

5

ERROR MESSAGES

The remote access server, to enable better problem diagnosis and complete problem reporting provides display of self-explanatory error messages whenever a problem is encountered.

At power-on the remote access server, it performs a detailed self-test of all basic components and verifies that they are alright. In case of errors, messages will be displayed which can be referred as **Diagnostic error messages.**

After booting, at the run time of the remote access server, if problems occurred, messages will be displayed which can be referred as **Run time error messages**.

Both **Diagnostic** and **Run time error** messages will be displayed on the console port. This chapter explains and lists down both types of error messages.

Diagnostic Error messages

At power-on the remote access server, it displays the Boot version of the download software as given below.

```
HCL Peripherals
LANReach Boot Version 1.00
Press Ctrl-C for Diagnostic Menu
```

After getting display of the above message, the user may press ^C to perform diagnostics test. Otherwise, within 3 seconds, the remote access server does a self-test of the components populated and display messages accordingly. Suppose, if main memory is not proper and 8 ports (S1-S8) of the remote access server are not properly working, it will display the following.

```
Self-Test Routine
Memory Test – Failed
Serial Controller Test
ACE Internal Loop back Test Failed for Port - 0
ACE Internal Loop back Test Failed for Port - 1
ACE Internal Loop back Test Failed for Port - 2
ACE Internal Loop back Test Failed for Port - 3
ACE Internal Loop back Test Failed for Port - 4
ACE Internal Loop back Test Failed for Port - 5
ACE Internal Loop back Test Failed for Port - 6
ACE Internal Loop back Test Failed for Port - 7
ACE Internal Loop back Test Failed for Port - 8
ACE Internal Loop back Test Passed for Port - 9
ACE Internal Loop back Test Passed for Port - 10
ACE Internal Loop back Test Passed for Port - 11
ACE Internal Loop back Test Passed for Port - 12
ACE Internal Loop back Test Passed for Port - 13
ACE Internal Loop back Test Passed for Port - 14
ACE Internal Loop back Test Passed for Port - 15
NVRAM present
FLASH1-AMD 29F080B
FLASH1-AMD 29F080B
```

The list of self-test diagnostic error messages that the remote access server can display is listed below.

```
NVRAM not present
FLASH-1 not present
FLASH-2 not present
Memory Test – Failed

No Memory module Detected
ACE Internal Loop back Test Failed for Port portnumber
ACE External Loop back Test Failed for Port portnumber
```

As stated earlier, the user has to press ^C to enter into diagnostics test mode. After pressing ^C, a menu will appear as given below.

```
                Menu
                -------

      1. Main Board Logic Tests
      2. Network Tests
      3. Async Ports Tests
      4. RTC Test
      5. Printer Port Tests
      6. System Debug Aid

      Enter Choice(1,2,3,4,5,6 or q - quit)?
```

By selecting **Main Board Logic tests** from the above menu, the user can test on-board components such as **FP/EDO DRAM SIMM module test**, **NVRAM test** and **Flash test**.

By selecting **Network Tests**, the user can perform **Internal loop back** and **external loop back** test of the Ethernet port.

By selecting **Async Ports Tests**, the user can perform **Internal loop back** and **external loop back** test for all the sixteen ports.

By selecting **RTC test**, the user can set **date** and **time** related parameters.

By selecting **Printer Port Tests**, the user can test the printer port by printing a single character.

By selecting **System Debug Aid**, the user can perform various related tests such as **Continuous Read Write Memory**, **Examine Memory** and **Dump Memory**.

Note

For Network External loop back test, an external loop back cable should be connected to the Ethernet port.

For ACE External loop back test an external loop back cable should be connected to ACE port under testing

The Printer should be connected to the printer port before to perform Printer port test

The list of error messages that the remote access server can display at the time of Diagnostics test is listed below.

```
Invalid address
Address not valid
NVRAM not present
NVRAM TEST FAILED
FLASH-1 not present
```

FLASH-2 not present
Memory Test - Failed
MAIN MEMORY TEST FAILED
Memory Module not found
No Memory module Detected
NVRAM memory not Detected
Internal Loop Back Test FAILED
External Loop Back Test FAILED
Error in TxD => RxD signal path
Error in DTR => DCD signal path
Error in DTR => DSR signal path
Error in DTR => DCD signal path
Error in DTR => DSR signal path
Error in RTS => CTS signal path
ACE Internal Loop back Test Failed for Port - *portnumber*
ACE External Loop back Test Failed for Port - *portnumber*
Address range is Discontinuous. Only 32 Kb can be used
Error in Location = %x, *memorylocation*
Location failed = 00
Invalid Hour
Invalid minutes
Invalid seconds
Invalid date
Invalid month
RTC returned invalid data\n Restoring factory default data
Erase Failed
Write - Verify Test failed
Unknown Flash type
RTC Not Proper!!! Unable to write to RTC
Network Tests cannot be performed
Printer is NOT READY

Note

The words in *italics* in the list of error messages will be replaced by values of the corresponding parameters in the actual error message displayed by the remote access server.

Run time Error Messages

Run time Error Messages provide more information on a running remote access server. The messages listed below are self-explanatory and hence no detailed explanation is provided.

Synchronizing system time with RTC to *time*
routed: started
rwhod: started
ACE(*unit*) not present
ace: tx_intr for closed port *portnumber*
ace: modem intr for closed port *portnumber*
channel *channel name* receiving inspite of having sent XOFF
boot_server=*hostname*
bootfile=*filename*
arg to set_interface0
flyd started
Setting system time from RTC to *time*.
AMD (*unit*): lost TINT(*interrupt*) interrupt
rlogin_rdwr(*tty*): received unknown event *event*
rlgin_rdwr: recd unknown event on tty *tty*
implicit(*tty*): unable to TCGETA *attribute*
implicit(*tty*): unable to TCSETA *attribute*
fixed(*tty*): unable to TCGETA *attribute*
fixed(*tty*): unable to TCSETA *attribute*
routed: select error *error number*
routed: terminating
routed: allocb failed to allocate an mp
rwhod: select error *error number*
rwhod: terminating
rwhod: received unknown version message *message* type from host
rwhod: received unknown message type *message* type from host
timeout: get_toutq fails
tcplrput: too many to drop(1)
tcplrput: too many (2)
telnet_rdwr(): received unknown event.
telnet_rdwr: recd unknown event *event* on tty *tty*
snmp_put
snmp_get
DNS is back in use
DNS coming up....
getgreaterifIndex
chkatifIndex
chkatnetaddr
ipForwardingGet
ipDefaultTTLGet
ipInReceivesGet
ipInHdrErrorsGet
ipInAddrErrorsGet
ipForwDatagramsGet
ipInUnknownProtosGet
ipInDiscardsGet

ipInDeliversGet
ipOutRequestsGet
ipOutDiscardsGet
ipOutNoRoutesGet
ipReasmReqdsGet
ipReasmOKsGet
ipReasmFailsGet
ipFragOKsGet
ipFragFailsGet
ipFragCreatesGet
ipRoutingDiscardsGet
ipAdEntAddrGet
ipAdEntIfIndexGet
ipAdEntNetMaskGet
ipAdEntBcastAddrGet
ipAdEntReasmMaxSizeGet
ipAddrGet
getAdNetAddr returning EINVAL
ipAddrNext:namelen
ipNtoMNext
ipNetToMediaTypeGet
ipRouteTypeGet
ipRouteAgeGet
ipRouteMaskGet
ipRouteNext:namelen
ipRouteDestGet
ipRouteIfIndexGet:
ipRouteMetric1Get
ipRouteMetric2Get
ipRouteMetric3Get
ipRouteMetric4Get
ipRouteNextHopGet
ipRouteProtoGet
ipRouteMetric5Get
ipRouteInfoGet
ipForwardNextHopASGet
ipForwardPolicyGet
ipAddrGet
ipAdEntAddrGet
ipAdEntIfIndexGet
ipAdEntNetMaskGet
ipAdEntBcastAddrGet
ipAdEntReasmMaxSizeGet
ipNtoMNext
ipNetToMediaTypeGet
ipRouteDestGet
ipRouteIfIndexGet
ipRouteMetric1Get
ipRouteMetric2Get
ipRouteMetric3Get
ipRouteMetric4Get
ipRouteNextHopGet
ipRouteTypeGet

ipRouteProtoGet
ipRouteAgeGet
ipRouteMaskGet
ipRouteMetric5Get
ipRouteInfoGet
ipforwardPolicyGet
ipForwardNextHopASGet
snrwOpVerify
snroOpVerify
snwoOpVerify
snwoOpVerify
Read of NVRAM failed in snPermsInit
smpInputEvent: aps Verify Failed
snmpInPktsGet
snmpOutPktsGet
snmpInBadVersionsGet
snmpInBadcommunityNamesGet
snmpInBadCommunityUsesGet
snmpInASNParseErrsGet
snmpInTooBigsGet
snmpInNoSuchNamesGet
snmpInBadValuesGet
snmpInReadOnlysGet
snmpInGenErrsGet
snmpInTotalReqVarsGet
snmpInTotalSetVarsGet
snmpInGetRequestsGet
snmpInGetNextsGet
snmpInSetRequestsGet
snmpInGetResponsesGet
snmpInTrapsGet
snmpOutTooBigsGet
snmpOutNoSuchNamesGet
snmpOutBadValuesGet
snmpOutGenErrsGet
snmpOutGetRequestsGet
snmpOutSetRequestsGet
snmpOutGetResponsesGet
snmpOutTrapsGet
snmpOutEnableAuthenTrapsGet
In snmpStatNext *namelenp
ifNext: NULL intcontptr
tcpRtoAlgorithmGet
tcpRtoMinGet
tcpRtoMaxGet
tcpMaxConnGet
tcpActiveOpensGet
tcpPassiveOpensGet
tcpAttemptFailsGet
tcpEstabResetsGet
tcpCurrEstabGet
tcpInSegsGet
tcpOutSegsGet

tcpRetransSegsGet
tcpInErrsGet
tcpOutRstsGet
n tcpStatNext
tcpConnStateGet
tcpConnLocalAddressGet
tcpConnLocalPortGet
tcpConndRemAddressGet
tcpConnLocalPortGet
In tcpconnexecfunc.cookie
get_tcpptr
Decode Failed
get_tcpptr Failed
tcpConnGet
get_conn_entry Failed
tcpConnGetSet
amdrsrv: canput fail
linemgr(*manager*): recd SIGINT on unknown stream
linemgr(*manager*): read() unknown signal *signal*
linemgr(*manager*): read() unknown error *error number*
cksum: out of data: *size.size2*
implicit: port *port*, TCSETA fails *error number*
implicit: port *port*, host is not set
implicit: port *port*, restore TCSETA fails *error number*
fixed: port *port*, TCSETA fails *error number*
fixed: port *port*, host is not set
fixed: port *port*, pty is not set
fixed: port *port*, restore TCSETA fails *error number*
routed: unable to create socket
routed: unable to bind socket *error number*
routed: could not bind to UDP post, instead bound to UDP *post*
routed: received exception
routed: recvfrom failed *error number*
routed: sendto *destination* failed *error number*
routed: addroute failed. Dest *destination* Gateway gateway Err *error*
rwhod: unable to create socket
rwhod: unable to bind socket *error number*
rwhod: could not bind to UDP *port*, instead bound to UDP *port*
rwhod: received exception
rwhod: recvfrom failed *error number*
rwhod: sendto *destination* failed *error number*
connect: received bad response *response type*
tcpuwserv: Unexpected message type *type* on control channel
tcpuwserv: on a Channelless queue
tcpuwserv: on a hungup channel
tcp: system error
telnet_rdwr(): socket exception *exception*
unknown ace_rxintr (*interrupt*) for port *port*
portno not present
portno not open
rtelnetd: failed to open socket
amdintr: Illegal INT *interrupt*
newpid: process table is full

pid *process-id*: cannot open port *portnumber*
load_config: *value* unsupported baud rate
Data read from RTC is invalid *data*
xmain(*port*): *value* Unsupported baud rate
xmain(*port*): TCSETA fails *error number*
linemgr: *value* Unsupported baud rate
linemgr: port *portnumber*, TCSETA fails *error number*
linemgr: *portnumber*, restore TCSETA fails *attribute*
port_init: cannot access port *portnumber*, manager *manager*
implicit pid *process-id*: cannot open port *portnumber*
implicit() pid *process-id* terminating
fixed pid *process-id*: cannot open port *portnumber*
fixed() pid *process-id* terminating
bufcall failed, no free buf_event. Fune = function arg = argument
tcpuwserv: q is free *value*
tcpurserv: q is free *value*
TCP: Valid message after release in receive queue
ace_ioctl(TCSETA): invalid values *0xvalue, 0xvalue*,
0xvalue, 0xvalue,value,value
unknown configure option
cannot open port
unsupported baud rate
TCP: valid message after release in receive queue
AMD Unit *number* V1.0 IRQ=*number* IOADDR = 0x*hexanumber*
POST Error (*hexanumber*)
AMD Unit *number* V1.0 IRQ = *number* IOADDR = 0x*hexanumber*. Not found
AMD*number*: Board Type(*hexanumber*) not correct,
replace network controller at *hexanumber*
AMD*number*: checksum error (*hexanumber, hexanumber*) at IOBASE *hexanumber*
AMD*number*: Ethernet address is not available
AMD(*number*): controller did not start *hexanumber*
AMD*number*: did not complete initialization (*hexanumber*)
AMD(*number*): not present
AMD(*number*): already open
Cannot allocate queue for AMD(*number*)
AMD(*number*): could not reset
spurious interrupt (*number*) on AMD Ethernet Controller
amdintr: AMD(*number*) not open *hexanumber*
ARP: Duplicate Network Address: *number.number.number.number*
His Ether Address=*string*
My Ether Address = *string*
AMD (*number*): Interface address *hexanumber* in use. Shutting down.
Recongifure interface correctly
amdwsrv: Unknown MSG type = *number*
amdnumber: Unknown message type 0x*hexanumber*
amdnumber: Unknown to_snp type 0x*hexanumber*
amdnumber: size number exceeding ETHERMTU
arp_who_has: allocb failed
Received ARP request on unknown protocol *hexanumber*
arp_resolve: Got an Unknown ARP opcode (0x*hexanumber*)
from *number.number.number.number*
arp_resolve: allocb failed
Internal RTC Battery Low

NVRAM Checksum Bad
rtcinit failed *number*
alarm_init failed *number*
FLASH Memory not Present
FLASH Memory Checksum Bad
The Interface address is not set properly. Please try again
amdopen fails
Booted version *string* from FLASH Memory. Update is not necessary
get_rtc_time failed *number*
Failed to erase address *hexanumber* data read *hexanumber*
cmn_err. Invalid message type 0x*hexanumber*
System has panic'ed
Line too long the *wrong line*
Nothing after Identifier *string*
invalid fixed port *string*
Password *string* too long in configuration
Error in rwhod mode *string*
Error in routed mode *string*
Error in Forwarding mode = *string*
Cannot set Console error level to *string*. Check value in configuration
Cannot set Buffer error level to *string*. Check value in configuration
Illegal Identifier *string*
Illegal line *string*
Name not found after address *string*
Invalid address in config *string* name i
Name length more than *number string*
Entry for address *string* already found in host table
Host table entry is *string*   *string*
Entry for name *string* already found in host table
Host table entry is *string*   *string*
Host table is full
Not a valid portname (*string*), param = *string*
Parameters expected for port *string*
Error in config for port string mode *string*
    Configuration for port *string* is set to default
Inconsistent configuration entry for port *string*
    Configuration for port *string* is set to default
load_config: port *number*, restore TCSETA fails *number*
Console not Present
Flash Memory not sensed (*hexanumber*), (*hexanumber*)
FLASH Memory checksum(*hexanumber*) is bad
Failed to program address *hexanumber* with data *hexanumber*
Unable to program FLASH Memory
Unable to program FLASH Memory with checksum (*hexanumber*)
string: No response from boot server
get_a_file: some data after Rx over
No response from hosts on network
Unexpected hardware interrupt IRQ *number* from 0x*hexanumber*
Unexpected Interrupt from 0x*hexanumber*
amdopen(0) fails
LP Unit *number* V1.0 IRQ = *number* IOADDR = 0x*hexanumber*
    POST Error (*hexanumber*)
LP Unit number V1.0 IRQ = *number* IOADDR = 0x*hexanumber*

Failed (*hexanumber*)
Cannot allocate stream for *string*
Cannot allocate lp queue for *string*
Boot Server(*string*) not set. Host data base not downloaded
Unable to write to NVRAM. return = *number*
socket: cannot allocate queue for protocol
socket: cannot open protocol *number*
recv: unknown TLI primitive *number*
streamer: interrupted *hexanumber*
unsleep: process (*number*) not in valid state = *number*
tcp_wr_processmsg: Message on a HUNGUP channel
tcplwserv:
tftpget: unable to create socket
tftpget: unable to bind socket *number*
tftpget: allocb fails
tftpget: sendto string failed *number*
tftpget: received exception
tftpget: recvfrom string failed *number*
Line too long. Correct configuration file. line is\n string
tftpget: allocb fails
Unexpected Trap type *number* from 0x*hexanumber*
div0trap from 0x*hexanumber*:0x*hexanumber*
dbgtrap from 0x*hexanumber*:0x*hexanumber*
nmiint from 0x*hexanumber*.0xhexanumber
breakpoint from 0x*hexanumber*:0x*hexanumber*
overflow int from 0x*hexanumber*:0x*hexanumber*
bounds trap from 0x*hexanumber*:0x*hexanumber*
invalid opcode [0x*hexanumber*] from 0x*hexanumber*:0x*hexanumber*
coprocessor not available from 0x*hexanumber*:0x*hexanumber*
double fault error code (0x*hexanumber*) from 0x*hexanumber*:0x*hexanumber*
coprocessor segment overrun from 0x*hexanumber*:0x*hexanumber*
invalid TSS error code (0x*hexanumber*) from 0x*hexanumber*:0x*hexanumber*
segment not present selector = 0x*hexanumber* from 0x*hexanumber*:0x*hexanumber*
stack exception selector = 0x*hexanumber* from 0x*hexanumber*:0x*hexanumber*
general protection exception error code (0x*hexanumber*) from
0x*hexanumber*:0x*hexanumber*
page fault error code (0x*hexanumber*), vaddr (0x*hexanumber*) from
0x*hexanumber*:0x*hexanumber*
coprocessor error from 0x*hexanumber*:0x*hexanumber*
stack trace reentered
ACE(*number*): already open
Cannot allocate stream for ACE(*number*)
Cannot allocate tty queue for ACE(*number*)
ace_open: allocb fails ACE(*number*)
ACE(*number*): received signal
ace_out_start: couldn’t get context for channel *number*
ACE Unit *number* V1.0 IRQ = *number,number,number*
MEM = *hexanumber* POST Error (*hexanumber,hexanumber*)
ACE Unit *number* V1.0 IRQ = *number,number,number*
MEM = *hexanumber* Failed (*hexanumber*)
install_isr: Illegal interrupt *number* = *number*
install_isr: handler is null
Illegal menu type *number*

Not a valid port name
Parameters expected for port
Error in config for port
Configuration for port is set to default
Inconsistent configuration entry for port
Unknown configure option
Internal RTC Battery low
NVRAM checksum bad
Console not present
Unknown Motherboard revision
Cannot create process
tftpget: Unable to create socket
flyd: Unable to create socket
System parameter domain name is corrupted and has NULL value
atifIndexGet
atifIndexGet
atRetrieve
atRetrieve:Wrong Index
atRetrieve:1 Absent
atRetrieve:NOSUCHNETADDR
atRetrieve:reqdarplink
getatnetaddr
Returning from atNext
atPhysAddressGet
atNetAddressGet
atGet:namelen
ifLookUp:item <=0
ifLookUp:item
ifLookUp:reqLink
ifIndexGet
entry addr
ifDescrGet
ifMtuGet
ifType
ifSpeedGet
ifPhysAddressGet
ifAdminStatusGet
ifAdminStatusGet
ifLastChangeGet
ifInOctetsGet
ifInUcastPktsGet
ifInUcastPktsGet
ifInDiscardsGet
ifInErrorsGet
ifInUnknownProtos
ifOutOctetsGet
ifOutUcastPktsGet
ifOutUcastPktsGet
ifOutDiscardsGet
ifOutErrorsGet
ifOutQLenGet
ifSpecificGet
ifRetrieve:item

ifTblGet
ifTblNext
Returning from 0 to ifTblNext
ifRetrieve:item
ifRetrieve:entry == 0
ifGet:namelen
Returning from 0 of ifNext
Returning from !=0 of ifNext
ifnet
ipForwardNumber
ipAddrNext:Decode Name failed
mixNext: AUTHCHKFAIL
mixGet: AUTHCHKFAIL
mixSet: AUTHCHKFAIL
snnaOpVerify
snmpd: unable to create socket
systmDescrGet
systmContactGet:
systmNameSet:
systmNameGet
systmLocationGet:
systmgetexec:cookie
systmGet:cookie
systmNext:cookie
systmContactGet:
systmLocationGet:
sntrap: unable to create socket
smpRequest failed
smpRequest Wok:Trap #
trapSend:dest
Starting time is same as ending time
Not permitted on sync port
Check for resources – system error
Invalid IP address
Invalid authentication type

6

TROUBLESHOOTING THE REMOTE ACCESS SERVER

This chapter describes how the administrator of the remote access server will troubleshoot at the installation and help provide information to the support personnel for remote problem analysis and resolution.

System Panic Messages

The error messages displayed by the remote access server are self-explanatory and the corrective action is often implicit. Wherever a specific action is required for resolution, the message specifies the same. Wherever the message implies a fatal situation the administrator is expected to report the problem to the support team explaining the exact error symptom, message and environment. A checklist indicating what information should be provided for problem reporting is provided in Appendix-E.

In case of error messages which are totally fatal and non-recoverable, the remote access server panics displaying the message on console. The administrator is expected to note the messages down and report the same to the support later on. To enable the administrator view the message subsequently, the messages are saved in the Non-Volatile RAM before the remote access server goes down.

Subsequently, when the remote access server is rebooted after the panic, the message

```
"There is a previous panic saved. Do you wish to see it?".
```

appears on the console. The default answer for this query is **yes**. The administrator may view the panic message once again to report the problem.

Subsequently, the message,

```
"Clear the previous panic ?"
```

appears on the console. The default answer for this query is **no**. The administrator may clear the saved message or may choose to retain the same so that it can be shown to the support team.

Only if the administrator explicitly answers with **yes** to the above query, the panic message will be cleared from the Non-Volatile Memory. Otherwise, it will exist across reboots, until another panic message gets overwritten.

The exact and complete reporting of error message including the values displayed in the message to the support team, will enable better and faster problem resolution.

The following is a list of panic messages displayed by the remote access server.

Exception : SWI at address 0x*hexanumber*
Exception : Undefined Instruction at address 0x*hexanumber*
Exception : Prefetch Abort at address 0x*hexanumber*

Exception : Data LOAD/Store Abort at address 0x*hexanumber*

Fixed Pty Messages

The remote access server provides a daemom *fptyd* which runs on the host system to provide services for fixed ports. This section describes the messages displayed by the daemon and the procedure to troubleshoot the problems associated with these messages.

The problems that may occur during the installation and setup of the fixed port daemon fptyd and the reason and remedial actions that need to be taken by the administrator are explained.

Note

While reporting problems with the fptyd server please indicate the version number of the fptyd server which is available in the host system' s log file. Refer to appropriate host manual for details on log file.

Error Message "fptyd: System configuration error"
Reason The maximum fixed ports limit has been exceeded. Refer to the appropriate host manual for the parameters to be configured. For example, in HP systems running HP-UX the *maxfiles* tunable parameter has to be increased. Refer to the HP-UX *System Administrator Task Manual for configuring maxfiles*.

Error Message "accept failed - *explanatory message*"
Reason A system error has occurred. After noting down the contents *of syslog*, contact Support team.

Error Message "Could not open socket - *explanatory message*"
Reason The fptyd server was unable to open a SOCK-STREAM socket for TCP. Check the host system to see whether sockets and ARPA services are properly installed.

Error Message "Couldnot bind socket - *explanatory message*"
OR
"Couldnot get required port *port port*"
Reason The tcp port number used by the fptyd (8065) is already being used by some other service or fptyd is being started a second time. Check */etc/services.*

Error Message "Select failed - *explanatory message*"
Reason The maximum fixed ports limit has been exceeded. Refer to the appropriate host manual for the parameters to be configured. For example, in HP systems running HP-UX the *maxfiles* tunable parameter has to be increased.

Refer to the HP-UX System *Administrator Task Manual for configuring maxfiles.*

Error Message "Cannot open config file filename - *explanatory message*"

Reason The configuration file (normally */etc/fptyd.conf*) cannot be accessed. Check if the file is present. Verify that the fptyd daemon is running as root.

Error Message "cannot understand a *line*"

Reason One of the lines (indicated in the message) in the configuration file (normally */etc/fptyd.conf*) cannot be understood. Please verify that the file contents match the format described in the ***LANReach*** *Remote access server Installation and Administration Guide.*

Error Message "could not locate name *tsname*"

Reason The name of the remote access server cannot be understood. It should either be an internet address, or the name (as specified in */etc/hosts*) of the remote access server. Please verify that the configuration file contents match the format described in the ***LANReach*** *Remote access server Installation and Administration Guide.*

Error Message "port number port out of range"

Reason The port number (at the remote access server) is out of range. It should be between 0 - 15 for the serial ports, and 16 for the parallel port.

Error Message "inconsistent line a line. This port already configure to tsname : port"

Reason The indicated line in */etc/fptyd.conf* is inconsistent. The indicated port on the remote access server is already marked as fixed.

Error Message "fixed pty table full"

Reason More than 510 fixed ptys have been configured. This server cannot handle more than 510 fixed ptys. Reduce the number of fixed ptys.

Error Message "ptyname too long ptyname"

Reason The ptyname (as specified in */etc/fptyd.conf*) is too long. The limit is 63 characters. Use a shorter name.

Error Message "pty ptyname already configured to *RAS:portno*"

Reason The ptyname is configured to more than one remote access server port. At any given time, one pty can be fixed to only one remote access server port. Correct the database, */etc/fptyd.conf.*

Error Message "could not stat ptyname"

Reason The ptyname configured cannot be accessed. Check if the device entry exists, and is a valid pty device. The number of pseudo ttys configured in the host may not be sufficient. Refer to appropriate host manual for the parameter and procedure to configure. For example, on HP systems running HP-UX, you may need to configure the "npty" tunable parameter in */etc/master*. Refer to the HP-UX *System Administrator Task Manual*.

Error Message "*ptyname* is not a character special device"

Reason The ptyname configured is invalid. Only pty devices should be specified here.

Error Message "*ptyname* invalid pty name"

Reason The ptyname configured is invalid. The server is not able to access the corresponding master device.

Error Message "could not open *ptymaster : error msg*"

Reason The master pty device could not be opened.

a) "Permission denied" - The master device file does not have read/write permission.

b) "No such file or directory" - The master device file name does not exist.

c) "No such device" - The specified device is not configured in the kernel. Configure the kernel parameter. For name of the parameter and the procedure to configure, refer to the appropriate host manual. For example, the *npty* tunable parameter should be configured and the device special files created in HP systems running HP-UX. Refer to the HP-UX *System Administrator Task Manual* for configuring the *npty* parameter.

d) "Too many open files" - The maximum fixed ports limit has been exceeded. Configure the appropriate kernel parameter. Refer to appropriate host manual for the parameter to be configured and procedure. For instance, the *maxfiles* tunable parameter has to be increased for HP systems running HP-UX. Refer to the HP-UX *System Administrator Task Manual* for configuring *maxfiles.*

e) "File table overflow" - The System file table is full.

Increase the file table size in the kernel by configuring the corresponding kernel parameter. Refer to appropriate host manual for details. For example, the *nfile* tunable parameter has to be increased for HP systems running HP-UX. Refer to the HP-UX *System Administrator Task Manual* configuring *nfile*.

Error Message "hostname hostname (*primary hostname*) has multiple address. Recognising only *internet address*"

Reason The remote access server name specified has multiple internet addresses. The server cannot decide which of the internet addresses to use - it is defaulting to the first address. If any other address is desired, please specify the internet address, instead of the ambiguous remote access server name in the configuration file.

7

WEB MANAGEMENT OF REMOTE ACCESS SERVER

Graphical browser, such as Internet Explorer and Netscape Navigator can be used to administer LANReach on the Web.

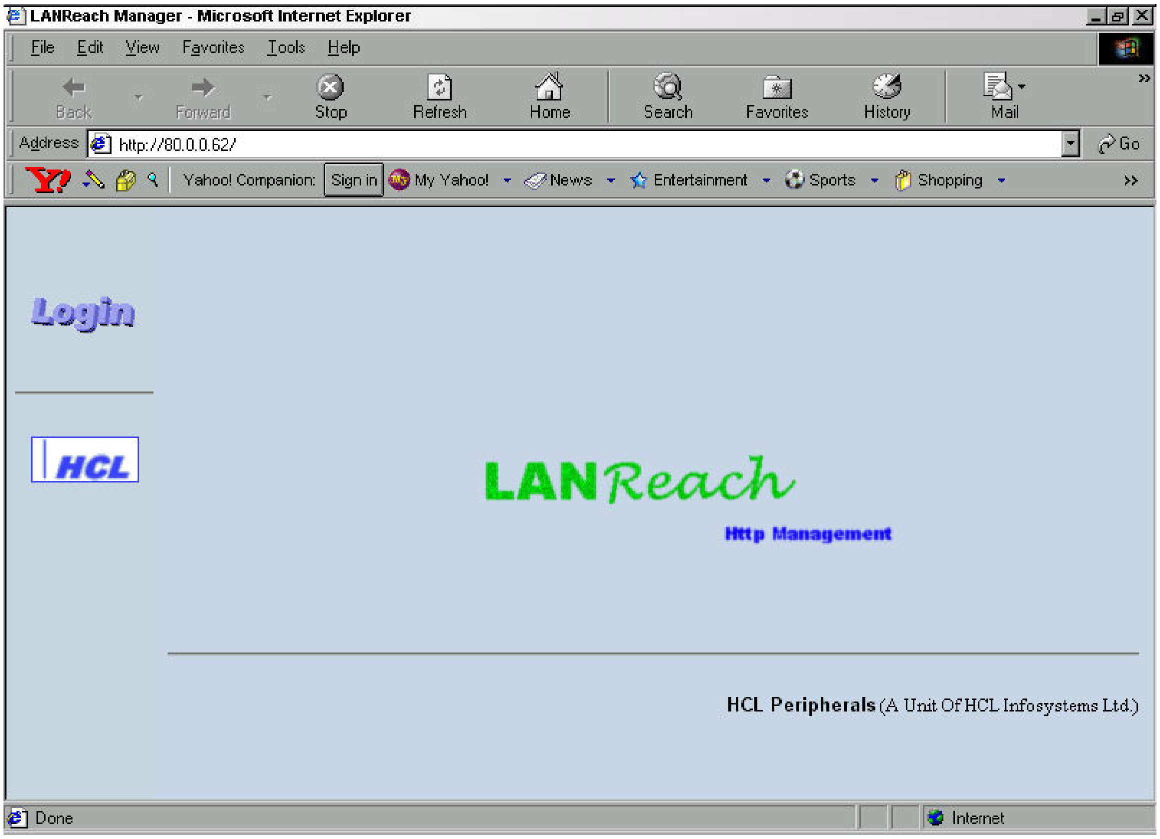

LANReach Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail
Address http://80.0.0.62/
Go
Yahoo! Companion: Sign in My Yahoo! News Entertainment Sports Shopping
Login
HCL
LANReach
Http Management
HCL Peripherals (A Unit Of HCL Infosystems Ltd.)
Done
Internet

Fig.7.1 LANReach Web interface startup page

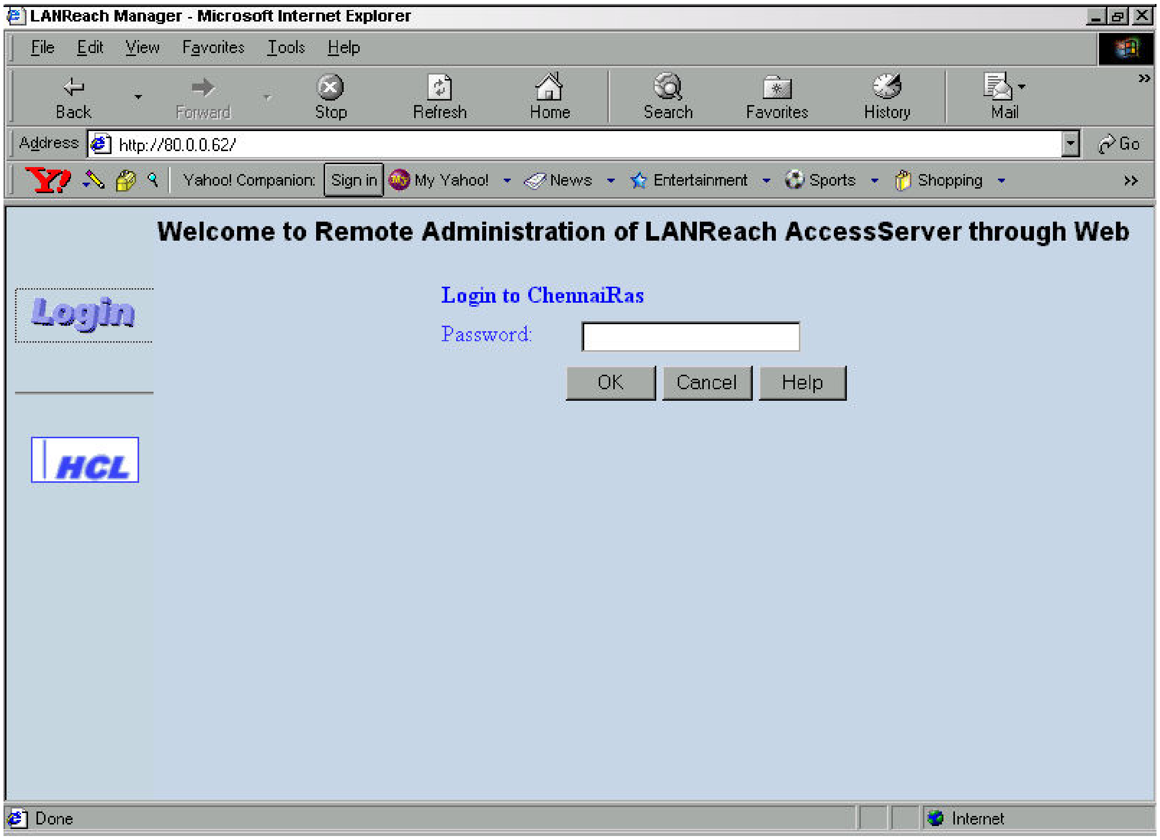
If DNS entry is made available for the LANReach on the DNS, this name or the address of the LANReach can be specified either in the address section of the toolbar or in the open edit box of the open dialog box if either Internet Explorer or Netscape Navigator is being used. Otherwise, the URL of the LANReach can also be specified either in the address section of the toolbar or in the open edit box of the open dialog box. Suppose **lanreach.hclp.com** is the DNS entry and **200.200.1.1** is the IP address for the LANReach, then the URL format will be either

http://lanreach.hclp.com/

or

http://200.200.1.1/

When this URL is opened, LANReach startup document is displayed. Administrator can click on the Login image. It opens Login document that containing following login form.



http://80.0.0.62/

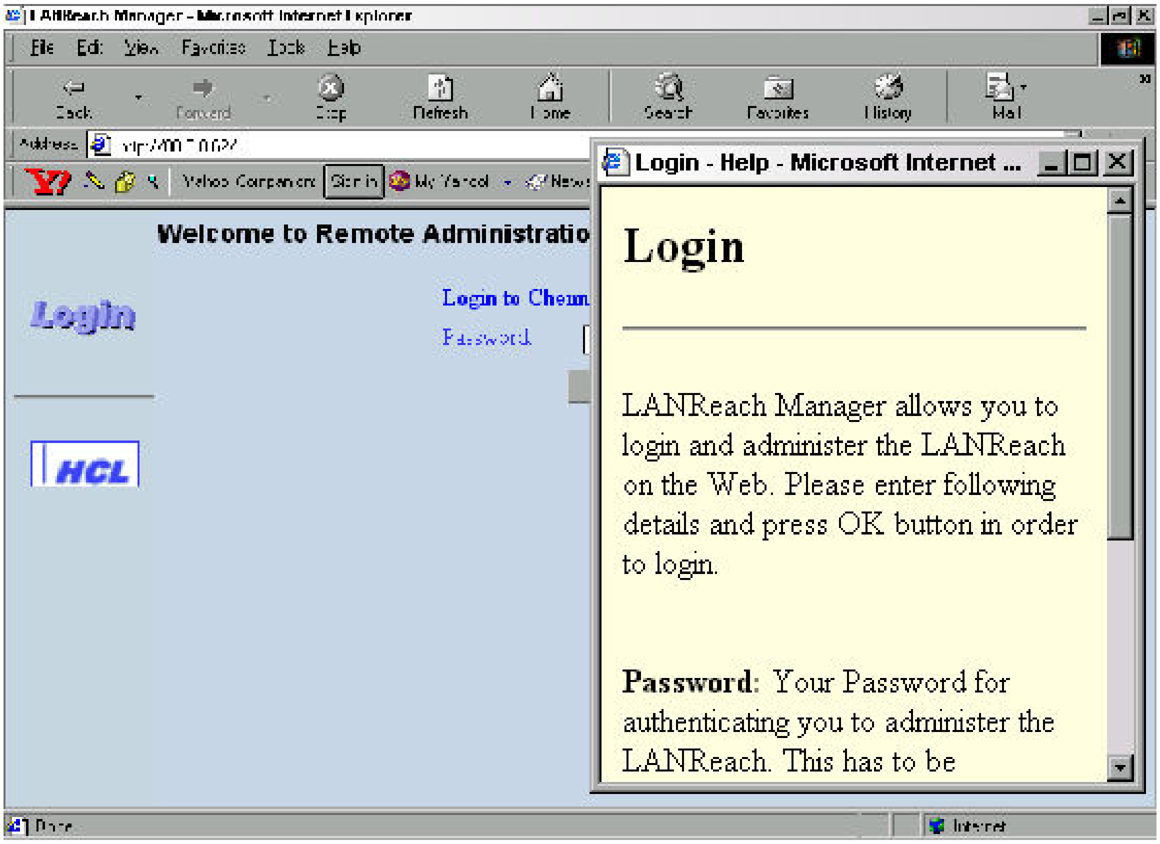
Welcome to Remote Administration of LANReach AccessServer through Web

Login to ChennaiRas

Password:

Fig.7.2 Login to LANReach on the Web using Internet Explorer

Here administrator can enter the Password to administer LANReach. The administrator also can get on-line help by clicking on the **Help** button whenever required.


LANReach Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail
Address
Yahoo Companion Sign In My Yahoo! News
Login
HCL
Done
Internet
Login - Help - Microsoft Internet ...

Welcome to Remote Administratio

Login to Chenn

Password

Login

LANReach Manager allows you to login and administer the LANReach on the Web. Please enter following details and press OK button in order to login.

Password: Your Password for authenticating you to administer the LANReach. This has to be

Fig.7.3 On-line Help for Login

Once login is successful, the administrator will be taken into **admin** mode screen. From here, the administrator can configure LANReach ports, PPP , SNMP and system parameters. The current mode **admin** will be displayed on the left side of the window.

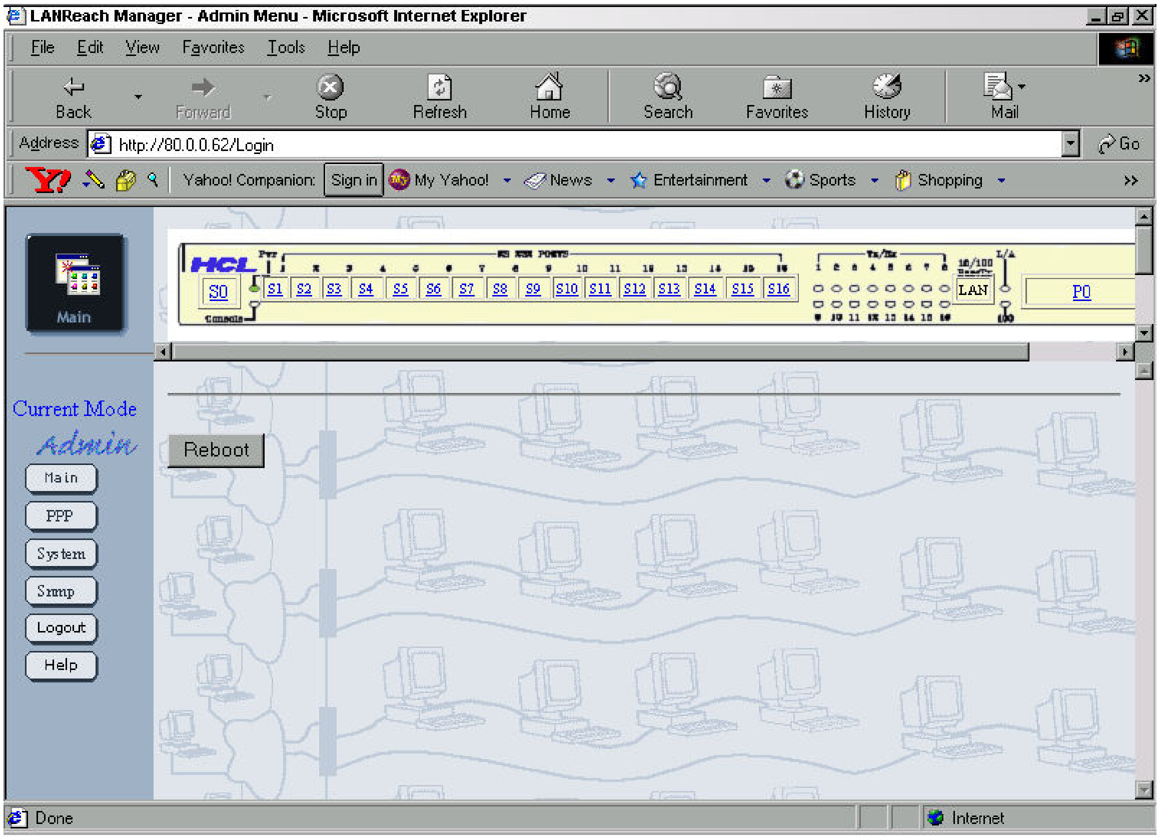
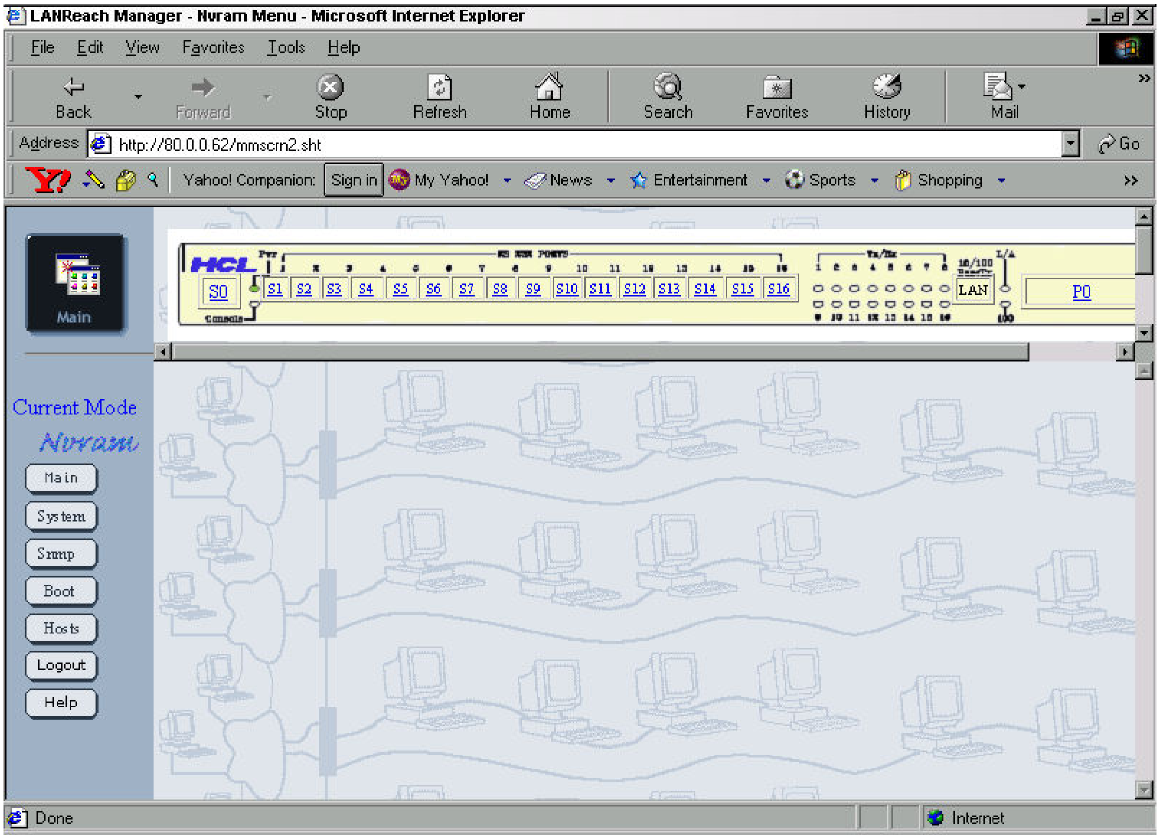

LANReach Manager - Admin Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail
Address http://80.0.0.62/Login
Go
Yahoo! Companion: Sign in My Yahoo! News Entertainment Sports Shopping
HCL
S0 S1 S2 S3 S4 S5 S6 S7 S8 S9 S10 S11 S12 S13 S14 S15 S16
LAN
P0
Main
Current Mode
Admin
Main
PPP
System
Snmp
Logout
Help
Reboot
Done
Internet

Fig.7.4 Admin menu

The current mode of working will be displayed on bottom of title *current Mode* in the admin window. The administrator can switch into **nvram** mode by pressing **admin** on the admin window.



LANReach Manager - Nvram Menu - Microsoft Internet Explorer

Address http://80.0.0.62/mmscrn2.sht

Current Mode
Nvram

Fig.7.5 Nvram menu

The administrator can logout by clicking on the **Logout** button if no longer wants to configure the LANReach.

A

CABLE CONNECTION DETAILS

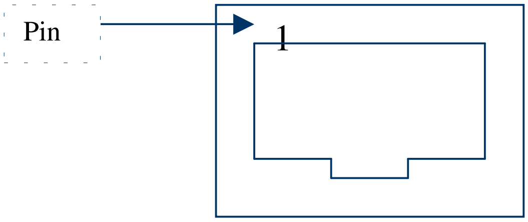
This appendix gives the serial and parallel port cable connection details for connecting the terminal and modem to the serial port of the remote access server and pinouts for connecting the parallel printer to the parallel port.

The connections are indicated using the standard RS232-C signals. For easy reference the RJ-45 serial port Jack' s pin out detals are given below:

Table A.1 : **Serial Port**

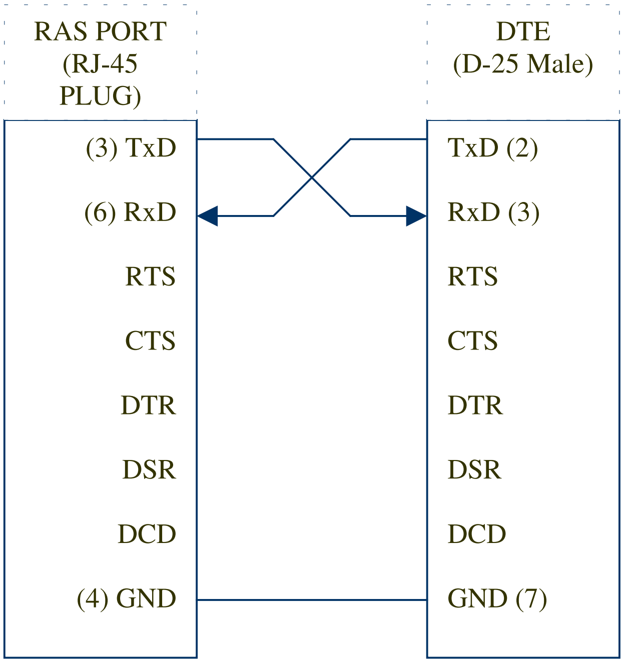
Pin No.	Signal	Description
1.	RTS	Request To Send
2.	DTR	Data Terminal Ready
3.	TX	Transmit
4.	GND	Ground
5.	CTS	Clear To Send
6.	RX	Receive
7.	DCD	Data Carrier Detect
8.	DSR	Data Set Ready

The front view of RJ-45 Jack is given in the following figure



Serial Port to Terminal Cable Connection - 3 Wire

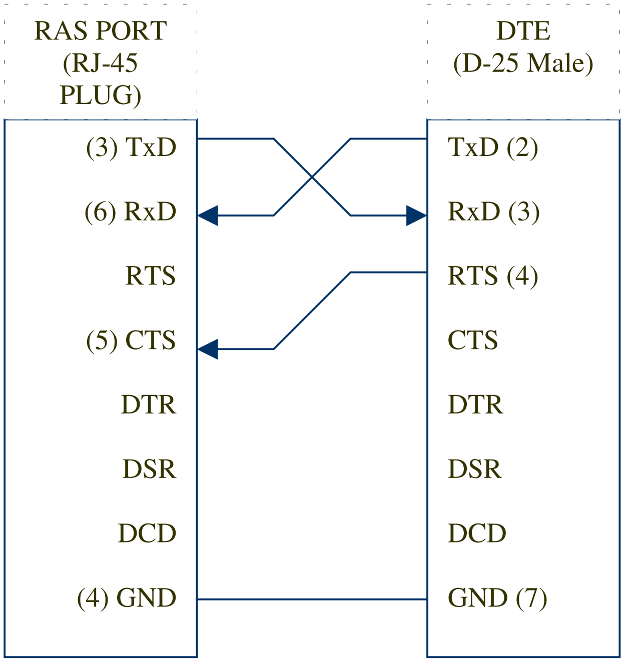
The simplest way of connecting a DTE (Data Terminal Equipment) to ***LANReach*** is by means of a 3 wire cable. The connection details of 3 wire cable are shown below:



For connecting DTEs, which do not support software flow control use either 4 wire or 8-wire connection whose details are described in the following pages.

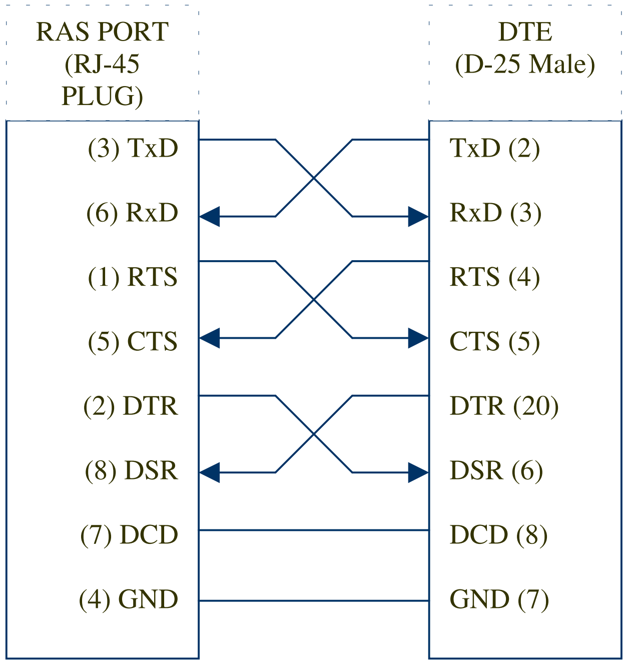
Serial Port to Terminal Cable Connection - 4 Wire

A 4 wire cable with connections as shown below, should be used with DTEs which support RTS flow control only. (i.e., the DTE deasserts its RTS when its input buffer is filled). When using this 4 wire cable the output hardware flow control for the associated port in ***LANReach*** should be set to CTS (set outhwflow = cts).



Serial Port to Terminal Cable Connection - 8 Wire

To support full hardware flow control, use 8 wire cable connection. The 8 wire cable connection is shown below,

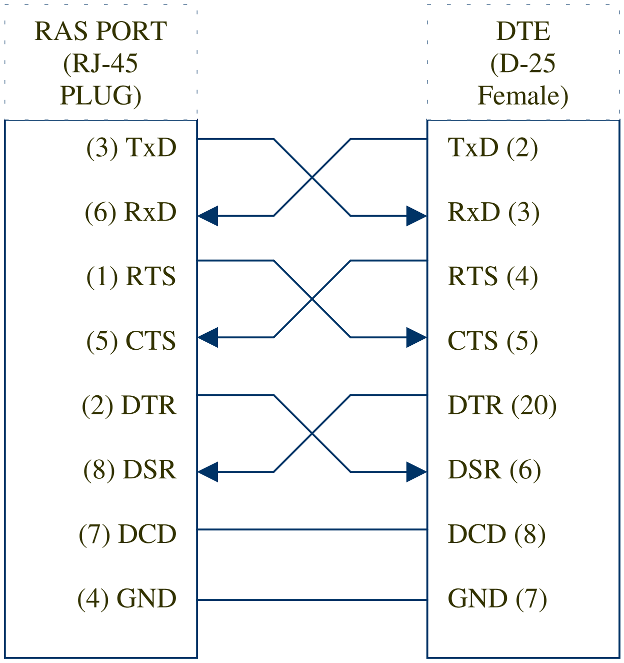


This is recommended to be used with terminals which support full hardware flow control, serial printers and plotters.

When using this option, output hardware flow control (outhwflow) and input hardware flow control (inhwflow) should be set in ***LANReach*** configuration. The value for these flow control options should be set corresponding to the type of flow control provided by DTE.

Cable for Compatibility with Exterm 1600

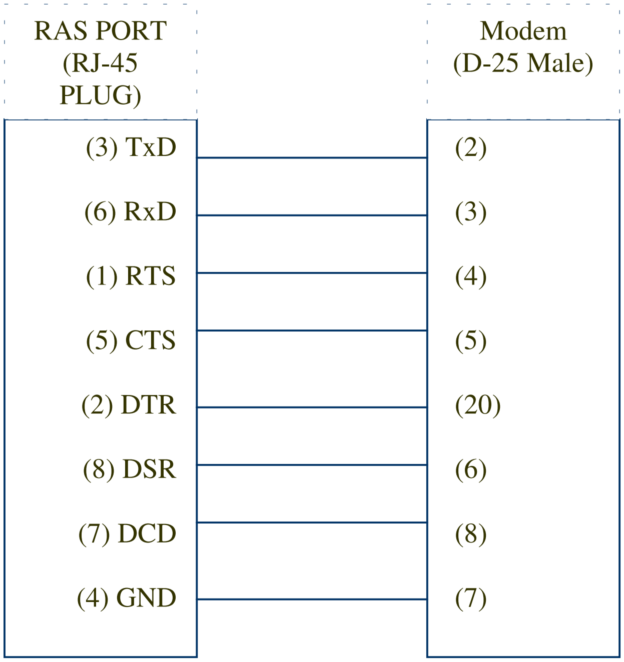
The Exterm 1600 Terminal Concentrator uses a D-25 female connector, to provide connectivity to serial devices. When Exterm 1600 TC, is being upgraded by ***LANReach***, the following cable converter should be used, to provide compatibility with the old external wiring.



Serial Port to Modem Cable Connection

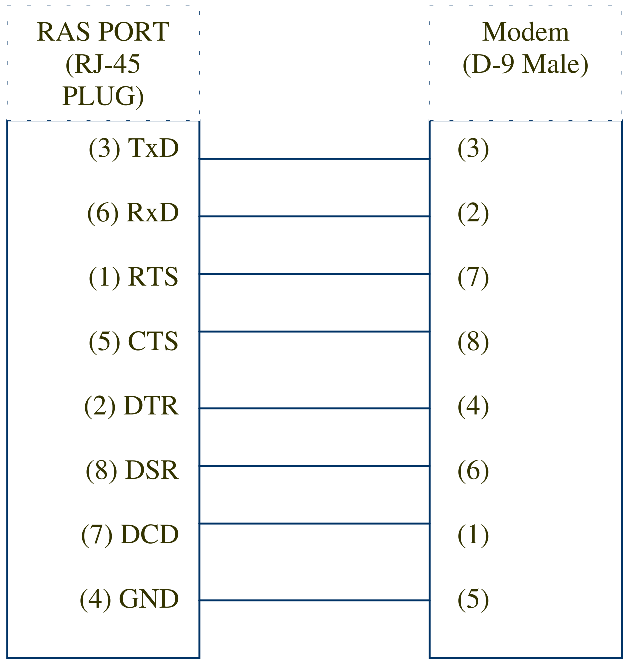
For connecting modems to ***LANReach***, the following cable connection is recommended. This cable connection will support full hardware flow control.

RJ45 Serial port to 25 Pin Modem cable



RAS PORT (RJ-45 PLUG)	Modem (D-25 Male)
(3) TxD	(2)
(6) RxD	(3)
(1) RTS	(4)
(5) CTS	(5)
(2) DTR	(20)
(8) DSR	(6)
(7) DCD	(8)
(4) GND	(7)

RJ45 Serial port to 9 Pin Modem cable



RAS PORT (RJ-45 PLUG)	Modem (D-9 Male)
(3) TxD	(3)
(6) RxD	(2)
(1) RTS	(7)
(5) CTS	(8)
(2) DTR	(4)
(8) DSR	(6)
(7) DCD	(1)
(4) GND	(5)

Parallel Printer Port Pin-outs

The pin outs of the Parallel printer Port are shown below.

D-25 Pin	Signal
1.	-STROBE
2.	Data Bit 0
3.	Data Bit 1
4.	Data Bit 2
5.	Data Bit 3
6.	Data Bit 4
7.	Data Bit 5
8.	Data Bit 6
9.	Data Bit 7
10.	-ACK
11.	BUSY
12.	PE
13.	SLCT
14.	-AUTO FEED XT
15.	-ERROR
16.	-INIT
17.	-SLCT IN
18 - 25	GND

Note

Minus (-) sign preceeding any of the signals listed above means, that the particular signal is ' active low' .

AUI Port (D-15) Pin-outs

The pin outs of the AUI Port are shown below.

D-15 Pin	Signal
2	CI A
3	DO A
4	DI Shield
5	DI A
6	GND
9	CI B
10	DO B
12	DI B
13	+12V

Twisted Pair Port Cabling

The PIN out for RJ-45 twisted pair interface connector are given below. The recommended color codes for crimping the plug to be used with the jack, are also given.

RJ-45 Pin	Signal	Color Code (base/stripe) for the plug
1	TX+	White/Orange
2	TX-	Orange/White
3	RX+	White/Green
4	NC	Blue/White
5	NC	White/Blue
6	RX-	Green/White
7	NC	White /Brown
8	NC	Brown/White

CLASSIFICATION OF REMOTE ACCESS SERVER PORTS

Port Type	Description	OS Applicable
Switched	A *Switched* type of serial port on the remote access server is not permanently associated with any specific host. From a *Switched* port, one can create standard TCP/IP based *rlogin* or *telnet* sessions to host systems supporting TCP/IP. One can even have multiple login sessions with more than one host system at the same time. A specific escape sequence (configurable by the user) will escape into the command mode at any time. In this mode, by using the *remote access server line manager commands*, one can switch from one session to another at will.	HP-UX / MAGNIX / SVR 4.x / SVR 3.2 / SCO OPEN SERVER / SCO UNIXWARE / SUN SOLARIS 4.x (SPARC) ; 5.x (SPARC, INTEL) / IBM AIX 4.x / DIGITAL UX 4.x ; 5.x / LINUX
Fixed	A *Fixed* port of remote access server is permanently associated with a specific tty device on a specified host system. The remote access server makes a permanent session between the remote access server port and the specified host tty. This tty device name can be used by UNIX processes to access the desired serial port. At the host end *getty* process can be configured to run on the *Fixed* port to give login service which is to all intents and purposes identical to a local terminal.	HP-UX / MAGNIX / SVR 4.x / SVR 3.2 / SCO OPEN SERVER / SCO UNIXWARE / SUN SOLARIS 4.x (SPARC) ; 5.x (SPARC, INTEL) / IBM AIX 4.x / DIGITAL UX 4.x ; 5.x

Port Type	Description	OS Applicable
Implicit	An *Implicit* port of a remote access server provides a permanent login session with a specific user name and a specific host. Here there is no permanent tty device name associated with.	HP-UX / MAGNIX / SVR 4.x / SVR 3.2 / SCO OPEN SERVER / SCO UNIXWARE / SUN SOLARIS 4.x (SPARC) ; 5.x (SPARC, INTEL) / IBM AIX 4.x / DIGITAL UX 4.x ; 5.x
Rtelnet	A reverse telnet port of the remote access server enables the users on host systems to share the device connected on that port.	HP-UX / MAGNIX / SVR 4.x / SVR 3.2 / SCO OPEN SERVER / SCO UNIXWARE / SUN SOLARIS 4.x (SPARC) ; 5.x (SPARC, INTEL) / IBM AIX 4.x / DIGITAL UX 4.x ; 5.x / LINUX

C

PHYSICAL AND ELECTRICAL PARAMETERS

Physical

Dimension	:	442mm (W) X 201mm (D) X 48mm (H)
Weight	:	2.65 Kg

Electrical Power

90-264 VAC, 47-63 Hz, 2 Amp (Max), 60 Watts (Max).

Environmental

Operating temperature	:	5^{o}C to 45^{o}c
Storage temperature	:	-20^{o}C to 66^{o}C
Humidity	:	10% to 90%, non condensing

HARDWARE FLOW CONTROL

The remote access server provides support for making use of hardware flow control signals with appropriate cables. By choosing a required option in the set command, the user can make use of the hardware flow control. The action taken by the remote access server for each of the hardware flow control options is given in this appendix. Note that the signal names and their nature (input or output) are mentioned with respect to the remote access server end.

Table D.1 : **Input Hardware Flow Control**

Option Used in set Command	**Action Taken By Remote access server**
None	no input hardware flow control
rts	Same as above, except that RTS output signal is used instead of DTR

Table D.2 : **Output Hardware Flow Control**

Option Used in set Command	**Action Taken By Remote access server**
None	no output hardware flow control
cts	Same as above, except that CTS input signal will be monitored for permission to transmit.

E

ERROR REPORTING

The following inputs need to be given while reporting a problem with remote access server. This is only the minimal input required. Additionally, user may provide more inputs relevant to the problem reported, in order to enable faster analysis.

Checklist of Inputs

I. Customer information

Date of report:

Name of the customer installation:

Contact person.

Address

Phone No.:

Fax No.:

II. Name of the regional office contact:

III. Installation Details:

LANReach Version No.:

Boot loader Version : B.

Download Software Version : D.

Systems in network :

No.	Node name	Node address	Configuration OS Version
1.			
2.			
3.			
...			

Customer Application :

IV. RAS Configuration file

Upload with putconfig and enclose

V. Problem Details :

Exact error messages if any :

Problem symptom :

Repeatable or not : Y/N

Activity to repeat :

Messages on host consoles, if any :

No.	Host name	Messages
1.		
2.		
...		

Any additional Information :

F

INSTALLING AND CONFIGURING REMOTE ACCESS SERVER IN VARIOUS UNIX MACHINES

This appendix gives detailed information about installation procedure and configuration setup of the Remote access server with various Unix machines listed below.

Digital Unix

IBMAIX

SCO Open

SCO Unix ware

Sun Solaris

SVR

FOR DIGITAL UNIX SERVER

The files required for LANReach configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

```
Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.DigitalUX5.0
fptyd.DigitalUX4.0
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts
```

* Extract the files using the command in a temporary directory say /temp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1. Check whether the file /etc/inetd.conf file contains an entry like one given

```
tftp dgram udp  wait root /usr/sbin/tftpd  tftpd  /tmp
```

2. If the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Change the /tmp to /tftpboot.

```
tftp dgram udp  wait root /usr/sbin/tftpd  tftpd  /tftpboot
```

Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lanreach.mem, logchar.ts, modemchar.ts, release.nte,
tsrpr.README,tsrpr.c,
user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory.
Check whether /etc directory has fptyd file. Check whether /sbin/rc3.d Contains file S86fptydaemon.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR DIGITAL UNIX

1. Login as Super User (root)

2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.

3. Do the following in /temp directory where you have extraced the files.

4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts, /tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
mkdir /tftpboot/etc/ts/lp
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts.  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
```

6. Copy the files tsprof.ser, tsprof.par into /tftpboot/etc/ts/lp directory using cp command

```
cp  tsprof.ser  /tftpboot/etc/ts/lp/tsprof.ser
cp  tsprof.par  /tftpboot/etc/ts/lp/tsprof.par
```

7. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

8. Change owner and group of lp and its subdirectory as lp using the following command

```
chgrp -R  lp  /tftpboot/etc/ts/lp
chown -R   lp  /tftpboot/etc/ts/lp
```

9. For Digital Unix 5.x Copy fptyd.DigitalUX5.0 file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.DigitalUX5.0    /etc/fptyd
```

For Digital Unix 4.x Copy fptyd.DigitalUX4.0 file into /etc directory as

/etc/fptyd using cp command

```
cp   fptyd.DigitalUX4.0    /etc/fptyd
and
chmod 555  /etc/fptyd
```

10. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp  fptyd.conf   /etc/fptyd.conf
```

11. Create a file /sbin/rc3.d/S86fptydaemon with the following content.

```
cd /sbin/rc3.d

vi S86fptydaemon
```

Add the following contents

```
#!/bin/sh
if [ -x /etc/fptyd ]
then
   echo "Starting fptyd daemon"
   /etc/fptyd
fi
```

save and exit.

```
chmod 500 /sbin/rc3.d/S86fptydaemon
```

12. Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following

```
* for login ports
log1:34:respawn:/usr/sbin/getty /dev/pts/10   console  vt100
* for serial printers
   ser1:34:off:/usr/sbin/getty /dev/pts/5   console  vt100
* for parallel printers
   par1:34:off:/usr/sbin/getty /dev/pts/15    vt100
* /etc/gettydefs file should have entry for "console" option
```

2. Entry for fptyd.conf file will be as follows

```
##device        IP Address          Port in lansterm
  /dev/pts/10   120.150.140.12          S1
  /dev/pts/5    120.150.140.12          S2
  /dev/pts/15   120.150.140.12          P0
```

Here /dev/pts/10 is pseudo tty and it should be available in system.

You have to verify this with system and then give.

This can be checked by logging into server from lansterm.

```
{
       TS>telnet DigitalUXserver(IP ADDRESS)
       $ tty
       /dev/??????
 In my case, it is /dev/pts/* type.
 }
```

3. The fptyd file should be in /etc and the daemon is in /sbin/rc3.d.
4. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

5. Reboot the server to configure the fixed ports.

For Fixed Printers for Digital UX 5.0

1. Configuring the printer Stop the Scheduler using

```
    /usr/lib/lpshut
Use lpadmin command to add printer
    /usr/lib/lpadmin -pparprn -v/dev/pts/15 -mstandard
Start the lpscheduler by running lpsched
    /usr/lib/lpsched
Make the printer interface accept requests by using accept command
    /usr/lib/accept parprn
Enable the printer using enable command
    enable parprn
```

2. Printing Printing can be done using

lp command lp -dparprn < file name with full path >

For Fixed Printers for DigitalUX 4.0

1. Add printer using lprsetup utility
2. Use the device that has been alloted for the port as the device.
3. Print using the command

```
lp -P<printer name> <file name>
```

CONFIGURING IMPLICIT LOGGING PORTS

In the lansterm side go to nvram mode and set the port as implicit with user and hosts,

for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

CONFIGURING THE REVERSE TELNET PRINTER for DigitalUX 5.0

1. First time Compilation:

This is done only once before the reverse telnet printer is to be added. Goto the /tftpboot/etc/ts directory.

```
cd  /tftpboot/etc/ts
```

There will be a file tsrpr.c. Compile the file using the following command

```
cc   -DHP_UX   -o tsrpr  tsrpr.c
```

2. Run Time Configuration:
3. In the server side open a file /etc/tsrpr.conf

```
vi /etc/tsrpr.conf
```

Add the following lines

```
< Printer name >   < Lansterm Name >    < TCP Port >
```

For eg.,

```
testprn              lansterm          2000
```

Add the IP address entry for lansterm in /etc/hosts file

```
vi  /etc/hosts
```

For the above example add a similar line

```
192.160.212.34       lansterm
```

Here 192.160.212.34 is the IP address for the lansterm.

4. In the lansterm side

Configure the port as rtelnet.

```
nvram>> set  P0  type=rtelnet  tcpport=2000 authen=off
allowsecond=no
```

Reboot The lansterm

For adding the printer.

Configuring the printer Stop the Scheduler using

```
/usr/lib/lpshut
```

Use lpadmin command to add printer

```
/usr/lib/lpadmin -ptestprn -v/dev/null -i/tftpboop/etc/ts/tsrpr
```

Start the lpscheduler by running lpsched

```
/usr/lib/lpsched
```

Make the printer interface accept requests by using accept command

```
/usr/lib/accept testprn
```

Enable the printer using enable command

```
enable testprn
```

Printing Printing can be done using

lp command lp -d testprn < file name with full path >

FOR IBM AIX4 SERVER

The files required for lansterm configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

```
Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.DigitalUX
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts
```

Extract the files using the command in a temporary directory say /temp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1. Check whether the file /etc/inetd.conf file contains an entry like one given

```
tftp dgram udp6  SRC root /usr/sbin/tftpd  tftpd -n /tftpboot
```

2. if the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lanreach.mem, logchar.ts, modemchar.ts, release.nte, tsrpr.README, tsrpr.c, user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory. Check whether /etc directory has fptyd file. Check whether /etc/inet/rc.inet file contains /etc/fptyd entry. Check whether
/usr/lib/lp/model directory contains tsmodel file.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR IBM AIX4

1. Login as Super User (root)
2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.
3. Do the following in /temp directory where you have extraced the files.

4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts, /tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
cp printconf /bin/printconf
chmod 777 printconf
```

6. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

7. Copy fptyd.sco5 file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.IBMAIX4    /etc/fptyd
and
chmod 555  /etc/fptyd
```

8. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp  fptyd.conf   /etc/fptyd.conf
```

9. Open the file /etc/rc.tcpip

```
cd /etc

vi rc.tcpip
```

Add the following content at the end

```
#!/bin/sh
if [ -x /etc/fptyd ]
then
    echo "Starting fptyd daemon"
    /etc/fptyd
fi
```

save and exit.

* Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following
 for login ports

```
log1:234:respawn:/usr/sbin/getty   -h   /dev/pts/10  console
```

 for serial printers and parallel printers

```
ser1:2:off:/etc/getty   -h   /dev/pts/5   9600
par2:2:off:/etc/getty   -h   /dev/pts/15
```

2. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

3. Reboot the server to configure the fixed ports.

FOR FIXED PRINTERS & PORTS

1. Run printconf using the command

```
printconf
```

for adding Printer or a fixed login port type ' 1' and enter

Now give the device name (eg., /dev/pts/4), IP address of the lansterm, Port Number of Lansterm and If it is a printer give the printer name. This will create a link in the name of the printer in the /dev directory.

restart the printer services.

for removing a Printer or a fixed port type ' 2' and enter

Now give the device name and it will remove the printer.

for viewing you can use ' 3' and '4' options.

Option 3 shows all the fixed devices and Option 4 shows only the Printer devices.

2. Run smit in the command and add a queue with the characteristics of "printing to device" with the device as the printer name.
3. Do not manually edit /etc/fptyd.conf file if you are using printconf utility.

CONFIGURING IMPLICIT LOGGING PORTS

In the lansterm side go to nvram mode and set the port as implicit with user and hosts,

for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

FOR SCO 5 SERVER

The files required for lansterm configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

```
Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.DigitalUX
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts
```

Extract the files using the command in a temporary directory say /temp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1. Check whether the file /etc/inetd.conf file contains an entry like one given

```
tftp dgram udp  wait root /etc/tftpd  tftpd -s /tftpboot
```

2. if the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lansterm.mem, logchar.ts, modemchar.ts, release.nte, tsrpr.README, tsrpr.c, user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory. Check whether /etc directory has fptyd file. Check whether /etc/inet/rc.inet file contains /etc/fptyd entry. Check whether /usr/lib/lp/model directory contains tsmodel file.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR SCO 5

1. Login as Super User (root)
2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.
3. Do the following in /temp directory where you have extraced the files.
4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts, /tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
mkdir /tftpboot/etc/ts/lp
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts.  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
```

6. Copy the files tsprof.ser, tsprof.par into /tftpboot/etc/ts/lp directory using cp command

```
cp  tsprof.ser  /tftpboot/etc/ts/lp/tsprof.ser
cp  tsprof.par  /tftpboot/etc/ts/lp/tsprof.par
```

7. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

8. Change owner and group of lp and its subdirectory as lp using the following command

```
chgrp -R  lp  /tftpboot/etc/ts/lp
chown -R   lp  /tftpboot/etc/ts/lp
```

9. Copy fptyd.sco5 file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.sco5    /etc/fptyd
and
chmod 555  /etc/fptyd
```

10. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp  fptyd.conf   /etc/fptyd.conf
```

11. Create a file /etc/rc2.d/S86fptydaemon with the following content.

```
cd /etc/rc2.d

vi S86fptydaemon

#!/bin/sh
if [ -x /etc/fptyd ]
then
   echo "Starting fptyd daemon"
```

```
        /etc/fptyd
      fi
    save and exit.
        chmod 500 /etc/rc2.d/S86fptydaemon
```

12. Copy tsmodel file into /usr/spool/lp/model directory using cp command

```
        cp  tsmodel   /usr/spool/lp/model/tsmodel
```

13. Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following

   for login ports

```
        log1:234:respawn:/etc/getty   -h   /dev/ttyp10  console
```

   for serial printers and parallel printers

```
      ser1:2:off:/etc/getty   -h   /dev/ttyp5  vt100
      par1:2:off:/etc/getty   -h   /dev/ttyp15  vt100
```

2. Entry for fptyd.conf file will be as follows

```
         ##device          IP Address          Port in lansterm
        /dev/ttyp10          80.0.0.15             S1
        /dev/ttyp5           80.0.0.15             S2
        /dev/ttyp15          80.0.0.15             P0
```

3. Here /dev/ttyp10 is pseudo tty and it should be available in system.

   You have to verify this with system and then give.

   This can be checked by logging into server from lansterm.

```
    {
          TS>telnet scoserver(IP ADDRESS)
          $ tty
          /dev/??????
     In my case, it is /dev/ttyp* type.
     }
```

4. In the ttytype add entry for the pts the terminal name as given below

```
      vt100    ttyp10
      vt100    ttyp5
      vt100    ttyp15
```

5. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

6. Reboot the server to configure the fixed ports.

FOR FIXED PRINTERS

1. Configuring the printer Stop the Scheduler using

```
        /usr/lib/lpshut
Use lpadmin command to add printer
        /usr/lib/lpadmin -pparprn -v/dev/ttyp15 -mstandard
Start the lpscheduler by running lpsched
        /usr/lib/lpsched
Make the printer interface accept requests by using accept command
        /usr/lib/accept parprn
Enable the printer using enable command
        enable parprn
```

2. Printing Printing can be done using

lp command lp -dparprn < file name with full path >

CONFIGURING IMPLICIT PRINTERS

1. Go to the nvram mode and configure the printer port as implicit and hosts = hostname or IP Address with user name as the printer name like as below

```
set P0 type=implicit hosts=80.0.0.1 user=parprn
```

and reboot the remote access server.

2. In server side login as root in the console and run scoadm in the console of ScoOS server, select user, add, save and add new user as below

```
login name = parprn ( same as the user name)
comment = implicit parallel printer
shell = /tftpboot/etc/ts/lp/tsprof.par
home dir = /home/parprn
save and give NO PASSWORD for the user and exit
```

3. Run userls in console and note down the uid and gid for lp entry, for Sco Os it will normally be 71 and 18.

4. Open /etc/passwd file and you will find an entry in the name of the printer as below

```
parprn:x:130:1:implicit parallel printer:/home/parprn:/tftpboot/etc/ts/lp/tsprof.par
```

change the first number entry 130 to 71 and change the second number entry to 18

5. Configuring the printer Stop the Scheduler using

```
            /usr/lib/lpshut
   Use lpadmin command to add printer
            /usr/lib/lpadmin -pparprn -v/dev/null -mtsmodel
   Start the lpscheduler by running lpsched
            /usr/lib/lpsched
   Make the printer interface accept requests by using accept command
            /usr/lib/accept parprn
   Enable the printer using enable command
            enable parprn
```

6. Printing Printing can be done using

```
lp command lp -dparprn < file name with full path >
```

<u>CONFIGURING IMPLICIT LOGGING PORTS</u>

In the lansterm side go to nvram mode and set the port as implicit with user and hosts,

for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

FOR SCO Unixware SERVER

The files required for lansterm configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

```
Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.DigitalUX
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts
```

Extract the files using the command in a temporary directory say /temp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1 Check whether the file /etc/inetd.conf file contains an entry like one given

```
    tftp dgram udp  wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

2. if the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lanreach.mem, logchar.ts, modemchar.ts, release.nte, tsrpr.README, tsrpr.c, user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory. Check whether /etc directory has fptyd file. Check whether /etc/inet/rc.inet file contains /etc/fptyd entry. Check whether /usr/lib/lp/model directory contains tsmodel file.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR SCOUnixware

1. Login as Super User (root)
2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.
3. Do the following in /temp directory where you have extraced the files.
4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts, /tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
mkdir /tftpboot/etc/ts/lp
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts.  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
```

6. Copy the files tsprof.ser, tsprof.par into /tftpboot/etc/ts/lp directory using cp command

```
cp  tsprof.ser  /tftpboot/etc/ts/lp/tsprof.ser
cp  tsprof.par  /tftpboot/etc/ts/lp/tsprof.par
```

7. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

8. Change owner and group of lp and its subdirectory as lp using the following command

```
chgrp -R  lp  /tftpboot/etc/ts/lp
chown -R   lp  /tftpboot/etc/ts/lp
```

9. Copy fptyd.SCO.Unixware file into /etc directory as /etc/fptyd using cp command

```
cp fptyd.SCO.Unixware /etc/fptyd
and
chmod 555  /etc/fptyd
```

10. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp fptyd.conf   /etc/fptyd.conf
```

11. Open the file /inet/rc.inet using vi command

```
vi  /etc/rc2.d/S90fptydaemon
```

add the following content

```
#!/bin/sh
if   [   -x   /etc/fptyd   ]
then
echo    "starting  fptyd  daemon  "
/etc/fptyd
fi
```

12. Save and exit

13. Copy tsmodel, tsfixed1, tsfixed2 files into /usr/spool/lp/model directory using cp command

```
cp  tsmodel   /usr/spool/lp/model/tsmodel
cp  tsfixed1   /usr/spool/lp/model/tsfixed1
cp  tsfixed2   /usr/spool/lp/model/tsfixed2
```

14. Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following

 * for login ports

```
log1:234:respawn:/usr/lib/saf/ttymon -g -h -p "TS LOGIN :" -d /dev/pts010
                                                                    -l 9600
```

* for serial printers

```
        ser1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts005 -l 9600
```

* for parallel printers

```
        par1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts015
```

* /etc/ttydefs file should have entry for "-l" option ie., 9600 as in above example.

2. Entry for fptyd.conf file will be as follows

```
  ##device        IP Address         Port in lansterm
/dev/pts010     120.150.140.12          S1
/dev/pts005     120.150.140.12          S2
/dev/pts015     120.150.140.12          P0
```

3. Here /dev/pts010 is pseudo tty and it should be available in system.

   You have to verify this with system and then give.

   This can be checked by logging into server from lansterm.

```
{
      TS>telnet SCO Unixware server(IP ADDRESS)
      $ tty
      /dev/??????
 In my case, it is /dev/pts* type.
 }
```

4. The fptyd file should be in /etc and the daemon is in /etc/rc3.d.

5. In the /etc/ttytype file add entry for the pts the terminal name as given below

```
vt100  pts010
vt100  pts005
vt100  pts015
```

6. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

7. Reboot the server to configure the fixed ports.

For Fixed Printers

1. Configuring the printer Stop the Scheduler using

```
/usr/lib/lpshut
```

Use lpadmin command to add printer

```
/usr/lib/lpadmin -pparprn -v/dev/pts/15 -mtsfixed1 (for parallel printer)
/usr/lib/lpadmin -pparprn -v/dev/pts/5 -mtsfixed1 (for serial printer)
```

Start the lpscheduler by running lpsched

```
/usr/lib/lpsched
```

Make the printer interface accept requests by using accept command

```
/usr/lib/accept parprn
```

Enable the printer using enable command

```
enable parprn
```

2. Printing Printing can be done using

lp command lp -dparprn < file name with full path >

CONFIGURING IMPLICIT PRINTERS

1. Go to the nvram mode and configure the printer port as implicit and hosts = hostname or IP Address with user name as the printer name like as below

```
set P0 type=implicit hosts=80.0.0.1 user=parprn
```

and reboot the remote access server.

2. In server side login as root in the console and run scoadmin in the console of SCO Unixware server, select Account manager and add new user as below

   login name = parprn (same as the user name)
   comment = implicit parallel printer
   shell = /tftpboot/etc/ts/lp/tsprof.par
   home dir = /home/parprn
   save and give NO PASSWORD for the user and exit

3. Run logins in console and note down the uid and gid for lp entry, for SCO Unixware it will normally be 7 and 9.

4. Open /etc/passwd file and you will find an entry in the name of the printer as below

```
parprn:x:130:1:implicit parallel printer:/home/parprn:/tftpboot/etc/ts/lp/tsprof.par
```

change the first number entry 130 to 7 and change the second number entry to 9

5. Configuring the printer Stop the Scheduler using

```
/usr/lib/lpshut
```

Use lpadmin command to add printer

```
/usr/lib/lpadmin -pparprn -v/dev/null -mtsmodel
```

Start the lpscheduler by running lpsched

```
/usr/lib/lpsched
```

Make the printer interface accept requests by using accept command

```
/usr/lib/accept parprn
```

Enable the printer using enable command

```
enable parprn
```

6. Printing Printing can be done using

```
lp command lp -dparprn < file name with full path >
```

CONFIGURING IMPLICIT LOGGING PORTS

In the lansterm side go to nvram mode and set the port as implicit with user and hosts,

for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

FOR SUN SOLARIS 5.6 SERVER

The files required for lansterm configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

```
Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts
```

Extract the files using the command in a temporary directory say /tmp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1. Check whether the file /etc/inetd.conf file contains an entry like one given

```
tftp dgram udp  wait root /etc/tftpd  tftpd -s /tftpboot
```

2. if the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lanreach.mem, logchar.ts, modemchar.ts, release.nte, tsrpr.README, tsrpr.c, user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory. Check whether /etc directory has fptyd file. Check whether /etc/inet/rc.inet file contains /etc/fptyd entry. Check whether /usr/lib/lp/model directory contains tsmodel file.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR SVR4.2

1. Login as Super User (root)
2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.
3. Do the following in /temp directory where you have extraced the files.

4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts, /tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
mkdir /tftpboot/etc/ts/lp
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts.  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
```

6. Copy the files tsprof.ser, tsprof.par into /tftpboot/etc/ts/lp directory using cp command

```
cp  tsprof.ser  /tftpboot/etc/ts/lp/tsprof.ser
cp  tsprof.par  /tftpboot/etc/ts/lp/tsprof.par
```

7. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

8. Change owner and group of lp and its subdirectory as lp using the following command

```
chgrp -R  lp  /tftpboot/etc/ts/lp
chown -R   lp  /tftpboot/etc/ts/lp
```

9. For Sun Solaris 5.6 in Intel Platform Copy fptyd.SunOS5 file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.SunOS5   /etc/fptyd
```

10. For Sun Solaris 5.6 in sparc Platform Copy fptyd.SunOS.5.sparc file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.SunOS.5.sparc   /etc/fptyd
```

11. For Sun Solaris 4.x in sparc Platform Copy fptyd.SunOS.4.sparc file into /etc directory as /etc/fptyd using cp command

```
cp   fptyd.SunOS.4.sparc   /etc/fptyd
and
chmod 555  /etc/fptyd
```

12. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp  fptyd.conf   /etc/fptyd.conf
```

13. Create a file /etc/rc2.d/S90fptydaemon with the following content.

```
cd /etc/rc2.d

vi S90fptydaemon

#!/bin/sh
if [ -x /etc/fptyd ]
then
    echo "Starting fptyd daemon"
    /etc/fptyd
fi
```

save and exit.

```
chmod 500 /etc/rc2.d/S90fptydaemon
```

14. Copy tsmodel,tsfixed1,tsfixed2 file into /usr/spool/lp/model directory using cp command

```
cp  tsmodel   /usr/spool/lp/model/tsmodel
cp  tsfixed1   /usr/spool/lp/model/tsfixed1
cp  tsfixed2   /usr/spool/lp/model/tsfixed2
```

15. Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following

* for login ports

```
log1:234:respawn:/usr/lib/saf/ttymon -g -h -p "TS LOGIN :" -d /dev/pts/10
                                                   -l 9600  -T vt100
```

* for serial printers

```
   ser1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts/5   -l 9600   -T vt100
```

* for parallel printers

```
   par1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts/15    -T vt100
```

* /etc/ttydefs file should have entry for "-l" option ie., 9600 as in above example.

2. Entry for fptyd.conf file will be as follows

```
##device         IP Address          Port in lansterm
```

```
    /dev/pts/10     120.150.140.12          S1
    /dev/pts/5      120.150.140.12          S2
    /dev/pts/15     120.150.140.12          P0
```

3. Here /dev/pts/10 is pseudo tty and it should be available in system.

You have to verify this with system and then give.

This can be checked by logging into server from lansterm.

```
{
      TS>telnet Sunserver(IP ADDRESS)
      $ tty
      /dev/??????
 In my case, it is /dev/pts/* type.
 }
```

4. The fptyd file should be in /etc and the daemon is in /etc/inet/rc.inet.

5. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

6. Reboot the server to configure the fixed ports.

<u>For Fixed Printers</u>

1. Configuring the printer Stop the Scheduler using

```
/usr/lib/lpshut
```

Use lpadmin command to add printer

```
/usr/lib/lpadmin -pparprn -v/dev/pts/15 -mstandard
```

Start the lpscheduler by running lpsched

```
/usr/lib/lpsched
```

Make the printer interface accept requests by using accept command

```
/usr/lib/accept parprn
```

Enable the printer using enable command

```
enable parprn
```

2. Printing Printing can be done using

lp command lp -dparprn < file name with full path >

CONFIGURATION FOR CONNECTING IMPLICIT PRINTERS

1. Go to the nvram mode and configure the printer port as implicit and hosts = hostname or IP Address with user name as the printer name like as below

   set P0 type=implicit hosts=80.0.0.1 user=parprn

   and reboot the remote access server.

2. In server side login as root in the console and run sam in the console of SUN SOLARIS server, select user, add, save and add new user as below

```
    login name = parprn ( same as the user name)
    comment = implicit parallel printer
    shell = /tftpboot/etc/ts/lp/tsprof.par
    home dir = /home/parprn
  save and give NO PASSWORD for the user and exit.
```

3. Run logins in console and note down the uid and gid for lp entry, for SUN SOLARIS it will normally be 7 and 9.

4. Open /etc/passwd file and you will find an entry in the name of the printer as below

parprn:x:130:1:implicit parallel printer:/home/parprn:/tftpboot/etc/ts/lp/tsprof.par

change the first number entry 130 to 7 and change the second number entry to 9.

5. Configuring the printer Stop the Scheduler using

```
    /usr/lib/lpshut
Use lpadmin command to add printer
    /usr/lib/lpadmin -pparprn -v/dev/null -mtsmodel
Start the lpscheduler by running lpsched
    /usr/lib/lpsched
Make the printer interface accept requests by using accept command
    /usr/lib/accept parprn
Enable the printer using enable command
```

```
enable parprn
```

6. Printing Printing can be done using

```
lp command lp -dparprn < file name with full path >
```

CONFIGURING IMPLICIT PORTS IN THE REMOTE ACCESS SERVER

In the lansterm side go to nvram mode and set the port as implicit with user and hosts, for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

IMPORTANT POINT TO BE NOTED IN SUN SOLARIS:

The Rlogin from lansterm to Sun Solaris wont work unless the tcpnodelack parameter in the configure option in the admin menu is "on". So while using Sun Solaris use the following command

In the admin mode

```
admin>> configure tcpnodelack=on
```

FOR SVR4.2 SERVER

The files required for lansterm configuration will be in the 1.44" Microfloppy in tar format. The files in the floppy are

Digital.txt
IBMAIX.txt
LTSPrinting.txt
SVR.txt
Sco.txt
Sunsolaris.txt
fptyd.IBMAIX4
fptyd.DigitalUX
fptyd.SCO.Unixware
fptyd.SunOS.4.sparc
fptyd.SunOS.5.sparc
fptyd.SunOS5
fptyd.conf
fptyd.hp.800
fptyd.hp.900
fptyd.ncr3
fptyd.sco5
fptyd.svr42
lanreach.mem
logchat.ts
modemchat.ts
path.ts
printconf
release.nte
tsfixed1
tsfixed2
tsinstall
tsmodel
tsprof.par
tsprof.ser
tsrpr.README
tsrpr.c
user.ts

* Extract the files using the command in a temporary directory say /temp

```
tar -xvf < floppy drive device >
```

AUTOMATIC INSTALLATION

1. Check whether the file /etc/inetd.conf file contains an entry like one given

```
tftp dgram udp  wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

2. if the entry is commented using ## uncomment it. If there is no entry then add the above entry and save. Create a directory named tftpboot in the root. Go to the /temp directory where the files have been extracted and run tsinstall using

```
sh tsinstall
```

3. If your machine is identified then you will be prompted for installation of files and after confirmation the files will be installed.

4. Check whether /tftpboot/etc/ts/lp directories are created. Check whether the files lanreach.mem, logchar.ts, modemchar.ts, release.nte, tsrpr.README, tsrpr.c, user.ts are present in the /tftpboot/etc/ts directory. Check whether the files tsprof.par, tsprof.ser files are present in the /tftpboot/etc/ts/lp directory. Check whether /etc directory has fptyd file. Check whether /etc/inet/rc.inet file contains /etc/fptyd entry. Check whether /usr/lib/lp/model directory contains tsmodel file.

KINDLY FOLLOW MANUAL INSTALLATION IF TSINSTALL FAILS

MANUAL INSTALLATION PROCEDURE FOR SVR4.2

1. Login as Super User (root)
2. Check the tftp service in "/etc/inetd.conf" file as in the automatic installation.
3. Do the following in /temp directory where you have extraced the files.
4. Create directories /tftpboot, /tftpboot/etc, /tftpboot/etc/ts,

/tftpboot/etc/ts/lp using the following commands

```
mkdir /tftpboot
mkdir /tftpboot/etc
mkdir /tftpboot/etc/ts
mkdir /tftpboot/etc/ts/lp
```

5. Copy the files lansterm.mem, user.mem, modemchat.ts, logchat.ts into /tftpboot/etc/ts directory using cp command

```
cp lansterm.mem  /tftpboot/etc/ts/lansterm.mem
cp user.ts.  /tftpboot/etc/ts/user.ts
cp modemchat.ts  /tftpboot/etc/ts/modemchat.ts
cp logchat.ts  /tftpboot/etc/ts/logchat.ts
```

6. Copy the files tsprof.ser, tsprof.par into /tftpboot/etc/ts/lp directory using cp command

```
cp  tsprof.ser  /tftpboot/etc/ts/lp/tsprof.ser
cp  tsprof.par  /tftpboot/etc/ts/lp/tsprof.par
```

7. Give full permissions for /tftpboot and its subdirectories

```
chmod -R  777  /tftpboot
```

8. Change owner and group of lp and its subdirectory as lp using the following command

```
chgrp -R  lp  /tftpboot/etc/ts/lp
chown -R   lp  /tftpboot/etc/ts/lp
```

9. Copy fptyd.SVR4.2 file into /etc directory as /etc/fptyd using cp command

```
cp fptyd.SVR4.2 /etc/fptyd
and
chmod 555  /etc/fptyd
```

10. Copy fptyd.conf file into /etc directory as /etc/fptyd using cp command

```
cp fptyd.conf   /etc/fptyd.conf
```

11. Open the file /inet/rc.inet using vi command

```
vi  /inet/rc.inet
```

add the following content at the end of the file

```
#!/bin/sh
if   [   -x   /etc/fptyd   ]
then
echo    "starting  fptyd  daemon  "
/etc/fptyd
fi
```

12. Save and exit

13. Copy tsmodel, tsfixed1, tsfixed2 files into /usr/spool/lp/model directory using cp command

```
        cp  tsmodel   /usr/spool/lp/model/tsmodel
        cp  tsfixed1   /usr/spool/lp/model/tsfixed1
        cp  tsfixed2   /usr/spool/lp/model/tsfixed2
```

14. Manual Installation is complete

CONFIGURING FIXED PORTS AND PRINTERS

1. In /etc/inittab file add the following

```
* for login ports
log1:234:respawn:/usr/lib/saf/ttymon -g -h -p "TS LOGIN :" -d /dev/pts010
                                                              -l 9600
* for serial printers
        ser1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts005 -l 9600
* for parallel printers
        par1:2:off:/usr/lib/saf/ttymon -g -h -d /dev/pts015
```

* /etc/ttydefs file should have entry for "-l" option ie., 9600 as in above example.

2. Entry for fptyd.conf file will be as follows

```
             ##device        IP Address          Port in lansterm
           /dev/pts010    120.150.140.12            S1
           /dev/pts005    120.150.140.12            S2
           /dev/pts015    120.150.140.12            P0
```

3. Here /dev/pts010 is pseudo tty and it should be available in system.

You have to verify this with system and then give.

This can be checked by logging into server from lansterm.

```
{
      TS>telnet SVRserver(IP ADDRESS)
      $ tty
      /dev/??????
 In my case, it is /dev/pts* type.
 }
```

4. The fptyd file should be in /etc and the daemon is in /etc/inet/rc.inet.

5. In the ttytype add entry for the pts the terminal name as given below

```
vt100  pts010
vt100  pts005
vt100  pts015
```

6. In lansterm side go to the nvram mode and set ports as fixed and give the host' s name or IP Address as below

```
TS>ts
Stat>ad
Password:
Admin>>nv
NVRAM>>set  S1-S2  type=fixed  hosts=80.0.0.15
NVRAM>>set  P0  type=fixed  hosts=80.0.0.15
```

For serial printer port set the transmission parameters

```
NVRAM>>stty  S2  cs8  -parenb  +ixon  +ixoff
```

and then reboot the remote access server.

7. Reboot the server to configure the fixed ports.

For Fixed Printers

1. Configuring the printer Stop the Scheduler using

```
/usr/lib/lpshut
```

Use lpadmin command to add printer

```
/usr/lib/lpadmin -pparprn -v/dev/pts/15 -mtsfixed1 (for parallel printer)
/usr/lib/lpadmin -pparprn -v/dev/pts/5 -mtsfixed1 (for serial printer)
```

Start the lpscheduler by running lpsched

```
/usr/lib/lpsched
```

Make the printer interface accept requests by using accept command

```
/usr/lib/accept parprn
```

Enable the printer using enable command

```
enable parprn
```

2. Printing Printing can be done using

lp command lp -dparprn < file name with full path >

CONFIGURING IMPLICIT PRINTERS

1. Go to the nvram mode and configure the printer port as implicit and hosts = hostname or IP Address with user name as the printer name like as below

```
  set P0 type=implicit hosts=80.0.0.1 user=parprn
```

and reboot the remote access server.

2. In server side login as root in the console and run sysadm in the console of SVR4.2 server, select user, add, save and add new user as below

```
login name = parprn ( same as the user name)
comment = implicit parallel printer
shell = /tftpboot/etc/ts/lp/tsprof.par
home dir = /home/parprn
save and give NO PASSWORD for the user and exit
```

3. Run logins in console and note down the uid and gid for lp entry, for SVR4.2 it will normally be 7 and 9.

4. Open /etc/passwd file and you will find an entry in the name of the printer as below

```
parprn:x:130:1:implicit parallel printer:/home/parprn:/tftpboot/etc/ts/lp/tsprof.par
```

change the first number entry 130 to 7 and change the second number entry to 9

5. Configuring the printer Stop the Scheduler using

```
                /usr/lib/lpshut
    Use lpadmin command to add printer
                /usr/lib/lpadmin -pparprn -v/dev/null -mtsmodel
    Start the lpscheduler by running lpsched
                /usr/lib/lpsched
    Make the printer interface accept requests by using accept command
                /usr/lib/accept parprn
    Enable the printer using enable command
                enable parprn
```

6. Printing Printing can be done using

```
                lp command lp -dparprn < file name with full path >
```

CONFIGURING IMPLICIT LOGGING PORTS

In the lansterm side go to nvram mode and set the port as implicit with user and hosts,

for example

```
set S1 type=implicit hosts=80.0.0.25 user=guest
```

and then reboot the remote access server.

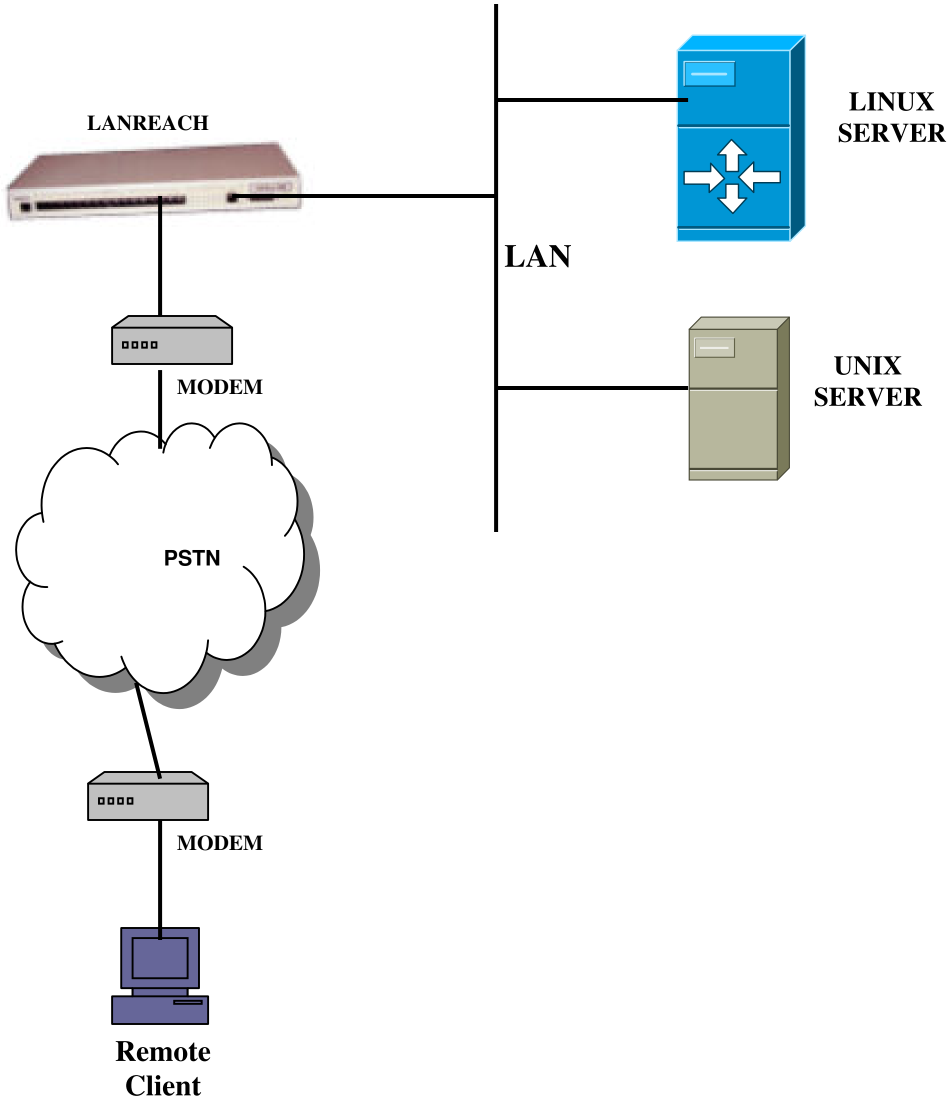
G

PPP DOCUMENTATION

- **Configuration for**
    1. **Remote Client**
    2. **LAN to LAN Operation**
- **Callback**
- **Error messages**
- **Miscellaneous**
    1. **Modem setup**
    2. **Dial up connection setup**

Remote Client

In this scenario, a remote client is enabled to access resources on a LAN through the LANReach connected to the LAN. The remote client may be a person traveling with a laptop computer, or a person at home with a PC. Popular third party software like Microsoft Window Dial up Networking may be used on the remote client. The LAN may be the office LAN. Using appropriate modems, the remote client may dial into LANReach connected to the LAN, through networks like PSTN (Public Services Telephone Network), ISDN (Integrated Services Digital Network), Radio links, VSATs (Very Small Aperture Terminals) or Cellular network. Once authenticated by LANReach, the remote client is virtually on the LAN and may access resources on the LAN as if were directly connected to the LAN. This includes other networks that may be connected to the LAN through devices like routers, bridges or voice-data multiplexers.



Configuration on LANReach Side (Dial in mode)

1. Set any one of the LANReach ports with the following settings.

```
S1  inhwflow=rts  outhwflow=cts  term=vt100  type=dialin  port_ip=80.0.0.23
auth_type=TS  path=test  modem=Hayes
```

Free IP should be given

If TS is given, post dial screen will appear in PC side

Modem standard that should be selected from the modem script

2. Set the stty parameters of the port with the following

```
S1  115200  cs8  -parodd  -parenb  -cstopb  -ixon  -ixoff  -clocal  +ignbrk
intr=^C  stop=^S  start=^Q  escape=disable
```

Baud rate should be high for better speed

3. Create a new user with the following settings in the path <admin/ppl/user>

```
------------------------------------------------------------------------------
Parameter                                  Current Value
------------------------------------------------------------------------------
UserID                    test
Start time (hhmmss)                         0
Stop time (hhmmss)                          0
Session(None/Path)                          Path
path name                                   test
password                                   ****
```

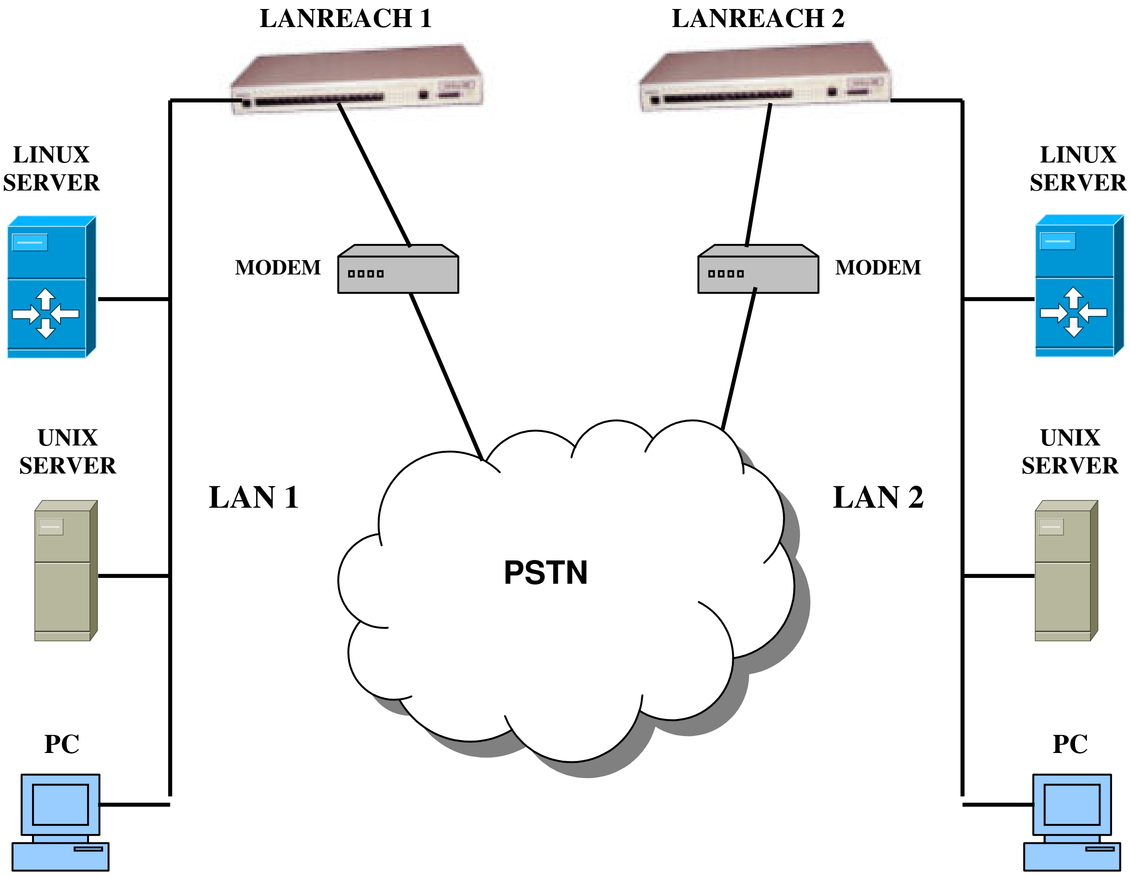
4. Make a new path with the following settings in the path <admin/ppl/path>

```
----------------------------------------------------------------------------------------
Parameter                                                     Current Value
----------------------------------------------------------------------------------------
Status (Enabled/Disabled)                                     Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)                       Client
Data Compression (None/RLE)                                   None
Protocol (SLIP/PPP/MLPPP)                                     PPP
IP Status (oN/oFf)                                            on
Destination IP Address                                        DYNAMIC
VJ Compression Status (oN/oFf)                                off
Primary DNS Server Address                                    0.0.0.0
Primary WINS Server Address                                   0.0.0.0
Secondary DNS Server Address                                  0.0.0.0
Secondary WINS Server Address                                 0.0.0.0
Negotiate Maximum Receive Unit (MRU)Yes/No)                   No
Negotiate Async map(Yes/No)                                   No
Negotiate Authentication(Yes/No)                              Yes
Authentication Protocol(PAP/CHAP)                             PAP
Protocol Field Compression(oN/oFf)                            Off
Address Control Field Compression(oN/oFf)                     Off
Magic Number Negotiation(oN/oFf)                              Off
Max. connection time (mins)                                   0
Call back type(None,Fixed,Variable)                           None
```

5. Dial from PC using Dial-up networking.

LAN to LAN operation

In this scenario, two remote LANs may access each others resources through LANReach connected to each of them. The two LANs may be a central office LAN and a branch office LAN. The workstations on the branch office LAN may need to access the servers on the central office LAN for applications like e-mail. The two LANReach on each of the LANs may be configured to establish a connection between them based on conditions like availability of user traffic. The connection, through the use of appropriate modems may be PSTN, ISDN, VSAT, Radio link or Cellular.



Different media may be used for different connections. Connection profiles may also be set up. Once connected, the devices on the two LANs are virtually on the same LAN and may access each other transparently. Since LANReach confirms to popular industry standard data communication and networking protocols, it is not mandatory that the remote access servers on both LANs should be same. LANReach can interoperated with other remote access servers which confirm to industry standard communications and networking protocols like PPP, SLIP and IP. However, if LANReach is used on both LANs, advanced features on the LANReach, like compression, may be used. This will save valuable bandwidth on the wide area connection.

Configuration on LANReach Side

For LAN to LAN operation, one LANReach should be configured to “Dial in” mode and the other LANReach should be configured to “Dial out” mode. For configuration of LANReach as Dial in mode, refer the previous section. The procedure to configure LANReach as “Dial out” mode is given in this section.

1. Create a new path with the following settings.

```
----------------------------------------------------------------------
Parameter   value                                  Current
----------------------------------------------------------------------
Status (Enabled/Disabled)                          Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)            Demand
Destination Type (Host/Gateway)                    Gateway
Logchat                                            ISDN
User Name                                          test
Password                                           ****
NAT(Enabled/Disabled)                              Disabled
Spoofing type(None/Triggered)                      None
Data Compression (None/RLE)                        None
Protocol (SLIP/PPP/MLPPP)                          PPP

IP Status (oN/oFf)                                 on
Destination IP Address                             REMOTE
VJ Compression Status (oN/oFf)                     off
Primary DNS Server Address                         0.0.0.0
Primary WINS Server Address                        0.0.0.0
Secondary DNS Server Address                       0.0.0.0
Secondary WINS Server Address                      0.0.0.0
Port Pool 1                                        S1
Telephone Number                                   22
Port Pool 2                                        -
Negotiate Maximum Receive Unit (MRU)(Yes/No) No
Negotiate Async map(Yes/No)                        Yes
Negotiate Authentication(Yes/No)                   No
Authentication Protocol(PAP/CHAP)                  PAP
Protocol Field Compression(oN/oFf)                 Off
Address Control Field Compression(oN/oFf)          Off
Magic Number Negotiation(oN/oFf)                   Off
Idle timeout (in mins)                             0
Max. connection time (mins)                        0
```

Network Address Translation (NAT) can be enabled with this option

Telephone number should be given here

2. Set any one of the LANReach ports with the following settings.

```
S1  inhwflow=rts  outhwflow=cts  term=vt100  type=test  modem=Hayes
```

3. Set the stty parameters of the port with the following values

```
S1  115200  cs8  -parodd  -parenb  -cstopb  -ixon  -ixoff  -clocal  +ignbrk
intr=^C  stop=^S  start=^Q  escape=disable
```

Note **For LAN to LAN operation, the option**

"Destination IP Address"

in the Path settings should be set to "REMOTE" in both LANReachs i.e. Dial in side LANReach and Dial out side LANReach

Callback

The callback feature instructs your LANReach to disconnect, and then to call you back, after you dial in. Callback provides cost advantages to you and security advantages to your network. By immediately hanging up, and then dialing you back, callback reduces your phone charges. Required callback enhances network security by ensuring that only users from specific locations can access the server. By dropping the call, and then calling back a moment later to the preassigned (In case of FIXED callback) number, most impersonators can be thwarted.

The following steps occur when your call reaches the LANReach:

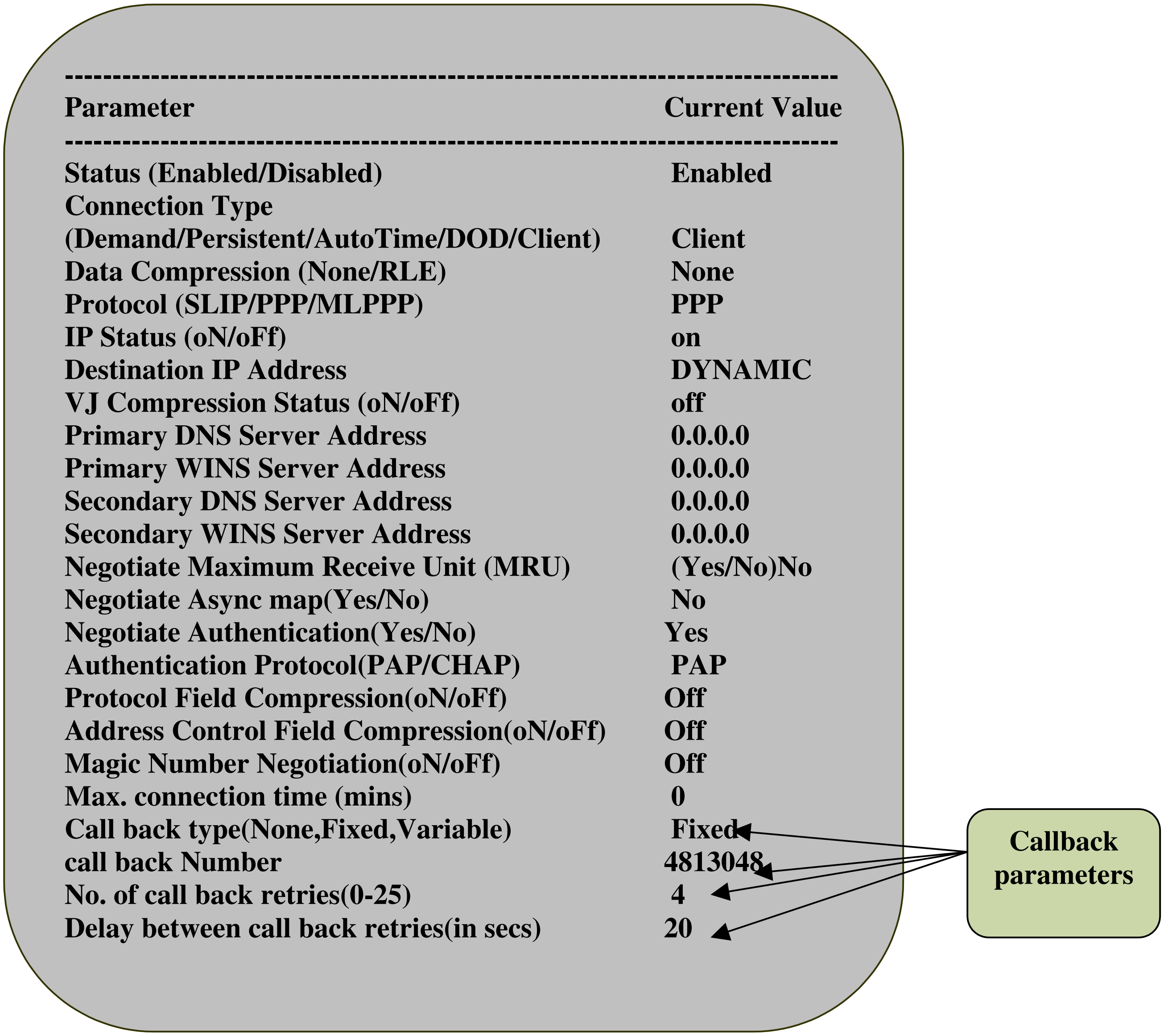
1. The LANReach determines whether your user name and password are correct.
2. If they are correct, the server will allot a magic number to you and disconnects the call.
3. It will call after some time (app. 1 minute).
4. You have to enter the magic number.
5. If the magic number is correct, the path will be started.

Types

LANReach supports two types of Callback, FIXED and VARIABLE. In case of Fixed callback, the LANReach will call back the preassigned number set in the Path configuration. Whereas in case of VARIABLE callback, the user can specify the telephone number to be called back.

To Configure Callback in LANReach

1. Open the Path (Admin/ppl/path> in LANReach menu) in which you want to enable Callback and configure the parameters as required.



```
--------------------------------------------------------------------------------
Parameter                                               Current Value
--------------------------------------------------------------------------------
Status (Enabled/Disabled)                                Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)                  Client
Data Compression (None/RLE)                              None
Protocol (SLIP/PPP/MLPPP)                                PPP
IP Status (oN/oFf)                                       on
Destination IP Address                                   DYNAMIC
VJ Compression Status (oN/oFf)                           off
Primary DNS Server Address                               0.0.0.0
Primary WINS Server Address                              0.0.0.0
Secondary DNS Server Address                             0.0.0.0
Secondary WINS Server Address                            0.0.0.0
Negotiate Maximum Receive Unit (MRU)                     (Yes/No)No
Negotiate Async map(Yes/No)                              No
Negotiate Authentication(Yes/No)                        Yes
Authentication Protocol(PAP/CHAP)                        PAP
Protocol Field Compression(oN/oFf)                      Off
Address Control Field Compression(oN/oFf)               Off
Magic Number Negotiation(oN/oFf)                        Off
Max. connection time (mins)                              0
Call back type(None,Fixed,Variable)                      Fixed
call back Number                                        4813048
No. of call back retries(0-25)                           4
Delay between call back retries(in secs)                20
```

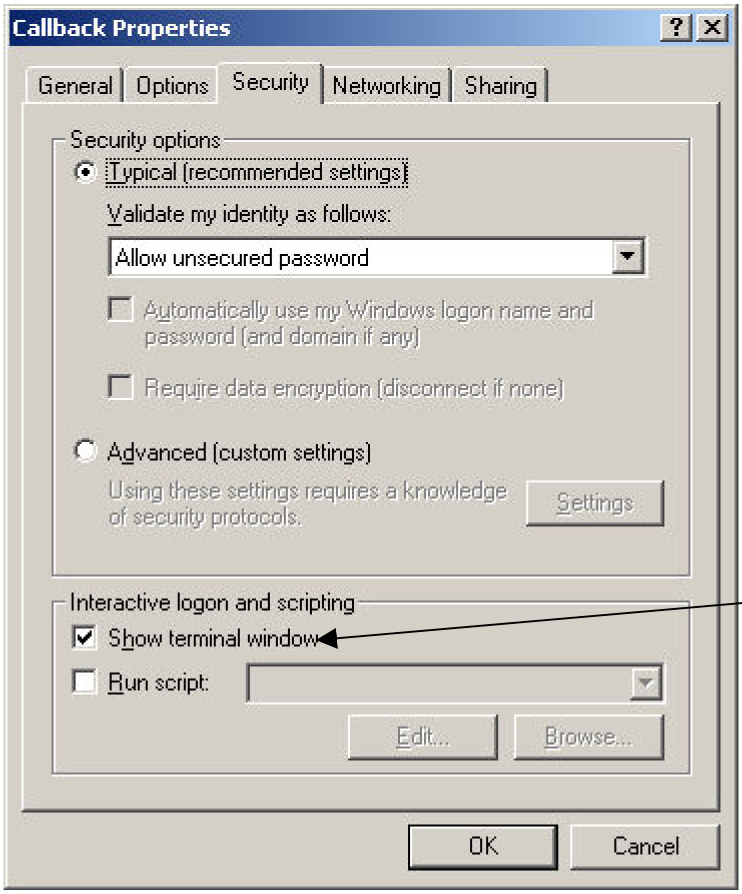
Callback parameters

2. Set the port type to "dialinout" type and select modem chatscript as "Cback". below.

```
S3  inhwflow=rts  outhwflow=cts  term=vt100  type=dialinout  port_ip=80.0.0.65
auth_type=TS  path=test  modem=Cback cdetect=off
```

Configuration required in Modem settings of Windows PC

In addition to the normal dialup settings, the Modem settings should be modified for Callback as given below.



Callback Properties

Security options

● Typical (recommended settings)

Validate my identity as follows:

Allow unsecured password

□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

○ Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

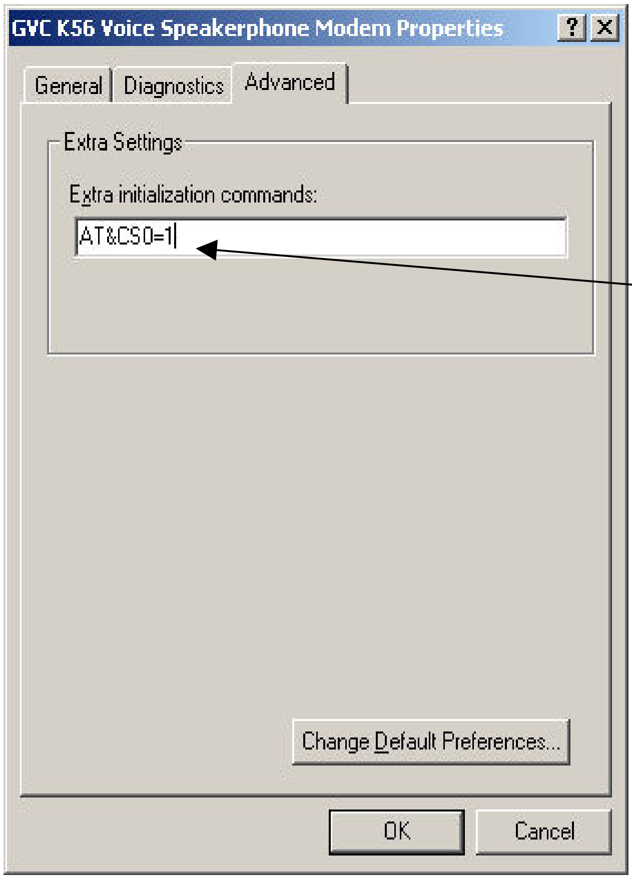
Interactive logon and scripting

☑ Show terminal window

□ Run script:

This option should be enabled so that the terminal window will appear after dial

The Initialisation commands should be added in the Modem settings to support callback as given below.


GVC K56 Voice Speakerphone Modem Properties
General
Diagnostics
Advanced
Extra Settings
Change Default Preferences...
OK
Cancel

Extra initialization commands: AT&CS0=1

What the strings will do ?

AT&C

This command Controls the Data Carrier Detect (DCD) signal level. DCD follows the state of carrier from the remote system and turns on after the connect message.

S0=1

This command forces the modem to Auto Answer mode.

Note:

The Dial up connection settings and modem settings may be different for different versions of windows OS and hence refer appropriate manuals for required configuration.

Error Messages

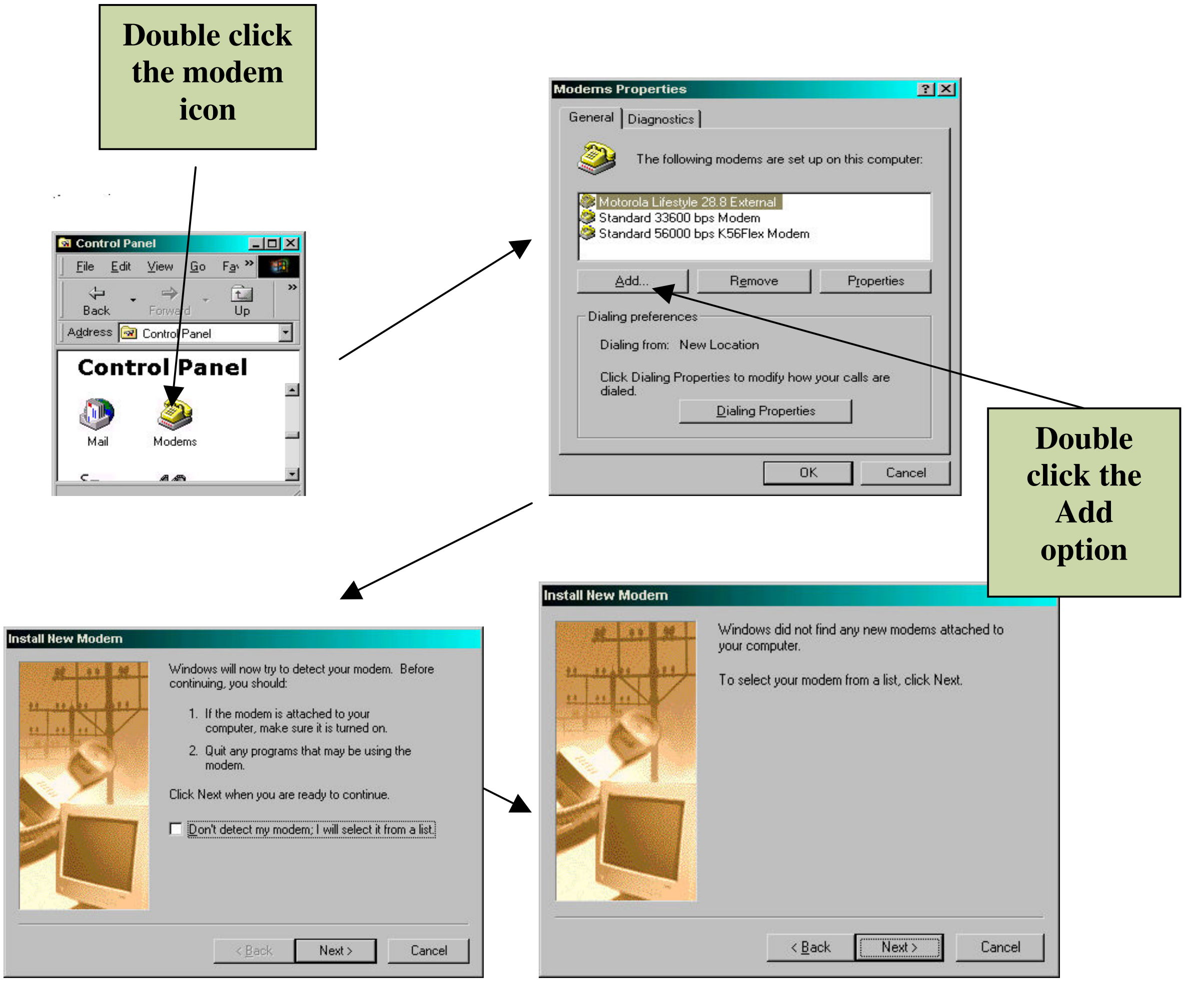
The following table lists the error messages that may appear while working with *ppl* menu commands. Cause for the error messages and corresponding corrective action are also discussed.

Error Message	Possible Cause for the Message	Corrective Action
Invalid option	Syntax error probably in spelling the option. The option name specified is not a known option	Retype the command again
passwords didn’t match	Re-entered password is different	Type the same password
Path ‘pathname” already exists	‘pathname ” is already configured	Use ‘show” to find out the currently configured paths in *ppl/path* menu
No free entries available	No free entry for configuring a path is available. All 16 paths are configured already	Delete a path which is not in use
Aborted Operation	Operation has been aborted	
No such path ‘pathname”	Probably trying to modify a path which is not configured	Use the ‘show” command to find the configured paths in *ppl/path* menu and find out the path to be modified
	Probably trying to start a which is not configured	Use the configured path for starting
Path ‘pathname” is in Use	Probably trying to modify or delete a path which is active	Shutdown ‘pathname” in *ppl* menu and try again
-d option requires a value	Command start is -d option is not typed fully. -d option requires value	Retype the command specifying a positive value in the range of 0-100 for -d option
d requires a positive integer(0-100)	Probably start command is typed with -d option with improper value	Retype the command specifying a positive value 0-100 for -d option
User not configured for dialout	Probably the ‘user” is configured for LOGIN only	Use ‘user show” to find the configuration about the ‘user”

Error Message	Possible Cause for the Message	Corrective Action
Path not configured for dialout	Path which is used for dialout might not be configured for: dialout	Use “show” to find out the configuration of pathname in *ppl/path* menu
No such path “pathname” is active	Path “pathname” is not active for shutting down	Use “list” to find out the active paths in *ppl* menu.
No such accesscode “accesscode” configured	Probably trying to modify or delete “accesscode” which is not configured	Use “show” command to find the configured accesscodes in *ppl/user* menu
Accesscode “accesscode” already exists	Probably trying to add “accesscode”, which is configured previously	Use “show” command to find the configured accesscodes in *ppl/user* menu
Path name should be unique	Probably trying to give the same path for more than one user	Use “show” to find the configured paths in *ppl/path* menu
No such accesscode “accesscode”	Probably trying to delete “accesscode”, who is not configured	Use “show” to find the configured accesscodes in *ppl/user* menu
Authentication Failed	Probably the given “accesscode” might not have configured or wrong password is given	Use “show” command to find the configured accesscodes in *ppl/user* menu
Duplicate user ID	If the user ID is already configured for some other accesscode	Give unique user ID
Login timeout. Connection closed	Password has not been entered in the post dial screen for three minutes	Try to give password within three minutes
“chatname” No such chat	Probably trying to delete a chatscript which is not available in the modemchat database	Download the modemchat script

Modem Setup

Setup the Modem as given in the following steps



Double click the modem icon

Control Panel

Modems Properties

The following modems are set up on this computer:

- Motorola Lifestyle 28.8 External
- Standard 33600 bps Modem
- Standard 56000 bps K56Flex Modem

Dialing preferences

Dialing from: New Location

Click Dialing Properties to modify how your calls are dialed.

Double click the Add option

Install New Modem

Windows will now try to detect your modem. Before continuing, you should:

1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.

Click Next when you are ready to continue.

□ Don't detect my modem; I will select it from a list.

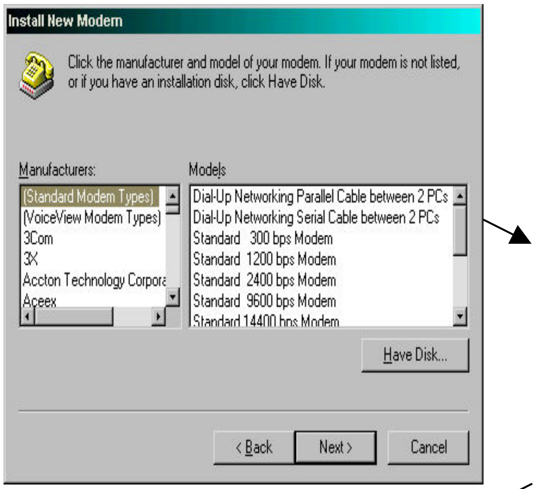
Install New Modem

Windows did not find any new modems attached to your computer.

To select your modem from a list, click Next.

Try to add a modem via Add option. If not possible, install as per given.

1. Select the (Standard Modem Type) in the manufacturers list.
2. Select the appropriate model from the (modem) list.
3. Select COM port of the modem.
4. After installation, perform diagnostics on the modem.

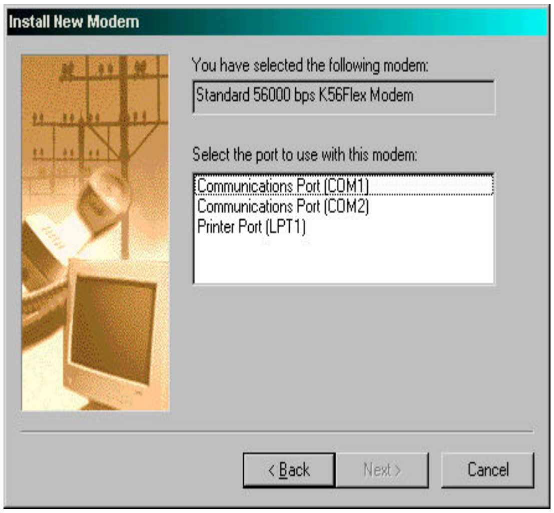


Install New Modem

Click the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.

Manufacturers:
(Standard Modem Types)
(VoiceView Modem Types)
3Com
3X
Accton Technology Corpora
Aceex

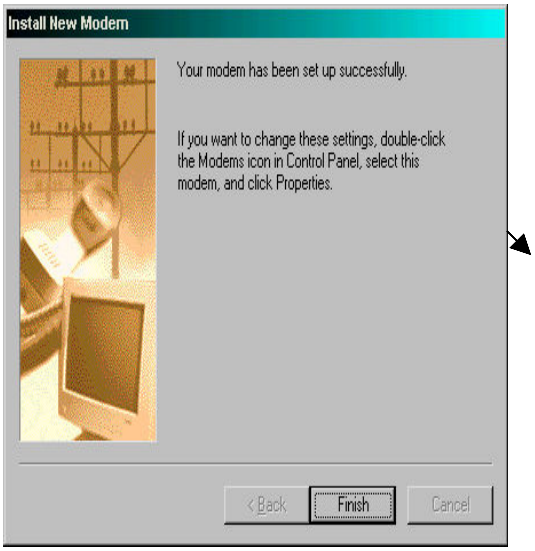
Models
Dial-Up Networking Parallel Cable between 2 PCs
Dial-Up Networking Serial Cable between 2 PCs
Standard 300 bps Modem
Standard 1200 bps Modem
Standard 2400 bps Modem
Standard 9600 bps Modem
Standard 14400 bps Modem



Install New Modem

You have selected the following modem:
Standard 56000 bps K56Flex Modem

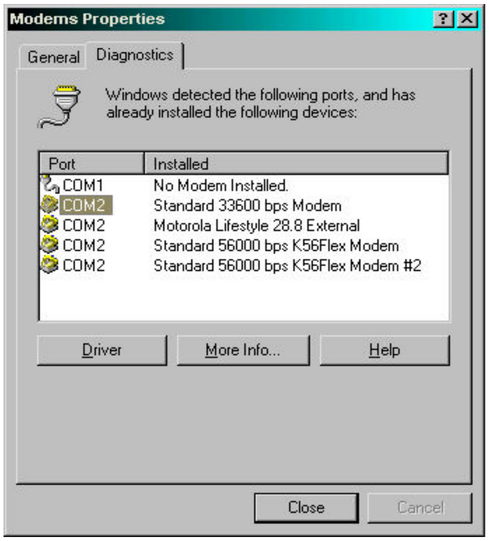
Select the port to use with this modem:
Communications Port (COM1)
Communications Port (COM2)
Printer Port (LPT1)



Install New Modem

Your modem has been set up successfully.

If you want to change these settings, double-click the Modems icon in Control Panel, select this modem, and click Properties.



Modems Properties

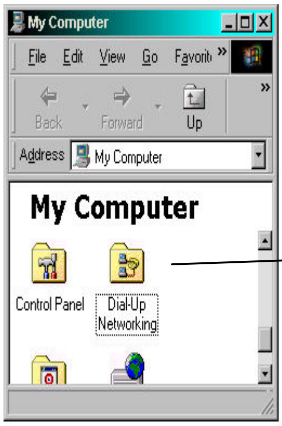
General | Diagnostics

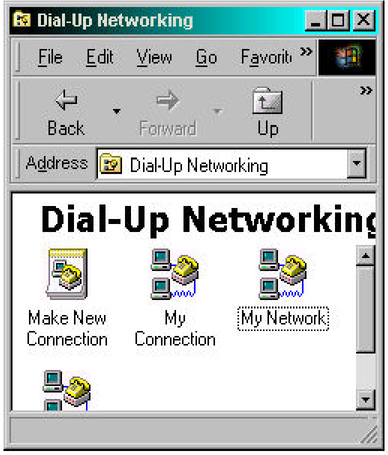
Windows detected the following ports, and has already installed the following devices:

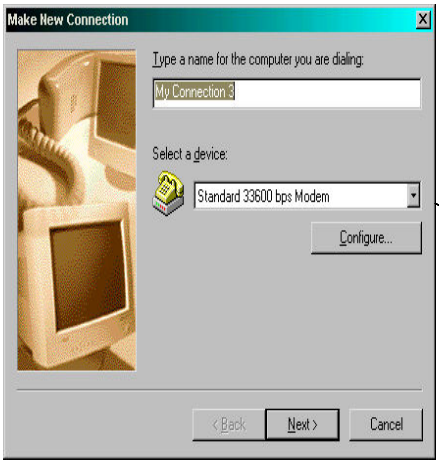
Port	Installed
COM1	No Modem Installed.
COM2	Standard 33600 bps Modem
COM2	Motorola Lifestyle 28.8 External
COM2	Standard 56000 bps K56Flex Modem
COM2	Standard 56000 bps K56Flex Modem #2

Modem Setup

Make a new connection using the ‘Dial -up networking” as given below

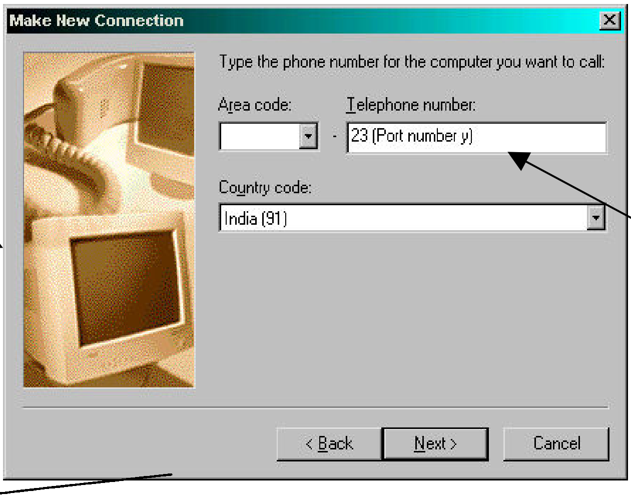






Type a name for the computer you are dialing: My Connection 3

Select a device: Standard 33600 bps Modem



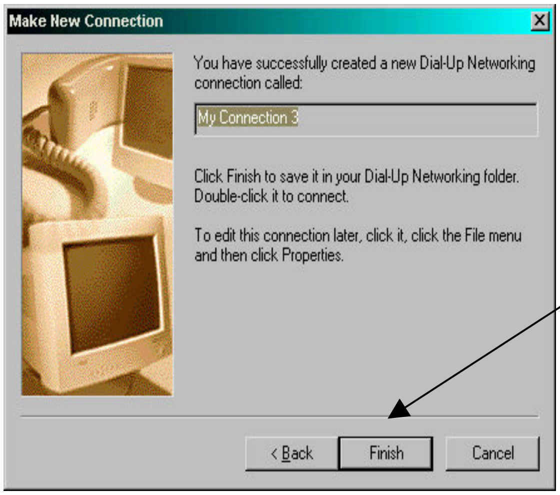
Type the phone number for the computer you want to call:

Area code: -

Telephone number: 23 (Port number y)

Country code: India (91)

Enter the telephone number



You have successfully created a new Dial-Up Networking connection called:

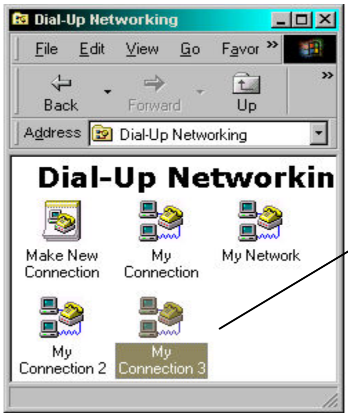
My Connection 3

Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.

To edit this connection later, click it, click the File menu and then click Properties.

When you click finish, a new connection name ‘My Connection 3” will created. We have to change the settings of this new connection by selecting the properties option. Change the settings as per the following

Dial up connection setup



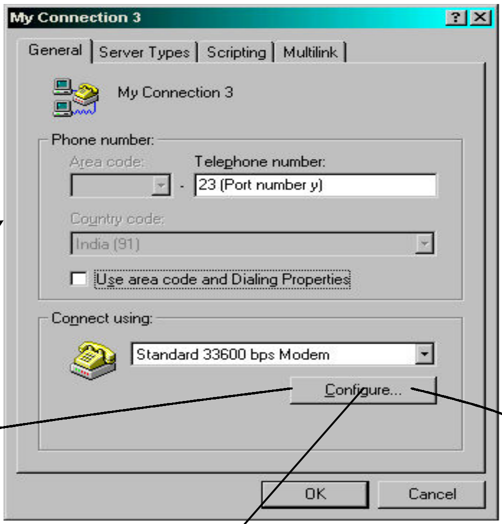
Dial-Up Networking

File Edit View Go Favor

Address: Dial-Up Networking

Dial-Up Networkin

Make New Connection · My Connection · My Network · My Connection 2 · My Connection 3



My Connection 3

General | Server Types | Scripting | Multilink

My Connection 3

Phone number:

Area code: · Telephone number: 23 (Port number y)

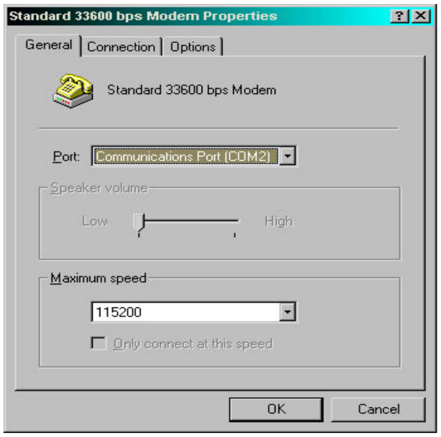
Country code: India (91)

□ Use area code and Dialing Properties

Connect using: Standard 33600 bps Modem

Configure...

OK · Cancel



Standard 33600 bps Modem Properties

General | Connection | Options

Standard 33600 bps Modem

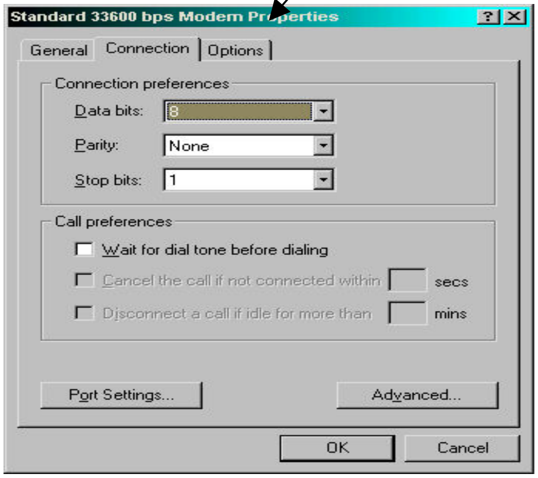
Port: Communications Port (COM2)

Speaker volume: Low – High

Maximum speed: 115200

□ Only connect at this speed

OK · Cancel



Standard 33600 bps Modem Properties

General | Connection | Options

Connection preferences

Data bits: 8

Parity: None

Stop bits: 1

Call preferences

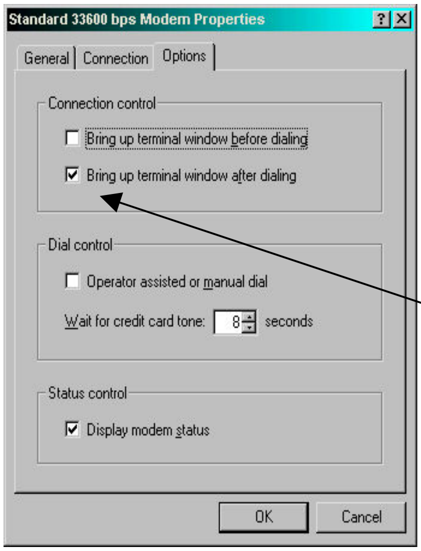
□ Wait for dial tone before dialing

□ Cancel the call if not connected within ___ secs

□ Disconnect a call if idle for more than ___ mins

Port Settings... · Advanced...

OK · Cancel



Standard 33600 bps Modem Properties

General | Connection | Options

Connection control

□ Bring up terminal window before dialing

☑ Bring up terminal window after dialing

Dial control

□ Operator assisted or manual dial

Wait for credit card tone: 8 seconds

Status control

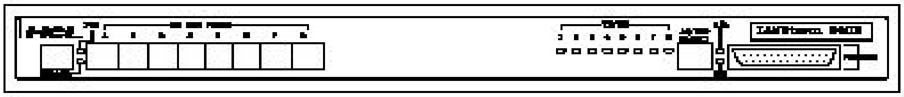
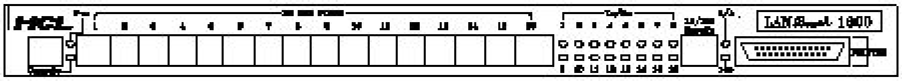
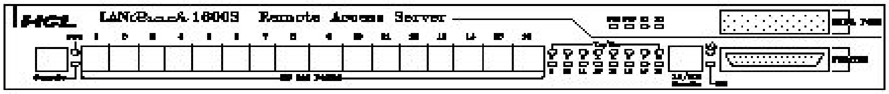
☑ Display modem status

OK · Cancel

This should be set, if <auth_type=TS> in the 'SET" parameters of Lansterm

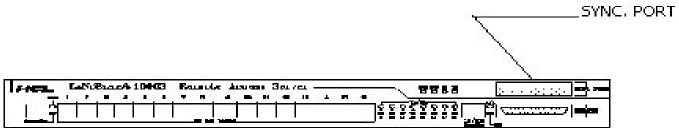
H

REMOTE ACCESS SERVER - MODELS

MODELS	FRONT PANEL VIEW
800-V4	
1600-V4	
1600-S	

SYNC PORT - DETAILS

LANReach 1600S

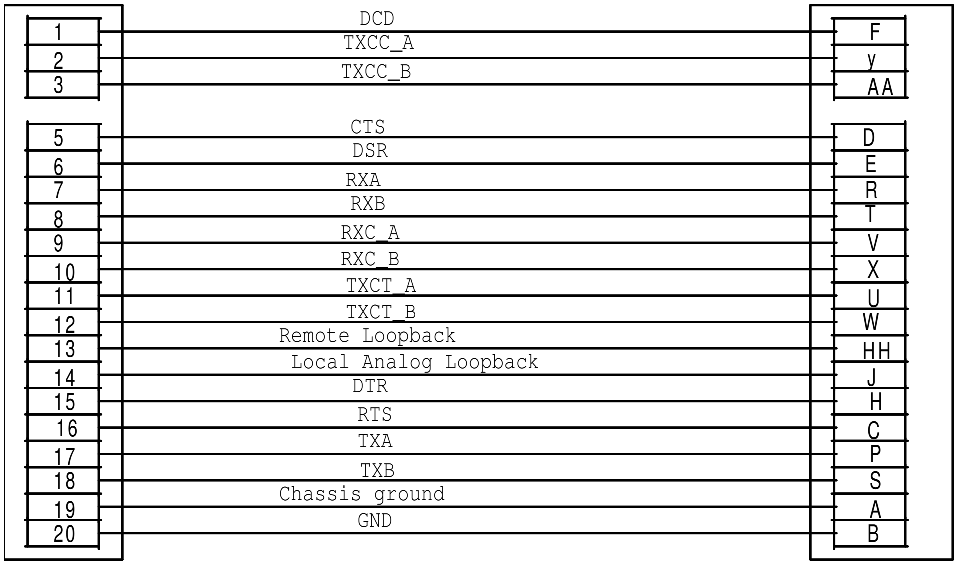


V.35 Cable Details

The connections for the cable from the DB25 male connector to the V.35 Modem connector (34 pin Block female connector) are as shown.

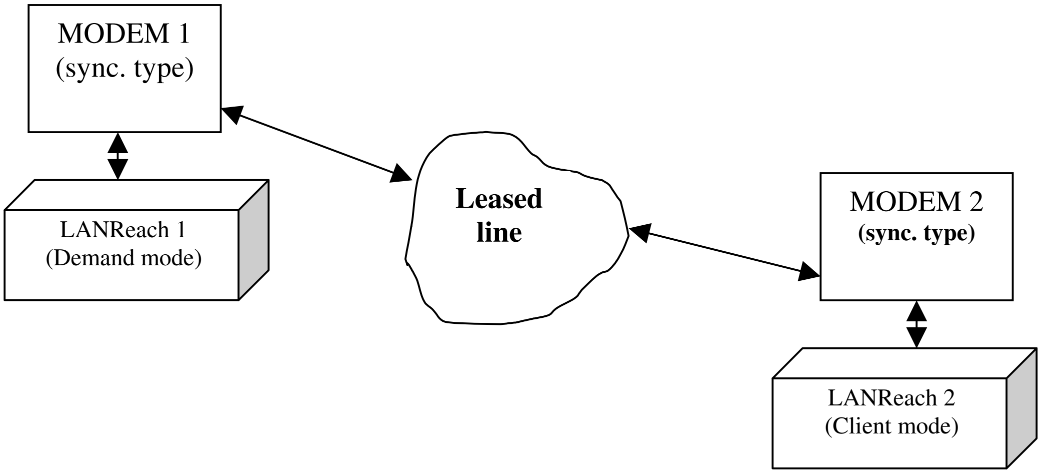
Signal Meaning	Pins on DB25 Female Connector	Pins on 34 pin Male block Connector
DCD (Carrier Detect)	1	F
TxccA (Transmit Timing A)	2	Y
TxccB (Transmit Timing B)	3	AA
CTS (Clear to Send)	5	D
DSR (Data Set Ready)	6	E
RxA (Receive Data A)	7	R
RxB (Receive Data B)	8	T
RxcA (Receive Timing A)	9	V
RxcB (Receive Timing B)	10	X
TxctA (Transmit Timing A)	11	U
TxctB (Transmit Timing B)	12	W
Remote Loopback	13	HH
Local Analog Loopback	14	J
DTR (Data Terminal Ready)	15	H
RTS (Request to Send)	16	C
TxA (Transmit Data A)	17	P
TxB (Transmit Data B)	18	S
Chasis Ground	19	A
GND (Signal Ground)	20	B

V.35 Interface with Sync Card



25 pin D Female Connector		34-Pin Stand-Alone, Male Connector
1	DCD	F
2	TXCC_A	y
3	TXCC_B	AA
5	CTS	D
6	DSR	E
7	RXA	R
8	RXB	T
9	RXC_A	V
10	RXC_B	X
11	TXCT_A	U
12	TXCT_B	W
13	Remote Loopback	HH
14	Local Analog Loopback	J
15	DTR	H
16	RTS	C
17	TXA	P
18	TXB	S
19	Chassis ground	A
20	GND	B

Configuration Details



Steps :

1. **Create a new path on LANReach 1 as shown below.**

```
-------------------------------------------------------------
Parameter                                           Current
                                                     Value
-------------------------------------------------------------
Status (Enabled/Disabled)                           Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)             Demand
Destination Type (Host/Gateway)                     Gateway
Logchat                                             ISDN
User Name                                           test
Password                                            ****
Spoofing type(None/Triggered)                       None
Data Compression (None/RLE)                         None
Protocol (SLIP/PPP/MLPPP)                           PPP
IP Status (oN/oFf)                                  on
Destination IP Address                              REMOTE
VJ Compression Status (oN/oFf)                      off
Primary DNS Server Address                          0.0.0.0
Primary WINS Server Address                         0.0.0.0
Secondary DNS Server Address                        0.0.0.0
Secondary WINS Server Address                       0.0.0.0
Port Pool 1                                         SY
Telephone Number                                    33
Port Pool 2                                         -
Negotiate Maximum Receive Unit (MRU)(Yes/No)        No
Negotiate Async map(Yes/No)                         No
Negotiate Authentication(Yes/No)                    Yes
Authentication Protocol(PAP/CHAP)                   PAP
Protocol Field Compression(oN/oFf)                  Off
Address Control Field Compression(oN/oFf)           Off
Magic Number Negotiation(oN/oFf)                    Off
Idle timeout (in mins)                              0
Max. connection time (mins)                         0
Call back type(None,Fixed,Variable)                 None
```

Username and password should be same as that of the user details (step 3) on Lanreach 2 side

Enter a dummy number, which will not have any significance on SYNC communicatio

2. **Make the Sync port (SY) settings on Lanreach 1 as shown below.**

```
SY  inhwflow=none  outhwflow=none  term=vt100  type=dialout
modem=NULL_MODEM cdetect=off
```

3. **Create a new user on LANReach 2 as shown below.**

```
-------------------------------------------------------------
Parameter                                     Current Value
-------------------------------------------------------------
User ID                                       test
Start time (hhmmss)                           0
Stop time (hhmmss)                            0
Session(Shell/Path)                           Path
path name                                     test
password                                      ****
```

4. Create a new path on LANReach 2 as shown below.

```
--------------------------------------------------------------
Parameter                                            Current Value
--------------------------------------------------------------
Status (Enabled/Disabled)                            Enabled
Connection Type
(Demand/Persistent/AutoTime/DOD/Client)              Client
Data Compression (None/RLE)                          None
Protocol (SLIP/PPP/MLPPP)                            PPP
IP Status (oN/oFf)                                   on
Destination IP Address                               REMOTE
VJ Compression Status (oN/oFf)                       off
Primary DNS Server Address                           0.0.0.0
Primary WINS Server Address                          0.0.0.0
Secondary DNS Server Address                         0.0.0.0
Secondary WINS Server Address                        0.0.0.0
Negotiate Maximum Receive Unit (MRU)(Yes/No)No
Negotiate Async map(Yes/No)                          No
Negotiate Authentication(Yes/No)                     Yes
Authentication Protocol(PAP/CHAP)                    PAP
Protocol Field Compression(oN/oFf)                   Off
Address Control Field Compression(oN/oFf)            Off
Magic Number Negotiation(oN/oFf)                     Off
Max. connection time (mins)                          0
Call back type(None,Fixed,Variable)                  None
```

5. Make the Sync port (SY) settings on Lanreach 2 as shown below.

```
SY  inhwflow=none  outhwflow=none  term=vt100  type=dialin
port_ip=0.0.0.0  auth_type=PC  path=test  modem=NULL_MODEM
cdetect=off
```

6. Start the path (Created in step 1) on Lanreach 1 side using <start> command in the <ppl> menu. Using <list> command, the user can ensure whether the path is running or not. The running path may be stopped using <stop> command in the <ppl> menu.

A

- Activity 73
- add 105, 107
  - DOD entry 109
  - filter 14, 72, 105, 106, 107, 108
  - filter entries 107
  - path 84, 117, 121, 128, 130, 277, 278
  - route 86
  - SAS entry 140
  - static route 112
  - user 125, 128
- addport 142
- ARP
  - ARP table 63
  - ARP trace 156
- auditlog 15
  - directory 128
- AUI 210

B

- baudrate 49, 99, 167
- boot 80, 83, 130
  - file 80, 117
  - flash 116, 117
  - message 130, 131
  - parameters 83, 84, 85, 105, 107, 115, 116, 117, 129, 201
  - server 72, 80, 105, 116, 117, 130, 198, 274
- boot file 28, 29, 30, 31, 80
- boot flash 10, 27
- boot message 26
- boot server 13, 28, 80
- bootconfig 83
- browser 198

C

- cable 24, 25, 183, 203, 275
- carrier 101, 169, 203, 267, 275
- centronics 9, 22, 25
- clear 108, 129
  - access code 126
  - DOD entry 110
  - filter entries 108
  - logchat 136
  - modem chat 133
  - SAS 141
- configure 83, 201, 202
  - download 80, 116, 117
  - UDP parameters 84
- Configure 155
  - boot 71, 80
  - server 71, 155
- connector 275
  - console 14, 18
  - D-15 210
  - D-25 22, 25, 207, 209

D

- database 13, 19, 30, 36, 64, 71, 80, 105, 106, 107, 108, 115, 116, 128, 129, 179
- date 77
- delete 105, 108
  - accesscode 125
  - DOD entry 109
  - filter entries 108
  - logchat 136
  - modemchat 133
  - path 122
  - route 86
  - SAS entry 140
  - staticroute entry 112
- delport 118
- detach 34, 46, 71, 78
- diagnostics 182, 183
  - error messages 181
  - run time messages 181
- display
  - filter entries 106
- DNS 64, 67, 75, 156, 157, 185, 198
  - entry 106, 107, 108, 115, 116, 128, 198
- DOD
  - commands 84, 105, 108, 116, 128

statistics 63
dot notation.................... 29, 87, 112, 113
download
accesscode 127
logchat 136
modemchat.................................. 133
path 122
webserver files 117
dynamic 11, 13, 20, 75, 157

E

erase character 49, 53, 100, 168
escape
default 80, 169
disable 42, 84, 117, 130, 131
ethernet 28, 30, 63, 81, 103, 183, 189
Ethernet 14, 83

F

Filter
commands 105
fixed port 178
fixed pty 74, 156
messages 195
flow control
hardware 93, 161
software 51, 100

G

gateway 12, 28, 30, 81, 87, 113
getconfig 79, 158
gethost 80, 81

H

help 84, 105, 116, 128
DOD... 109
logchat 135
modemchat.................................. 132
path 120
ppl menu 119
SAS 139
staticroute.................................... 111
telnet 147
user.. 124
Help 199, 200, 201, 202
history 14, 146
hosts.... 16, 28, 34, 35, 56, 59, 64, 80, 83, 115, 116
HTML 198

I

ifconfig 72, 103, 104
implicit 11, 14, 17, 19, 154, 162, 172
manager 19
insert
filter entries.................................. 107
Insert.. 105, 107
installation 21
hardware 22
software 27
internet......... 9, 12, 14, 16, 18, 28, 29, 34
address ... 12, 19, 29, 63, 80, 115, 173, 198
Internet 198, 199
IP forward.................................. 75, 157

K

kmesg 56, 58

L

LAN...................... 20, 24, 106, 257, 258
LED
console port.................................... 24
LAN port... 24
power 24, 26
line manager 19, 101, 169, 212
list 84, 105, 116, 117, 128, 278
active paths 118, 144, 269
sessions 34, 44

M

main
memory 182
prompt...................................... 14, 33

manager
- fixed 19
- line 19
- SNMP 13

maxsession 93, 94, 161, 162, 171
memory
- flash 10, 27, 32, 154
- NVRAM 11, 79
- on-board.. 10

Memory 83
MIB 13
models 274
modem 9, 16, 49, 52, 101, 118, 168, 203, 208
modify 83, 84, 85, 107, 115, 117, 122
- path 122
- port parameters 47, 49
- SAS 141
- SNMP options 164
- UDP parameters.............................. 84
- user... 126
- webserver parameters 117

N

namesession.................................. 34, 43
netstat 61
- sampling.. 62

network....................... 12, 13, 14, 18, 20
- address 12, 18, 35, 64, 87, 103, 112
- interface 63, 103
- statistics 61

Network Address Translation.............. 15
node 12, 13, 18
NVRAM 83, 128
nvram menu.................................. 84, 85

P

panic 58, 194
parallel port 9, 18, 19, 22, 173, 176, 177, 196, 203
parity.................26, 49, 50, 99, 167, 176
password... 11, 33, 39, 57, 69, 70, 74, 76, 114, 125, 154, 199
Password 154
port
- characteristics 34, 71, 155
- console ... 9, 14, 19, 22, 24, 26, 32, 33, 181
- fixed 14, 17, 93, 95, 161, 195, 197
- implicit. 11, 19, 93, 95, 161, 162, 172, 176
- parameters. 11, 34, 47, 49, 71, 92, 155
- serial...... 10, 16, 22, 25, 178, 196, 212
- switched 19, 92, 94, 160, 171
- unused 94, 95, 162

Port 85, 117, 129, 130
PPP 118, 121, 138, 143, 201, 257, 261
preferred boot server 27, 29
printer
- fixed 171, 179
- implicit... 171
- parallel 10, 25, 203
- serial... 10

Protocol Filters 14, 105
pseudo tty 223, 234, 240, 248, 254
pty....................... 74, 156, 173, 174, 179
pty name 197
putconfig......... 71, 82, 83, 155, 159, 216

Q

quit...................................... 85, 117, 131
- filter manu.................................... 108
- logchat menu................................ 137
- modemchat menu.......................... 134
- path 127
- ppl menu 123

R

Remote Administration facility........... 68
resume 34, 45
reverse telnet .. 12, 76, 95, 157, 163, 175, 213
RIP................................. 12, 75, 91, 157
RJ-45 .... 22, 25, 203, 211
rlogin 9, 12, 39, 43, 54, 68
route.. 86
- commands...................................... 86
- show 86

RS232-C..........9, 10, 19, 22, 24, 25, 203
rwhod..............................59, 74, 75, 156

S

secondary boot server.................... 13, 29
Secondary Boot Server........................ 83
session 18
- active... 19
- detach... 46
- maximum 40
- multiple... 12
- name... 19
- number 19
- rlogin.. 39
- switched port.................................. 19
- telnet 54

session number 43, 44, 45, 46
set47, 92
Set.. 275
setup 28, 30, 69, 81, 83, 154, 170
show 83, 85, 105, 106, 115, 116, 117, 129
- boot config..................................... 80
- DOD entries................................. 110
- modemchat................................... 132
- path 120
- route 86
- SAS entries 139
- UDP parameters.............................. 85
- user... 124
- webserver parameters 116

SNMP
- parameters.................................... 155
- support 13

software update 31, 32
start.. 278
- character.. 49
- path 138

stat 57, 68, 114
stop
- character........................... 49, 53, 168
- path 138

stop bit 26, 168
stty 49, 99
subnet 12
- mask.. 12

suspend 34, 45
- session.. 41

T

TCP/IP.................................... 9, 12, 212
telnet 12, 54
tftp 82, 159
timeout.. 172
twisted pair 9

U

UDP configuration 15
upload
- path 122
- user... 126

Upload 128
URL... 198, 199

W

wall 71, 102
Web 198, 199
web management......... 14, 116, 117, 198
webserver
- commands.................................... 116

write... 72, 102