PO993516
Issue 1.0

April 2002

LinkPlexer 1.1 Installation and Configuration Guide

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, MSymposium, SCCS, Meridian, MSL-100, and DMS-100 are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation.

Symantec and pcAnywhere are trademarks of Symantec Corporation.

Intel and Pentium are trademarks of Intel Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Statement of conditions

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Contents

Figures

Tables

Preface

This document describes how to install and configure the Nortel Networks LinkPlexer 1.1 application.

Before you begin

This guide is designed to be read by the following:

- Nortel Networks customers
- Nortel Networks personnel
- Nortel Networks distributors

This guide assumes familiarity with the following:

- Microsoft Windows NT
- TCP/IP networking concepts such as IP address, subnet mask and port
- CompuCall or ICM on DMS or MSL-100 switches

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that the reader chooses the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
braces ({})	Indicates required elements in syntax descriptions where there is more than one option. The reader may choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicates that the reader repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Related publications

For more information about the LinkPlexer 1.1, refer to the following publications (you can find most documents listed in the Customer Support section at www.nortelnetworks.com):

- *Nortel Networks Symposium Call Center Server and DMS Switch Guide*, (part number 911815).
- Nortel Networks Symposium Call Center Server Installation and Configuration guide (part number PO910112).
- ICM TAPI Network Managers Guide (part number PO881940)
- Peri Link Server Installation Guide
- MIS-Q218-1 SCAI Interface Specification
- CompuCall Interface Specifications, refer to http://triweb/ACD/icm/ICM.html

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections required, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

The selected documentation sets, CDs, and technical publications can be purchased through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to get help

If a service contract for your Nortel Networks product has been purchased from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Chapter 1
Overview

This chapter is an overview of the architecture and features of LinkPlexer 1.1. It contains the following sections:

LinkPlexer 1.1 Architecture

LinkPlexer 1.1 is a Windows NT application that enables multiple IP clients to share the same session and DMS/MSL-100 resources, by acting as a proxy server between the two. LinkPlexer 1.1 can connect to the switch via IP (ICM) or X.25 (CompuCALL). When LinkPlexer 1.1 acts as an IP capable server it allows applications that can only connect via IP to communicate with a switch that uses an X.25 connection.

LinkPlexer 1.1 allows applications to share DN (Directory Number) association between different eBusiness applications.

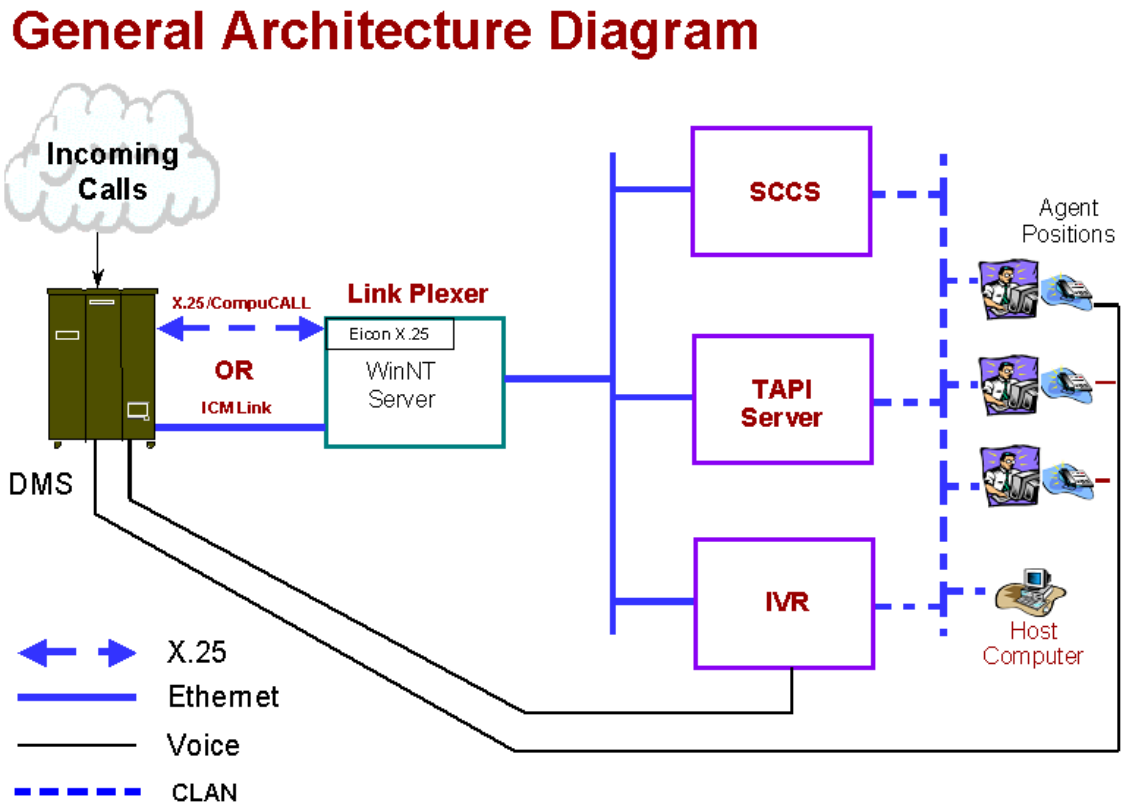
For example:

- Interactive Voice Response (IVR) voice ports controlled by IVR and monitored by Symposium Call Center Server (SCCS)
- A system where, SCCS performs the call routing, the IVR controls the voice response system, and TAPI Symposium Server/Symposium Agent controls softphones and screen pops

- When agent positions are controlled by TAPI Server/Symposium Agent (TAPI) (or desktop CTI) and monitored by SCCS
- In systems where call queues and agent positions monitored by third party applications, such as voice recorders

Figure 1 describes the general architecture of LinkPlexer 1.1.

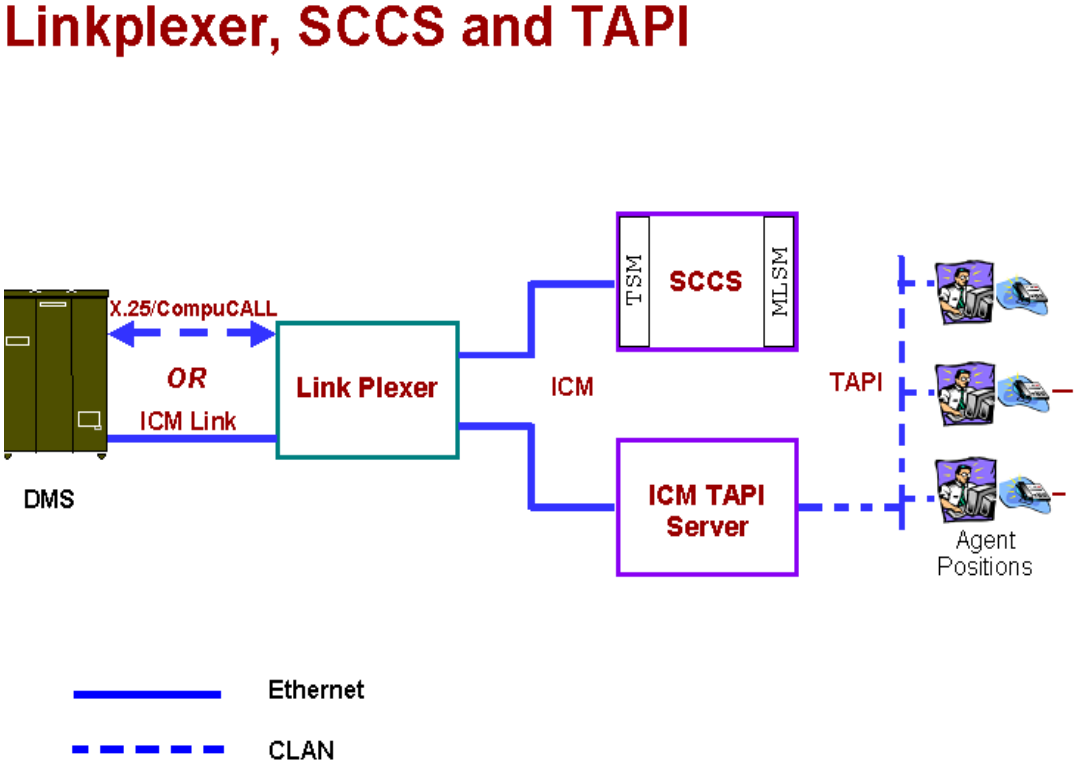
Figure 1 General architecture diagram



In Figure 1 CLAN refers to the Customer LAN ; Ethernet refers to the ELAN.

Figure 2 describes the architecture for LinkPlexer 1.1, SCCS and TAPI

Figure 2 LinkPlexer 1.1, SCCS & TAPI



Features

The main features of LinkPlexer 1.1 are described in the following sections:

- “DN association sharing” , next
- “ICM application multiplexing” on page 20
- “Connectivity of ICM client to Compucall” on page 20
- “Messaging” on page 20
- “Session Management” on page 21
- “Client connection management” on page 22

DN association sharing

Both CompuCALL and Intelligent Call Management (ICM) limit the association of resources to a single session. Two host applications with simultaneous CompuCALL/ICM application sessions established with a given switch cannot have the same resource associated with the two sessions at the same time.

LinkPlexer 1.1 overcomes this limitation by propagating all resource messages from the DMS/MSL-100 to all clients.

For example:

A dv-call-offered message from the DMS/MSL-100 is propagated to all clients and not just the client that originally issued the dv-dn-association request.

ICM application multiplexing

The DMS/MSL-100 only allows one resource to be associated per link session with the switch. However, LinkPlexer 1.1 acts as a proxy server between multiple ICM applications and a DMS, MSL-100 CompuCALL, or ICM switch link. It enables ICM clients to share, via TCP/IP, the same session and DMS/MSL-100 resources and manages messages to and from the switch.

Connectivity of ICM client to Compucall

LinkPlexer 1.1 supports a single connection to the DMS/MSL-100 switch, either Ethernet TCP/IP or X.25. This connection allows ICM-only applications to access CompuCall-equipped systems. LinkPlexer relays messages to the X.25/ICM link on the switch

Messaging

LinkPlexer 1.1 has three general types of messaging and tracks each message from an application to the DMS/MSL-100. The initial response message is sent only to the sending application. Event messages are broadcast to all connected applications.

To the application communicating with LinkPlexer 1.1 the socket exactly emulates the DMS/MSL-100 ICM interface.

Session Management

There are three session management options for LinkPlexer:

- “Internal session management with DN associate filtering OFF” , next (recommended option)
- “Allow a primary application to handle session management” on page 21
- “Internal session management with DN associate filtering ON” on page 22

Internal session management with DN associate filtering OFF

Nortel Networks recommends use of the LinkPlexer 1.1 internal session management without DN associate filtering.

In this configuration:

- The SessionPort is not specified in the DMSGlobal.ini file.
- Set the DN associate filter option to OFF.

  Add the following line to the Switch-n section of the DMSGlobal.ini file:

  ```
  DnAssociateFilter=OFF
  ```

Allow a primary application to handle session management

In this configuration:

- The SessionPort is specified in the DMSGlobal.ini file.
- A primary application such as Symposium Call Center Server or TAPI Server is responsible for starting the switch link and associating all DNs.
- Ensure the following lines are included in the DMSGlobal.ini file (note: 2600 is an example of a SessionPort value):
  - `DnAssociateFilter=OFF`
  - `SessionPort=2600`

Internal session management with DN associate filtering ON

In this configuration:

- The SessionPort is not specified or is commented out in the DMSGlobal.ini file
- The following line must be added to the DMSGlobal.ini file:
  - `DnAssociateFilter=ON`
- All client applications must connect to the ListenerPort.

Client connection management

LinkPlexer 1.1 manages all client connections. A client connection is any successful socket connection to LinkPlexer 1.1. Each connection uses one client license. The number of client connections is limited, by the keycode, to 150.

LinkPlexer 1.1 maintains the integrity of the connection between the LinkPlexer 1.1 server and each connected client. This allows LinkPlexer 1.1 to:

- Free the client license when a client disconnects

The client connection integrity is maintained at the ICMP level and the application level. These are described in the following sections:

- “ICMP connectivity checking” , next
- “Application-level connectivity checking” on page 23

ICMP connectivity checking

To enable ICMP connectivity checking, set the parameters in the DMSGlobal.ini files to the following values:

- <AgentPingTest=ON>

  This setting turns on ICM connectivity checking. The default value is OFF.

- <AgentPingInterval=120>

  This specifies a 120 second time period between checks. The default value is 120 seconds.

If specific values are not set for these parameters, LinkPlexer 1.1 uses the default values.

Application-level connectivity checking

To enable application-level connectivity checking, set the AgentContinuityTest parameter in DMSGlobal.ini file to the following value:

- AgentContinuityTest=ON

With this parameter turned on, LinkPlexer:

- Forwards the message to the Session Manager (Internal or External)
- Forwards the message to all connected LinkPlexer agents
- On receipt of a timely reply from the Session Manager, a positive acknowledgement (RETURN-RESULT) is sent to the DMS.
- Any agents that don't respond to the message in a timely fashion are disconnected and the agent licence becomes available.
- If the session Manager doesn't respond the Session Manager Connection, the DMS Connection and connections to all active agents are disconnected.

If specific values are not set for these parameters, LinkPlexer 1.1 uses the default value i.e.:

- AgentContinuityTest = OFF

With this parameter set to OFF, LinkPlexer:

- Forwards the message to the Session Manager (Internal or External)
- On receipt of a timely reply form the Session Manager, a positive acknowledgement (RETURN-RESULT) is sent to the DMS
- If the session Manager doesn't respond the Session Manager Connection, the DMS Connection and connections to all active agents are disconnected.

Benefits

The main benefits of LinkPlexer 1.1 are described in the following sections:

Migration

LinkPlexer 1.1 facilitates the introduction of Nortel applications (such as SCCS) into existing customer CompuCall or ICM-based networks without the need to displace the existing applications. LinkPlexer 1.1 architecture is componentized architecture, rather than a monolithic model with SCCS as the focal point.

Connectivity

LinkPlexer 1.1 provides conversion of ICM to X.25 and vice-versa allowing ICM-only applications to be used with existing CompuCall links.

Compatibility

LinkPlexer performs no protocol conversion. Applications conforming to the NIS Q218 CompuCALL/Meridian SCAI Interface Specification should work in a Linkplexer integrated environment.

Considerations & Limitations

Co-residency

Note: LinkPlexer 1.1 will install and co-reside with ICM TAPI and Symposium Agent however this configuration is not recommended by Nortel Networks.

LinkPlexer 1.1 may operate co-resident with ICM TAPI and or Symposium Agent. However, Nortel Networks recommends that LinkPlexer 1.1 be installed on a separate server due to the following reasons:

- Reliability: with LinkPlexer 1.1 running on a separate server you can make changes to ICM TAPI and or Symposium Agent without affecting the status of their link to the switch - this allows call centre activity to continue for other applications in the solution.
- Trouble Shooting: with LinkPlexer 1.1 running on a separate server, diagnosis of issues would be limited to LinkPlexer and other applications conflicting with the operations of LinkPlexer software would not have to be eliminated.

Refer to “Startup Procedures for Nortel Networks Call Centre Equipment” on page 107, for pertinent startup information.

Application Considerations

Associated LinkPlexer 1.1 applications must cooperate in controlling common resources

- A ‘race’ condition will result if two applications attempt to change the state of the same device at the same time
- One application should control the device, others monitor events only

The applications must also be tolerant of receiving events related to resources that the application had not previously been associated with

- The impact of receiving these unexpected events cans only be determined through testing the application in a LinkPlexer 1.1 environment
- Applications may still get events on devices they have disassociated
- Applications that disassociate resources may also affect other applications using those resources

- Applications will receive messages about resources that they are not monitoring, but other applications are monitoring.

Limitations

LinkPlexer 1.1 has the following known limitations:

- X.25 Bandwidth
  - EMPC interface limited to 19,200bps
- 512 Invoke IDs
  - Invoke Ids are shared between applications
  - Maximum of 512 invoke Ids in either direction
  - Can run out of invoke IDs if switch latency is long
- Remote Alarm Monitoring is not supported

Engineering Guidelines

Nortel Networks does not recommend connecting more than 10 applications to LinkPlexer 1.1

For information on ICM Guidelines refer to http://triweb/ACD/icm/ICM.html

Chapter 2
Pre- Installation Requirements & Procedures

This chapter contains the following sections:

System Requirements

A LinkPlexer 1.1 system consists of a PC running MS Windows NT 4.0 Server. The system is connected to a DMS/MSL-100 switch. System requirements are described in the following sections:

Note: Refer to the Microsoft Hardware Compatibility list (http://www.microsoft.com/hcl/default.asp) to ensure hardware and Operating System compatability. Refer to the hardware manufacturers web site to ensure that the operating system is supported by them.

Minimum server requirements

The following are the minimum server requirements:

- Pentium III - 933MHz
- MS Windows NT 4.0 service pack 6a

- 128 MB RAM
- 18 GB storage
- Security dongle and keycode
- Parallel port for dongle
- LinkPlexer supports two NIC cards. Two NIC cards are required if LinkPlexer is co-resident with the ICM TAPI Driver.
- If X.25 (CompuCall) is being used, the following requirements are necessary:
  - Two comm ports (only one is required for ICM)
  - Eicon card
  - Motorola V.3600 modem

Note: Nortel Networks does not support the installation of LinkPlexer 1.1 on MS Windows 2000.
Note: LinkPlexer 1.1 is a software only product and Nortel Networks is not responsible for replacing hardware components.
Note: .LinkPlexer 1.1 will install and co-reside with ICm TAPI and Symposium Agent however this configuration is not recommended by Nortel Networks.

TCP/IP requirements

To connect to DMS/MSL-100 via TCP/IP the minimum requirements are:

- An EIU on the DMS/MSL-100 switch
- A 10Mb or 10/100 Mb ethernet card on the LinkPlexer 1.1 server

X.25 requirements

To connect via X.25 the minimum requirements are:

- An EMPC/MOC or IOM card on the DMS/MSL-100 switch
- An EICON C20 or C90 card on the LinkPlexer 1.1 server
- A pair of Motorola V.3600 stand alone modems

Other considerations

The minimum switch requirements are:

- MSL-100: MSL-09 or later
- DMS-100: CCM10 (MMP10) or later

Administrator rights on the Local Server are required for LinkPlexer Installation.

Nortel Networks recommends the following:

- PC Anywhere V9.2, on systems which require remote administration.
- UPS backup power supply

Pre-installation procedures

LinkPlexer 1.1 requires the following pre-installation procedures:

- TCP/IP must be configured and working prior to beginning the LinkPlexer installation. See the system administrator's manual for MS Windows NT 4.0 for information.
- MS Windows NT must be installed on the PC and installation of LinkPlexer must be completed using the local administrator account.
- Nortel Networks requires that installation of pcAnywhere before installation of LinkPlexer 1.1.
- An ICM or CompuCall line to switch must be in place. See the Symposium Network Managers guide or the ICM guide for more information.
- LinkPlexer 1.1 supports the X.25 network protocol to communicate with the DMS/MSL-100 switch. If using this protocol the hardware and network configuration must be completed before installing LinkPlexer 1.1. For more information See Chapter 6, "Installing and configuring the Eicon X.25 card," on page 81 and Chapter 4, "Configuring LinkPlexer," on page 49.

Chapter 3
Installing LinkPlexer 1.1

This chapter describes how to install and start LinkPlexer 1.1. It contains the following sections:

LinkPlexer 1.1 Checklist

The following items are supplied with LinkPlexer 1.1:

- LinkPlexer 1.1 CD, this includes the following folders and files:
  - Documentation
    - — LinkPlexer 1.1 Installation & Configuration Guide.pdf
  - ThirdParty
    - — DallasDongleDriver
    - — pcAnywhere_v9.2
    - — WindowsNTServicePack6
  - Setup.exe and ancillary files
- iButton TMEX RTE dongle (with parallel port adapter) and associated keycodes

Windows NT 4.0 Service Pack Installation

One of the minimum requirements for LinkPlexer 1.1 is for Service Pack 6 to be installed. To check if service pack 6 is present go to Start\Settings\Control Panel\Add/Remove Programs, on the LinkPlexer machine, and click to open it. Scroll through the list of programs and locate ‘Windows NT 4.0 Service Pack 6’.If this is found, service pack 6 is present and no further actions are required. The service pack version may also be found by typing ‘winver’ at the Start\Run...\Open: location.

If ‘Windows NT 4.0 Service Pack 6’ is not present it must be installed.

1. Insert the LinkPlexer CD into the CD-ROM drive
2. In Windows Explorer, navigate to the E:\ThirdParty\WindowsNTServicePack6 folder (where E: is the CD-ROM drive).
3. Double click on executable sp6i386.exe
4. Follow the installation instructions - more installation information is available at http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/readme.asp

At the time of printing, there were not any Windows NT hot fixes required. Refer to http://www.microsoft.com for more information on relevant hot fixes.

Dongle Installation

Nortel Networks provides an iButton TMEX RTE dongle (consists of an iButton and a Parallel Port Adapter), associated key codes, and Dallas Semiconductor 1-Wire Driver (Win32) v3.20 with LinkPlexer 1.1.

Figure 3 iButton TMEX RTE Dongle: Parallel Port Adapter (top) and iButton

To install the dongle and dongle drivers:

1. Attach the iButton TMEX RTE dongle to the parallel port of the LinkPlexer 1.1 server.
2. Insert the LinkPlexer 1.1 CD into the CD-ROM drive.
3. In Windows Explorer, navigate to the E:\ThirdParty\DallasDongleDriver folder (where E: is the CD-ROM drive).
4. Double click the Install_1_Wire_Drivers_v320 icon.

   Figure 3 shows the InstallShield dialog box.

Figure 4 1-Wire Drivers InstallShield Self-extracting EXE

5. Click Yes to continue.

   Figure 5 shows the USB dialog box.

Figure 5 USB dialog box

6 If there is a 1-Wire USB device attached to the LinkPlexer 1.1 server PC, unplug it. Note that a 1-wire USB device is not required for LinkPlexer 1.1

7 Click OK.

The Software Licence Agreement is displayed.

8 Click Yes to continue the installation.

The Readme Information dialog box is displayed.

9 Click Next.

The Choose Destination Location dialog box is displayed.

10 Click Next to accept the default location.

The Select Program Folder dialog box is displayed.

11 Click Next.

Figure 6 shows the BOOT Option dialog box.

Figure 6 1-Wire Drivers BOOT Option

12 Click OK.

The Setup Complete dialog box is displayed.

13 Click Finish.

14 Restart the LinkPlexer 1.1 server.

LinkPlexer Installation

This section describes how to install the LinkPlexer 1.1 application from the CD. The supplied keycode is necessary to complete the installation.

To install LinkPlexer 1.1:

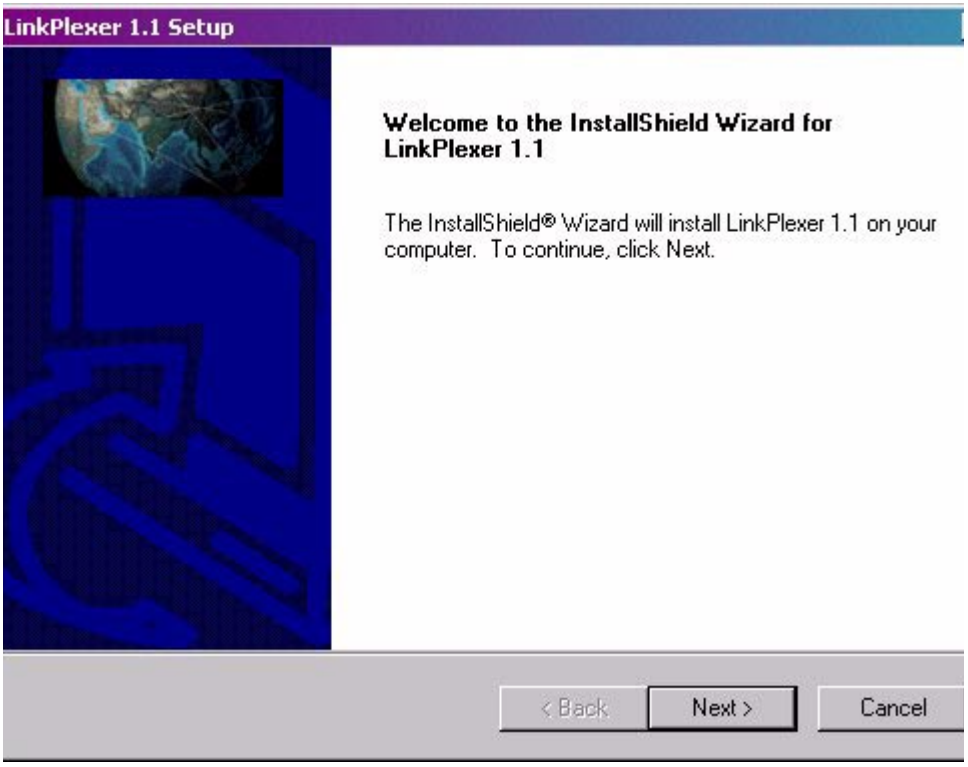
1 Insert the LinkPLexer 1.1 CD into the CD-ROM drive.

2 In Windows Explorer, navigate to the CD-ROM drive folder

3 Double click the Setup icon.

Figure 7 shows the InstallShield Wizard for LinkPlexer 1.1

Figure 7 LinkPlexer 1.1 Setup



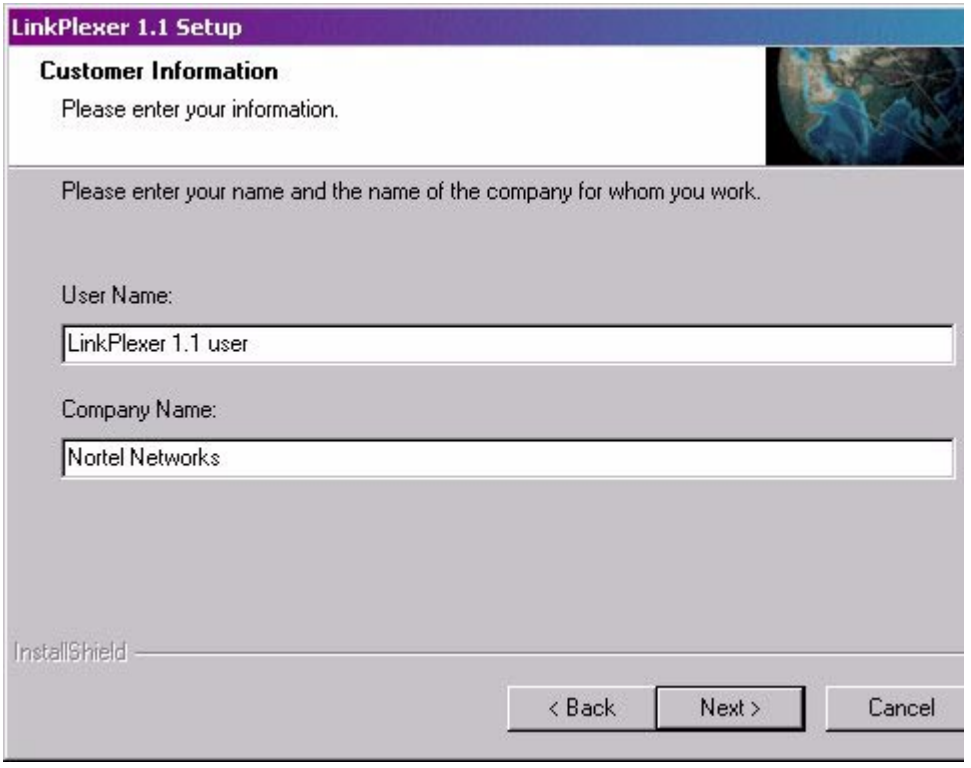
4 Click Next.

The License Agreement dialog box is displayed.

5 To accept the terms of the LinkPlexer 1.1 license agreement, click Yes.

Figure 8 shows the Customer Information dialog box.

Figure 8 Customer Information



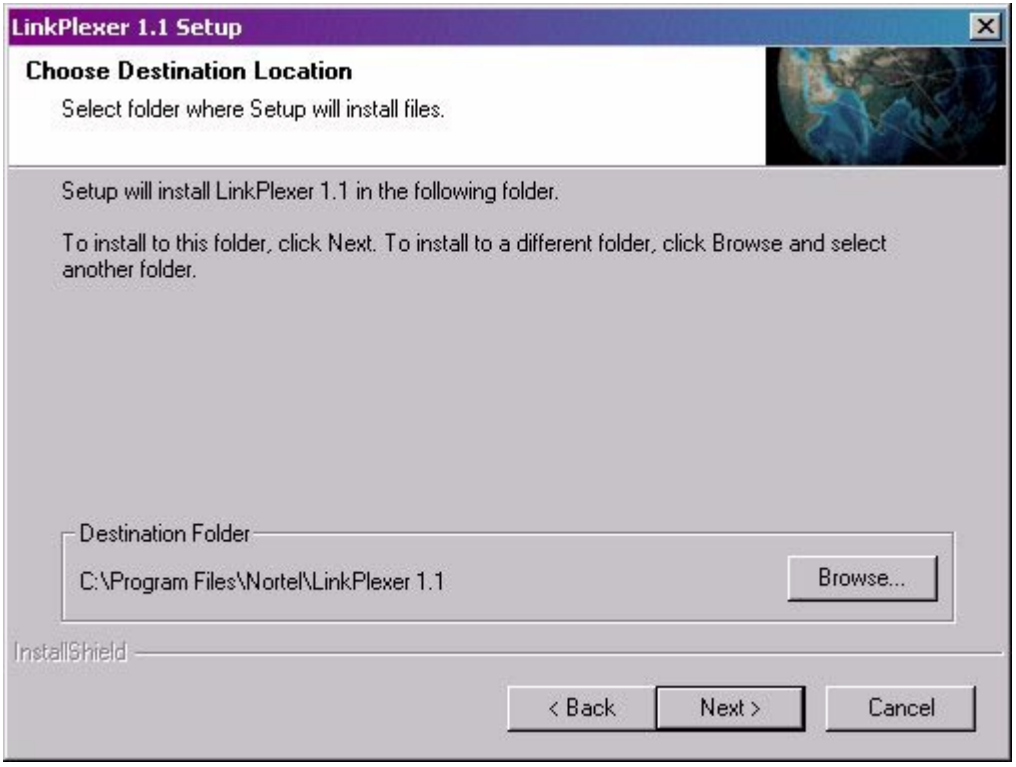
6 Type a user name in the User Name text box.

7 Type the relevant company name in the Company Name text box.

8 Click Next.

Figure 9 shows the Choose Destination Location dialog box.

Figure 9 Choose Destination Location

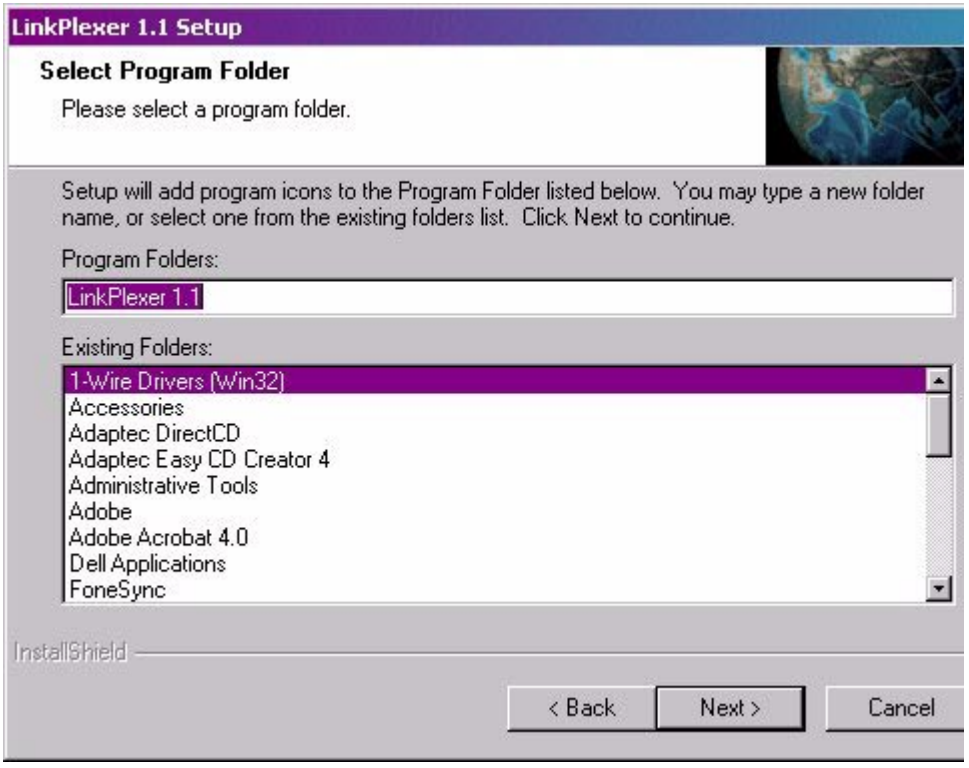


9 To accept the default destination folder, click Next.

10 Click Next.

Figure 10 shows the Select Program Folder dialog box.

Figure 10 LinkPlexer 1.1 Setup Select Program Folder



11 To accept the default program folder, click Next. To select a new folder, type the folder name in the Program Folders text box. To select an existing folder highlight it in the Existing Folders list.

12 Click Next.

Figure 11 shows the Setup Complete dialog box.

Figure 11 Setup Complete

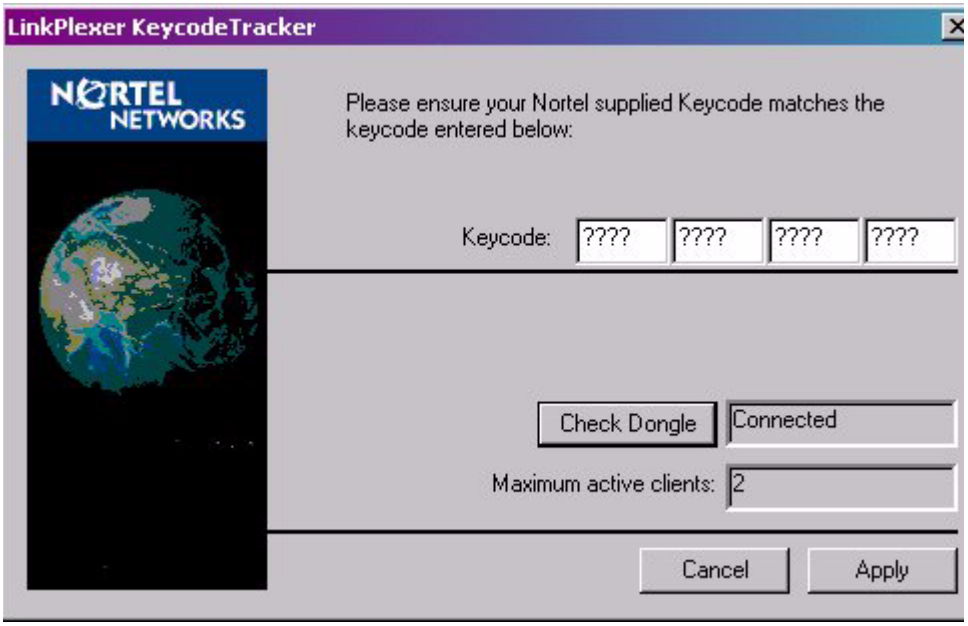
13 To launch LinkPlexer 1.1 Keycode Tracker:

a Select the I would like to enter the LinkPlexer 1.1 Keycode Tracker check box. Note, this can be launched separately by clicking on the link in Start\Program Menu\Nortel LinkPlexer 1.1\Keycode Tracker

b Click Finish.

Figure 12 shows the keycode dialog box.

Figure 12 LinkPlexer KeycodeTracker



c Type the supplied keycode in the Keycode text boxes.

d Click Apply.

The LinkPlexer 1.1 KeycodeTracker dialog closes.

The Setup Complete dialog box is displayed.

e Deselect the I would like to enter the LinkPlexer 1.1 Keycode Tracker check box in the Setup Complete dialog box.

14 To display the readme file:

a Select the I would like to view the readme file check box and click Finish.

b Read and close the Readme file.

The Setup Complete dialog box is displayed.

c Deselect the I would like to view the readme file check box in the Setup Complete dialog box.

15 Click Finish.

Starting the LinkPlexer 1.1 service

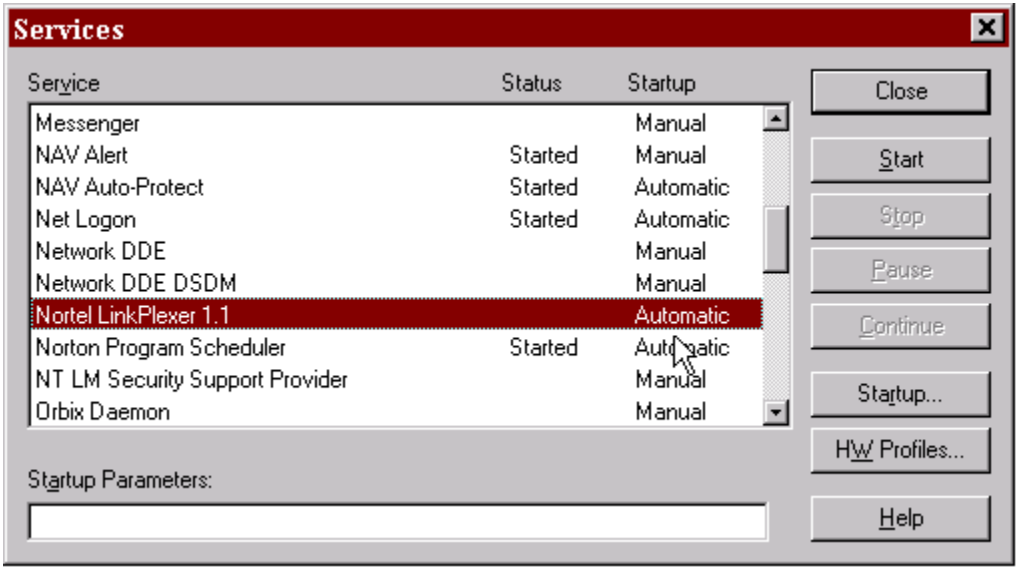
Note: LinkPlexer 1.1 must be configured prior to starting the service (refer to Chapter 4: Configuring LinkPlexer 1.1 for details)

To start LinkPlexer 1.1:

1. From the Windows NT Start menu, select Settings, and click Control Panel.
2. Double-click Services.

   The Services window is displayed as in Figure 13.

Figure 13 Services Control Panel



3. Select Nortel LinkPlexer in the scroll box.
4. Click the Start button.

   LinkPlexer starts.

If LinkPlexer 1.1 does not start correctly see Chapter 7, “Maintenance & Troubleshooting LinkPlexer,” on page 87.

Additional applications

The LinkPlexer 1.1 installation includes 2 additional applications, these are discussed in the following sections:

LinkPlexer Tracker

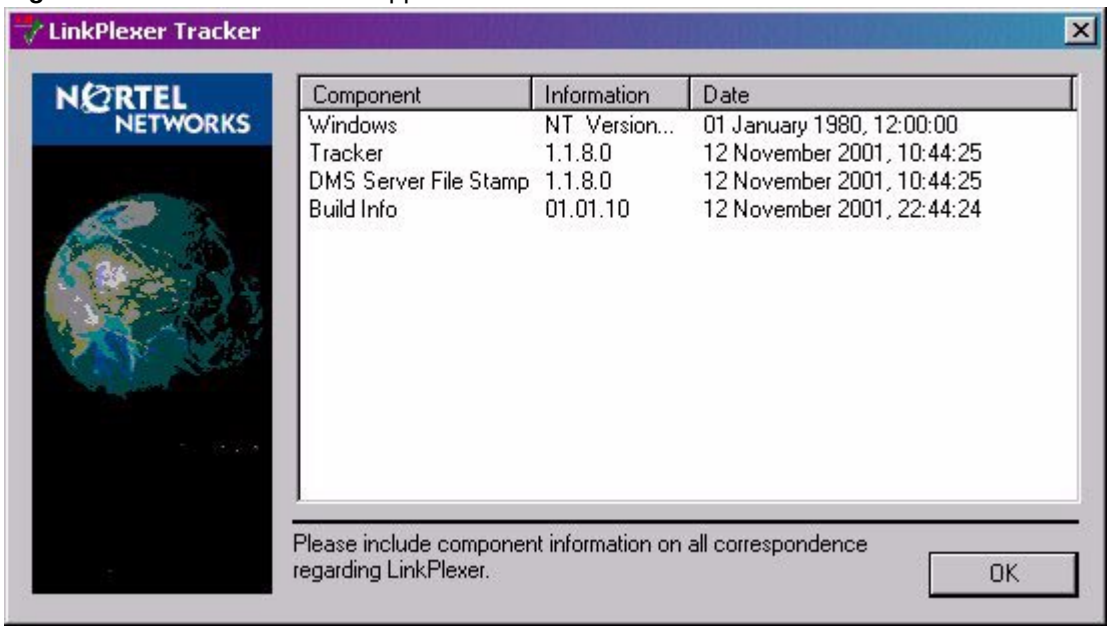
The LinkPlexer Tracker application provides information about the LinkPlexer 1.1 build version and the MS Windows NT system. It detects and displays information on the MS Windows NT version, the build number and date of the installation, and the version number and date of install of any PEP installation.

To launch the Tracker application:

➔ From the Start menu, select Programs>Nortel LinkPlexer 1.1>Tracker

Figure 14 shows the Tracker application window.

Figure 14 LinkPlexer Tracker application window



The LinkPlexer Tracker application window displays the following Components and Information:

- Windows: This refers to the operating system and service pack versions
- Tracker: indicates the current version of the LinkPlexer Tracker application
- DMS Server File Stamp: refers to the version of the File Stamp
- Build Info: indicates the LinkPlexer 1.1 build.

The Date for the Tracker, DMS Server File Stamp and Build Info components refers to the date LinkPlexer 1.1 was installed.

LinkPlexer Keycode Tracker

The LinkPlexer Keycode Tracker application enables the entering of the dongle keycodes. It also displays the number of agents that can connect to the LinkPlexer 1.1 server.

The Keycode Tracker is also used to confirm dongle detection. If a dongle is detected the ‘Check Dongle’ box, on the Keycode Tracker window, displays ‘Connected’ as in Figure 15. If the dongle is not detected the user will see ‘Not Connected’. If this occurs refer to Chapter 7, “Maintenance & Troubleshooting LinkPlexer,” on page 87.

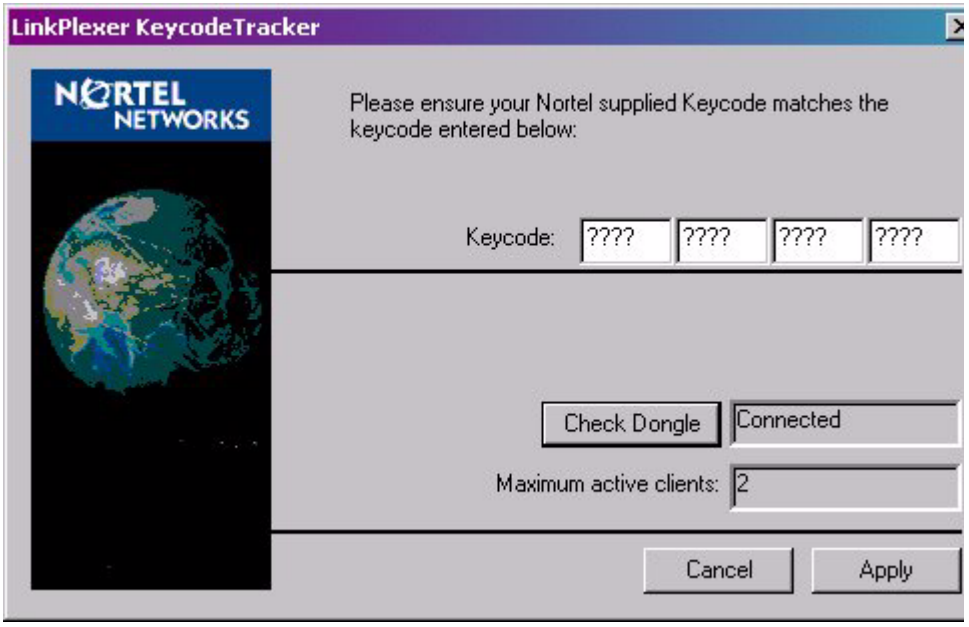
Alternatively, the dongle may be also be detected using iButton applications as referred to at http://www.ibutton.com/software/tmex/index.html

To enter keycodes with LinkPlexer Keycode Tracker:

1 From the Start menu, select Programs>Nortel LinkPlexer 1.1>Keycode Tracker.

Figure 15 shows the Keycode Tracker window.

Figure 15 LinkPlexer Keycode Tracker



2 Type the supplied 20-character keycode in the Keycode text boxes.

3 Click Apply.

Un-installing LinkPlexer 1.1

To un-install LinkPlexer 1.1 using the Add/Remote Programs control panel:

1. Close all running applications and close all open windows on the desktop including Windows Explorer.
2. From the Start menu, select Settings>Control Panel.
3. Open the Add/Remove Programs control panel.
4. Select LinkPlexer 1.1 in the Install/Uninstall tab screen, and click OK.

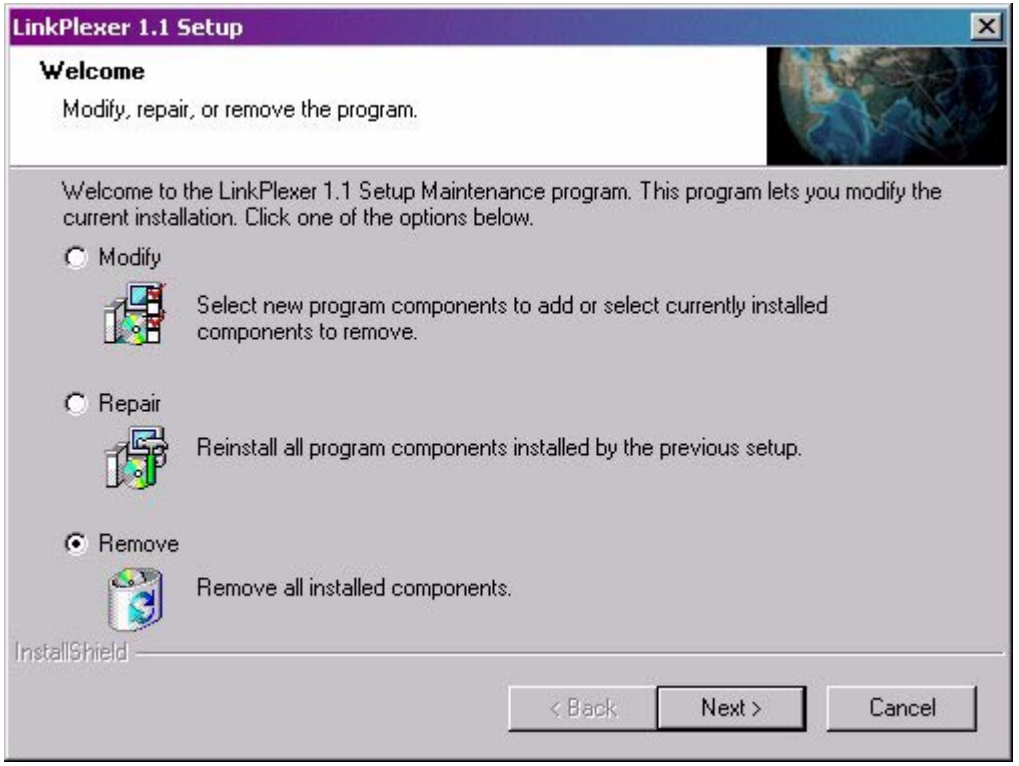
   LinkPlexer 1.1 is removed from the system

To uninstall LinkPlexer 1.1 using the LinkPlexer Setup program:

1. Close all running applications and close all open windows on the desktop.
2. Insert the LinkPLexer 1.1 CD into the CD-ROM drive.
3. Navigate to the CD-ROM drive, via the My Computer icon on the desktop.
4. Double click the Setup icon.

   Figure 16 shows the Modify, repair, or remove the program dialog box.

Figure 16 Modify, repair, or remove the program



5 Select the Remove radio button, and click Next.

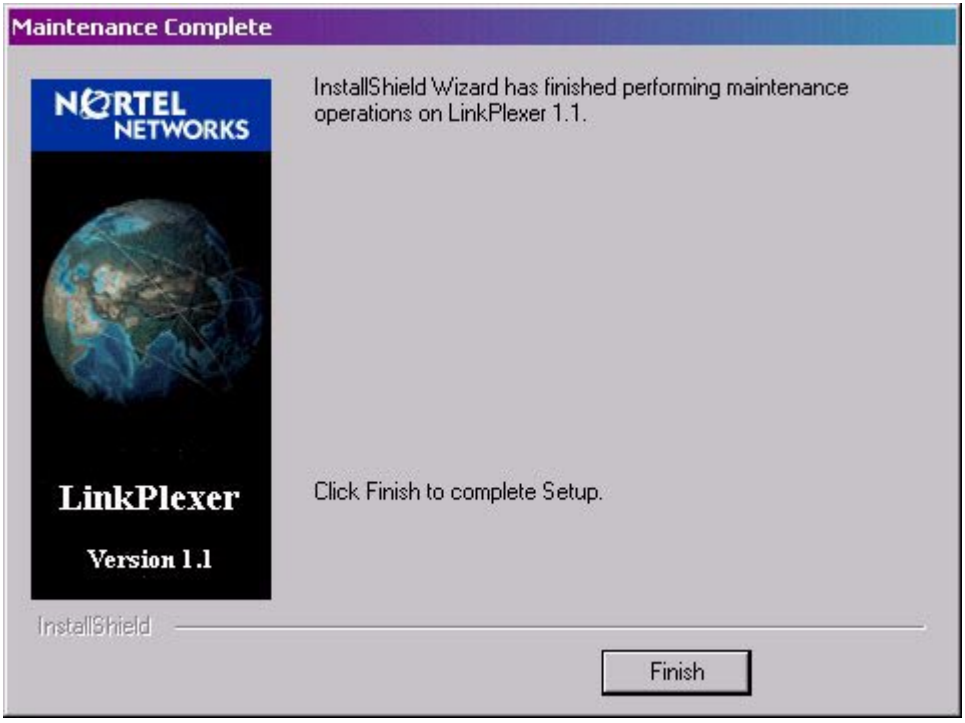
Figure 17 shows the Confirm File Deletion dialog box.

Figure 17 Confirm File Deletion

6 Click OK.

Figure 18 shows the Maintenance Complete dialog box.

Figure 18 Maintenance Complete



7 Click Finish.

The LinkPlexer 1.1 application is removed from the system.

Chapter 4
Configuring LinkPlexer

This chapter contains information on the following topics:

INI configuration files

The INI configuration files specify the information needed to run LinkPlexer 1.1. The INI files are described in the following sections:

DMSLocal.ini

The DMSLocal.ini file must be present and it must be located on the same machine as the LinkPlexer 1.1 application.

If a ServerAddress is not specified in the DMSLocal.ini file, the LinkPlexer 1.1 application uses the values specified in the local DMSGlobal.ini file.

The LinkPlexer 1.1 machine must contain both the DMSLocal.ini and DMSGlobal.ini files. Table 1 describes the DMSLocal.ini file parameters.

Table 1 DMSLocal.ini [configuration] section parameter descriptions

Parameter	Value type	Description
ServerAddress (not required)	IP address in dotted decimal notation:port number. For example: 127.0.0.1:2500	This is an optional parameter. Nortel Networks recommends that this parameter be left blank. This parameter specifies the location of the Primary Server (LinkPlexer 1.1). The DMSGlobal.ini is located on this server.
Standalone	TRUE or FALSE (default is FALSE)	This parameters value must be set to FALSE or remove it completely from the DMSLocal.ini file.
ApplicationID	Integer	This is the unique ID for this LinkPlexer. This parameter specifies which configuration information to use from the DMSGlobal.ini file. A value must be specified for this parameter. This should be set to 12 for the SCCS

Figure 19 Default Content of DMSLocal.ini

```
[Configuration]
Standalone=FALSE
ApplicationID=2
```

DMSGlobal.ini

The DMSGlobal.ini file is a global configuration file. It is used to configure the common system wide parameters for LinkPlexer 1.1. This file must exist on the same machine as LinkPlexer 1.1 and the DMSLocal.ini file.

The number specified as the Call Centre Group Number in the Queue-Status section of the DMSGlobal.ini represents the ACD Queue or set of DNs that will be monitored. Table 2describes the sections and parameters in the DMSGlobal.ini file.

Table 2 DMSGlobal section and parameter descriptions

Section/ Parameter	Value Type	Description
[Common]		This section contains common parameters for all applications.
RequestTimeout	integer (optional)	Specifies the timeout value (in milliseconds) for network messages. The default value is 1000 ms.
TraceLevel	0..3 (optional)	Specifies the function tracing level. 0 – Tracing off (default) 1 – Trace major functions 2 – Trace major and minor functions 3 – Trace all functions
AgentPingTest	ON or OFF	If Agent pinging is enabled all servers/machines running active LinkPlexer agents (SCCS, TAPI etc.) are pinged at the configured time interval. Any agent machines that don't respond to the ping in a timely fashion have their connections to LinkPlexer disconnected and the agent licence becomes available. Default setting is OFF
AgentPingTestInterval	integer (optional)	If AgentPingTest is ON this determines the interval at which the agents connected to LinkPlexer will be pinged.
AgentContinuityTest	ON or OFF	Everytime LinkPlexer receives a Continuity Test message from the DMS the AgentContinuityTest configuration entry is read and the appropriate action is taken depending on whether it is set or not. The log file DMSError1.log contains information about the operation of Agent COntinuity testing.
hexTraceLevel	0 or 1	Specifies whether or not SCAI (hex) messages should be logged 0 – Tracing off (default) 1 – Tracing on
[Switch-n]		The variable n must match the ApplicationID parameter, in the DMSLocal.ini file
DNAssociateFilter	On or Off'	Specifies wether DN Associate requests from client applications are filtered. Setting to 'Off' allows client applications such as SCCS or TAPI Server to associate their own DNs.
Type	DMS or DMSX25 (required)	Specifies the type of switch/server. Currently only DMS and DMSX25 are supported.

Table 2 DMSGlobal section and parameter descriptions (continued)

ListenerAddress	IP address (required)	IP address of the machine where the server resides. This must also be defined in DMS/MSL-100in IPADDR in table SCAICOMS.
ListenerPort	integer (required)	Port which the server listens on for connection requests from a secondary application.This must be set to 2500 when SCCS is being used by the call centre.
DMSAddress	IP address: integer (required) Called DNA, Calling DNA:1	IP address and port of the DMS/MSL-100 which this server connects to (defined in DMS/MSL-100 in CMIPADDR in table IPNETWRK). Specified using standard method (address:port) i.e. 127.0.0.1:2500 This formatting will also apply to X.25 addressing i.e. 11111111, 12345678:1
SessionPort	integer (optional)	If specified, then the Link Router waits for a connection from a primary application. NOTE: the following parameters (i.e. NetID ate. al.) are necessary only if SessionPort is not set.
Continuity	integer (optional)	If a SessionPort is NOT specified AND this value is specified, then this value is the interval in seconds for the internal session manager to do continuity tests. If not specified, then no testing is done. NOTE: minimum interval is same as RequestTimeout (in seconds).
NetID	integer	Network Node ID (defined in DMS/MSL-100 in NETNODID of table SCAIGRP).
ServiceID	integer	Service ID (defined in DMS/MSL-100 in PROFKEY.LINKSET.SRVCID of table SCAIPROF).
ServiceVer	integer	Service Version of the DMS/MSL-100 to be used (provided by DMS/MSL-100 Administrator).This should be 12.
BusGrpID	integer	Business Group ID (defined in DMS/MSL-100 in BGID in table BGDATA and ECM option in table CUSTNTWK).
Password	integer	ICM Link login password (defined in DMS/MSL-100 in PASSWORD in table SCAIGRP). This must be entered in capital letters.
LinksetName	integer	Linkset Name (defined in DMS/MSL-100 in LINKSET in table SCAICOMS). This must be entered in capital letters.
DN Digits (1 line per DN)	[ACD_DN, SDN]	Specifies a DN to associate, and the type of association required. This should also include the CDN.
[Queue Status]		Use this section to define queue information and estimated wait time.

Figure 20 Default Content of DMSGlobal.ini

```
[Common]

RequestTimeout=5000
TraceLevel=0
```

```
hexTraceLevel=0
AgentPingTest=OFF
AgentPingInterval=60
AgentContinuityTest=ON


[Switch-2]
Type=DMS
ListenerAddress=127.0.0.1
ListenerPort=4000
;SessionPort=2700
Continuity=120
DMSAddress=127.0.0.1:2500
DnAssocFilter=OFF
NetID=1
ServiceID=11
ServiceVer=11
BusGrpID=2
Password=RT1000
LinksetName=TAPITEST
;4168437000=ACD_DN
;4168438000=ACD_DN
;4166432613=SDN

[Queue-Status]
;0=4168437000:60
;1=4168438000
;DefaultCallTime=60
```

Note: Any changes that are made to DMSGlobal.ini and DMSLocal.ini parameters require a LinkPlexer 1.1 service restart. The AgentPingTest, AgentPingTestInterval and AgentContinuityTest parameters are the only parameters that are dynamic i.e. do not require a LinkPlexer service restart when changed.

X.25 configuration

Chapter 6, “Installing and configuring the Eicon X.25 card,” on page 81 describes how to install and configure the Eicon X.25 card.

To specify X.25 as the protocol that LinkPlexer 1.1 uses to communicate with the DMS/MSL-100 switch:

1. Ensure that the DMS/MSL-100 datafill specifies the correct setup information for the X.25 link.

   For more information, see “Configuring the DMS/MSL-100 switch” on page 56.

2. Configure the parameters in the [Switch-n] section of the DMSGlobal.ini file:

   a. Set the Type parameter to DMSX25.

   b. Ensure that the DMSAddress parameter contains the necessary X.25 information to connect to the DMS/MSL-100 i.e. the Calling DNA (in table SCAICOMS), the Called DNA (in SVCDNA in table MPCLINK), and the port number.

      This information is specified in DMSGlobal.ini as follows:

      ```
      DMSAddress=[Calling DNA],[Called DNA]:[port number]
      ```

      For example:

      ```
      DMSAddress=111111111,111222333:2500
      ```

3. Use the error log files to verify that the X.25 connection is established correctly when LinkPlexer 1.1 is started.

TCP/IP Connections

To specify TCP/IP as the protocol that LinkPlexer 1.1 uses to communicate with the DMS/MSL-100 switch:

1. Ensure that the DMS/MSL-100 switch datafill specifies the correct setup information for the TCP/IP link.

2. Configure parameters in the [Switch-n] section of the DMSGlobal.ini file:

a Set the Type parameter to DMS.

b Ensure that the DMSAddress parameter contains the necessary TCP/IP information to connect to the DMS/MSL-100 i.e. the IP address and port of the DMS/MSL-100 which this server connects to (defined in the CMIPADDR parameter in the IPNETWRK table).

This information is specified in DMSGlobal.ini as follows:

```
DMSAddress= IP Address:Port
```

For example:

```
DMSAddress=123.4.5.6:2500
```

3 Use the error log files to verify that the TCP/IP connection is established correctly when LinkPlexer 1.1 is started.

LinkPlexer Configurations

There are three possible configurations for LinkPlexer 1.1 software. However, the configuration which allows the setup of one of the applications as the session controller is not considered for implementation.The restart procedures for both options is found in chapter 7 under “Startup Procedures for Nortel Networks Call Centre Equipment” on page 107

Option 1 “Pass Through”

The first configuration is LinkPlexer 1.1 setup as a pass through software. This configuration allows for multiple applications to talk to and acquire switch resources through LinkPlexer 1.1. The DMSGlobal.ini file (“DMSLocal.ini” on page 49) will only be datafilled with the switch connection information and no CDN’s (Control Directory Number), ACD queues or SDN’s (Secondary Directory Number). DN associate filter is also set to OFF.

With LinkPlexer set up in such a manner, it enables the end customer to add and change information about a line, queue or CDN without having to restart the software. As the information about any of the switch resources can be affected by another application, the restart procedures and the time required to recover from a planned or unplanned outage should be considered.

Option 2 “Filtered”

The second configuration involves using LinkPlexer with all of the CDN’s. ACD queues and SDN’s datafilled in the DMSGlobal.ini and DN Associate filter set to ON. In this configuration, all of the switch resources are registered when the LinkPlexer software is started.

The applications may send registration messages to LinkPlexer for the switch resources, but the applications will be given a positive response to the request. The positive response will be sent regardless of whether the device is actually associated on the switch. This is a function of the DN Associate filter being ON - all messages about the resources are filtered out by LInkplexer 1.1

When using this option, new CDN’s, ACD queues and SDN’s need to be added to the DMSGlobal.ini file and LinkPlexer restarted in order to ensure successful registration. As a result of this, other LinkPlexer client applications will not function during the time that LinkPlexer is down.

Another consideration is that the restart of the other applications is dependent on LinkPlexer starting first. This is due to the fact that LinkPlexer is completing the registration of all of the switch resources. If a new number is added to the SCCS or ICM TAPI database, while in this configuration, the administrator of the SCCS or TAPI packages will see the resource successfully acquired. However, since the message is filtered in LinkPlexer, the resource has not actually been acquired in the switch.

Configuring the DMS/MSL-100 switch

To configure the DMS/MSL-100 switch the ACD groups information must be specified. The required information is specified in the DMS/MSL-100 Switch tables by the administrator of the DMS/MSL-100 switch. Definitions, and examples, of these are found in Appendix B page 122.

Configuring SCCS to use LinkPlexer 1.1

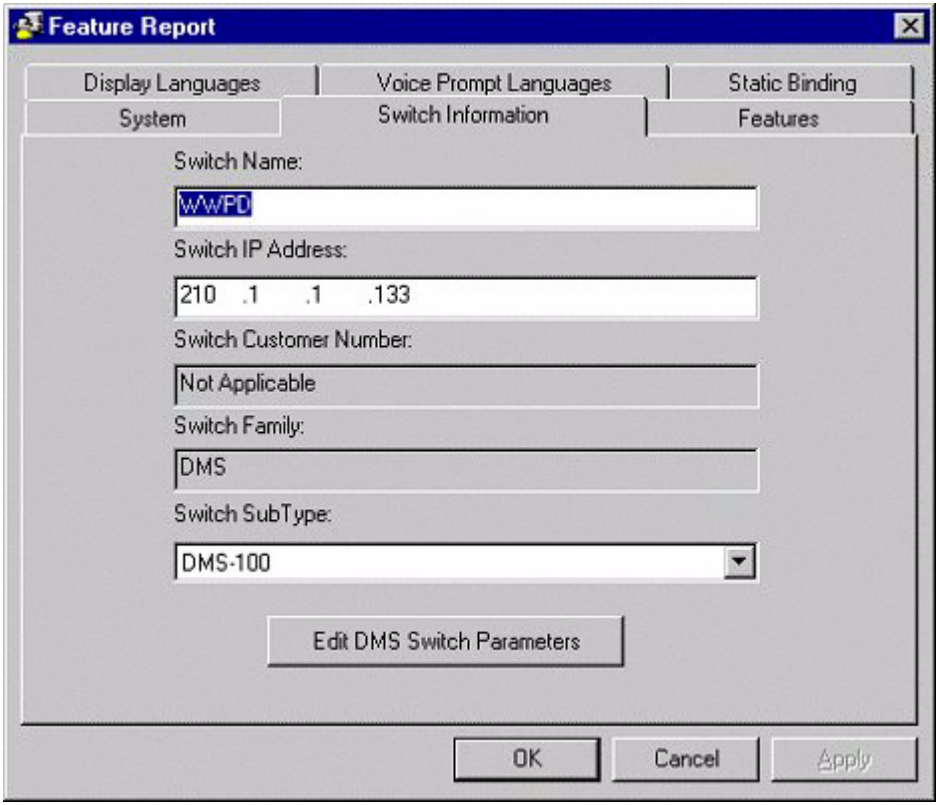
To configure the SCCS to use the LinkPlexer 1.1 application:

1 From the SMI window, choose System Administration>System Configuration>Server Settings.

The Feature Report dialog box is displayed.

2 Select the Switch Information tab. Figure 21 shows the Switch Information tab dialog box.

Figure 21 Feature Report Switch Information dialog box



3 In the Switch Name text box, type the name of the switch.

4 In the Switch IP Address text box, type the IP address of the LinkPlexer 1.1 ListenerAddress.

The IP address of the LinkPlexer 1.1 is defined by the ListenerAddress parameter in the DMSGlobal.ini file and by the IPADDR parameter in the DMS/MSL-100 switch SCAICOMS table.

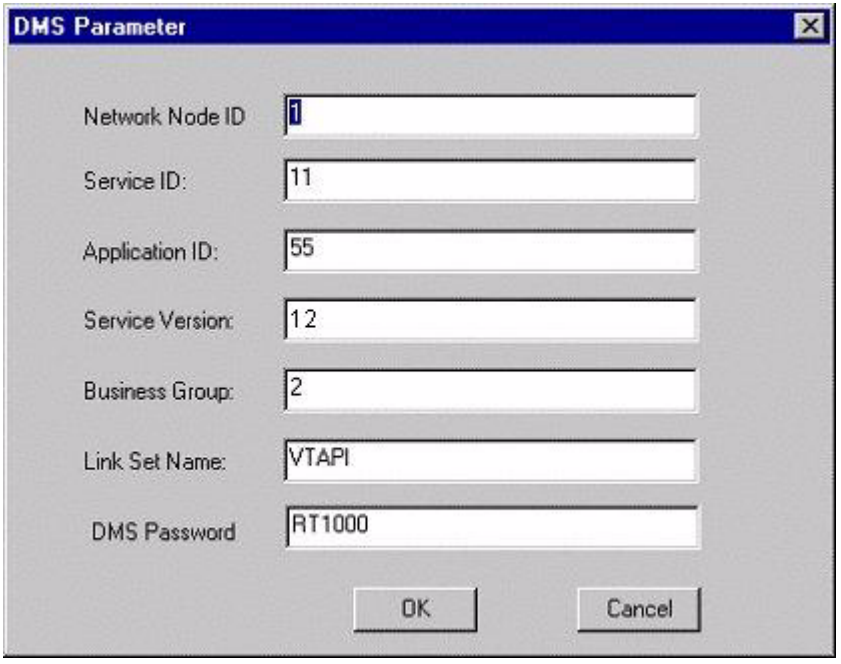
SCCS assumes the port number is 2500.

5 In the Switch Sub Type text box, select DMS-100 from the pull-down menu.

6 Click on the Edit DMS Switch Parameters button.

The DMS Parameter dialog box is displayed. Figure 22 shows the DMS Parameter dialog box.

Figure 22 DMS/MSL-100 Parameter dialog box



7 Set the parameters in the DMS/MSL-100 Parameter dialog box to match the settings in the DMSGlobal.ini file, the DMSLocal.ini file, and the DSM/MSL-100 Switch tables.

Table 3 shows the location of the parameter values.

Table 3 DMS/MSL-100 Parameter value locations

Parameter	INI file and Parameter	DMS/MSL Switch table and parameter
Network Node ID	DMSGlobal.ini file, NetID parameter	SCAIGRP table, NETNODID parameter
Service ID	DMSGlobal.ini file, ServiceID parameter	SCAIPROF table, PROFKEY.LINKSET.SRVCID parameter

Table 3 DMS/MSL-100 Parameter value locations

Parameter	INI file and Parameter	DMS/MSL Switch table and parameter
ApplicationID	DMSLocal.ini file, ApplicationID parameter	
Service Version	DMSGlobal.ini file, ServiceVer parameter	Provided by the DMS/MSL-100 Switch administrator
Business Group	DMSGlobal.ini file, BusGrpID parameter	BGDATA table, BGID parameter CUSTNTWK table, ECM parameter
LinkSet Name	DMSGlobal.ini file, LinksetName parameter	SCAICOMS table, LINKSET parameter
DMS Password	DMSGlobal.ini file, Password parameter	SCAIGRP table, PASSWORD parameter

8 Click OK to close the DMS Parameter dialog box.

9 Click OK to close the Feature Report dialog box.

For more information, including information about the relationships between fields and tuples (parameters and values) in the DMS/MSL-100 switch tables, see the *Nortel Networks Symposium Call Center Server and DMS Switch Guide,* part number 911815.

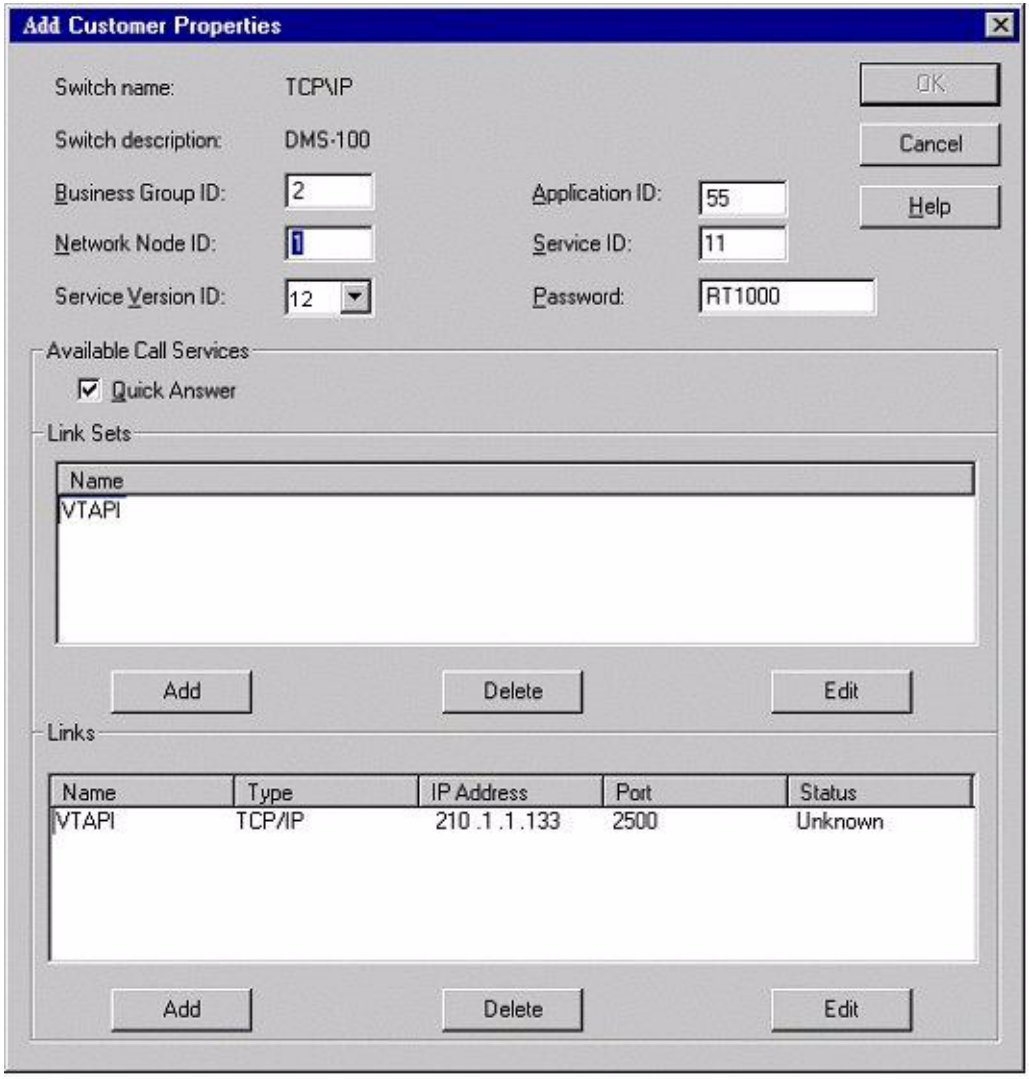
Configuring the ICM TAPI Driver to use LinkPlexer 1.1

To configure the ICM TAPI driver (on the ICM TAPI server) to use the LinkPlexer 1.1 application:

1 Open the Add Customer Properties dialog box.

Figure 23 shows the Add Customer Dialog box.

Figure 23 Add Customer Properties dialog box



2 Set the parameters in the Add Customer Properties dialog box to match the settings in the DMSGlobal.ini file, the DMSLocal.ini file, and the DMS/MSL-100 Switch tables.

Table 4 shows the location of the parameter values.

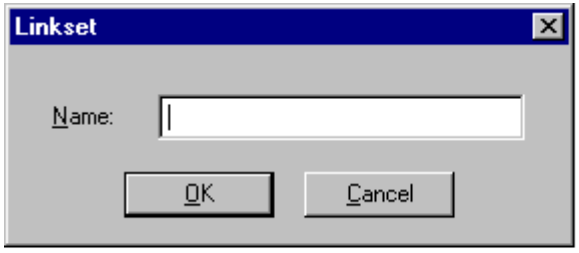
Table 4 DMS/MSL-100 Parameter locations

Parameter	INI file and parameter	DMS/MSL Switch table and parameter
Network Node ID	DMSGlobal.ini file, NetID parameter	SCAIGRP table, NETNODID parameter
Service ID	DMSGlobal.ini file, ServiceID parameter	SCAIPROF table, PROFKEY.LINKSET.SRVCID parameter
Application ID	DMSLocal.ini file, ApplicationID parameter	
Service Version ID	DMSGlobal.ini file, ServiceVer parameter	Provided by the DMS/MSL-100 Switch administrator
Business Group ID	DMSGlobal.ini file, BusGrpID parameter	BGDATA table, BGID parameter CUSTNTWK table, ECM parameter
LinkSet Name	DMSGlobal.ini file, LinksetName parameter	SCAICOMS table, LINKSET parameter
Password	DMSGlobal.ini file, Password parameter	SCAIGRP table, PASSWORD parameter

3 In the Link Sets section of the Add Customer Properties dialog box, click Add.

The Add Link Sets dialog box is displayed as in.

Figure 24 Link Set Dialog box



4 Type the Link Set name for this link set.

The link set name is defined by the LinksetName parameter in the DMSGlobal.ini file, and by the LINKSET parameter in the DMS/MSL-100 switch SCAICOMS table.

5 In the Name text box, type the name of this link.

6 In the Type pull-down menu, select TCP/IP.

Select TCP/IP, even if LinkPlexer 1.1 uses an X.25 connection to the switch.

7 In the IP Address text box, type the IP address of the LinkPlexer 1.1 Listener Address.

The IP address of the LinkPlexer 1.1 is defined by the ListenerAddress parameter in the DMSGlobal.ini file and by the IPADDR parameter in the DMS/MSL-100 switch SCAICOMS table.

8 In the Port text box, type the port number, 2500.

9 To close the Add Customer Properties dialog box, click OK.

For more information on configuring the ICM TAPI drivers, refer to ICM TAPI Network Managers Guide (part number PO881940).

Configuring Periphonics VPS/IS (Peri-ICM) to use LinkPlexer

To configure a Peri-ICM package on a Link Server for use with LinkPlexer 1.1 the PBX Link Connection must be configured.

1 Locate the `hosts` file in C:\WINNT\system32\drivers\etc\hosts on the Peri-ICM server.

2 The `hosts` file must be edited by adding the PBX Link IP address using the PBX Configuration Edits, for example: `192.84.161.227 pbxlink`

3 For DMS100 connection with PERI-ICM, SCCS and/or TAPI server, add the LinkPlexer's (CLAN) IP address as `pbxlink` in the `hosts` file.

For more information on configuring the Peri-ICM package, refer to the MPS and VPS/is interface to M1/DMS100 (peri-IPML v2.0, Peri-ICM v2.0) document (part number P0988599).

Chapter 5
Installing and configuring pcAnywhere

One copy of pcAnywhere version 9.2 is provided for the LinkPlexer 1.1 server. The installer application is located in the ThirdParty folder on the LinkPlexer 1.1 CD.

In the case of co-residency with TAPI, a modem is not supported and the TAPI guidelines, found in the ICM TAPI Network Managers Guide (part number PO881940), must be followed. Chapter 5 Additional Tools, of the ICM TAPI Network Managers Guide contains a section on pcAnywhere configuration.

This chapter contains the following sections:

Before Installation

pcAnywhere should be installed before installing the LinkPlexer 1.1 software.

The following system requirements are necessary for pcAnywhere operation:

- 486 or higher microprocessor
- 16MB RAM
- VGA or higher resolution display adapter
- Hard disk drive, one CD-ROM drive
- At least 32MB free disk spacer

Installing pcAnywhere version 9.2

To install pcAnywhere version 9.2

1. Log on to the server as Administrator.
2. Shut down all running applications
3. Insert the LinkPlexer 1.1 CD into the CD-ROM drive.
4. In Windows Explorer, navigate to the E:\ThirdParty\pcAnywhere_v9.2\Disk 1 folder (where E: is the CD-ROM drive).
5. Double click the Setup.exe file.

   The Symantec installation wizard window is displayed.
6. Click Next.

   The License agreement is displayed.
7. Select I accept the terms, then click Next.

   The Customer Information window is displayed.
8. Type the User Name and Organization name, then click Next.

   The Setup Type window is displayed.
9. Select Typical, then click Next

   The Ready to Install window is displayed
10. Click Install. Wait until the setup is complete.

    The Support Solutions window is displayed.
11. Click Next.

    The Windows Solutions window is displayed.
12. Click Next.

    The How to Reach Symantec Online Information window is displayed.
13. Click Next

    The Some Additional Options window is displayed.
14. Clear all the check boxes, then click Next.

    The Registration window for pcAnywhere is displayed.

15 Click Skip.

The confirmation prompt is displayed.

16 Click Yes.

The `Symantec pcAnywhere successfully installed` message is displayed.

17 Click Finish

The user is prompted to restart the server.

Updating the MS Windows NT registry

To avoid problems during the pcAnywhere operation on multi-processor systems, an entry in the MS Windows NT registry must be added.

1 Click No (restart the server later).

2 In the MS Windows NT Explorer, navigate to the E:\ThirdParty\pcAnywhere_v9.2\Disk 1 (where E is the CD-ROM drive).

3 Double-click the AddProcMask.reg file.

A message is displayed, indicating that the information in the file has been successfully entered into the registry.

4 Click OK.

5 Remove the CD from the CD-ROM drive.

6 Choose Shutdown from the MS Windows NT Start menu.

The Shut Down Windows dialog box is displayed

7 Select Restart from the pull-down menu.

8 Click OK.

The server PC restarts. If the server hangs, restart it manually.

Configuring pcAnywhere

Administrator privileges on the server PC are necessary to configure pcAnywhere.

This section contains the following topics:

Password recommendations

Plan the passwords required for the user accounts. Use the same passwords for the pcAnywhere caller passwords that are planned for use with the Windows NT accounts. This simplifies the remote logon process.

To maintain remote access security, change the passwords for the caller accounts regularly. Continue to match the pcAnywhere caller passwords to the Windows NT user account passwords.

For more information on resetting caller account passwords, See “Changing pcAnywhere caller passwords” on page 70.

Starting pcAnywhere for the first time

To start pcAnywhere for the first time:

1. Log on to MS Windows NT as Administrator.
2. From the Windows Start menu choose Programs>Symantec>pcAnywhere.
3. If asked to register pcAnywhere, select Skip, and then choose Yes when asked to confirm.

   The Smart Setup Wizard window is displayed.

   The system prompts for the modem device.
4. Choose the entry that matches the modem in use, then click Next. Note, if the driver supplied by the modem vendor is not listed, then it must be installed.

The system prompts for network device selection.

5 Ensure that only TCP/IP is selected, then click Next.

The system prompts for port selection.

6 Select COM1, then click Next.

7 Click Finish.

The pcAnywhere main window is displayed.

Changing User access rights

If during pcAnywhere configuration, a message is received indicating that the user does not have the rights to modify a setting or create a new caller, the user must change the Windows NT User access rights for pcAnywhere files.

To change the Windows NT User access rights for pcAnywhere files:

1 Ensure that pcAnywhere is not running.

2 Navigate to %Systemroot%Profiles\All Users\Application Data\Symantec.

3 Select the pcAnywhere directory.

4 Right-click the directory icon, choose Properties, and then click the Security tab.

5 Click on Permissions and, for Administrators, select Type of Access: Full Control.

6 Click OK to save changes.

7 Click OK to close the Properties window.

Setting the video mode

To set the pcAnywhere video mode:

1 Open pcAnywhere.

2 Choose Tools>Application Options.

3 Click the Host Operation tab.

4 For Video mode, ensure that the option selected in the drop-down list is Default.

5 Click Apply to save the changes.

6 Click OK to exit.

Configuring pcAnywhere host PC network properties

To configure pcAnywhere network properties on a host PC:

1 Log on to Windows NT as Administrator.

2 From the Windows Start menu, choose Programs>Symantec pcAnywhere.

pcAnywhere starts.

3 Select Be a Host PC.

4 Select the Network icon.

Do not double-click the icon or a pcAnywhere session will begin.

5 From the File menu, choose Properties.

The NETWORK Properties window is displayed.

6 Select a tab window to view the network property options. For information on configuring tab window properties refer to the following sections:

- “Configuring connection information” , next
- “Configuring settings” on page 69
- “Configuring callers” on page 70
- “Setting security options” on page 73
- “Setting Conference options” on page 74
- “Password controlling network configuration” on page 75

7 When all the settings in the NETWORK Properties tab windows have been configured, click OK to save the settings and close the window.

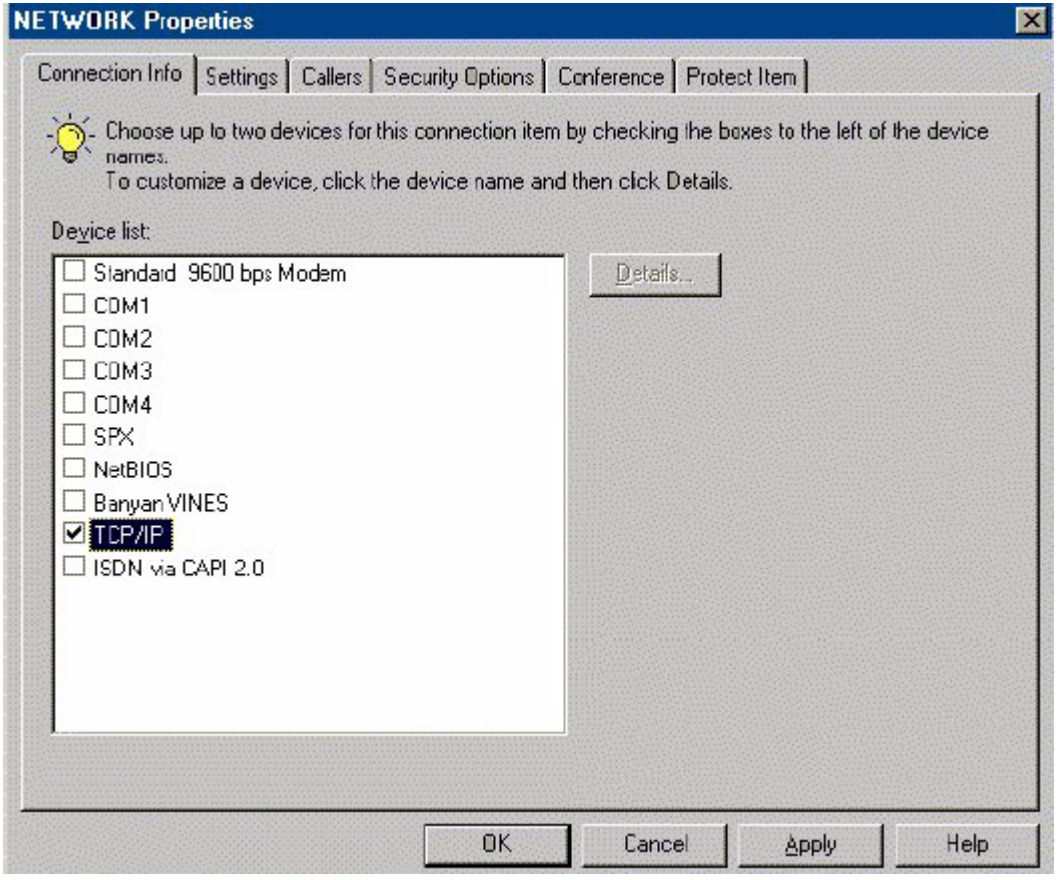
Configuring connection information

To configure network connection settings:

1 Click the Connection Info tab.

Figure 25 shows the NETWORK Properties Connection Info tab window.

Figure 25 NETWORK Properties Connection Info tab window



2 Ensure that only TCP/IP is checked.

3 Click Apply to save changes.

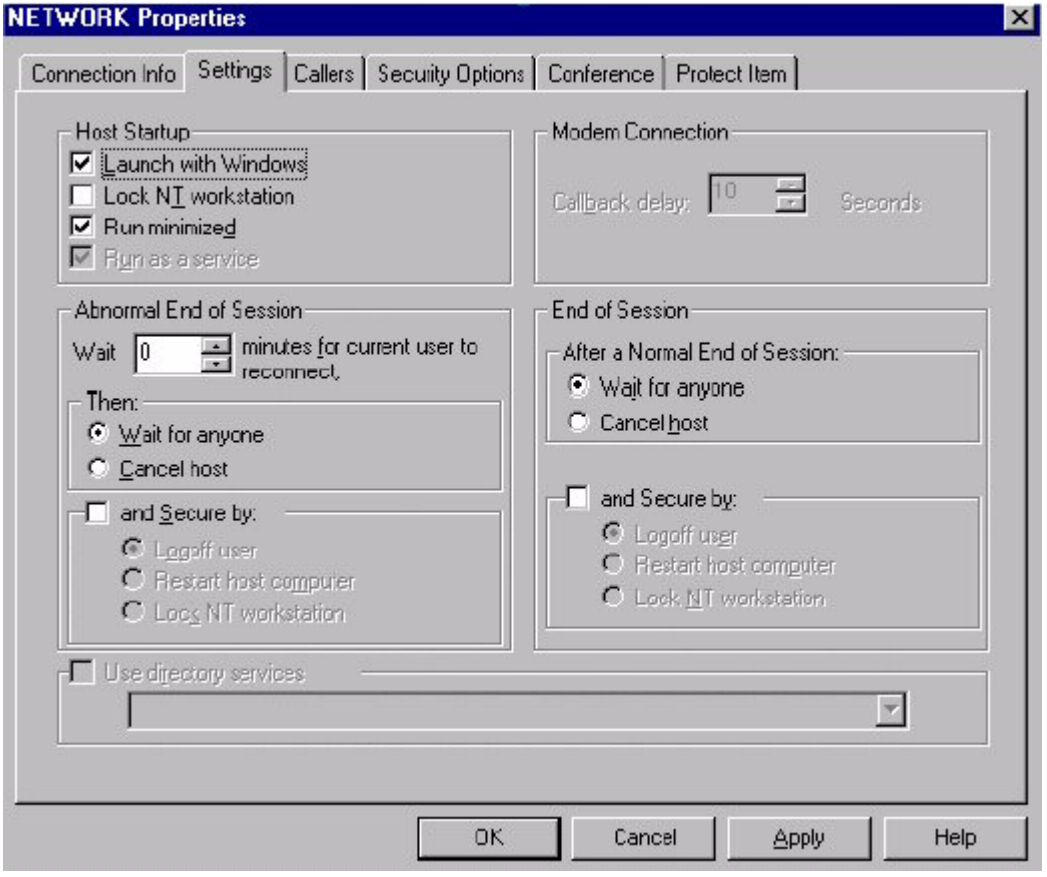
Configuring settings

To configure the network settings:

1 Click the Settings tab.

Figure 26 displays the NETWORK Properties Settings tab window.

Figure 26 NETWORK Properties Settings tab window



2 Ensure that the settings match those shown in Figure 26.

3 Click Apply to save changes.

Configuring callers

To allow remote users to connect to the LinkPlexer 1.1 server PC caller accounts must be configured. If creating an account to allow remote administration of LinkPlexer 1.1, then at least one account will full administrator access must be created.

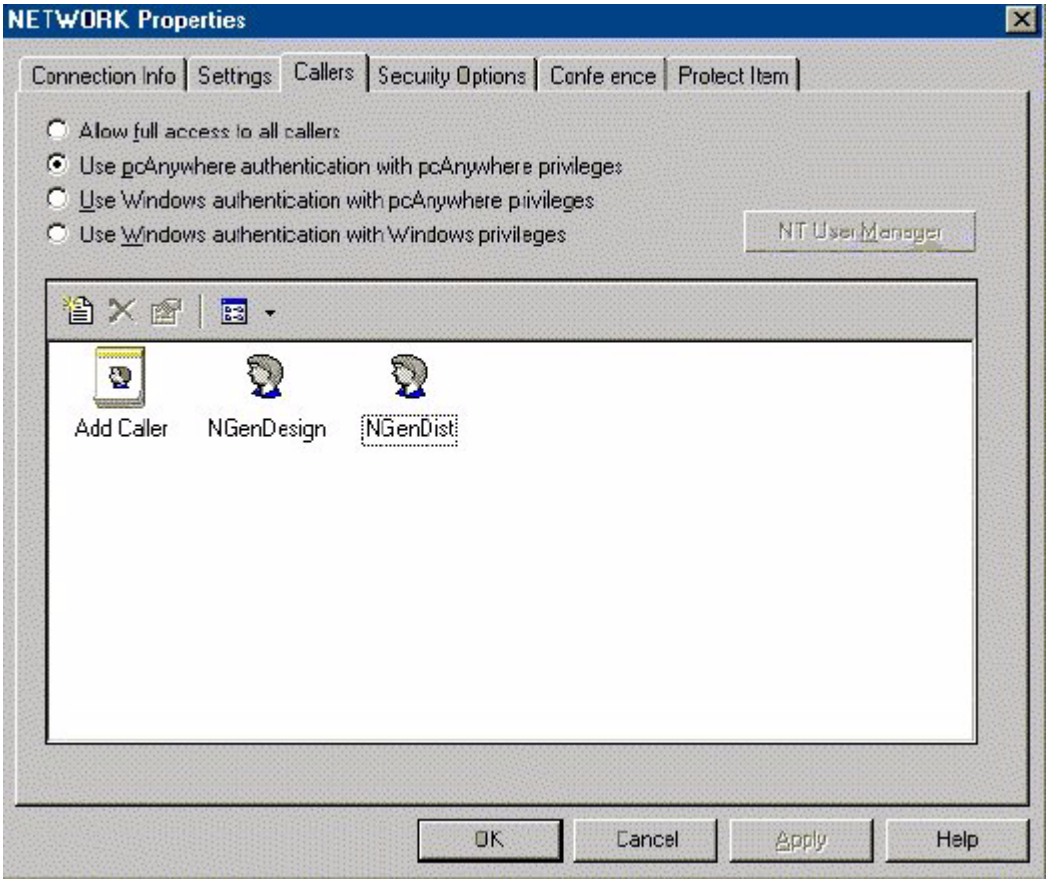
This section describes how to create and configure two remote users, NGenDist and NGenDesign. The suggested passwords and login names are for example purposes only. Passwords and login names should be configured to match the Windows NT user accounts on the LinkPlexer server PC.

To configure caller accounts:

1 Click the Callers tab.

Figure 27 shows the NETWORK Properties Callers tab window.

Figure 27 NETWORK Properties Callers tab window



2 Select the Use pcAnywhere authentication with pcAnywhere privileges radio button.

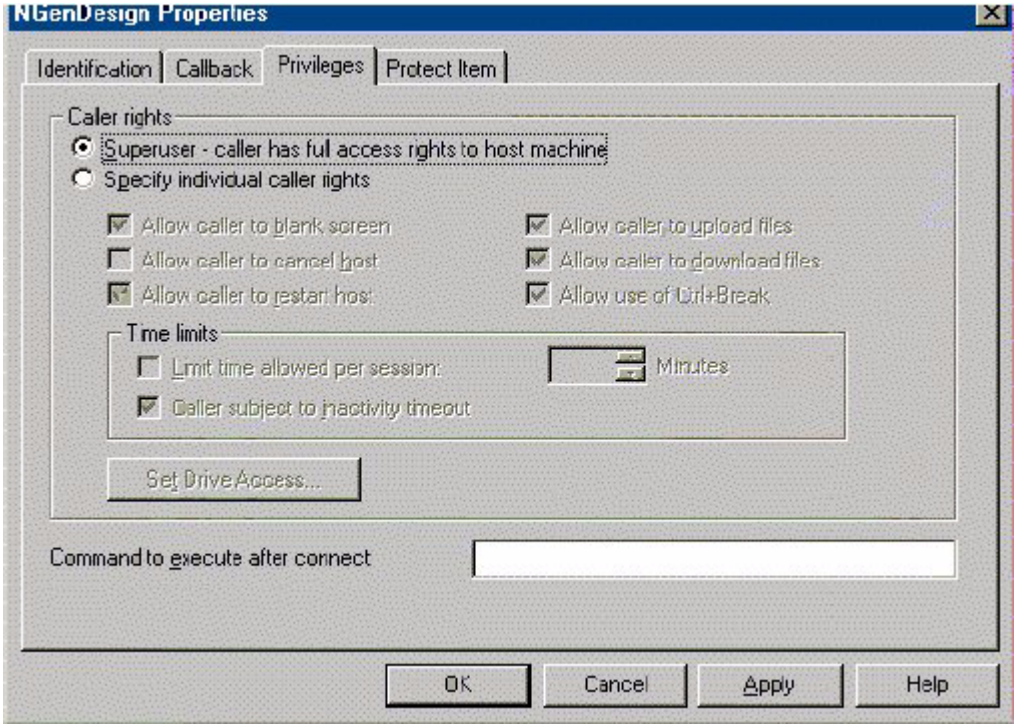
3. Place the mouse in the blank area and right-click to display the properties dialog box.
4. Select New to add a new caller.

   The New Caller Properties window is displayed.
5. Type the Login name **NGenDist** and the password **ntdist**.
6. In the Confirm Password box, retype the password.
7. Click OK to save the changes.

   The Callers tab window is displayed.
8. Right-click the NewCaller icon, select rename, and type **NGenDist**.
9. Repeat steps 3 to 8 to create the **NGenDesign** caller, using the password **Nortel**.
10. Right-click the NGenDesign caller icon, and then select Properties.
11. Click the Privileges tab.

    Figure 28 shows the NGenDesign Properties Privileges tab window.

Figure 28 NGenDesign Properties Privileges tab window



12 Select the Superuser radio button.

13 Click Apply to save the changes.

14 Repeat steps 10 to 13 for the NGenDist caller.

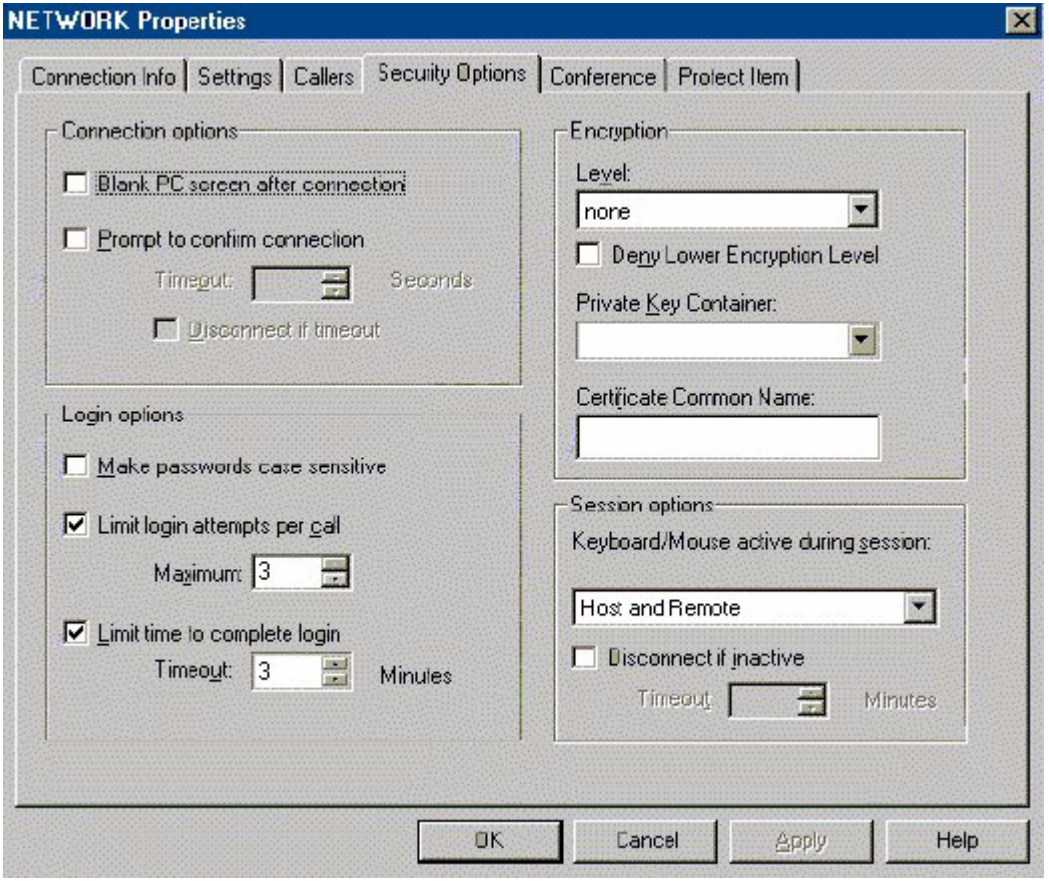
Setting security options

To configure security options:

1 Click the Security Options tab.

Figure 29 shows the NETWORK Properties Security Options tab window.

Figure 29 NETWORK Properties Security Options tab window



2 Ensure that the settings match those shown in Figure 29.

3 Click Apply to save changes.

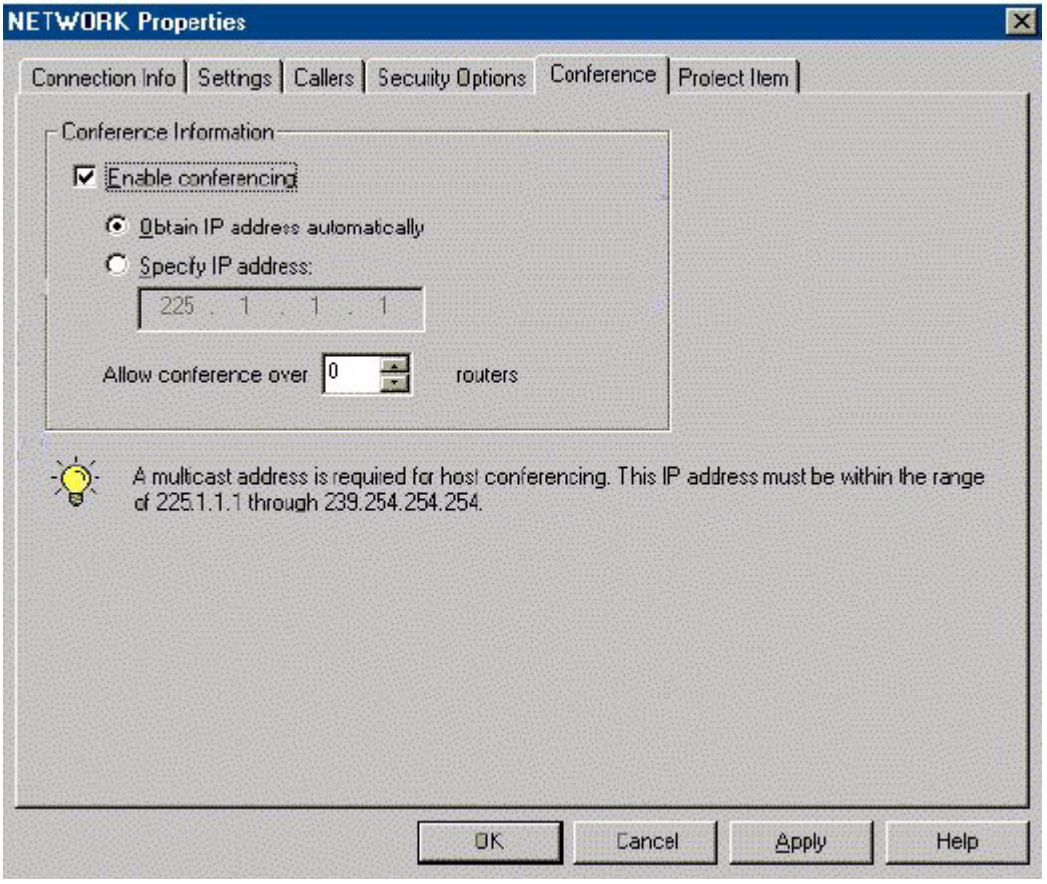
Setting Conference options

To configure conference options:

1 Click the Conference tab.

Figure 30 shows the NETWORK Properties Conference tab window.

Figure 30 NETWORK Properties Conference tab window



2 Ensure that Enable conferencing and Obtain IP address automatically are selected.

3 Click Apply to save changes.

Password controlling network configuration

To control access to network configuration options:

1 Click the Protect Item tab.

2 To assign a password to control who can modify the Network icon settings, enter a password on this screen.

3 Click Apply to save changes.

Caution: If the option Required is selected in order to modify properties, the password must be entered each time a setting is changed. The password should be recorded and a copy of it kept in a safe place. If the password is forgotten, non of the settings can be changed.

Changing pcAnywhere caller passwords

During the installation and configuration of pcAnywhere, login passwords for the NGenDist and NGenDesign callers are specified. To maintain system security, change these passwords periodically.

To simplify the remote login process, the same passwords for the pcAnywhere NGenDist and NGenDesign caller passwords should be used as those planned for use with the MS Windows NT NGenDist and NGenDesign accounts. Change the pcAnywhere caller passwords and the Windows NT user account passwords for NGenDist and NGenDesign at the same time.

For more information, See “Password recommendations” on page 66.

To change passwords:

1 Log on to Windows NT as Administrator.

2 From the Windows Start menu, choose Programs>Symantec pcAnywhere.

pcAnywhere starts

3 Select Be a Host PC.

4 Click Network.

Do not double-click the icon or a pcAnywhere session will begin.

5 From the File menu, choose Properties.

The NETWORK Properties property sheet appears.

6 Click the Callers tab.

7 Click Specify individual caller privileges.

8 Right-click the NGenDist icon and then select Properties.

9 Click the Identification tab.

10 In the Password text box, type a new NGenDist password.

11 In the Confirm Password text box, type the NGenDist password again.

12 Click Apply.

13 Click OK.

14 Right-click the NGenDesign icon. Then select Properties.

15 Repeat steps 8 to 13 to assign a new password to NGenDesign.

16 Click OK to return to the main pcAnywhere window.

17 Exit pcAnywhere.

Establishing a pcAnywhere dial-up connection

This section describes how to establish a pcAnywhere connection with the server using a dial-up connection. It contains information on the following topics:

- “Creating a server connection profile” , next
- “Creating a server connection profile” on page 77

Creating a server connection profile

To create a server connection profile for a MS Windows 95 or MS Windows 98 client PC:

1 From the Windows Start menu, choose Programs> Accessories>Dial-Up Networking or Programs>Accessories>Communication>Dial-Up Networking.

2 If no connections have been defined on this PC, the Make New Connection wizard is displayed.

3 If one or more connections have been created on the PC, click the Make New Connection icon in the Dial-Up Networking window to display the wizard.

4 Enter a name for the connection and select a modem.

5 Click Next.

6 Enter the server telephone number, and then click Next.

7 Click Finish.

Once the server connection profile has been created, the profile must be configured. For information on configuring a server connection profile, see “Configuring a server connection profile” , next

Configuring a server connection profile

To configure a LinkPlexer 1.1 server connection profile:

1 Right-click on the server connection profile icon, and then select Properties.

2 Verify the information on the General property page, and correct it if necessary.

3 Click Configure.

The Modem Properties window is displayed.

4 Update the properties as required. Click OK.

5 Click Server Types.

6 For Dial-Up Server, select PPP:Windows NT.

7 For the network protocols, select only TCP/IP and NETBEUI.

8 Click TCP/IP settings.

The TCP/IP Settings properties window is displayed.

9 Select Specify an IP address, and type the server IP address.

10 De-select Use default gateway on remote network.

11 The remaining boxes are optional. Fill them in as required for the customer’s network.

12 Click OK.

The connection properties window is displayed.

13 Click OK.

Uninstalling pcAnywhere 9.2

Before uninstalling pcAnywhere, ensure there is no pcAnywhere Waiting icon on the desktop. If the icon is on the desktop, right-click it and select Cancel Host.

1. From the Windows Start menu, choose Settings>Control Panel.
2. Double-click the Add/Remove Programs control panel.
3. Select Symantec pcAnywhere and click Add/Remove.

   The Symantec pcAnywhere Setup window is displayed.
4. Click Next.

   The Program Maintenance options window appears.
5. Select Remove and click Next.

   The Remove the Program window appears.
6. Click Remove.
7. When the process completes, click Finish.
8. From the Windows Start menu, choose Shutdown.

   The Shut Down Windows dialog box appears.
9. Select Restart, and then click Yes.

   The server shuts down and then begins starting up. If the system does not restart, it must be restarted manually.

Chapter 6
Installing and configuring the Eicon X.25 card

This chapter contains the following sections:

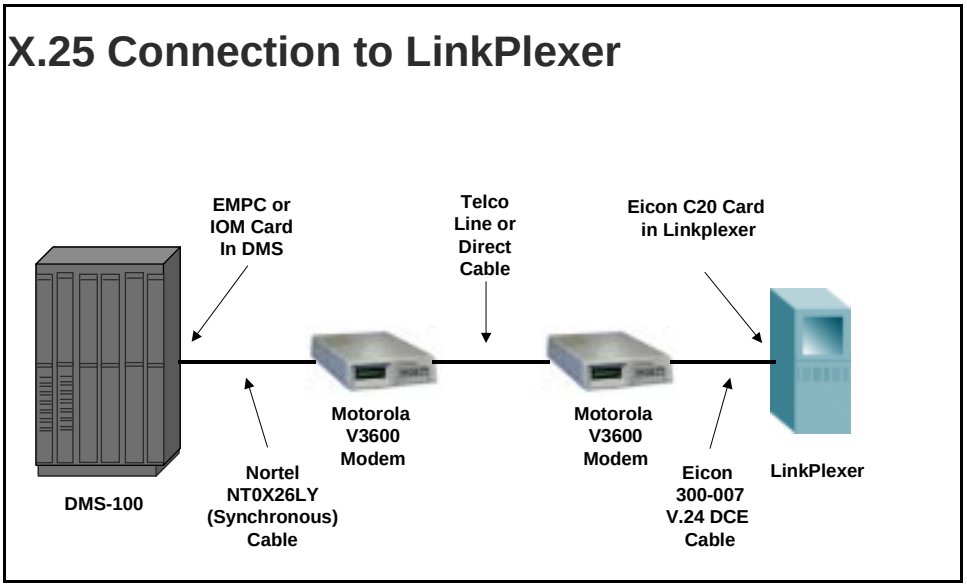
Supported configurations for X.25

There are 2 supported configurations for X.25:

- A direct connection using a modem eliminator (or null modem) for distances of 50 feet or less.
- A normal modem connection for distances greater than 50 feet.

Figure 31 shows the X.25 connection configuration to LinkPlexer 1.1.

Figure 31 Switch Connections



Note: The supported modem is the Motorola V.3600 modem. For further information on specifications and configuration refer to the V.3600 Modem User guide, a copy of which is located at http://www.arcelect.com/V3600_Modem_manual.htm. http://www.motorola.com may also be used for reference.

Installing the Eicon X.25 card

To install and configure the Eicon X.25 card:

1. Insert the Eicon Card (C20 or C90) into the slot in the computer. It is not necessary to change any settings on the card. Refer to the following website for detailed installation instructions http://www.eicon.com/worldwide/support/docs.htm?en_prod=Eiconcard_C20
2. Connect the Eicon Card and the modem using the V24 cable (db25 to db25).
3. Install the Driver:

a The driver for Windows NT 4.0 (c4wntv4r2c.exe) is available from the following website: http://www.eicon.com/cnnt/wanic/downld.htm

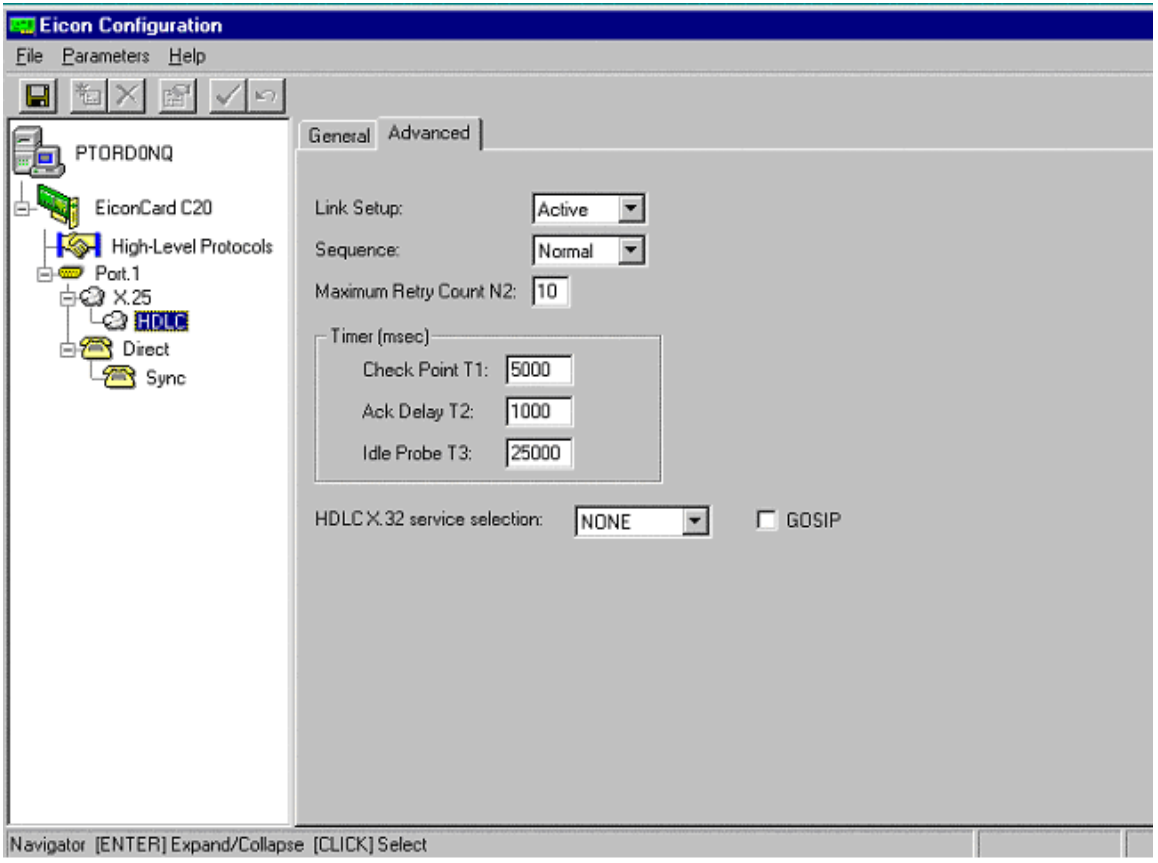
b Choose Add in the Network Adapter

c Choose Eicon Wan Adapters and select the location of the downloaded executable.

4 The Eicon card may be configured with the default values, except in the HDLC\Advanced tab which must use the values as in Figure 32. Appendix A on page 113 includes screenshots of the Eicon Configuration windows with appropriate values for LinkPlexer 1.1

Note: The 'Check Point T1' Timer in this dialog box must be changed to 5000mSec. The default timer in the DMS/MSL-100 is 5000ms and the Eicon default is 2900. Hence there will be a conflict if the timer is not changed to 5000mSec.

Figure 32 Eicon Configuration HDLC:Advanced



5 Choose Yes to install OEM Option

6 Add the Eicon Performance Counter

7 Restart the computer

Figure 33 shows an example of the TAPI Server parameters and DMS-100 Datafill values for X.25 connections.

Figure 33 Example TAPI Server parameters & DMS-100 Datafill

TAPI Server parameters and DMS-100 Datafill for X.25 Connection

Business Computer Parameters			DMS-100 Datafill		Message Type
Parameters Name	Value	Table	Field	Value	
Version of X.25	1980	MPC	DLDFILE	MPC003AC	
Version of X.25	1980	MPCLINK	PROTOCOL	X2580	
Two way SVC	1	MPCLINK	SVCS2WAY	1	
Called DNA (DMS)	2222222	MPCLINK	EXINFO.SVCDNA.DIGITS	2222222	X.25 CALL_REQUESTLAYER 1
Calling DNA (BC)	11111111	SCAICOMS	LINK_DEFINITION.REMDNA	11111111	X.25 CALL_REQUESTLAYER 1
Protocol (User Data)	0 0 0 0	SCAICOMS	PROTOCOL	0 0 0 0	X.25 CALL_REQUESTLAYER 1
Business Group ID	2	BGDATA	BGID	2	DV_APPL_LOGONLAYER 7
Password	TESTER	SCAIGRP	PASSWORD	TESTER	DV_APPL_LOGONLAYER 7
Network Node ID	25	SCAIGRP	NETNODID	25	DV_APPL_LOGONLAYER 7
Business Group ID	2	SCAIGRP	BGID	2	DV_APPL_LOGONLAYER 7
Service ID	1	SCAIPROF	PROFKEY.LINKSET.SRVCID	1	DV_APPL_LOGONLAYER 7
Service Version	8				DV_APPL_LOGONLAYER 7
Application ID	333				DV_APPL_LOGONLAYER 7

Chapter 7
Maintenance & Troubleshooting LinkPlexer

This section contains information on maintenance and troubleshooting common problems with LinkPlexer 1.1. It contains the following topics:

Common problems

Table 5 describes the solutions to some of the problems that can occur when running LinkPlexer 1.1.

Table 5 Common problems

Problem	Solution
LinkPlexer not running	Ensure that the LinkPlexer software has been installed, configured, and is running. Ensure that the dongle is connected and flagged as connected in the Keycode Tracker application. To check if LinkPlexer is running, access the drive where LinkPlexer is installed, and check the dmserror0.log. If LinkPlexer did not start correctly, this log file should contain a startup error such as “invalid IP address” or “X.25 error”. A pop-up message may appear when attempting to start LinkPlexer, indicating a problem.
DMS/MSL-100 is down... network problems	Ensure that all of the machines involved are up and communicating properly (usually pinging one machine from another is sufficient)
Invalid DNs to be monitored	Ensure that the ACD groups have been properly configured on the switch, and that the DMSGlobal.ini file matches that configuration

Table 5 Common problems (continued)

Problem	Solution
Call Info or Transfer fails (on client applications)	Ensure that the RequestTimeout value is set to something reasonable (generally 5000 or more). Smaller values may cause client requests to time out without giving the switch time to complete a requested action.
No response to AgentContinuity Message	The switch expects a positive acknowledgement (RETURN-RESULT) from the Session Manager within 10 seconds. If the Session Manager doesn't respond the Session Manager connection, the DMS connection and connections to all active agents are disconnected. Any agent that does not respond to the message in a timely fashion (5 seconds) will be disconnected, and that agent license becomes available, but the Session Manager connection, the DMS connection and all the other agents remain connected.

Frequently Asked Questions

Table 6 shows the answers to some frequently asked questions about LinkPlexer 1.1 installation and configuration.

Table 6 Frequently asked questions

Question	Answer
How do I interpret LCD and LED fault indicators on the Motorola V.3600 modem?	Motorola modems have six LEDs on the front and a display panel. When LinkPlexer is running correctly, the first four LEDs are lit and the last two blink. The display shows the words ON-LINE. Any other combination indicates that the modem is not working.
How do I install and migrate from one server to another?	LinkPlexer can not migrate from one server to another. However, if the DMSGlobal.ini and DMSLocal.ini files are backed up, found in the C:\Program Files\Nortel\Linkplexer folder, then LinkPlexer can be installed on a new server. Replace the DMSGlobal.ini and DMSLocal.ini files with the old ones without re-configuration.
How do I identify the latest version number or review fixes for LinkPlexer 1.1?	To identify the latest software version number, go to http://sulaco.europe.nortel.com:8080/mpl/core_mm_view.cfm and under each build folder there is a list of pertinent PEPs. The applied software versions are available in the Tracker application. Ensure that this information is communicated with problem reports.
How do I use the front panel on a line driver to set the configuration?	See Chapter 4 of the *Motorola V.3600 Series Modem User's Guide*, Part # T0097,C for information.
What if the hard disc fails? How is the system recovered?	Setting up the new machine. Install LinkPlexer 1.1 from the CD-ROM. Replace the DMSGlobal.ini file and the DMSLocal.ini file with backup copies of the original files. Refer to "Back-up of LinkPlexer 1.1 and Restoration to a New Server" on page 103

Table 6 Frequently asked questions (continued)

Question	Answer
Does upgrading LinkPlexer require an outage?	Yes.
What is the sequence of CTI servers?	The recommended boot sequence is: 1. Linkplexer 1.1 server 2. SCCS 3. TAPI. However, if Linkplexer is restarted, the switch link and all associations are dropped as well as the connections to SCCS and TAPI. Both SCCS and TAPI go into a link restart phase trying to reconnect to the 'switch'. When Linkplexer comes up, it establishes the connection to the switch and allows SCCS and TAPI to reconnect to it. SCCS and TAPI then reassociate (reacquire) the lines and continue normally. If the connection between the switch and Linkplexer is lost and Linkplexer continues to run, it will drop the connection to SCCS/TAPI, forcing them into the link restart phase. Any server should be able to be restarted without impacting the others.
If there is a problem with the Eicon X.25 card, how are the X.25 commands diagnosed?	Refer to the Problem Determination Guide at http://www.eicon.com/support/helpweb/connt/PDmenu.htm for Eicon Card X.25 command diagnostics.

Log files

Log files are stored in the folder selected during LinkPlexer 1.1 installation (by default this is C:\Program Files\Nortel\LinkPlexer 1.1). These files record significant events and errors for the user.

Never turn the logging process off. Messages occur infrequently and the performance impact is minimal. One log file is produced for each thread this allows the user to pin-point the origin of each log.

Note: LinkPlexer is designed to use the TCP/IP protocol, therefore in the case of X.25 some messages in the error log may look incorrect. If the information written in the error log entries matches the data in the INI files, ignore the formatting of the message.

Table 7 shows the filenames of all the logs generated by the LinkPlexer 1.1 application.The Filenames are sample names, as the actual number appended to the filename will depend on the thread allocation.

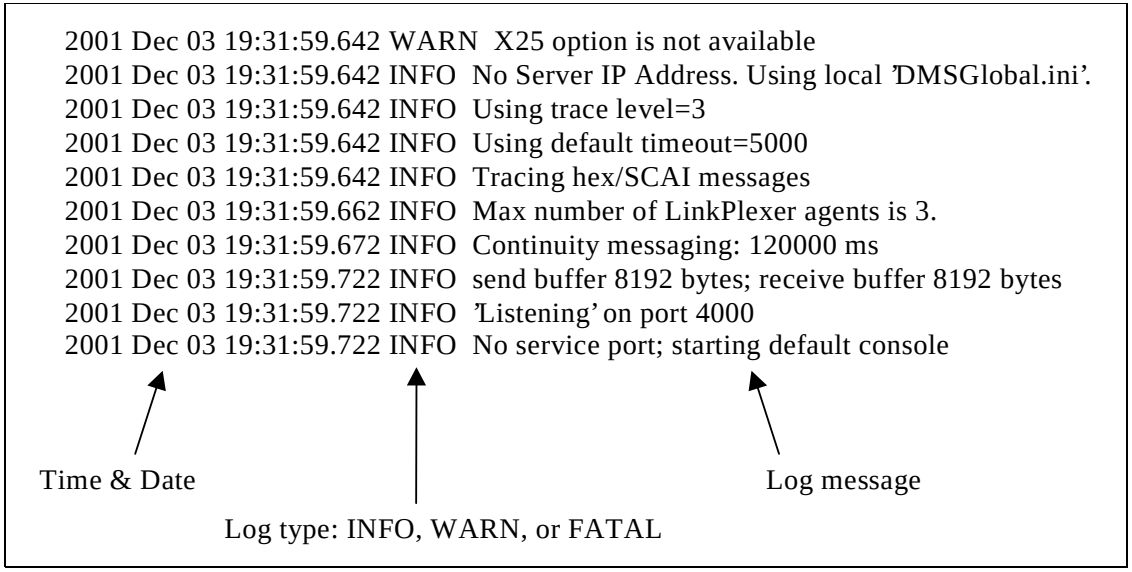
Table 7 LinkPlexer 1.1 log files

Filename	Thread	Contents
DMSError0.log	Main	Main program status
DMSError1.log	OSTimerThread	Timer status
DMSError2.log	DMSSessionQueue	Session queue status
DMSError3.log	ICMClientQueue	Switch connection status
DMSError4.log	ICMClientSocket	Switch session status
DMSError5.log	DMSAgentHub	Application connection status
DMSError6.log	DMSAgentQueue(0)	1st application status
DMSError7.log	DMSAgentSocket(0)	1st application session status. Shows the Associations, Failures and filtered operations)
DMSError8.log	DMSAgentQueue(1)	2nd application status
DMSError9.log	DMSAgentSocket(1)	2nd application session status. (Shows Associations, Failures and filtered operations)
DMSrecv4.log	ICMClientSocket	Captured data received from switch
DMSsend3.log	ICMClientQueue	Captured data sent to switch_

Log file format

There is a consistent log file format, as shown in Figure 34, which allows quick interpretation of events

Figure 34 Log file format



Sample log files

This section contains sample annotated log files, that are generated by the LinkPlexer 1.1 application.

Note: The following log file captures are examples only. Content may differ in individual LinkPlexer operations.

Figure 35 shows the DMSerror0.log file

Figure 35 DMSerror0.log file sample

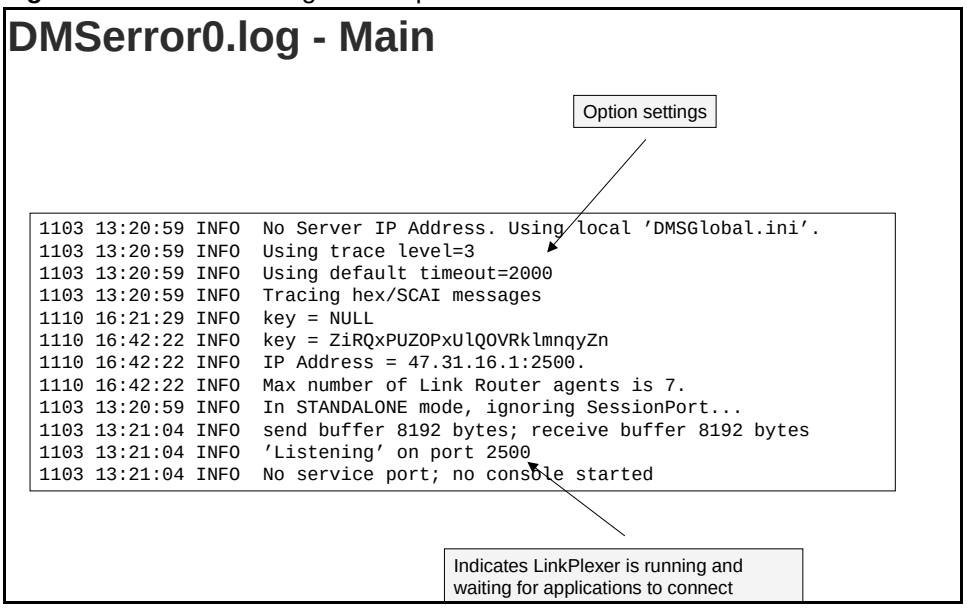


Figure 36 shows the DMSerror1.log file.

Figure 36 DMSerror1.log file sample

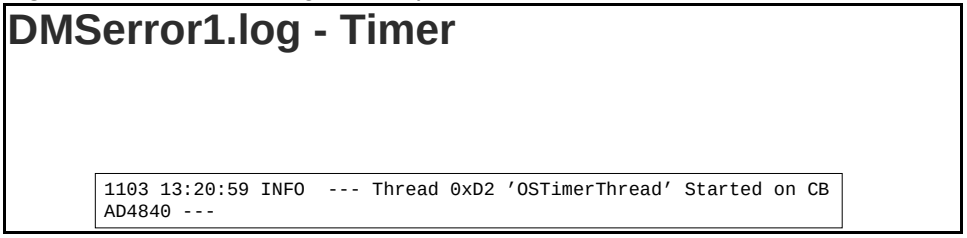


Figure 37 shows the DMSerror2.log file.

Figure 37 DMSerror2.log file sample

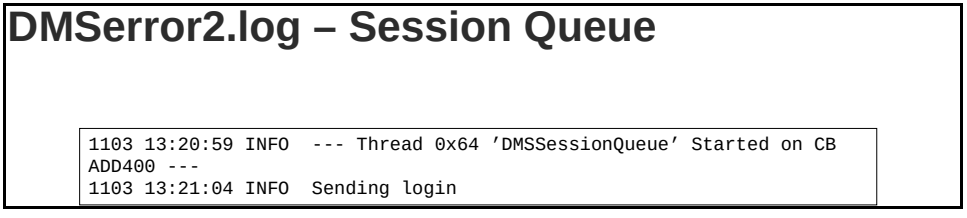


Figure 38 shows the DMSerror3.log file.

Figure 38 DMSerror3.log file sample

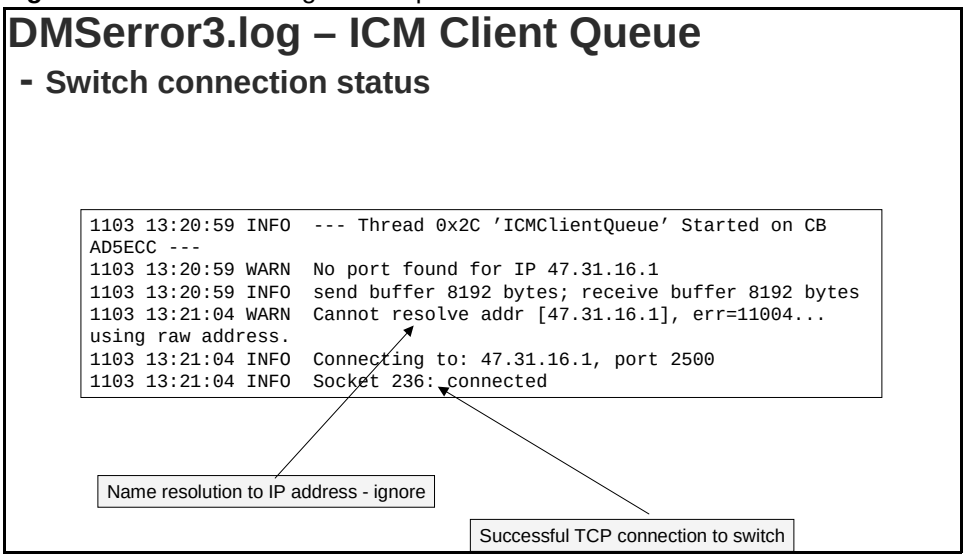


Figure 39 shows the DMSrecv4.log file.

Figure 39 DMSrecv4.log file sample

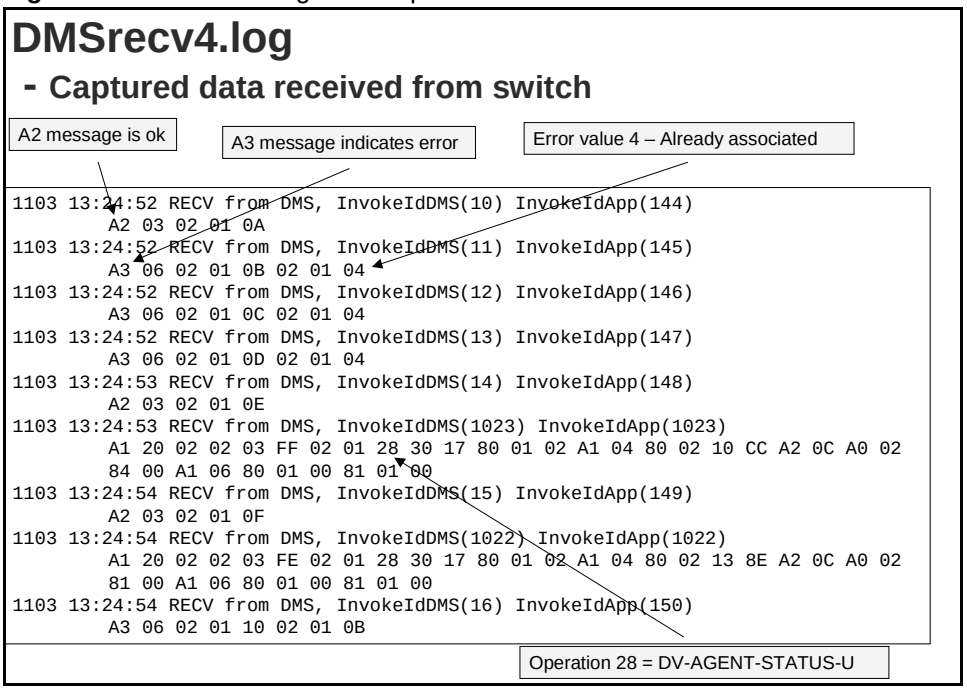


Figure 40 shows the DMSerror5.log file.

Figure 40 DMSerror5.log file sample

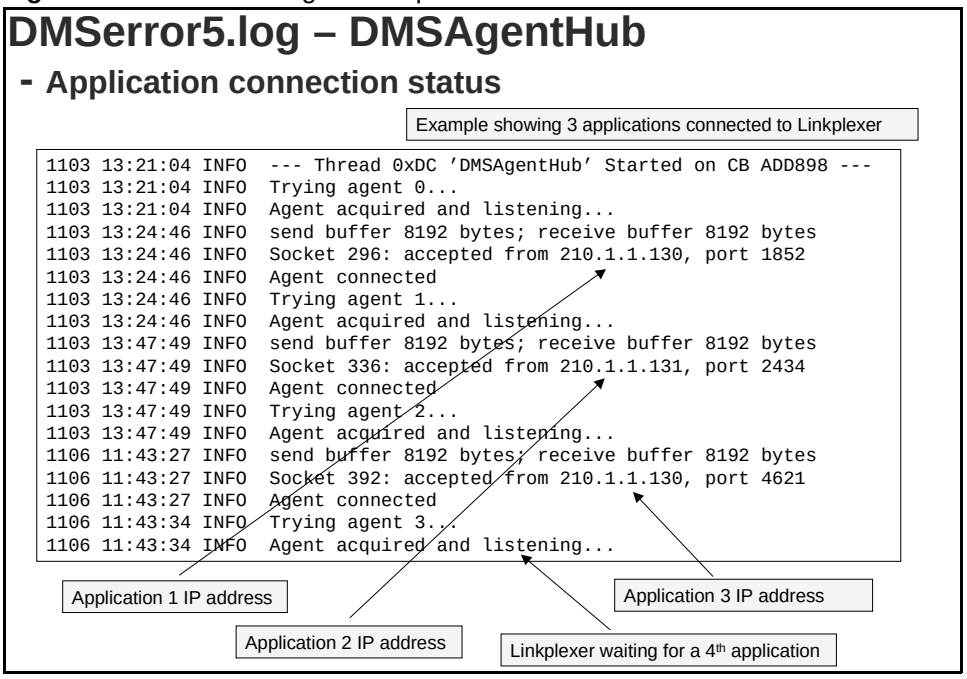


Figure 41 shows the DMSerror6.log file.

Figure 41 DMSerror6.log file sample

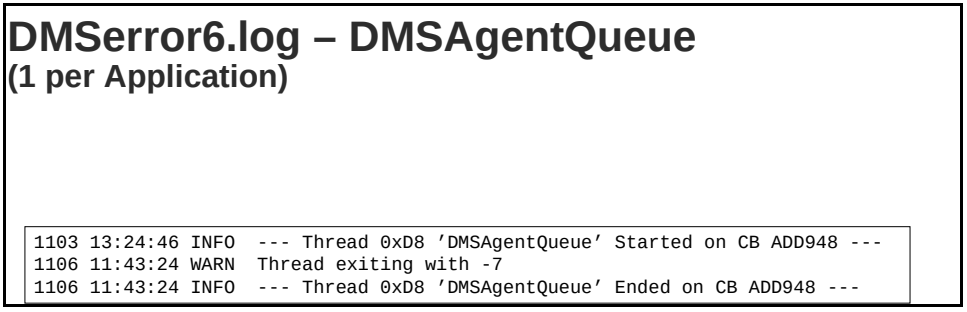


Figure 42 shows the DMSerror7.log file

Figure 42 DMSerror7.log file sample

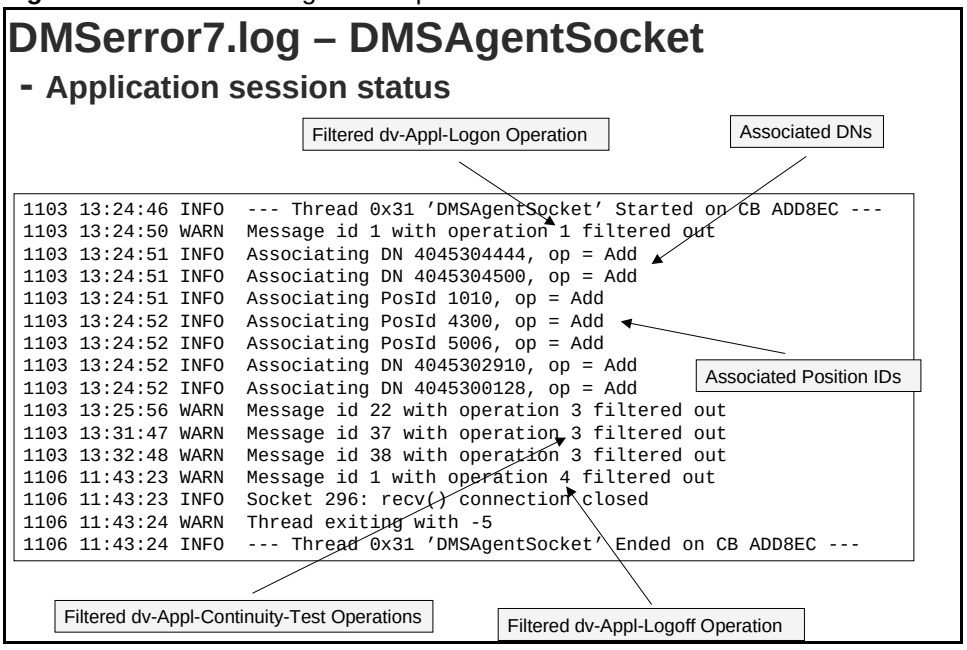


Figure 43 shows the DMSrecv4.log file

Figure 43 DMSrecv4.log file sample

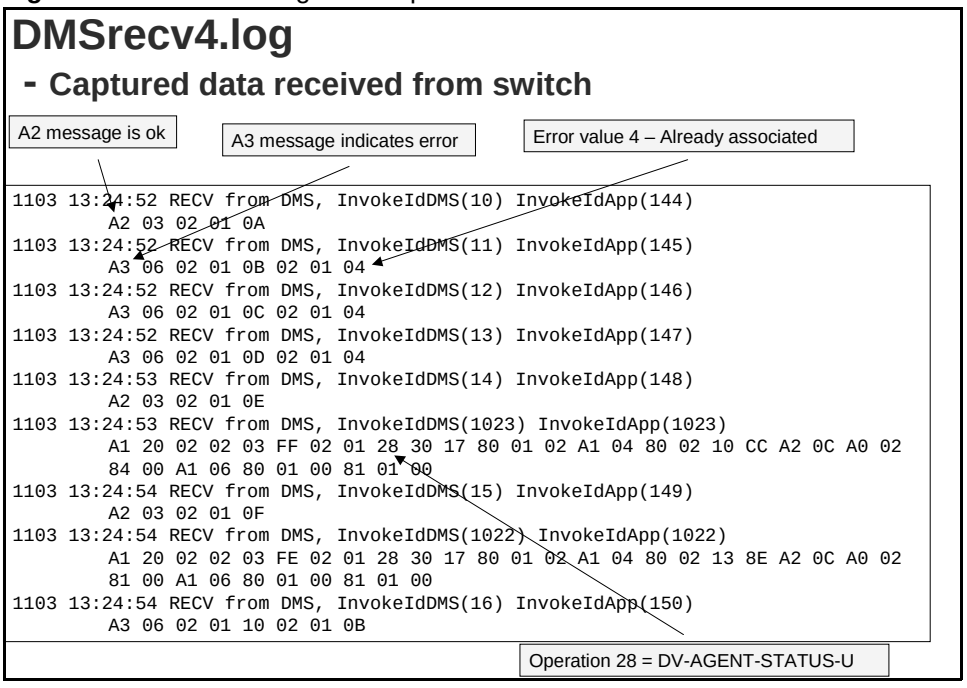
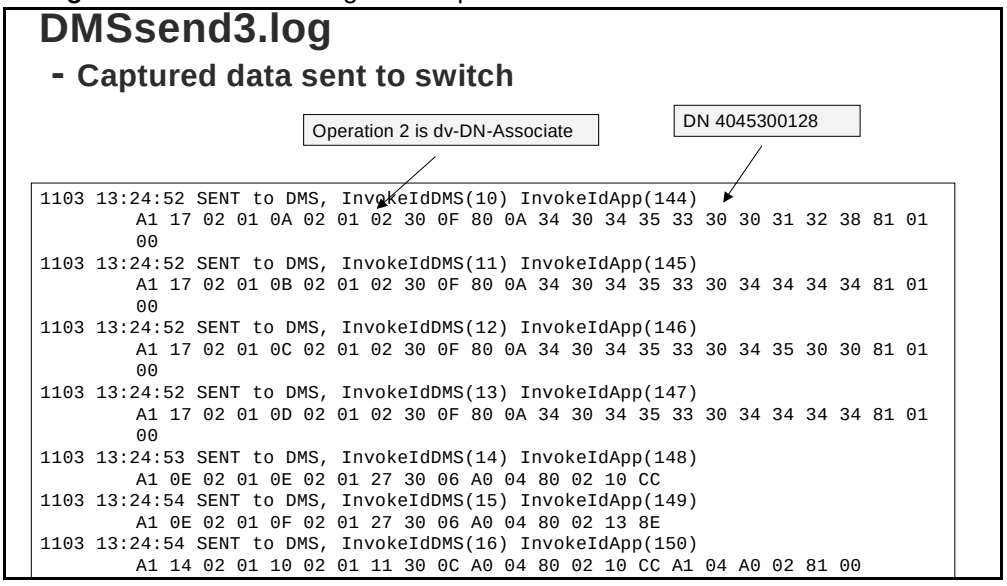


Figure 44 shows the DMSsend3.log file.

Figure 44 DMSsend3.log file sample



Note: DMSError0.log through to DMSError5.log, DMSrec#.log and DMSsend#.log are static and the rest of the log files can vary from site to site.

Note: If problem diagnosis requires further explanation of these logfiles, contact your support organisation.

LinkPlexer Procedures

This section looks at LinkPlexer 1.1 procedures of operation. It contains the following sections:

Backup of LinkPlexer 1.1 to enable restoration - in the event of a faulty PEP

Builds affected

All Builds and PEPs

Background

The LinkPlexer 1.1 file content may be updated or added to by the use of the LinkPlexer 1.1 PEP installer. This will read the LinkPlexer 1.1 Path from the registry keys and install the modifications in the Nortel LinkPlexer 1.1 folder.

However in the case that there is a fault in the PEP installation and/or PEP file content, it is advisable to have a backup copy of the original LinkPlexer 1.1 files.

Procedure

1. Locate the LinkPlexer 1.1 folder. By default this is located in C:\Program Files\Nortel\LinkPlexer 1.1
2. Copy this folder (and consequently all the files) to another location
3. Close all applications that are currently running
4. Proceed with the PEP installation (refer to the PEP Installation procedure on page 91)

1. If there has been a problem with the PEP installation, delete the LinkPlexer 1.1 folder located, by default, at C:\Program Files\Nortel\LinkPlexer 1.1
2. Restore the LinkPlexer 1.1 folder to C:\Program Files\Nortel
3. LinkPlexer 1.1 and its associated applications may be run as usual now.

PEP Installation

Builds affected

All builds and PEPs

Background

The LinkPlexer 1.1 file content may be updated or added to by use of the LinkPlexer 1.1 PEP (Product Enhancement Package) installer. This will read the LinkPlexer 1.1 Path from the relevant registry keys and install the modifications in the Nortel LinkPlexer 1.1 folder (default C:\Program Files\Nortel\LinkPlexer 1.1.

The latest PEP for a particular build is available from http://sulaco.europe.nortel.com:8080/mpl/core_mm_view.cfm where under each build folder there is a list of pertinent PEPs. The latest PEP for a given software build (e.g. 01.01.10) will always contain all the fixes/changes contained in earlier PEPs for the same build. Thus, only the latest PEP need be applied to the release.

It is advisable to follow the procedure “Backup of LinkPlexer 1.1 to enable restoration - in the event of a faulty PEP” prior to beginning this procedure.

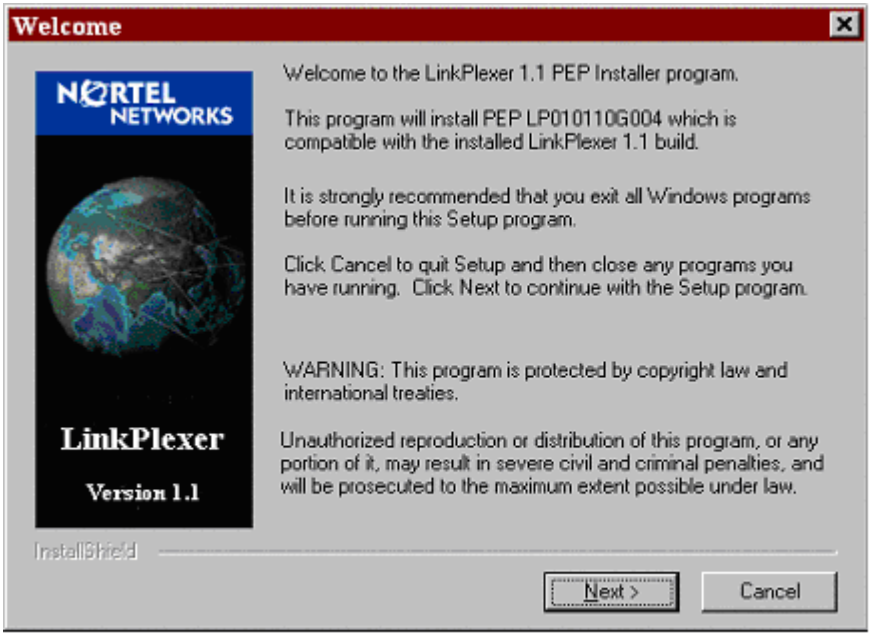
Procedure

Assumptions:

- LinkPlexer 1.1 is installed
- All unassociated applications are closed

1. Locate the correct PEP for the installed build on the following website: http://sulaco.europe.nortel.com:8080/mpl/core_mm_view.cfm. Unzip the file and click on the setup icon (setup.exe)
2. The dialog box in Figure 45 shows the InstallShield Welcome dialog box for PEP LP010110G004

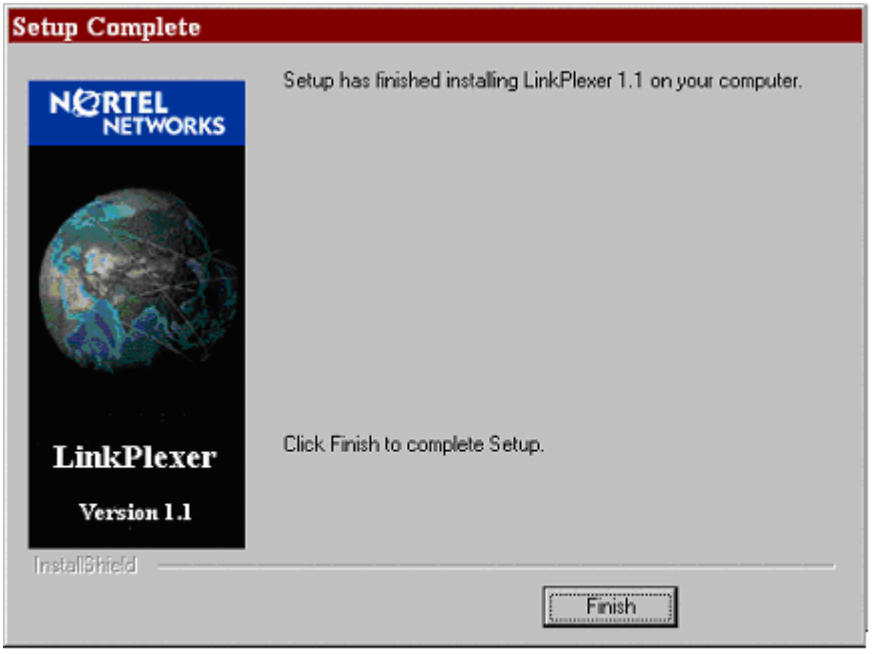
Figure 45 PEP Installation - welcome dialog box



3 Click Next. The PEP files will now be installed into the LinkPlexer 1.1 folder (by default this is C:\Program Files\Nortel\LinkPlexer 1.1)

4 After installation, the following dialog box, as in Figure 46, will be visible

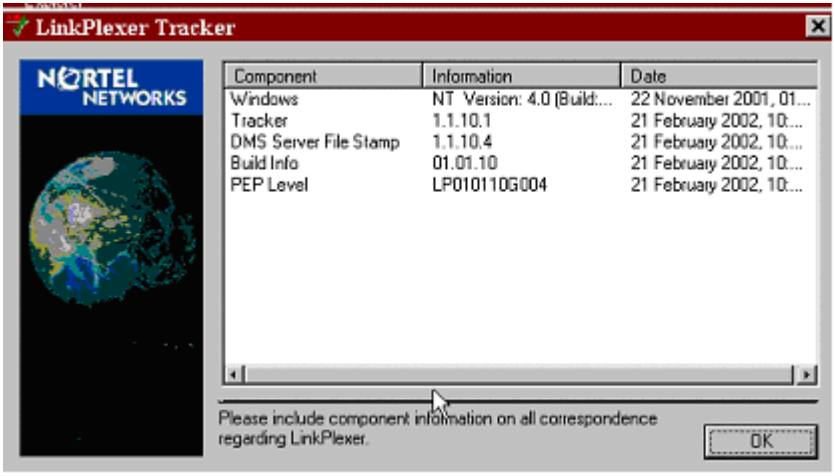
Figure 46 PEP Installation - finish dialog box



5 Click Finish. The PEP has now been installed. The Tracker application can be used to verify the PEP.

6 Tracker may be launched from Start\Programs\Programs\Nortel LinkPlexer 1.1\Tracker. It will display the PEP level and the date as illustrated in Figure 47.

Figure 47 Tracker with PEP details



Back-up of LinkPlexer 1.1 and Restoration to a New Server

Builds affected

All builds and PEP's.

Background

This procedure documents the steps to take in order to ensure that the current configuration of LinkPlexer 1.1 (and hence the LinkPlexer files) is backed up. It also outlines the steps to restore LinkPlexer to a new server in the case of a fault/ damage to the original server.

Procedure

1. Locate the LinkPlexer 1.1 folder. By default this is located in C:\Program Files\Nortel\LinkPlexer 1.1
2. Copy this folder (and consequently all the files) to another location. This step ensures that there are backup copies of all the installed files.
3. Make separate copies of the DMSGlobal.ini and DMSLocal.ini files, which have been adapted locally for LinkPlexer 1.1 configuration. The copies of these files should be held externally e.g. on a separate machine.

4 Install LinkPlexer 1.1 on the new server (follow Chapter 2, “Pre- Installation Requirements & Procedures,” on page 27 and Chapter 3, “Installing LinkPlexer 1.1,” on page 31).

5 Locate the LinkPlexer 1.1 folder. By default this is located in C:\Program Files\Nortel\LinkPlexer 1.1.

6 Retrieve the copied DMSGlobal.ini and DMSLocal.ini - copy these into the LinkPlexer 1.1 folder over the default DMSGlobal.ini and DMS Local.ini files.

7 Open DMSGlobal.ini and change the ListenerAddress parameter to the IP address of the machine where the server now resides. See Table 2 on page 51 for more information. Save the file.

8 The TCP/IP or X.25 connections must also be re-configured. Refer to “X.25 configuration” on page 54 and “TCP/IP Connections” on page 54.

Upgrade Procedure for LinkPlexer 1.0 to LinkPlexer 1.1

Builds

LinkPlexer Release 1.0 and all LinkPlexer 1.1 builds and PEPs

Background

This procedure is not supported, but the following guidelines outline the necessary steps for upgrading the application from Release 1.0 to Release 1.1

Procedure

1 Locate the LinkPlexer folder. By default this is located in C:\Program Files\Nortel\LinkPlexer

2 Copy this folder (and consequently all the files) to another location. This step ensures that there are backup copies of all the Release 1.0 files, in case of a fault during LinkPlexer 1.1 Installation.

3 Make separate copies of the DMSGlobal.ini and DMSLocal.ini files, which have been adapted locally for LinkPlexer 1.0 configuration. The copies of these files should be held externally i.e. on a separate machine for reference when completing the configuration for LinkPlexer 1.1

4 Uninstall LinkPlexer 1.0, by clicking on Start\Settings\Control Panel\Add/Remove Programs and selecting Nortel LinkPlexer.

5 LinkPlexer 1.1 can be installed and configured as directed in Chapter 3, "Installing LinkPlexer 1.1," on page 31 and Chapter 4, "Configuring LinkPlexer," on page 49.

Manually Enabling LinkPlexer 1.1/Symposium Agent/TAPI Co-residency

Builds affected

Up to and including Build 01.01.10 with PEP LP010110G004

Background

Co-residency of these three applications was initally blocked due to dongle incompatibility. However, ICM TAPI does not require a dongle and Symposium Agent's dongle consists of just the parallel port adapter. LinkPlexer 1.1 requires an iButton and a parallel port adapter. The LinkPlexer 1.1 iButton can be inserted into Symposium Agent's parallel port adapter and with the addition of new keys to the registry the incompatibility can be overcome.

This dongle configuration and the registry entries will enable dongle recognition and subsequently LinkPlexer 1.1 operation.

Note: LinkPlexer 1.1 will install and co-reside with ICM TAPI and Symposium Agent however this configuration is not recommended by Nortel Networks.

Procedure

Assumptions

- LinkPlexer 1.1's iButton is inserted into the Symposium Agent dongle (i.e. Symposium Agent's parallel port adapter)

1 Open the Registry:

- Click Start and Run

- Open: Regedit

2 Open HKEY_LOCAL_MACHINE\\SOFTWARE\\Nortel

3 Select the Nortel key; right click and in the pop-up menu select ‘New’ and then ‘Key’

4 Name the key “Base”

5 Select the Base key; right click and in the pop-up menu select ‘New’ and then ‘Key’

6 Name the key “Configuration”

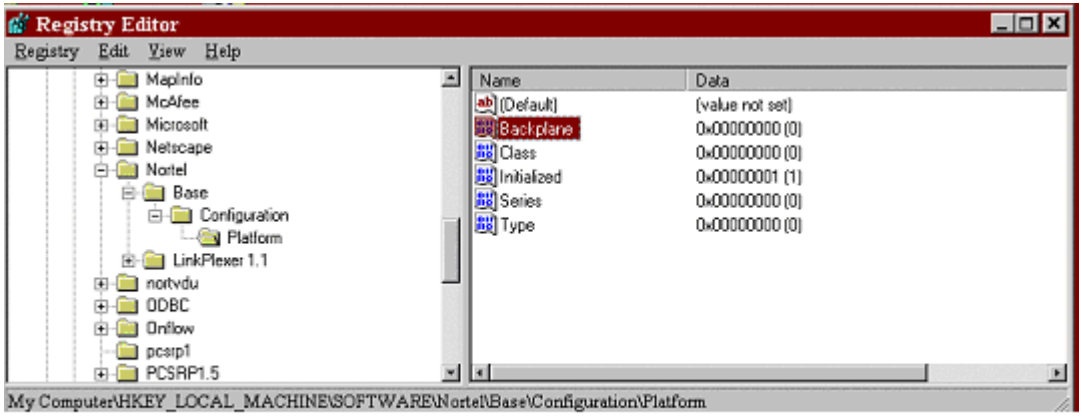
7 Select the Configuration key; right click and in the pop-up menu select ‘New’ and then ‘Key’

8 Name the key “Platform”; right click and in the pop-up menu select ‘New’ and then ‘DWORD Value’

9 Enter the following DWORD values (as in Figure 48)

- Backplane 0x00000000(0)
- Class 0x00000000(0)
- Initialized 0x00000001(1)
- Series 0x00000000(0)
- Type 0x00000000(0)

Figure 48 Registry DWORD values



10 After inputting these values, exit the Registry Editor

11 Start Keycode Tracker (from Start\Programs\Nortel LinkPlexer 1.1). The 'Check Dongle' box should display Connected. Continue with installation as instructed in the LinkPlexer 1.1 Installation and Configuration Guide.

12 If Keycode Tracker still does not recognises the dongle, ensure that 1-Wire Driver is installed. This is available from the LinkPlexer 1.1 cd under DallasDongleDriver\Install_1_Wire_Drivers_v320.exe. If this is installed, and the dongle is still not detected, consult the section Common Problems on page 79.

Startup Procedures for Nortel Networks Call Centre Equipment

Builds affected

All Builds and PEPs

Background

This procedure is linked to the section "LinkPlexer Configurations" on page 55

Option 1 "Pass Through" Procedure

When restarting Nortel Networks call centre equipment the following is the recommended sequence:

1 Start the Nortel Networks LinkPlexer 1.1 service

2 Start the services on the SCCS server (all services must be started before proceeding to the next step)

3 Start the ACD proxy service on the TAPI server (this will also start Telephony Services). Note, ensure Call Monitor is running - a restart may be necessary

4 Start the Nortel Networks Startup Services on the Peri Link Server (this establishes the socket connection to the TAPI server)

5 Make test calls into the VPS system to ensure the calls are being handled correctly

If there is to be a planned outage to the SCCS - for full backups or PEP installations, the order in which the systems are brought down should start at step 4 and go to step 1.

The following steps demonstrate how to stop the services:

Caution: Do not hard reboot the Peri Link

1. On the Peri Link server open the Services for the server and select the Periphonics Startup Services and click Stop
2. On the TAPI server, at the Run line type **killtapi.** This will shutdown the ACD proxy and Telephony Services.
3. If performing a Full Backup of the SCCS server, wait for the services to stop and go to the next step (step 4). If a PEP is being installed on the server, wait for the services to stop or for the server to start the reboot process before proceeding to the restarting sequence
4. After the SCCS services have stopped, or the server is rebooting, open the Services for the server and select Nortel LinkPlexer 1.1 and click Stop. This will disconnect the link with the switch. Note, the link needs to be reestablished by restarting the LinkPlexer 1.1 Service before the SCCS tries to restart.

Option 2 “Filtered” Procedure

1. Prior to starting the LinkPlexer 1.1 software, ensure that the CDN’s, ACD queues and SDN’s are properly datafilled in the DMSGlobal.ini file.
2. Upon confirmation that the information is correct, LinkPlexer 1.1 can be started.
3. Once LinkPlexer 1.1 is running, the remaining components of the call centre solution may be started

Note: although it is not required, it is recommended that the ICM TAPI Driver be started prior to the Peri ICM server.

Precautions

The end user should be aware of the following scenarios when restarting the call centre or during an outage situation:

1. If a caller is receiving music or RANS's and the SCCS is taken down or looses control of a CDN during call processing, the caller will not be placed back into the default routing of the switch. At this point, the switch is still looking for a message to terminate the call handling. All new callers or callers, not receiving the above treatments, will be defaulted to the switch where they will not receive any treatments when their call arrives at the switch.
2. With Option 1 (Pass Through), if either of the Peri Link, ICM TAPI or SCCS applications go down, the other applications will stop receiving messages about the resources being shared. This also includes CDN's and associated ACD queues.

   The affected applications can recover by reacquiring the resources in the switch, this would involve manual intervention by the site administrator.
3. With Option 2 (Filtered), if either the Peri Link, SCCS or ICM TAPI applications go down, the other applications will still receive messaging about the acquired resources from the switch, because the resources are being acquired by LinkPlexer 1.1 software.

   The only time all applications would be affected is if the Link to the switch were lost. This could occur if the LinkPlexer server failed or there was a failure on the LAN between the switch and LinkPlexer.
4. In the case of a LinkPlexer failure, all applications would loose control of the acquired resources and the calls would return to the switch default routing. This holds true for either option selected during configuration of LinkPlexer.

Guidelines for the use of Anti-Virus software on LinkPlexer 1.1

It should be noted that the risk of virus infection on the LinkPlexer 1.1 server is minimal due to the limited access required for support of the server. LinkPlexer 1.1 is compatible with and supports anti-virus software with known and documented guidelines.

Nortel Networks has carried out testing on a representative sample of Anti-virus software packages (Norton, McAfee and Innoculate) in order to determine generic guidelines for the use of Antivirus software:

- The LinkPlexer server software must be installed before installing the Anti-Virus software. When the Anti-Virus software is installed, it is the implementation personnel's responsibility to perform testing.
- During PEP installations all Anti-Virus functionality should be disabled and should not startup automatically until the entire installation procedure is completed. Re-enable afterwards as required.
- Infected file quarantine policy on the LinkPlexer 1.1 server: the anti-virus software should not be configured to deal automatically with suspected infected files. In the event of infected files being located, there should be no attempt to replace or remove them. Contact the local Nortel Support representative for assistance in determining if the file(s) are part of the LinkPlexer 1.1 application or a critical system file.
- It is strictly unsupported to connect the LinkPlexer 1.1 server directly to the Internet for the downloading of Virus definitions or updated files. Instead, Virus definitions and update files should be downloaded to another locations on the customer network, and manually loaded to the LinkPlexer 1.1 server. This is the same recommended procedure for downloading Symposium PEPs. This limits access to the Internet, and thus reduces the risk or downloading infected files.
- In addition, all PEP files, CD-ROMs and floppy disks should be scanned prior to installation or uploading to the server. This will minimise any exposure to infected files from outside sources.

- Capacity considerations: Customers should note that running virus scan software can place an additional load on the LinkPlexer 1.1 server. It is the implementation personnel's responsibility to run the WINNT 4.0 Performance Monitor tool on the server to gauge CPU utilisation. If the Anti-Virus software scan causes the LinkPlexer 1.1 server average CPU utilisation to become excessive then that Anti-Virus software should not be loaded onto the LinkPlexer 1.1 server.

Note: Nortel does not provide support on the configuration of anti-virus scan software. Questions or problems on Anti-Virus software should be directed to the appropriate vendor.

Note: The above recommendations are intended as guidelines only, and do not constitute a guarantee of compatability. Nortel does not plan to perform ongoing compatability testing, or testing on other Anti-Virus packages.

Note: If performance or functionality issues are raised to Nortel support, as part of the fault diagnosis process, the customer/distributor may be asked to remove third party utility software or Anti-Virus software.

-

Appendices

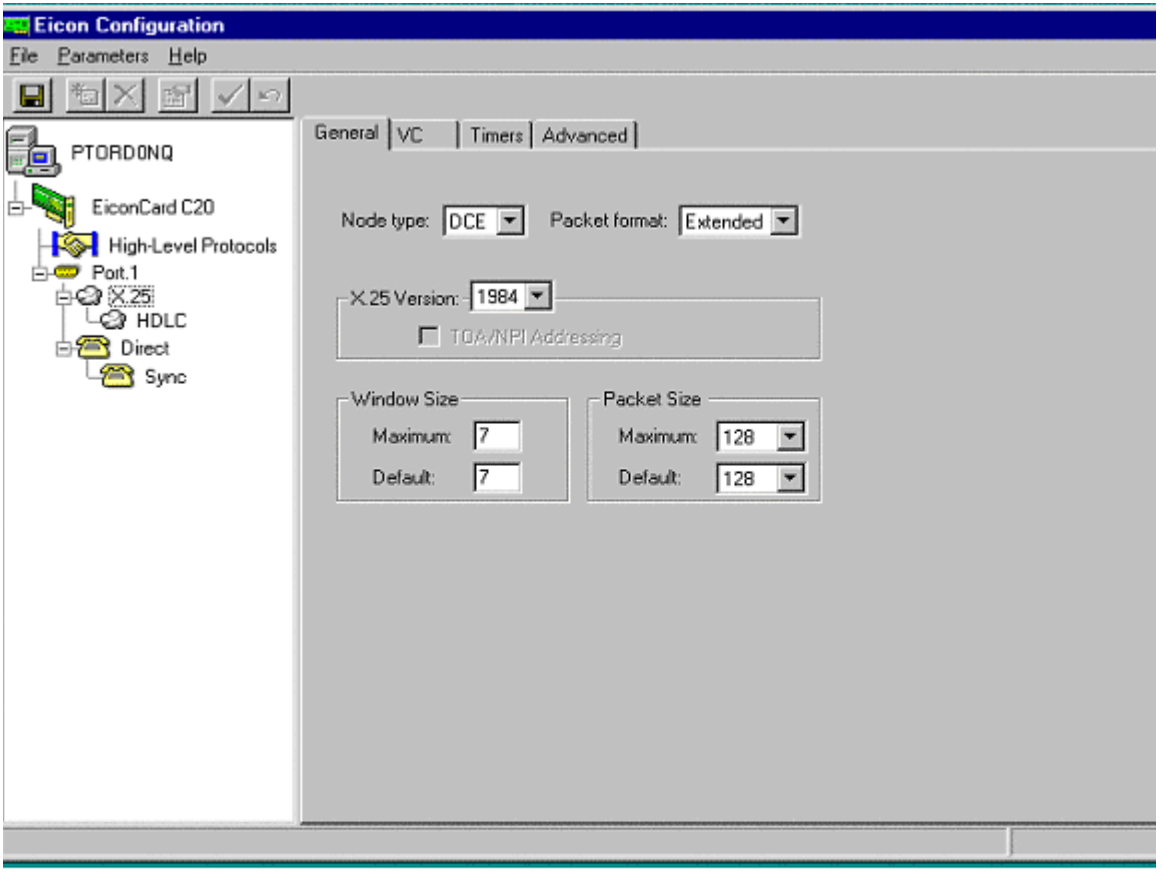
Appendix A

This Appendix refers to Chapter 6, “Installing and configuring the Eicon X.25 card, and the section “Installing the Eicon X.25 card” on page 82.

The following sequence of Screenshots can be used as a template for configuring the Eicon card for use with LinkPlexer 1.1.

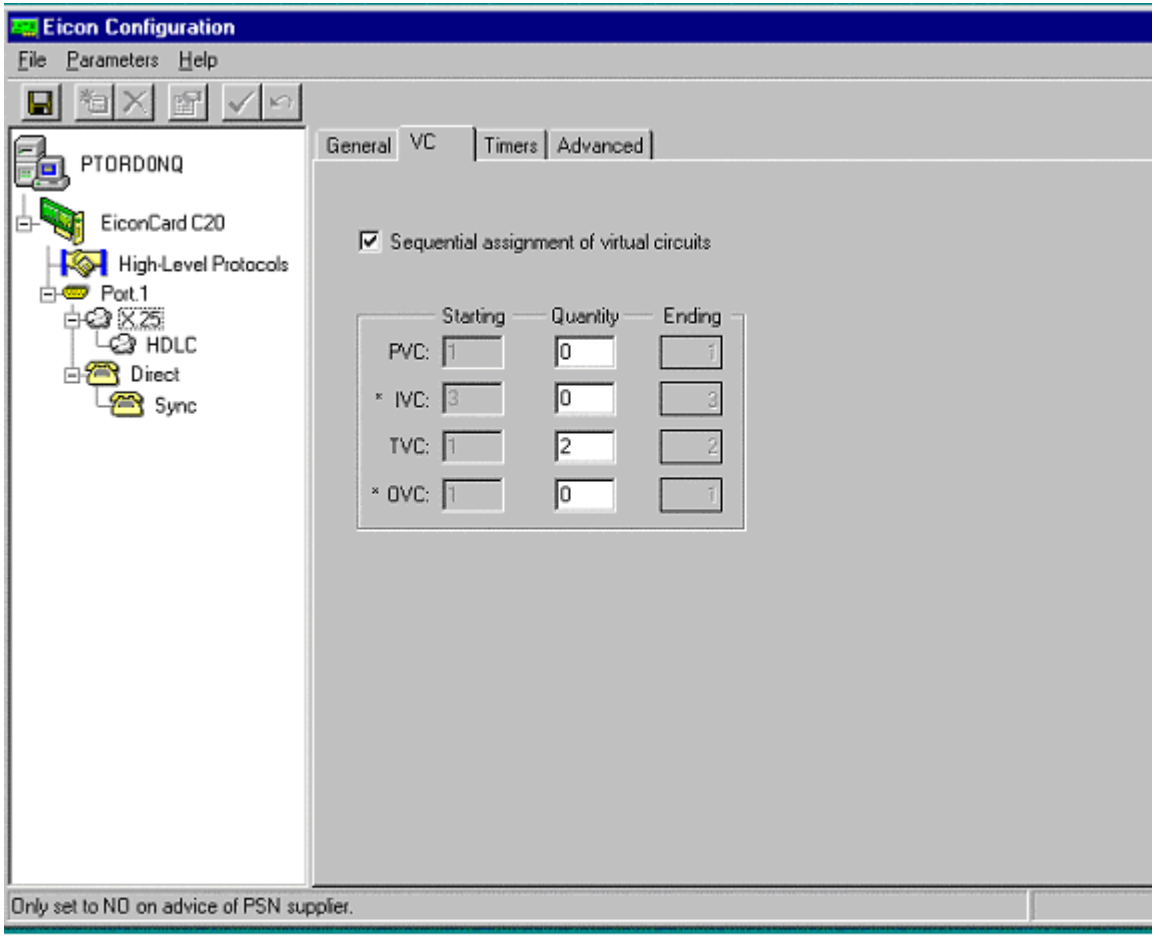
a X.25: General - values as in Figure 49

Figure 49 Eicon Configuration X.25:General



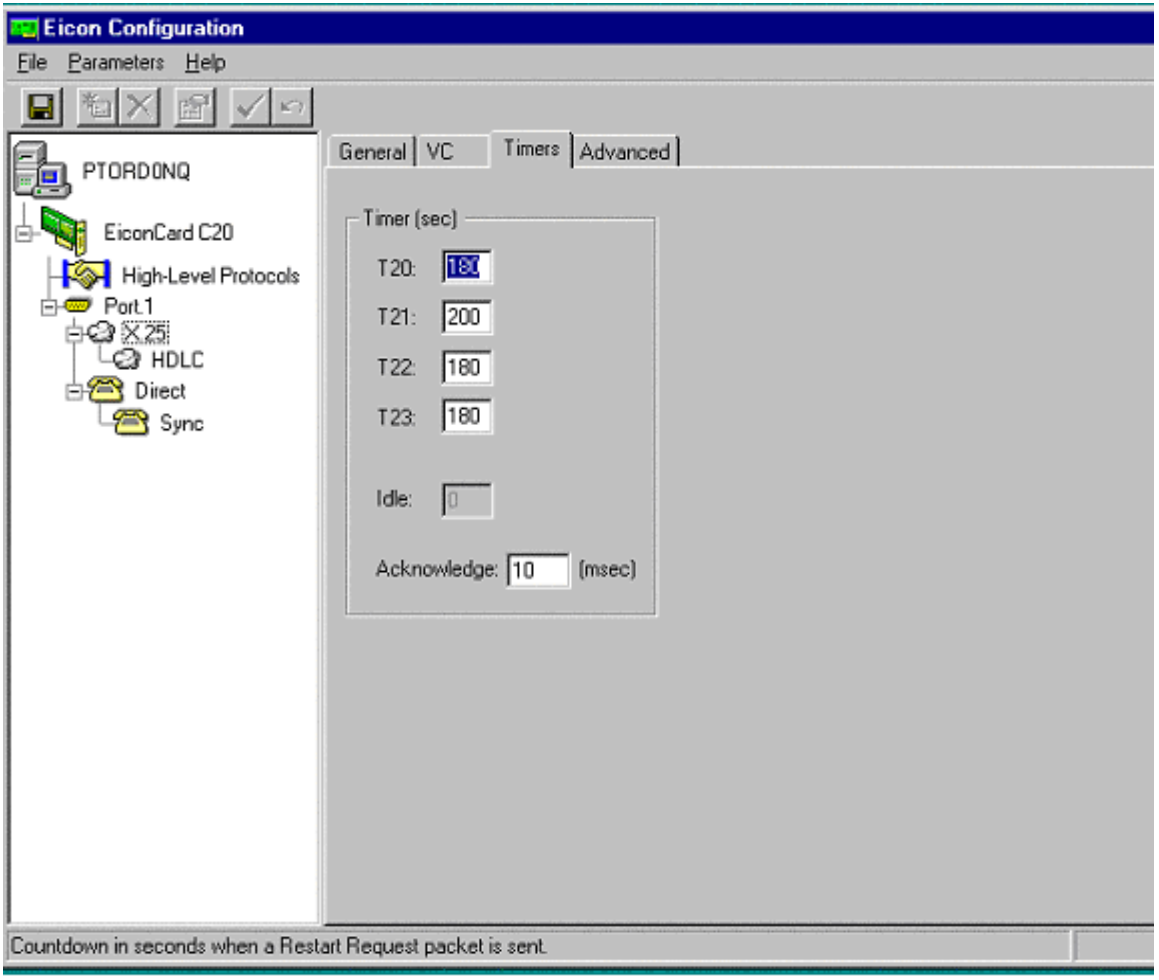
b X.25: VC - values as in Figure 50

Figure 50 Eicon Configuration X.25:VC



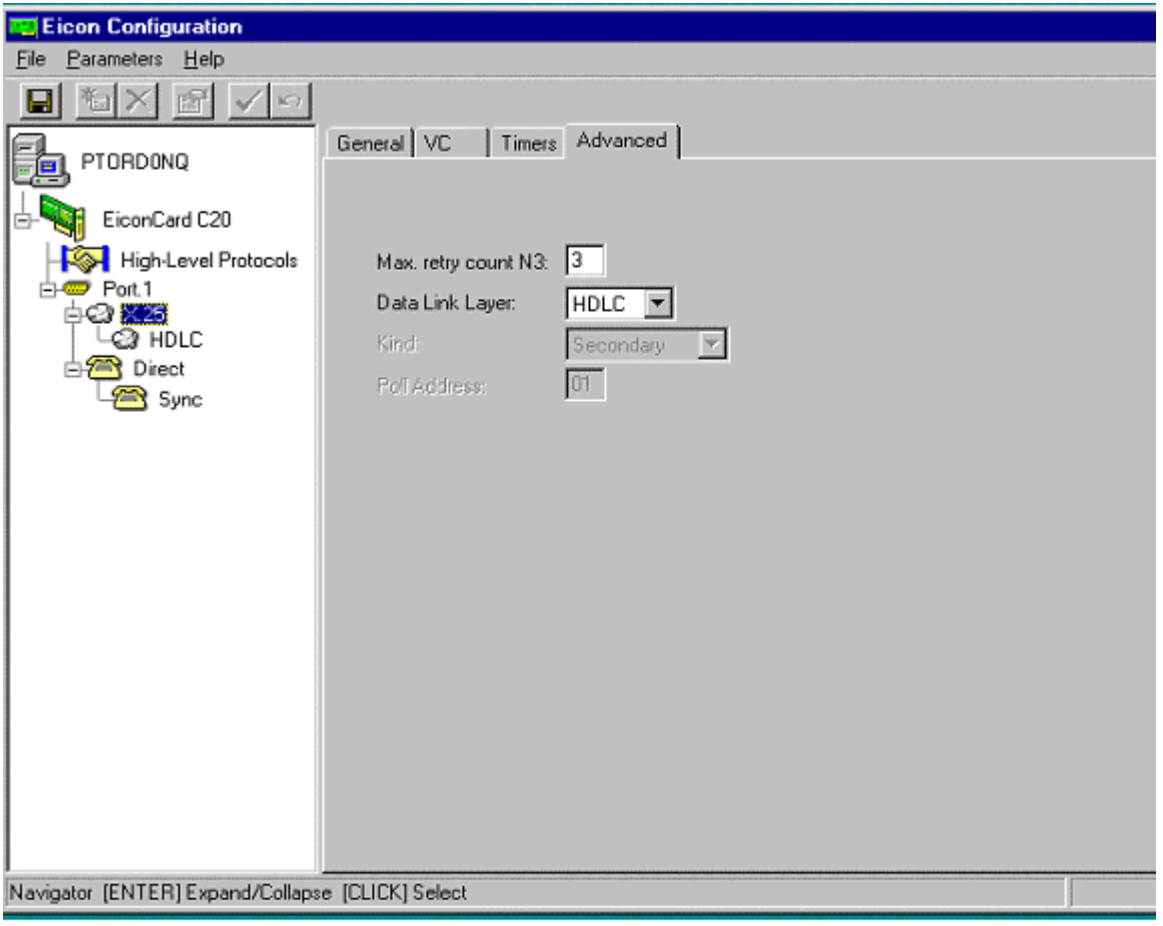
c X:25: Timers - values as in Figure 51

Figure 51 Eicon Configuration X.25: Timers



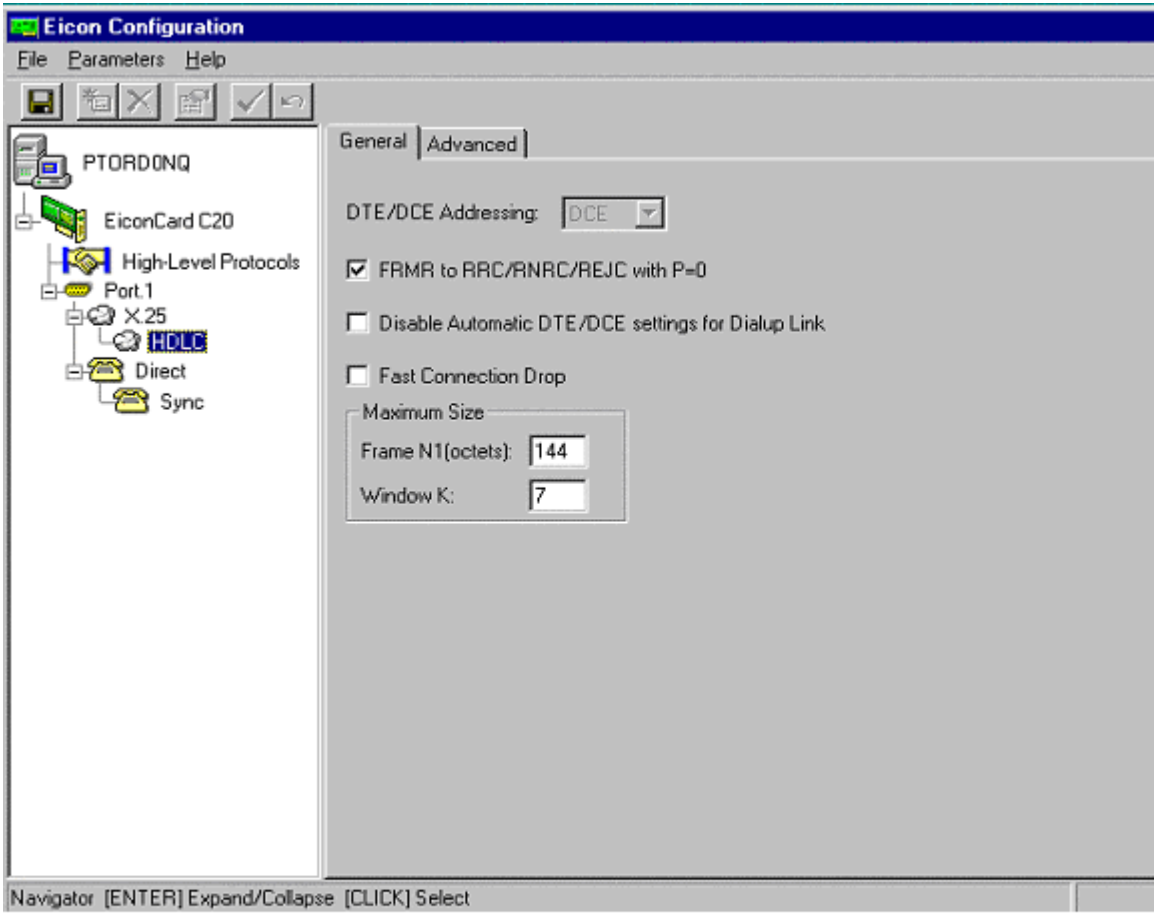
d X.25: Advanced - values as in Figure 52

Figure 52 Eicon Configuration X.25:Advanced



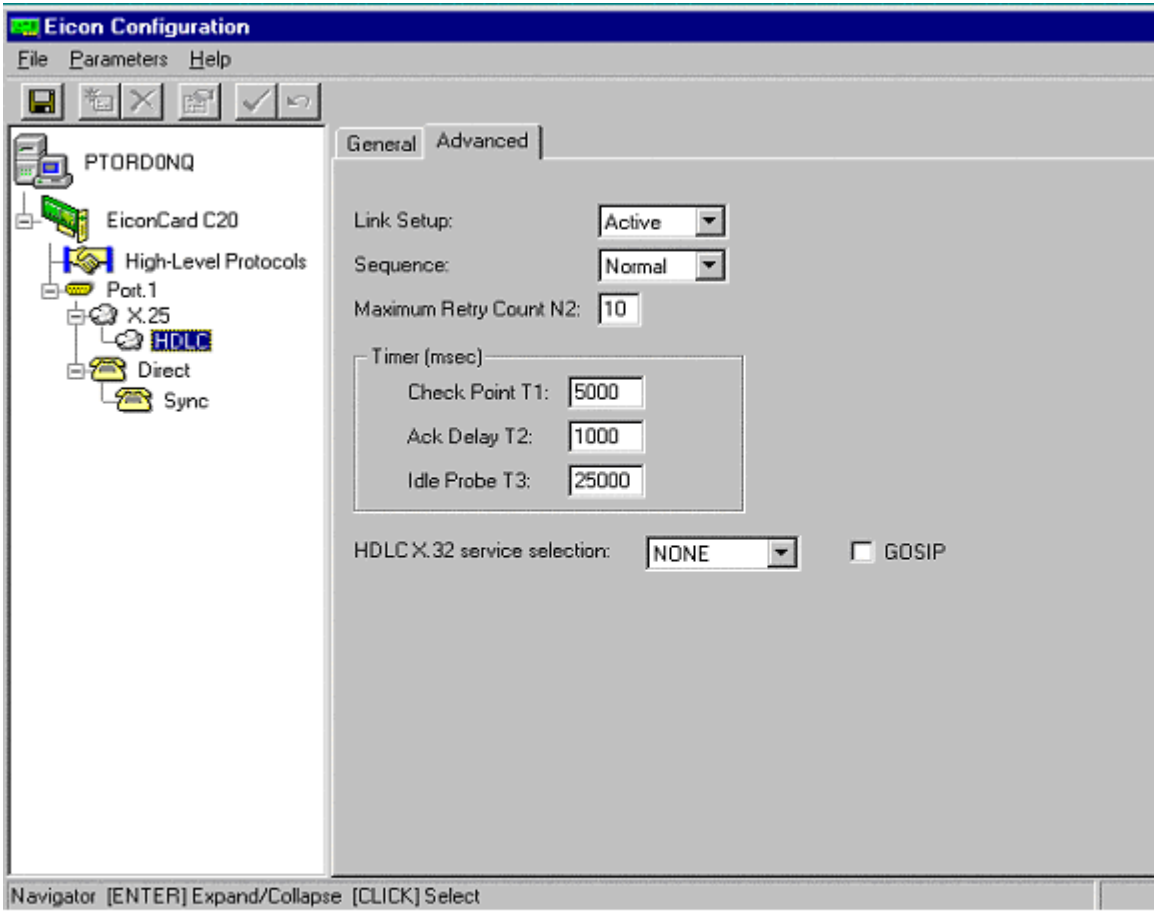
e HDLC: General - values as in Figure 53

Figure 53 Eicon Configuration HDLC: General



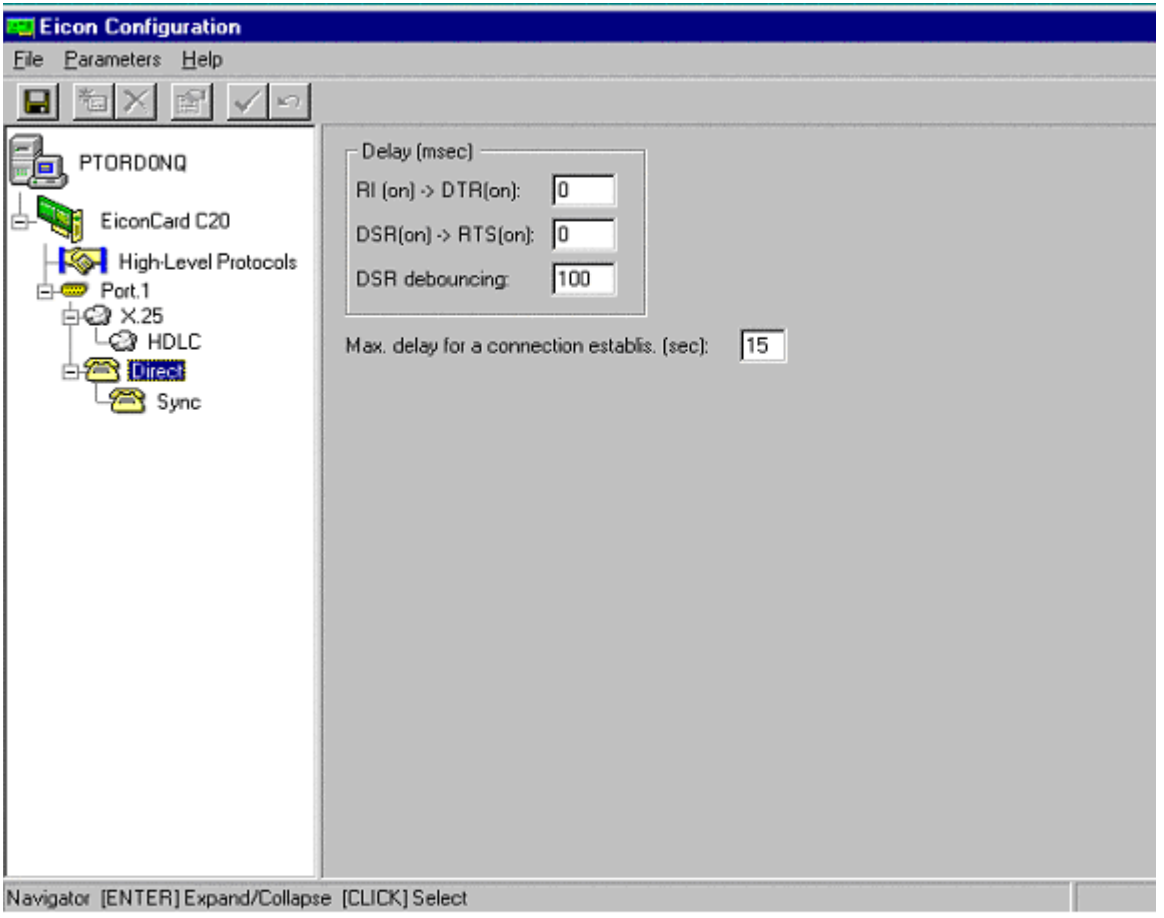
f HDLC: Advanced - values as in Figure 54

Figure 54 Eicon Configuration HDLC:Advanced



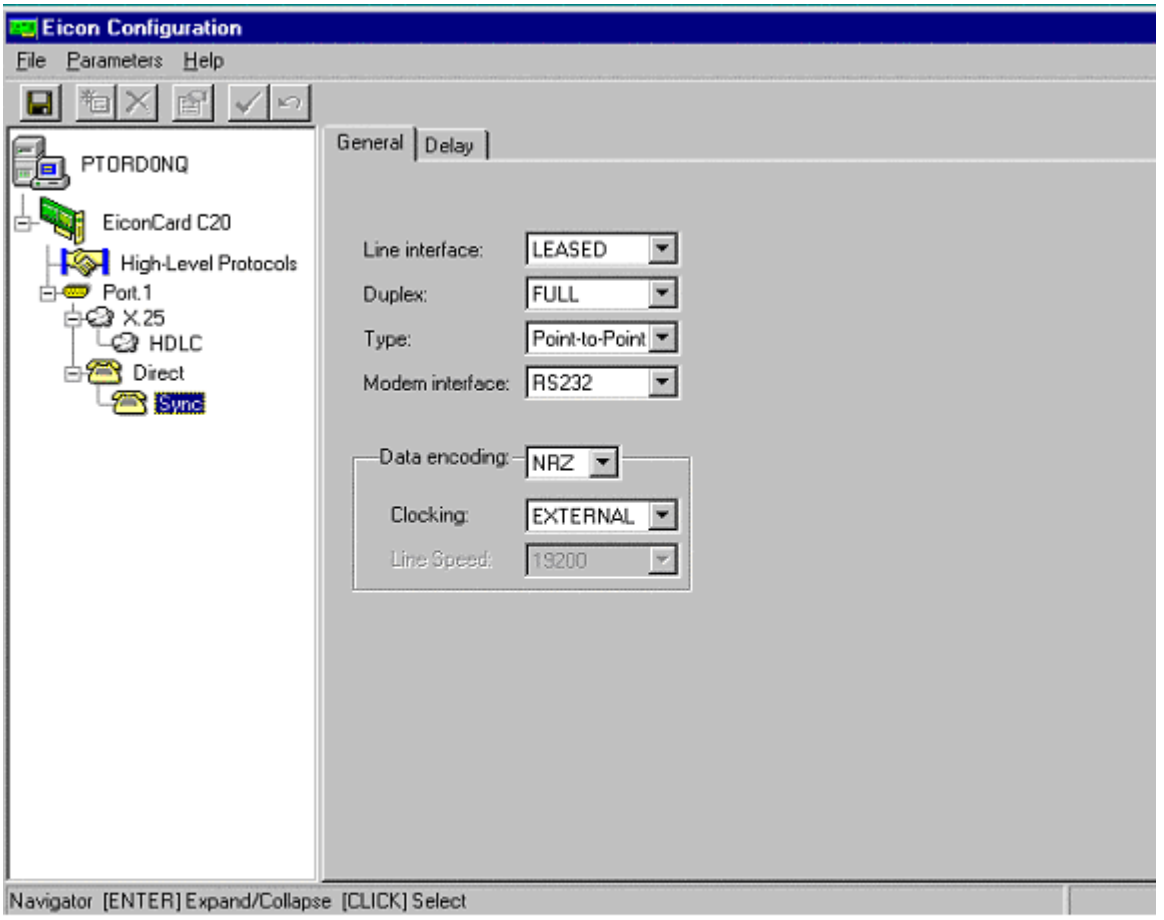
g Direct - values as in Figure 55

Figure 55 Eicon Configuration Direct



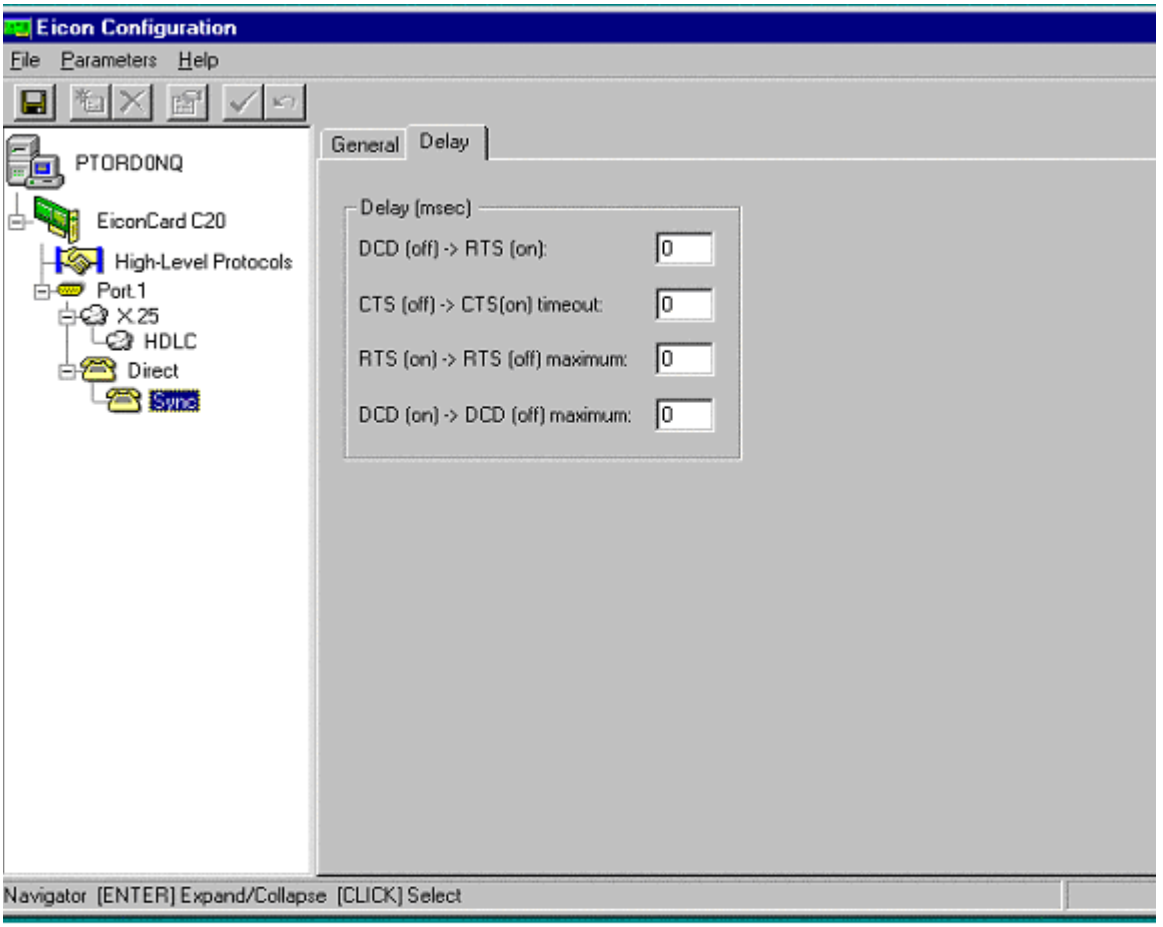
h Synch: General - values as in Figure 56

Figure 56 Eicon Configuration Synch:General



i Synch: Delay - values as in Figure 57

Figure 57 Eicon Configuration Synch:Delay



Appendix B

This Appendix refers to “Configuring the DMS/MSL-100 switch” on page 56. It provides the table definitions and examples of the table contents that are relevant for a call centre for DMS/MSL 100 (SCAI Linkset).

BGDATA

Table BGDATA is used to store information relating to multiswitch business groups (MBG). This table sets the customer group that the linkset will be able to access. If a line is in another customer group than the one defined in this table the call center will not be allowed to acquire/monitor the line or ACD group

BGID BGXLA OPTIONS

LOCAL 2 $ (CUSTGRP TAS1 N 24 Y 0 0) $

SCAICOMS

Table SCAICOMS defines a linkset for use by a switch/computer applications interface (SCAI) group. This table sets the type and address of the host application. Most of the sites will be TCP type. The IPADDRESS in this table MUST match the IP of the host application or the switch will not allow login. The ENHASSOC feature allows for a max of 100 CDN's to be acquired on this link.

LINKSET SCAILINKS OPTIONS

NORTEL TCP 47 104 99 88 N (ENHASSOC 100) $

SCAIGRP

Table SCAIGRP stores all the switch computer application interface (SCAI) groups within a switch. Each SCAI group has a password, network node identifier (ID) and business group ID (BGID). This table sets the login options for the linkset. The PASSWORD, NETNODID and BGID must be unique. The password and netnodid are defined only in this table. The BGID is the one datafilled in table BGDATA

SCAIDNAM PASSWORD NETNODID BGID OPTIONS

NORTEL ABC123 1 LOCAL 2 (LINKSET (NORTEL) $)$

SCAIPROF

Table SCAIPROF serves as a lookup table for switch computer application interface (SCAI) CompuCALL service profiles. A service profile is a set of CompuCALL messages and associated options that are available during a HIGHEST level of messaging that the link can support. The Subservice must be datafilled in table SCAISSRV in order to put it in this table. The Service ID is also datafilled in this table as part of the KEY Field.

NORTEL 1(CTXEVENT13$) (ACDEVENT12$) (ROUTING35$) (TPCC14$) (RESOURCE11$) (TPAC12$) (CALLINIT07$) (SCAI3WC14£) (SCAIMWTI13$) (DNQUERY07$) (SCAICC08$) (TPQC10$) (ICCM10$) (CPEVENT14$)$

Note: The $ after the subservice name denotes a default subservice that was already datafilled in table SCAISSRV.

SCAISSRV

Table SCAISSRV acts as a reference table for CompuCALL service categories. This table sets the type of data you will get during the call flow for each type of CompuCALL message. This table can be changed, but it is highly suggested that it not be changed from the default without careful engineering and customer call flow consideration

CTXEVENT12$ CTXEVENT (SETOFFHK Y Y Y) (CALLOFFR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLANSWR Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y) (CALLREL Y Y Y Y) (CALLNAME Y Y Y Y Y)$

CUSTNTWK

Table CUSTNTWK is used to define options available to the customer group. This table only needs one option added to the customer group that was defined in table BGDATA. The option ECM must be assigned to the customer group so that NON-ACD lines with the option ECM added to them in servord can be controlled or monitored with the CTI.

CUSTNAME NETNAME NETCGID DNREVXLA OPTIONS

TAS1 PRIVATE 1 $ (CLID INTRAGRP) (ECM) (NTWKEMW) (RNID INTRAGRP) $

LIUINV

Table LIUINV contains the configuration data for each ASU in an LPP or ELPP. The EIU is an interface between the DMS-bus and an Ethernet local area network (LAN). The MAC address in this table has to come from the program manager for the site.

LIUNAME LOCATION LOAD PROCINFO CARDINFO

EIU 2 MS 12 0 2 8 ETC15BC NTEX22BB NT9X84AA NT9X8522 NO 000075F01AD0

IPNETWRK

The IPNETWRK table describes the CM node and default EIU. Table LIUINV must be datafilled before table IPNETWRK. Changes made to the IP address component in table IPNETWRK force automatic reconfiguration of the IP address components of all nodes listed in tables IPHOST and IPROUTER. SCRNFLAG must always be set to N. By default all ICMP messages will go out the first EIU datafilled in this table. In this case it would be tuple 0. This IPAddress of 0 is the ELAN IP for the call centre. All telnet and ftp connections will take place on the second EIU in this table. Only two EIU's can be datafilled or physically inserted in the switch for a SNSE. Adding a third EIU will cut the amount of bandwidth into 3 equal pipes, even though the third one is not in service.

KEYREF CMIPADDR SUBNET OPTION PARMAREA

0 156 42 126 193 8 $ (SCRNFLAG N) (EIU_INTERFACE EIU 2)$ 1 156 42 19 1 8 $ (SCRNFLAG N) (DFLT_GTWY_IPADDR 156 42 4 252) (EIU_INTERFACE EIU 13) (DFLT_INTERFACE Y) $

IPHOST

The IPHOST table is responsible for configuring DMS nodes as Internet hosts. It activates the TCP layer and its applications on those nodes. For interface EIU's, only datafill the CM in this table.

```
INDEX NODENAME NODEINFO
- - - - - - - - - - - - -
0 CM 0 47 8 8
```

IPTHRON

Table IPTHRON contains IP THROttling numbers. The IP message flow from switch hosts requires throttling to control message congestion in the bandwidth-limited shared communication resources between the local message switch (LMS) and message switch (MS). The IP throttling numbers datafilled in this table derive the level of such throttling to and from each of the IP hosts.

Throttling capacity fields should not be zeros, the IP throttling numbers default to zero (100% throttling) for all EIUs datafilled in table LIUINV. If the throttling capacity numbers are not datafilled to non zero values, the EIU cannot communicate to destination nodes.

```
LMSNODE TXCAPCT RXCAPCT OPTION
- - - - - - - - - - - - - - -
EIU 2 32000 32000 (CM 32000) $

EIU 13 32000 32000 $
```