Token-Ring Adapter

Features

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 87.

Fifth Edition (June 2000)

This edition applies to the IBM token-ring adapters.

You can submit comments online to `http://www.networking.ibm.com/support/feedback.nsf/docsoverall`.

Contents

About this manual vii
Who should read this manual. vii
How this manual is organized vii
Related publications vii

Chapter 1. Introduction 1
Downloads 1
CD-ROM for IBM Token-Ring PCI Family Adapters 1
CD-ROM for other IBM token-ring adapters 1
Web 2

Chapter 2. RPL/PXE 3
PCI token-ring adapter RPL feature 3
Supported environments 3
PCI token-ring adapter PXE feature. 3
Supported environments 3
Overview 3
Installation and configuration 4
Setting up your client computer to support RPL/PXE 4
Enabling the RPL/PXE feature on the adapter 4
Making the RPL/PXE feature the first bootable device 4
Changing the boot protocol 5
Changing the boot protocol (PXE 1.x) 5
Changing the boot protocol (PXE 2.x) 6
Setting up your OS/2 LAN Server to support RPL 9
Setting up your Novell NetWare server to support RPL 10
Setting up your Windows NT 4.0 server to support RPL 12
Installing the Remoteboot service 12
Configuring DOS RPL client network settings 12
Installing DOS files on the Remoteboot server 13
Creating Remoteboot configurations for the PCI token-ring adapters 14
Creating a new workstation record automatically 15
RPL messages 15
PXE messages 17
Troubleshooting RPL problems 19
IBM Turbo 16/4 Token-Ring PC Card 2 RPL feature 22
Supported environments 22
Overview 22
Installation and configuration 23
Setting up your Windows NT 4.0 server to support RPL 23
Installing the Remoteboot service 24
Configuring DOS RPL client network settings 24
Installing DOS files on the Remoteboot server 25
Creating Remoteboot configurations for the IBM Turbo 16/4 Token-Ring Adapter 26
Creating a new workstation record automatically 26
RPL messages 27
Troubleshooting RPL problems 28

Chapter 3. IBM LAN Client 31
Supported environments 31
Supported IBM LAN adapters 31
Supported software 31

Supported operating systems . . . 32
Restrictions for this release . . . 32
Overview . . . 32
Benefits . . . 32
DOS conventional memory usage reduction . . . 33
Installation and configuration . . . 33

Chapter 4. LAN Adapter Management Agent . . . 35
Supported environments . . . 35
LAN adapters . . . 35
Operating systems . . . 35
Overview . . . 35
Benefits . . . 36
System requirements . . . 36
Windows NT, Windows 95, Windows 98, and Windows 2000 software requirements . . . 36
OS/2 software requirements . . . 36
IBM Nways Management Applications . . . 36
Installation and configuration . . . 36
Windows NT, Windows 95, Windows 98, and Windows 2000 . . . 36
OS/2 . . . 37
Example scenarios . . . 37
Remote DMI . . . 37
MIB browsing . . . 38

Chapter 5. Route Switching . . . 39
Supported environments . . . 39
History . . . 39
Overview . . . 40
Benefits . . . 41
Example scenarios . . . 41
One-armed router . . . 41
Managing Route Switching with IBM LAN Adapter Management Agent . . . 41
System requirements . . . 42
Installation and configuration . . . 42
Route Switching parameters . . . 42
Windows 95, Windows 98, Windows NT, and Windows 2000 . . . 44
Novell NetWare server . . . 45
IBM LAN Client . . . 45
OS/2 . . . 46

Chapter 6. Class of Service . . . 47
Supported environments . . . 47
Overview . . . 48
Benefits . . . 48
Example scenarios . . . 48
Win32 and OS/2 environments . . . 49
Win32 environments . . . 49
System requirements . . . 49
Installation and configuration . . . 49
CoS for IP parameters . . . 50
Windows 95, Windows 98, Windows NT, and Windows 2000 . . . 50
Novell NetWare Server . . . 52
LAN Client . . . 52
OS/2 . . . 53

Chapter 7. Redundant NIC 55
Supported environments 55
Overview 55
Benefits 56
Example scenarios 56
Managing a Redundant NIC NT server with the Agent 56
Quick Failover 56
Installation and configuration 57
Windows NT 57
NetWare 57
Using Redundant NIC software 62
Messages 67

Chapter 8. Tivoli Management Agent 75
Supported environments 75
Overview 75
Installation and configuration 75
Windows NT 75
Windows 95 and Windows 98 76
NetWare 3.x 76
NetWare 4.x and 5.x 76
OS/2 77
Windows 3.x 77
Activating the Tivoli Management Agent 77
Windows NT 77
Windows 95 and Windows 98 78
NetWare 3.x 79
NetWare 4.x and 5.x 80
OS/2 81
Windows 3.x 82

Chapter 9. Network adapter performance tuning 85

Appendix. Notices 87
Trademarks 88
NetWare Network Computing Products from IBM 88

Glossary 91

Index 103

About this manual

This manual contains information about installing and configuring the features of IBM token-ring adapters.

Who should read this manual

This manual is intended for use by network administrators and other end users who install and configure the features of IBM token-ring adapters.

How this manual is organized

"Chapter 1. Introduction" on page 1 describes where to download the software for your adapter.

"Chapter 2. RPL/PXE" on page 3 describes the Remote Program Load (RPL) function for your adapter.

"Chapter 3. IBM LAN Client" on page 31 describes how to install and configure the IBM LAN Client.

"Chapter 4. LAN Adapter Management Agent" on page 35 describes how to install and configure the IBM LAN Adapter Management Agent.

"Chapter 5. Route Switching" on page 39 describes how to install and configure Route Switching.

"Chapter 6. Class of Service" on page 47 describes how to install and configure the Class of Service (CoS) for IP function.

"Chapter 7. Redundant NIC" on page 55 describes how to install and configure the Redundant NIC function.

"Chapter 8. Tivoli Management Agent" on page 75 describes how to install and configure the Tivoli Management Agent.

"Chapter 9. Network adapter performance tuning" on page 85 describes how to get the best performance from your adapter.

Related publications

Refer to these publications for additional information:

- *IBM 16/4 Token-Ring Low Profile PCI Management Adapter User's Guide*
- *IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter User's Guide*
- *IBM 16/4 Token-Ring PCI Management Adapter User's Guide*
- *IBM 16/4 Token-Ring CardBus Adapter User's Guide*
- *IBM Token-Ring PCI Family Adapter User's Guide*
- *IBM Turbo 16/4 Token-Ring PC Card 2 User's Guide*
- *IBM Token-Ring Network Problem Determination Guide*, SX27-3710
- *IBM DOS LAN Services and Windows User's Guide*, S10H-9684
- Manuals for Novell IntranetWare Client for DOS and Windows 3.1 and Novell NetWare Server 4.x

- Manuals for Novell TCP/IP interface

Novell documentation can be obtained by contacting Novell on the Web or by calling their toll-free number:

`http://www.novell.com`

`1-800-NETWARE (1-800-638-9273)`

IBM adapter books and other documentation are available on the IBM Networking Web site:

`http://www.ibm.com/networking`

Chapter 1. Introduction

A local area network (LAN) adapter exists at the intersection of two complex environments—the computer and the network. The purpose of this manual is to provide the additional information necessary to extend the function of your token-ring adapter in the dimensions of the computer and the network.

This manual complements the installation and testing instructions manual or the user's guide for your adapter.

Operating efficiently in complicated multi-vendor environments requires a standards-based solution. The features in this manual are based on industry-wide standards such as the Intel® Wired for Management Baseline, the DMTF Desktop Management Interface, and the IETF Next Hop Routing Protocol. These standards-based solutions create a solid foundation for future enhancements necessary to keep pace in an ever-changing networked world.

These features take advantage of the increasing processing power in computers and provide adapter-based solutions in the areas of remote system setup, manageability, IP switching, class of service, and high availability. These solutions help your computer and network operate at a higher level of efficiency.

You should be familiar with the computer in which the features will be installed and the computer's operating system and network software.

Downloads

You can download the software implementing these features from the adapter CD-ROM or from the Web.

CD-ROM for IBM Token-Ring PCI Family Adapters

This procedure applies to the following adapters:

- IBM 16/4 Token-Ring PCI Adapter 2
- IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
- IBM High-Speed 100/16/4 Token-Ring PCI Adapter

To download software from the CD-ROM, perform the following steps:

1. Point your Web browser to *x*:\web\essmain (where *x* is your drive letter).
2. Select the appropriate adapter.
3. Select **Downloads**.
4. Select an operating system to expand its section and then select a download package.

CD-ROM for other IBM token-ring adapters

This procedure applies to the following adapters:

- IBM Turbo 16/4 Token-Ring PC Card 2
- IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring CardBus Adapter
- IBM 16/4 Token-Ring Low Profile PCI Management Adapter

To download software from the CD-ROM, perform the following steps:

1. Point your Web browser to *x*:\startcd (where *x* is your drive letter).
2. Select the appropriate adapter.
3. Select **Downloads**.
4. Select an operating system to expand its section and then select a download package.

Web

To download software from the Web, perform the following steps:

1. Point your Web browser to `http://www.ibm.com/networking/support`
2. Select the appropriate adapter from the list of IBM Networking Hardware products.
3. Select **Downloads**.
4. Select an operating system to expand its section and then select a download package.

Select the appropriate adapter from the list of IBM Networking Hardware products and then select **Downloads**. Select an operating system to expand its section, and then select a download package.

Chapter 2. RPL/PXE

This chapter describes the Remote Program Load (RPL) feature and the Preboot Execution Environment (PXE) feature.

PCI token-ring adapter RPL feature

If you are using the IBM Turbo 16/4 Token-Ring PC Card 2, see “IBM Turbo 16/4 Token-Ring PC Card 2 RPL feature” on page 22. Otherwise, see the following information.

Supported environments

RPL is supported on the following PCI adapters:
- IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Adapter 2
- IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
- IBM High-Speed 100/16/4 Token-Ring PCI Adapter
- IBM PCI Token-Ring Adapter
- IBM PCI Wake on LAN Token-Ring Adapter

The adapter supports RPL from the following servers:
- IBM OS/2® LAN Server Version 3.0
- IBM OS/2 LAN Server Version 4.0
- IBM OS/2 Warp Server
- Novell NetWare 4.11 or 4.2
- Novell NetWare 5.0
- Microsoft® Windows NT® 4.0
- IBM LANClient Control Manager (LCCM)

PCI token-ring adapter PXE feature

PXE is supported by several IBM token-ring PCI adapters.

Note: Consult your system administrator for information about whether your server supports PXE.

Supported environments

PXE is supported on the following adapters:
- IBM 16/4 Token-Ring Low Profile PCI Management Adapter
- IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Adapter 2
- IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
- IBM High-Speed 100/16/4 Token-Ring PCI Adapter
- IBM PCI Wake on LAN Token-Ring Adapter

Overview

The RPL feature enables an adapter to boot a computer using files that the computer receives from a LAN server. The computer that requests these files is referred to as the *client computer*, and the computer that responds with these files is referred to as the *LAN server*. In order for RPL to take place, two things must

occur. First, the RPL feature of the adapter in the client machine initiates the RPL request. Second, a LAN server responds to the RPL request with the files to bring up, or boot, the client computer.

The PCI token-ring adapters support PXE from any server that supports PXE 2.x. You can download the PXE specification from `http://developer.intel.com/ial/wfm/wfmspecs.htm`.

The following topics are addressed in this section:

- "Installation and configuration"
- "Setting up your OS/2 LAN Server to support RPL" on page 9
- "Setting up your Novell NetWare server to support RPL" on page 10
- "Setting up your Windows NT 4.0 server to support RPL" on page 12
- "RPL messages" on page 15
- "Troubleshooting RPL problems" on page 19

Installation and configuration

Setting up your client computer to support RPL/PXE

For the RPL/PXE process to begin, the feature must be enabled on the adapter installed in the client computer, and the client computer must recognize the RPL/PXE feature of the adapter as the first or only bootable device present.

Enabling the RPL/PXE feature on the adapter

The adapter is shipped with the RPL/PXE feature enabled. You can ensure that it is enabled by running the diagnostics and, at the diagnostics test panel, pressing **F5** to view or change the RPL setting.

Making the RPL/PXE feature the first bootable device

All IBM PCs support RPL, and many IBM-compatible PCs also do. If your computer is not an IBM PC, refer to your computer's user's manual or contact the manufacturer if you are not sure whether it supports RPL.

On most IBM PCs you can make this adapter the first bootable, or startup, device by choosing **Network** as the first startup device in the startup sequence in the configuration utility (usually you enter the configuration utility by pressing **F1** when the IBM logo and Configuration Utility program symbol appear during the power-on process). If drive A is the first bootable device, consider making the adapter the second bootable device. Refer to the user's manual for your IBM PC if you need further instructions for altering the startup sequence or entering the configuration utility.

Many non-IBM machines and some older IBM machines do not have a configuration utility, or do not allow a choice of a network-bootable device in the configuration utility. On these machines you can either remove the hard disk or use the RPLENABL.EXE utility program provided with this adapter in the RPLPKG.EXE package on the CD-ROM to disable the hard disk as a bootable device. After the hard disk is disabled as a bootable device, computers that support RPL adapters will attempt to boot from the network as long as no diskette is in the diskette drive.

Changing the boot protocol

The procedure for changing the boot protocol depends on your adapter's microcode level. To determine your adapter's microcode level, look at the AL- field displayed on the DHCP/PXE or RPL screen. There are two fields displayed, such as AL-00001 ALB1BG2.

If the second field has only six digits, or if the seventh digit is ″1″, as shown in the following examples, the microcode supports PXE 1.

```
AL-00001 PX10AH
AL-00001 ALB1BG1
```

If the seventh digit is ″2″, as shown in the following example, the microcode supports PXE 2.

```
AL-00001 ALB1BG2
```

The following adapters ship with PXE 1:

- IBM PCI Wake on LAN Token-Ring Adapter
- IBM 16/4 Token-Ring PCI Adapter 2
- IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
- IBM High-Speed 100/16/4 Token-Ring PCI Adapter

A PXE 2 flash update is available for these adapters at `http://www.ibm.com/networking/support`.

For the procedure to change the boot protocol, see "Changing the boot protocol (PXE 1.x)".

The following adapters ship with PXE 2:

- IBM 16/4 Token-Ring Low Profile PCI Management Adapter
- IBM 16/4 Token-Ring PCI Management Adapter
- IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter

A PXE 1 flash update is available at `http://www.ibm.com/networking/support`.

For the procedure to change the boot protocol, see "Changing the boot protocol (PXE 2.x)" on page 6.

Changing the boot protocol (PXE 1.x)

If the microcode on your adapter is flashed to support PXE 1.x, use the following procedure to change the boot protocol. If the microcode on your adapter is flashed to support PXE 2.x, see "Changing the boot protocol (PXE 2.x)" on page 6.

After you select RPL as the first startup, or boot, device you will see a DHCP panel when your client machine is booting. By default, the adapter will first try Dynamic Host Configuration Protocol (DHCP) as the first protocol. Any time before the client has connected to the DHCP server, you can press **Alt+S** to switch to RPL. The following figure is an example of the DHCP panel:

```
                  IBM PCI Token-Ring DHCP
ET-02:15:36
ID-268 0030
BU-0000
AA-0004AC570001
AL-000001 PX10AH
BL-CD0110
RM-C800
OP-0000 16

DD-0002
AR-
DR-
XR-
TR-
AC-8C00 00002000 8820
AE-000 OP-0011
Press ALT-S to switch to RPL
Press ESC to return to BIOS
Ending DHCP
```

```
                  IBM PCI Token-Ring RPL
ET-02:15:36
ID-268 0030
BU-0000
AA-0004AC570001
AL-000001 PX10AH
BL-CR1.0243
RM-C800
OP-0000 16

RQ-000F
SF-
SN-
RS-2010
PC-0606
AC-8C00 00002000 8820
AE-000 OP-0011
Press ALT-S to switch to DHCP
Press ESC to return to BIOS
Ending RPL
```

This example shows all of the possible error and status message prefixes. You will normally not see the error status condition prefixes, such as PC-, unless an error condition occurs. These error and status messages are described in “RPL messages” on page 15.

Changing the boot protocol (PXE 2.x)

If the microcode on your adapter is flashed to support PXE 2.x, use the following procedure to change the boot protocol. If the microcode on your adapter is flashed to support PXE 1.x, see “Changing the boot protocol (PXE 1.x)” on page 5.

Current operating system software installation programs either require your attendance in order to enter information in response to system prompts (attended installation) or do not require your attendance (unattended installation). To accommodate this mix of attended versus unattended, a menu in the Token Ring Option ROM is provided to guide you in setting up your Token Ring Option ROM.

You can access the menu at Option ROM initialization time. Use this menu to change the protocol (RPL or PXE) and the protocol’s behavior if the protocol fails to reach a boot server of the selected protocol or if the initial bootstrap returns control to the boot ROM code.

At option ROM initialization time, the following line is displayed:

```
Token-Ring ROM Initializing......
```

After the line appears, you have 5 seconds to press **Ctrl+S** to access the PCI Token Ring's boot protocol/protocol failure menu, as shown in the following example. If you do not press **Ctrl+S** within five seconds, the PCI token-ring's option ROM settings remain unchanged and the system boot continues.

If you press **Ctrl+S** within five seconds, the following options are displayed:

```
Token-Ring ROM Initializing......
1 PXE/Local Boot <<<< Current Mode
2 PXE only
3 RPL/Local Boot
4 RPL only
5 Local Boot
ESC-No Change
```

Note: <<<< Current Mode displayed beside an option indicates the current adapter setting. If you change the setting, <<<< Current Mode will display next to the new option the next time you reboot your system.

The options are described in the following table:

Option	Description
1 PXE/Local Boot	Use the PXE protocol. If the PXE protocol fails, or the initial downloaded bootstrap returns control to the token-ring adapter's boot ROM code, the boot ROM code will return control back to BIOS, and onto the next boot device.
2 PXE only	Use the PXE protocol. If the PXE protocol fails, or the initial downloaded bootstrap returns control to the token-ring adapter's boot ROM code, the boot ROM code will retry the PXE protocol. This will continue indefinitely.
3 RPL/Local Boot	Use the RPL protocol. If the RPL protocol fails, or the initial downloaded bootstrap returns control to the token-ring adapter's boot ROM code, the boot ROM code will return control back to BIOS, and onto the next boot device.
4 RPL only	Use the RPL protocol. If the RPL protocol fails, or the initial downloaded bootstrap returns control to the token-ring adapter's boot ROM code, the boot ROM code will retry the RPL protocol. This will continue indefinitely.
5 Local Boot	This option informs BIOS that this option ROM is not an IPL device, and therefore the option ROM will not be called to execute its boot protocol.
ESC	The current boot protocol or protocol failure is unchanged.

Select an option by pressing the option's number on the number row on your keyboard or on the numeric keypad (with the NumLock function enabled). The display confirms your selection.

Remember the following key points:

- The factory default setting is PXE only.
- After you have selected a different option, that option is saved between system reboots. If the menu prompt times out, the panel associated with this option is displayed.

- The **Ctrl+S** function is only for use by the system administrator. This key is not displayed on any of the panels.

If you select 1 PXE/Local Boot or 2 PXE only, a series of panels appear. The first panel appears during the initialization and opening of the adapter onto the ring.

```
                          PCI Token-Ring PXE                                CS200
ET-00:00:00                                                                 016Mb
ID-2460 068
BU-0000
AA-00112233445566
AL-000001 PX14CN2
BL-CS200
RM-C800
OP-0000 0016









RS-2010
AC/PC-0606
AE-000  OP-0011
```

The second panel appears after the adapter successfully opens onto the ring and starts the PXE/DHCP protocol.

```
                             PCI Token-Ring PXE                             CS200
ET-00:00:00                                                                 016Mb
UU-11223344556677889900112233445566           IP-17.17.17.2
DD-0001                                       SM-255.255.255.0
AR-0002                                    DHCPSvr-10.10.10.3
DR-0001                                     Router-17.17.17.8
XR-0001                                        SR1-0.0.0.0
                                               SR2-0.0.0.0
                                             BINL-10.10.10.5



TF-             TFTP IP-10.10.10.5        TFTPGW-17.17.17.8
c:\path\filename.ext
Press space bar to suspend NBP download




RS-2010
AC/PC-0606
AE-000  OP-0011
```

The third panel appears if the boot server has provided a PXE Boot menu giving you the option of which boot server to use.

```
                              PCI Token-Ring PXE                              CS200
ET-00:04:10                                                                   016Mb
Select Boot Server 10                          IP-17.17.17.2
Local Boot                                     SM-255.255.255.0
Bootserver 1                                DHCPSvr-10.10.10.3
Bootserver 2                                 Router-17.17.17.8
                                                SR1-0.0.0.0
                                                SR2-0.0.0.0
                                              BINL-10.10.10.5


BD-0001         BootSrv-10.10.10.4
TF-0001         TFTP IP-10.10.10.5        TFTPGW-17.17.17.8
c:\path\filename.ext
Press space bar to suspend NBP download  3
BIS-21



RS-2010
AC/PC-0606
AE-000  OP-0011
```

If you select 3 RPL/Local Boot or 4 RPL only, the following panel appears.

```
                            PCI Token-Ring RPL
  ET-00:15:36
  ID-268 0030
  BU-0000
  AA-0004AC570001
  AL-000001 PX14CN2
  BL-CS200
  RM-C800
  OP-0000 0016
  RQ-000F
  SF-
  SN-
  RS-2010
  PC-0606
  AC-8C00 00002000 8820
  AE-000 OP-0011
```

The example panels show all of the possible error and status message prefixes. You will normally not see the error status condition prefixes, such as PC-, unless an error condition occurs. These error and status messages are described in “RPL messages” on page 15.

Setting up your OS/2 LAN Server to support RPL

This manual assumes that you have already set up your OS/2 LAN Server for RPL and installed the DOS or OS/2 RPL image. If you have not, refer to the OS/2 LAN Server documentation and install RPL support before installing RPL support for the adapter on the OS/2 LAN Server. In summary, at this point you should have already performed the following steps:

1. Installed OS/2 LAN Server DOS or OS/2 RPL support.
2. Run RIPLINST.EXE if you installed OS/2 RPL support, to install an OS/2 RPL image. The RIPLINST.EXE utility is normally on diskette 7 of the OS/2 installation diskettes. You must use the **OS/2 unpack** command to unpack the RIPLINST file before you can run it.
3. Installed any service fix packs required:
   - LAN Server 3.0: IP07060 or later
   - LAN Server 4.0: IP08152 or later

Use the **OS/2 syslevel** command on your OS/2 LAN Server to check the CSD level.

4. Run any post-service updates for RPL described in the fix pack IP*xxxxx*.INF file (where *xxxxx* is the fix pack level being applied).
5. Run GETRPL.EXE to update the RPL access profiles. To do this, you must stop the RPL service and be logged on with administrator authority.
6. Enter **net start rpl** to start the RPL service.

After these steps are complete, run the following steps on the OS/2 LAN Server to add RPL support for the adapter:

1. Run *x*:\RPL\CFGRPL.CMD from the CD-ROM (where *x* is your CD-ROM drive letter) or the NDIS Drivers diskette in an OS/2 window.
2. Enter **net stop rpl** to stop the RPL service.
3. Run GETRPL.EXE to update the RPL access profiles To do this, you must stop the RPL service and be logged on with administrator authority.
4. Enter **net start rpl** to start the RPL service.
5. Create an RPL workstation image for each client computer with an adapter installed. This procedure is described in the LAN Server documentation. For the Server Record Identifier use:

Client Operating Environment	Record Identifier
OS/2 3.0	R_230_DTKTRP
DOS	R_DTKTRP_NDIS

Setting up your Novell NetWare server to support RPL

1. Power on a NetWare Client machine and log on to the NetWare Server with supervisor authority.
2. Copy the RPL.NLM file to the NetWare server \SYSTEM directory from the \RPL directory on the CD-ROM.
3. Copy the _0249.RPL file to the NetWare server \LOGIN directory from the \RPL directory on the CD-ROM.
4. Generate a bootable client diskette for this adapter, and run the DOSGEN program located in the \SYSTEM directory on the Novell NetWare Server. For information on running DOSGEN or for more detailed information on setting up unique RPL images for specific adapters, refer to the Novell NetWare documentation.

   The following steps are a sample procedure for creating a NetWare Client boot image:

   a. Prepare a bootable DOS diskette. Perform either step 4a1 for a VLM image or step 4a2 on page 11 for a NETX image:

      1) VLM image

         Place the following files on the bootable DOS diskette:

```
LSL.COM      AUTOEXEC.BAT  CONFIG.SYS    NET.CFG
VLM.EXE      IBMTRPO.EXE   ROUTE.COM     IPXODI.COM
REDIR.VLM    CONN.VLM      SECURITY.VLM  NWP.VLM
PRINT.VLM    IPXNCP.VLM    NDS.VLM       FIO.VLM
NETX.VLM     TRAN.VLM      BIND.VLM      GENERAL.VLM
```

         Your CONFIG.SYS file should have the following statements:

```
REM Use the DOS= and DEVICE= statements if you want to use high memory and XMS memory.
REM DOS=HIGH
REM DEVICE=A:\HIMEM.SYS
```

```
REM DEVICE=A:EMM386.EXE NOEMS
FILES=40
BUFFERS=20
LASTDRIVE=Z
```

Your AUTOEXEC.BAT file should have the following statements:

```
PATH A:\
SET NWLANGUAGE=ENGLISH
LSL
IBMTRPO
ROUTE
IPXODI
REM If you issue commands that reload COMMAND.COM,
REM you must also copy COMMAND.COM
REM to the NetWare Server \system directory and
REM uncomment the COMSPEC command statement below.
REM SET COMSPEC=F:\SYSTEM\COMMAND.COM
VLM
LOGIN yourID
```

2) NETX image

Place the following files on the bootable DOS diskette:

```
IBMTRPO.EXE  AUTOEXEC.BAT  LSL.COM       NETX.EXE
ROUTE.COM    IPXODI.COM    NET.CFG
```

Your AUTOEXEC.BAT should have the following statements:

```
PATH A:\
LSL
IBMTRPO
ROUTE
IPXODI
REM If you issue commands that reload COMMAND.COM,
REM you must also copy COMMAND.COM
REM to the NetWare Server \system directory and
REM uncomment the COMSPEC command statement below.
REM SET COMSPEC=F:\SYSTEM\COMMAND.COM
NETX
F:
LOGIN yourID
```

b. Update the diskette with IBMTRPO.EXE from the CD-ROM.

c. Generate the image using DOSGEN (see the Novell documentation for information regarding creating images and running DOSGEN).

Following is a sample of the NET.CFG file for VLM or NETX clients:

```
Link Driver IBMTRPO
        FRAME TOKEN-RING MSB
        DATARATE AUTO
        RXBUFFERS 9
        TXBUFFERS 1

NetWare DOS Requester
        FIRST NETWORK DRIVE = F
        NETWARE PROTOCOL = NDS BIND
```

5. Add the following two lines to the AUTOEXEC.NCF file located in the \SYSTEM directory on the NetWare Server:

```
load rpl
bind rpl to <driver>
```

where <driver> is the token-ring driver loaded on your NetWare Server.

Setting up your Windows NT 4.0 server to support RPL

Refer to the chapter on Remoteboot in the *Microsoft Windows NT Networking Guide* for the following features:

- Enabling TCP/IP or IPX support or both for your RPL client
- Troubleshooting problems in configuring Remoteboot service
- Configuring memory for MS—DOS RPL clients
- Using the Remoteboot Command Utility (RPLCMD.EXE)
- Using other Remoteboot Features and configuration shortcuts

Installing the Remoteboot service

1. If the DLC and NetBEUI protocols on the server are not already installed, click **Start → Settings → Control Panel**.
2. Double-click the **Protocol** tab and add the protocols.
3. Click the **Services** tab on the Network Dialog box and add the Remoteboot service.
4. In the Remoteboot Setup dialog box, make sure that c:\winnt\rpl is the correct path to install this service.
5. Leave Migrate Remoteboot directory from LAN Manager 2.2 unchecked and click **OK**.
6. When prompted, load the NT 4.0 server CD-ROM and access the subdirectories \i386 and \client\RPL to update the system.
7. Reboot the system to apply the changes.

Configuring DOS RPL client network settings

At a command prompt on the server, change to the c:\winnt\RPL\bblock\netbeui directory and create a directory named ibmtrp. Within the ibmtrp subdirectory create a PROTOCOL.INI file that has the following data in it:

```
 [protman]
  drivername = protman$
  dynamic = yes
  priority = netbeui

[netbeui_xif]
  drivername = netbeui$
  bindings = ibmtrp_nif
  names = 6
  ncbs = 12
  packets = 20
  pipeline = 10
  sessions = 6
  stacksize = 512
  lanabase = 0

[xnsnb_xif]
  drivername = xnsnb$
  bindings = ibmtrp_nif
  load = xnsnb[cbr]
  lanabase = 1

[xnstp_xif]
  drivername = xnstp$
  bindings = ibmtrp_nif
  load = xnstp[ub]
  lanabase = 1

[tcpip_xif]
  drivername = TCPIP$
  disabledhcp = (TCPIP_NO_DHCP)
```

```
  ipaddress0 = (TCPIP_ADDRESS)
  subnetmask0 = (TCPIP_SUBMASK)
  defaultgateway0 = (TCPIP_GATEWAY)
  tcpsegmentsize = 1450
  tcpwindowsize = 1450
  nbsessions = 6
  load = tcptsr[c],tinyrfc[c],emsbfr[cr]
  unload = "unloadt /notsr[dc]"
  bindings = ibmtrp_nif
  lanabase = 1

[ipx_xif]
  drivername = ipx$
  load = ipxmark[u],ipx[u]
  unload = ipxrel[c]
  bindings = ibmtrp_nif
  lanabase = 1

[msdlc_xif]
  drivername = msdlc$
  bindings = ibmtrp_nif
  load = msdlc[ub]
  unload = msdlc[u]

[ibmtrp_nif]
  drivername = ibmtrp$
  MaxTransmits = 2
  MaxTxFrameSize = 2048
  MinRcvBuffs = 8
  RcvBuffSize = 1120
```

Also, within that same subdirectory ibmtrp create a DOSBB.CNF file that has the following data in it:

```
;DOS RPL with IBM PCI Token-Ring Adapter
BASE CCH
RPL BBLOCK\RPLBOOT.SYS
LDR BBLOCK\RPLSTART.COM ~
DAT BBLOCK\NETBEUI\IBMTRP\PROTOCOL.INI
;DAT BBLOCK\NDIS\IBMTRP\LA1.MSG
DRV BBLOCK\RPLDISK.SYS ~ ~
EXE BBLOCK\RPLPRO1.COM ~ 2 ~
EXE BBLOCK\I13.COM ~ ~ ~
EXE BBLOCK\RPLBIND2.EXE ~ ~
EXE BBLOCK\PROTMAN.EXE ~ ~
EXE BBLOCK\RPLBIND1.EXE ~ ~
;DRV BBLOCK\IPXNDIS.DOS  ~ ~ ~
;DRV BBLOCK\TCPDRV.DOS /IDOS ~ ~
EXE BBLOCK\NETBEUI\NETBEUI.EXE ~ 10 ~
DRV BBLOCK\NDIS\IBMTRP.DOS /NOMSG 22 ~
DRV BBLOCK\PROTMAN.DOS /IDOS ~ M
```

Go to `http://www.ibm.com/networking/support` and download the IBM PCI Token-Ring Adapter driver diskette. Copy the following files from the DOS directory (a:\dos) to c:\winnt\rpl\bblock\ndis:

IBMTRP.DOS
LA1.MSG

Installing DOS files on the Remoteboot server

The Windows NT 4.0 Server support for RPL does not include the image for IBM DOS.

Note: If the DOS image is already on the server, skip to "Creating Remoteboot configurations for the PCI token-ring adapters".

1. Under winnt\rpl\rplfiles\binfiles on the RPL server, create a DOS700 directory.
2. Type **net use v:\\servername\rplfiles** to connect another computer running DOS with NDIS 2 networking support to the remoteboot server fplfiles share folder.
3. Copy all of the DOS files from the DOS client to the v:\binfiles\DOS700 directory as illustrated below as non hidden files:

```
Copy c:\dos\*.* v:\binfiles\dos700
Attrib -s -h c:\io.sys
Attrib -s -h c:\msdos.sys
Copy c:\io.sys v:\binfiles\dos700
Copy c:\msdos.sys v:\binfiles\dos700
Attrib +s +h c:\io.sys
Attrib +s +h c:\msdos.sys
```

4. Go to the winnt\rpl\fit directory on the RPL server.
5. Copy DOS622*.FIT to DOS700*.FIT.
6. Edit DOS700*.FIT and change all references of DOS622 to DOS700.
7. Go to the directory winnt\rpl\rplfiles\configs on the RPL server.
8. Create a DOS700 directory.
9. Copy all files and subdirectories from DOS622 to DOS700 (use the**xcopy** command with the /s option).
10. Make any custom modifications to the CONFIG.SYS or AUTOEXEC.BAT files.

Creating Remoteboot configurations for the PCI token-ring adapters

From a command prompt on the server, run RPLCMD.EXE. This utility allows you to add boot block records for the adapter and vendor ID. Use the following illustration to set up and configure a boot image for your adapter.

```
c:\> rplcmd
Adapter Boot Config Profile Service Vendor Wksta [Quit]: b
Add Del Enum: a
BootName=DOS700     **rpl client environment**
VendorName=002035   **the first 6 digits of the adapter's hexadecimal MAC address**
BbcFile=bblock\netbeui\ibmtrp\dosbb.cnf
     All other parameters are optional
BootComment=DOS 700 IBM PCI TOKEN RING
WindowSize=0

Adapter Boot Config Profile Service Vendor Wksta [Quit]: v
Add Del Enum: a
VendorName=002035      **the first 6 digits of the adapter's hexadecimal MAC address**
VendorComment=DOS 700 IBM PCI TOKEN RING

Adapter Boot Config Profile Service Vendor Wksta [Quit]: c
Add Del Enum: a
ConfigName=DOS700C

BootName=DOS700
DirName=DOS
DirName2=DOS700
FitShared=fits\dos700.fit
FitPersonal=fits\dos700p.fit
     All other parameters are optional
ConfigComment=DOS 700 IBM PCI TOKEN RING   ** Shown in step 4 below **
DirName3=
DirName4=

Adapter Boot Config Profile Service Vendor Wksta [Quit]: q
```

Creating a new workstation record automatically

1. Click **Start → Settings → Control Panel**.
2. From the Control Panel, select **Services**.
3. If the Remoteboot service is not set to automatic, click the **Start** button.
4. Click **Start → Programs → Administrative Tools →Remoteboot Manager**.
5. On the Remoteboot Manager window menu bar, select **Remoteboot → New Profile** from the menu bar.
6. In the Configuration list box, select **DOS 700 IBM PCI TOKEN RING**.
7. Type the name for the profile in the Profile Name field. For example, **TURBOTR1**.
8. On the Remoteboot Manager window menu bar, click **Remoteboot → New Workstation**.
9. On the New Remoteboot Workstation window, type the RPL client IBM PCI TOKEN RING MAC address in the Adapter ID field.
10. Type the workstation name in the Wksta Name field. For example, **WORKSTATION1**.
11. Type a brief description (optional). For example, **PCI TR IBM DOS 700**.
12. Change the password (optional).
13. Select shared or personal (optional).
14. Select **PCITR1 DOS 700 IBM PCI TOKEN RING** from the Wksta In Profile list box.
15. Configure the TCP/IP Settings (optional).
16. Click the **Add** button when done.

RPL messages

ET-00:00:45

Explanation: Elapsed Time. A continuously updated field indicating the elapsed time since the RPL feature gained control.

ID-268 BBDF

Explanation: Identification. An indication of which adapter is using the RPL feature. 268 indicates a PCI token-ring adapter. BBDF indicates the PCI bus, device, and function number for the PCI slot in which the adapter is inserted.

BU-0000

Explanation: Bring-Up. This field is displayed as X'0000' if the adapter has been successfully initialized and opened. If not, a code other than X'0000' is displayed and the field is highlighted. See “Troubleshooting RPL problems” on page 19.

AA-08005A2B0000

Explanation: Adapter address. The permanently encoded address of the token-ring adapter in your computer. This address is always 12 hexadecimal characters (6 bytes) long.

AL-000001 PX10AH

Explanation: Adapter Level. The Engineering Change (EC) level of the code on the token-ring adapter.

BL-CD0106

Explanation: BIOS Level (module level). The EC level of the code in the RPL feature.

RM-CC00

Explanation: Memory (read-only memory). Segment address in memory where BIOS has placed the RPL ROM.

OP-0000 0004

Explanation: Open Return Code. The first 4 digits are X'0000' and the last 4 digits identify the adapter data rate, if the adapter has been successfully opened and attached to the network. If not, a code other than X'0000' is displayed and the field is flashing. See “Troubleshooting RPL problems” on page 19.

RQ-0001

Explanation: Request Count (FIND Frame Count). The number in hexadecimal of FIND frames that have been transmitted. An excessive request count indicates that the LAN server is not present, is congested, or is not correctly configured to RPL this adapter.

SF-0001

Explanation: SEND.FILE.REQUEST Frame Count. The number of SEND.FILE.REQUEST frames that have been transmitted. An excessive SEND.FILE.REQUEST frame count indicates that the LAN server is not responding after having been found.

SN-0023

Explanation: File Response Sequence Number. This value is displayed when the LAN server has responded to the SEND.FILE.REQUEST. It indicates how many times valid FILE.DATA.RESPONSE frames have been received.

RS-0040

Explanation: Ring Status. This field displays a code indicating the status of the network. The field will be highlighted if the operation cannot continue; it will not be highlighted if processing can continue. See “Troubleshooting RPL problems” on page 19.

PC-4020

Explanation: Computer error. This field displays an error code indicating that the adapter has difficulty in functioning with the computer. In most cases, the panel will be frozen and this field will be highlighted because the adapter cannot continue. See “Troubleshooting RPL problems” on page 19.

AC-0040 0000 0000 0000

Explanation: Adapter check. The adapter has detected an internal error and cannot continue. Reboot your computer. If this problem persists, record the adapter check code, and contact your network administrator.

AE-*nnn* XX-0011

Explanation: Adapter error. The adapter in your computer could not establish communication with the LAN server. The *nnn* indicates the instance number. The reason for this error is indicated by the XX message to the right of AE-nnn. XX can be either BU or OP. The BU and OP messages are described previously in this section.

PXE messages

ET-00:00:45

Explanation: Elapsed Time. A continuously updated field indicating the elapsed time since the RPL feature gained control.

ID-268 BBDF

Explanation: Identification. An indication of which adapter is using the RPL feature. 268 indicates a PCI token-ring Adapter. BBDF indicates the PCI bus, device, and function number for the PCI slot in which the adapter is inserted.

BU-0000

Explanation: Bring-Up. This field is displayed as X'0000' if the adapter has been successfully initialized and opened. If not, a code other than X'0000' is displayed and the field is highlighted. See “Troubleshooting RPL problems” on page 19.

AA-08005A2B0000

Explanation: Adapter address. The permanently encoded address of the token-ring adapter in your computer. This address is always 12 hexadecimal characters (6 bytes) long.

AL-000001 PX10AH

Explanation: Adapter level. The Engineering Change (EC) level of the code on the token-ring adapter.

BL-CD0106

Explanation: BIOS level (module level). The EC level of the code in the RPL feature.

RM-CC00

Explanation: Memory (read-only memory). Segment address in memory where BIOS has placed the RPL ROM.

OP-0000 0004

Explanation: Open return code. The first 4 digits are X'0000' and the last 4 digits identify the adapter data rate, if the adapter has been successfully opened and attached to the network. If not, a code other than X'0000' is displayed and the field is flashing. See “Troubleshooting RPL problems” on page 19.

DD-0001

Explanation: DHCP discover count. The number in hexadecimal of DHCP Discover frames that have been transmitted. The field will be highlighted with a value of 0004 10 if the server is not present, is congested, or is not currently configured to respond to DHCP messages.

AR-0001

Explanation: ARP request count. The number in hexadecimal of ARP Requests broadcasted onto the network. If the field is highlighted as XXXX 00, the client received a reply to its ARP request. Check to see if any other machine is assigned the client’s IP address and check the DHCP server’s DHCP scope of addresses.

DR-0001

Explanation: DHCP request count. The number in hexadecimal of DHCP Request packets transmitted to the DHCP server/Proxy DHCP server. The field will be highlighted with a value of XXXX 10 if the server is not present, is congested, or is not correctly configured to respond to DHCP Request messages.

XR-0001

Explanation: Extended DHCP request count. The number in hexadecimal of Extended (PXE) DHCP Request packets transmitted to the Boot Image Negotiation Layer (BINL) server. The field will be highlighted with a value of XXXX 10 if the server is not present, is congested, or is not correctly configured to respond to Extended (PXE) DHCP Request messages.

TF-0009

Explanation: TFTP block count. The number in hexadecimal of UDP data packets received during the TFTP of the initial bootstrap program. The field will be highlighted with a value of XXXX 10, indicating a general timeout, if the server is not present or is congested. If the field is highlighted with a value of XXXX 3X, check the path and filename of the initial bootstrap program on the server and check if the server's TFTP program is active.

RS-0040

Explanation: Ring status. This field displays a code indicating the status of the network. The field will be highlighted if the operation cannot continue; it will not be highlighted if processing can continue. See "Troubleshooting RPL problems" on page 19.

PC-4020

Explanation: Computer error. This field displays an error code indicating that the adapter has difficulty in functioning with the computer. In most cases, the panel will be frozen and this field will be highlighted because the adapter cannot continue. See "Troubleshooting RPL problems" on page 19.

AC-0040 0000 0000 0000

Explanation: Adapter check. The adapter has detected an internal error and cannot continue. Reboot your computer. If this problem persists, record the adapter check code, and contact your network administrator.

AE-*nnn* XX-0011

Explanation: Adapter error. The adapter in your computer could not establish communication with the LAN server. The *nnn* indicates the instance number. The reason for this error is indicated by the XX message to the right of AE-nnn. XX can be either BU or OP. The BU and OP messages are described previously in this section.

IP-17.17.17.2

Explanation: This client's IP address provided by the DHCP server.

SM-255.255.255.0

Explanation: The subnet mask provided by the DHCP server.

DHCPSvr-10.10.10.3

Explanation: IP address of the DHCP server.

Router-17.17.17.8

Explanation: IP address of the router or gateway provided by the DHCP server.

SR1-0.0.0.0

Explanation: IP address of a static route provided by the DHCP server.

SR2-0.0.0.0

Explanation: IP address of a static route provided by the DHCP server.

BINL-10.10.10.5

Explanation: IP address of the Boot Image Negotiation Layer (BINL) service machine.

BD-0001

Explanation: How many boot server requests sent to the boot server.

BootSrv-10.10.10.4

Explanation: IP address of the boot server currently being queried for the initial Network Boot Program (NBP) or the IP address of the boot server providing the credentials for NBP authentication.

BIS-21

Explanation: A highlighted field indicating a Boot Integrity Services error has occurred.

Select Boot Server 10

Explanation: A list of available boot servers. The prompt is displayed followed by the number of seconds remaining before the first item in the boot menu is auto-selected. If a number is not present, there is no timeout. Use the up and down arrow keys to traverse the menu and press enter to select.

TFTP IP-10.10.10.5

Explanation: IP address of the server currently being used to download the initial Network Boot Program (NBP).

TFTPGW-17.17.17.8

Explanation: IP address of the gateway currently being used to download the initial Network Boot Program (NBP).

Troubleshooting RPL problems

If you do not get the expected results when using an RPL feature on a client computer, see Table 1 on page 20.

If other computers on the network need problem determination, you might need one or more of the following documents:

- The operator's guide for your computer
- The problem determination guide for network-related problems

Table 1. Failure indication messages

Failure Indication	Action
The computer's BASIC panel appears, or the computer boots to the hard disk or diskette drive.	Perform the steps in "Installation and configuration" on page 4.
The BU field on the client computer display panel is highlighted.	See "Bring-up error".
The OP field on the client computer display panel is highlighted.	See "Open error".
The RS field on the client computer display panel has a value other than zero (0) and is highlighted.	See "Ring status error" on page 21.
The PC field on the client computer display panel is highlighted or is shown with counters not being updated.	See "PC Error" on page 21.
The client computer display panel shows any response that has not been identified.	Contact your network administrator.

Bring-up error

The client computer display panel shows that the elapsed time (ET) field has stopped with only a few seconds of time accumulated, and the bring-up (BU) error field is highlighted. The RPL feature tried three times and was unable to initialize the adapter for use. The BU error codes and the action to take are listed in Table 2.

Table 2. Bring-up error causes and actions

BU Error Code	Cause	Action
0020-002F, 0030-003F	A module on the adapter is not responding correctly.	The adapter appears defective. Run the diagnostics.
0048	Initialize timeout.	The adapter appears defective. Run the diagnostics.
All others	Adapter failure	The adapter appears defective. Run the diagnostics. Contact your network administrator if problems persist.

Open error

The open error (OP) field contains an error code. This code might be displayed normally or flashing.

If the error code is flashing, the RPL feature is trying to open the adapter after an unsuccessful attempt.

If the problem persists, record the 4 digits of the flashing OP field. Using Open Error and the Reason Code as the symptom, refer to the *IBM Token-Ring Network Problem Determination Guide* to resolve the problem.

Table 3. Open error causes and actions

OP Error Code	Cause	Action
0011, 0010	No media attached.	Connect the UTP or STP cable to the adapter.
002D	A client computer is trying to be the first active computer on a token-ring network.	Start your RPL server. If the error persists, reboot the client computer.

Table 3. Open error causes and actions (continued)

OP Error Code	Cause	Action
All others	Adapter open failure.	Refer to the *IBM Token-Ring Network Problem Determination Guide*.

Ring status error

A ring error was detected when the RPL feature or bootstrap program was executing. The ring status (RS) error field contains the error code. Locate the error code in Table 4 to determine the correct action to take. Some values might be displayed that are a combination of the values listed in the table. The *x*'s used in the RS Error Code column can be any hexadecimal number from 0 through F.

Table 4. Ring status error causes and actions

RS Error Code	Cause	Action
C*xxx* to D*xxx*	• No receive signal was detected. • The network is beaconing. • The adapter is transmitting beacon frames.	Refer to the *IBM Token-Ring Network Problem Determination Guide*.
2000	This adapter has detected a soft-error condition.	No action required.
08*xx*	Wire fault. The adapter has detected a problem in itself or in its lobe.	Refer to the *IBM Token-Ring Network Problem Determination Guide*.
04*xx*	The adapter detected an internal hardware error.	Contact your network administrator.
*x*1*xx*	Remove received. This adapter was removed from the network.	Contact your network administrator for assistance.
0080	Counter overflow. One of the error log counters has incremented past 256.	Restart the computer.
0040 or 0060	Single station. The adapter has opened and is the only station on the network. This bit resets when another station inserts.	No action is required unless other stations are known to be operating on this network. If other stations are on the network, refer to the *IBM Token-Ring Network Problem Determination Guide*.
0020	Ring recovery. The adapter is transmitting or receiving claim token frames.	No action is required.
0004	Full-duplex. The adapter is operating in full-duplex mode.	No action is required.
All others	Reserved.	Contact your network administrator for assistance.

PC Error

The RPL feature has detected a problem with either the software or hardware in the client computer. Retry the operation by restarting the computer at least once. If the problem persists, locate the error code in Table 5 on page 22 to determine the correct action to take.

Table 5. PC error causes and actions

PC Error Code	Cause	Action
05*xx*	An invalid command control block (CCB) code was issued to the adapter support subset. *xx* = the CCB code.	Check the bootstrap program if it is user-written. If not, contact your network administrator for assistance. Provide the CCB code.
06*xx* (not highlighted)	PROGRAM.ALERT frames being transmitted. The *xx* portion of the value represents the alert code. 00 = Unexpected error response frame received. 02 = File not found. 04 = Out of memory space. 06 = Memory overrun. 08 = Unexpected DLC status received.	Restart the computer. If this error persists, contact your network administrator for assistance.
07*xx*	The adapter failed a wrap test. *xx* = system status block (SSB) return code.	The adapter appears defective. Run the diagnostics. Contact your network administrator if problems persist.
All others	A computer hardware or software error has occurred.	Perform the computer diagnostic test procedure or contact your network administrator for assistance.

IBM Turbo 16/4 Token-Ring PC Card 2 RPL feature

Supported environments

The IBM Turbo 16/4 Token-Ring PC Card 2 supports RPL from the following servers:

- IBM OS/2 LAN Server Version 3.0
- IBM OS/2 LAN Server Version 4.0
- IBM OS/2 Warp Server
- Novell NetWare 4.11 or later
- Novell NetWare 5.0
- Microsoft NT Server 4.0 Service Pack 3 or later

Overview

The Remote Program Load (RPL) function enables an adapter to boot a computer using files that the computer receives from a LAN server. The computer that requests these files is referred to as the *client computer*, and the computer that responds with these files is referred to as the *LAN server*. In order for RPL to take place, two things must occur. First, the RPL feature of the adapter in the client machine initiates the RPL request. Second, a LAN server responds to the RPL request with the files to bring up, or boot, the client computer.

The following sections are included here:

- "Installation and configuration" on page 23
- "Setting up your Windows NT 4.0 server to support RPL" on page 23
- "Setting up your OS/2 LAN Server to support RPL" on page 9
- "Setting up your Novell NetWare server to support RPL" on page 10
- "RPL messages" on page 27

Installation and configuration

Setting up your client computer to support RPL

For the RPL process to begin, the feature must be enabled on the adapter installed in the client computer, and the client computer must recognize the RPL feature of the adapter as the first or only bootable device present.

Enabling the RPL feature on the adapter

The adapter is shipped with the RPL feature enabled. To ensure that it is enabled, run the diagnostics and, at the diagnostics test panel, press **F5** to view or change the RPL setting.

Making the RPL feature the first bootable device

All IBM PCs support RPL, and many IBM-compatible PCs also do. If your computer is not an IBM PC, refer to your computer user manual or contact the manufacturer if you are not sure whether it supports RPL.

On most IBM PCs you can make this adapter the first bootable, or startup, device by selecting **Network** as the first startup device in the startup sequence in the configuration utility (usually you enter the configuration utility by pressing **F1** when the IBM logo and Configuration Utility program symbol appear during the power-on process). If drive A is the first bootable device, consider making the adapter the second bootable device. Refer to the user manual for your IBM PC if you need further instructions for altering the startup sequence or entering the configuration utility.

After you have successfully selected RPL as the first startup, or bootable, device you will see an RPL panel when your client computer is booting.

```
IBM Turbo 16/4 T-Ring PC Card RPL v1.01 (980921)
(C) Copyright 1991-1994 Novell, Inc. All Rights Reserved.
(C) Copyright 1996 IBM Corp. All Rights Reserved.

RPL-ROM-HSM: 200 BU-0000
RPL-ROM-HSM: 201 OP-0000 16

RPL-ROM-ADR: 0020 3556 6D87
RPL-ROM-IRQ: 2
RPL-ROM-MM1: D600
RPL-ROM-PIO: 0A20

RPL-ROM-FFC: 01
RPL-ROM-SFC: 02
RPL-ROM-SEQ: 01
RPL-ROM-ERR:
```

This example shows all of the possible error and status message prefixes. You will normally not see the error status condition prefixes, such as `RPL-ROM-ERR`, unless an error condition occurs. These error and status messages are described in “RPL messages” on page 27.

Setting up your Windows NT 4.0 server to support RPL

Please refer to the chapter on Remoteboot in the *Microsoft Windows NT Networking Guide* for the following features:

- Enabling TCP/IP or IPX support or both for your RPL client
- Troubleshooting problems in configuring Remoteboot service
- Configuring memory for MS-DOS® RPL clients
- Using the Remoteboot Command Utility (RPLCMD.EXE)
- Using other Remoteboot Features and configuration shortcuts

Installing the Remoteboot service

1. If the DLC and NetBEUI protocols on the server are not already installed, click **Start → Settings → Control Panel**.
2. Double-click the **Protocol** tab and add the protocols.
3. Click the **Services** tab on the Network Dialog box and add the Remoteboot service.
4. In the Remoteboot Setup dialog box, make sure that c:\winnt\rpl is the correct path to install this service.
5. Leave Migrate Remoteboot directory from LAN Manager 2.2 unchecked and click **OK**.
6. When prompted, load the NT 4.0 server CD-ROM and access the subdirectories \i386 and \client\RPL to update the system.
7. Reboot the system to apply the changes.

Configuring DOS RPL client network settings

At a command prompt on the server, change to the c:\winnt\RPL\bblock\netbeui directory and create a directory named ibmtokcs. Within the ibmtokcs subdirectory create a PROTOCOL.INI file that has the following data in it:

Note: Even though the DOS device driver file is called IBMTOKCS, the device driver is known to the operating system as IBMTOK.

```
 [protman]
  drivername = protman$
  dynamic = yes
  priority = netbeui

[netbeui_xif]
  drivername = netbeui$
  bindings = ibmtok_nif
  names = 6
  ncbs = 12
  packets = 20
  pipeline = 10
  sessions = 6
  stacksize = 512
  lanabase = 0

[xnsnb_xif]
  drivername = xnsnb$
  bindings = ibmtok_nif
  load = xnsnb[cbr]
  lanabase = 1

[xnstp_xif]
  drivername = xnstp$
  bindings = ibmtok_nif
  load = xnstp[ub]
  lanabase = 1

[tcpip_xif]
  drivername = TCPIP$
  disabledhcp = (TCPIP_NO_DHCP)
  ipaddress0 = (TCPIP_ADDRESS)
  subnetmask0 = (TCPIP_SUBMASK)
  defaultgateway0 = (TCPIP_GATEWAY)
  tcpsegmentsize = 1450
  tcpwindowsize = 1450
  nbsessions = 6
  load = tcptsr[c],tinyrfc[c],emsbfr[cr]
  unload = "unloadt /notsr[dc]"
```

```
  bindings = ibmtok_nif
  lanabase = 1

[ipx_xif]
  drivername = ipx$
  load = ipxmark[u],ipx[u]
  unload = ipxrel[c]
  bindings = ibmtok_nif
  lanabase = 1

[msdlc_xif]
  drivername = msdlc$
  bindings = ibmtok_nif
  load = msdlc[ub]
  unload = msdlc[u]

[ibmtok_nif]
  drivername = ibmtok$
  MaxTransmits = 2
  MaxTxFrameSize = 2048
  MinRcvBuffs = 8
  RcvBuffSize = 1120
```

Also, within that same subdirectory ibmtokcs create a DOSBB.CNF file that has the following data in it.

```
;DOS RPL with IBM Turbo 16/4 Token-Ring Adapter
BASE 1A0H
RPL BBLOCK\RPLBOOT.SYS
LDR BBLOCK\RPLSTART.COM ~
DAT BBLOCK\NETBEUI\IBMTOKCS\PROTOCOL.INI
;DAT BBLOCK\NDIS\IBMTOKCS\LA1.MSG
DRV BBLOCK\RPLDISK.SYS ~ ~ ~
EXE BBLOCK\RPLPRO1.COM ~ 2 ~
EXE BBLOCK\I13.COM ~ ~ ~
EXE BBLOCK\RPLBIND2.EXE ~ ~
EXE BBLOCK\PROTMAN.EXE ~ ~
EXE BBLOCK\RPLBIND1.EXE ~ ~
;DRV BBLOCK\IPXNDIS.DOS  ~ ~ ~
;DRV BBLOCK\TCPDRV.DOS /IDOS ~ ~
EXE BBLOCK\NETBEUI\NETBEUI.EXE ~ 10 ~
DRV BBLOCK\NDIS\IBMTOKCS.DOS
DRV BBLOCK\PROTMAN.DOS /IDOS ~ M
```

Go to `http://www.ibm.com/networking/support` and download the IBM Turbo 16/4 Token-Ring Adapter driver diskette. Copy the following files from the DOS directory (a:\dos) to c:\winnt\rpl\bblock\ndis:

IBMTOKCS.DOS
LA1.MSG

Installing DOS files on the Remoteboot server

The Windows NT 4.0 Server support for RPL does not include the image for IBM DOS.

Note: If the DOS image is already on the server, skip to “Creating Remoteboot configurations for the IBM Turbo 16/4 Token-Ring Adapter” on page 26.

1. Under winnt\rpl\rplfiles\binfiles on the RPL server, create a DOS700 directory.
2. Type **net use v:\\servername\rplfiles** to connect another computer running DOS with NDIS 2 networking support to the remoteboot server fplfiles share folder.

3. Copy all of the DOS files from the DOS client to the v:\binfiles\DOS700 directory as illustrated below as non hidden files:

```
Copy c:\dos\*.* v:\binfiles\dos700
Attrib -s -h c:\io.sys
Attrib -s -h c:\msdos.sys
Copy c:\io.sys v:\binfiles\dos700
Copy c:\msdos.sys v:\binfiles\dos700
Attrib +s +h c:\io.sys
Attrib +s +h c:\msdos.sys
```

4. Go to the winnt\rpl\fit directory on the RPL server.
5. Copy DOS622*.FIT to DOS700*.FIT.
6. Edit DOS700*.FIT and change all references of DOS622 to DOS700.
7. Go to the directory winnt\rpl\rplfiles\configs on the RPL server.
8. Create a DOS700 directory.
9. Copy all files and subdirectories from DOS622 to DOS700 (use the**xcopy** command with the /s option).
10. Make any custom modifications to the CONFIG.SYS or AUTOEXEC.BAT files.

Creating Remoteboot configurations for the IBM Turbo 16/4 Token-Ring Adapter

From a Windows NT 4.0 Remoteboot server command prompt, run RPLCMD.EXE. This utility allows you to add boot block records for the adapter and vendor ID. Follow the illustration below to set up and configure a boot image for your adapter.

```
c:\> rplcmd
Adapter Boot Config Profile Service Vendor Wksta [Quit]: b
Add Del Enum: a
BootName=DOS700     **rpl client environment**
VendorName=002035   **the first 6 digits of the adapter's hexadecimal MAC address**
BbcFile=BBLOCK\NETBEUI\IBMTOKCS\DOSBB.CNF
     All other parameters are optional
BootComment=DOS 700 IBM TURBO 16/4 TOKEN RING
WindowSize=0

Adapter Boot Config Profile Service Vendor Wksta [Quit]: v
Add Del Enum: a
VendorName=002035 **the first 6 digits of the adapter's hexadecimal MAC address**
VendorComment=DOS 700 IBM TURBO 16/4 TOKEN RING

Adapter Boot Config Profile Service Vendor Wksta [Quit]: c
Add Del Enum: a
ConfigName=DOS700C

BootName=DOS700
DirName=DOS
DirName2=
FitShared=fits\dos700.fit
FitPersonal=fits\dos700p.fit
     All other parameters are optional
ConfigComment=DOS 700 IBM TURBO 16/4 TOKEN RING   ** shown in step 4 below **
DirName3=
DirName4=

Adapter Boot Config Profile Service Vendor Wksta [Quit]: q
```

Creating a new workstation record automatically

1. Click **Start → Settings → Control Panel**.
2. From the Control Panel, select **Services**.
3. If the Remoteboot service is not set to automatic, click the **Start** button.

4. Click **Start → Programs → Administrative Tools →Remoteboot Manager**.
5. On the Remoteboot Manager window menu bar, select **Remoteboot → New Profile** from the menu bar.
6. In the Configuration list box, select **DOS 700 IBM TURBO 16/4 TOKEN RING**.
7. Type the name for the profile in the Profile Name field. For example, **TURBOTR1**.
8. On the Remoteboot Manager window menu bar, click **Remoteboot → New Workstation**.
9. On the New Remoteboot Workstation window, type the RPL client IBM TURBO 16/4 TOKEN RING MAC address in the Adapter ID field.
10. Type the workstation name in the Wksta Name field. For example, **WORKSTATION1**.
11. Type a brief description (optional). For example, **TURBO TR IBM DOS 700**.
12. Change the password (optional).
13. Select shared or personal (optional).
14. Select **TURBOTR1 DOS 700 IBM TURBO 16/4 TOKEN RING** from the Wksta In Profile list box.
15. Configure the TCP/IP Settings (optional).
16. Click the **Add** button when done.

RPL messages

RPL-ROM-HSM: BU-0000

Explanation: Bring-Up. This field is displayed as X'0000' if the adapter has been successfully initialized. If not, a code other than X'0000' is displayed and the field is highlighted. See “Troubleshooting RPL problems” on page 28.

RPL-ROM-HSM: OP-0000 16

Explanation: Open Return Code. The first 4 digits are X'0000' and the last 2 digits identify the adapter data rate, if the adapter has been successfully opened and attached to the network. If not, a code other than X'0000' is displayed and the field is flashing. See “Troubleshooting RPL problems” on page 28.

RPL-ROM-ADR: 0020 3556 6D87

Explanation: Adapter Address. The permanently encoded address of the token-ring adapter in your computer. This address is always 12 hexadecimal characters (6 bytes) long.

RPL-ROM-IRQ: 2

Explanation: Interrupt. The system interrupt level that the adapter currently occupies.

RPL-ROM-MM1: D600

Explanation: Memory (read-only memory). Segment address in memory where BIOS has mapped the RPL ROM code.

RPL-ROM-MM2: D800

Explanation: Memory (random-access memory). Segment address in memory where BIOS has mapped the token-ring adapter’s RAM.

RPL-ROM-PIO: 0A20

Explanation: System I/O address. The I/O address that the adapter currently occupies in the system.

RPL-ROM-FFC: 01

Explanation: Request Count (FIND Frame Count). The number (in hexadecimal) of FIND frames that have been transmitted. An excessive request count indicates that the LAN server is not present, is congested, or is not correctly configured to RPL this adapter.

RPL-ROM-SFC: 02

Explanation: SEND.FILE.REQUEST Frame Count. The number of SEND.FILE.REQUEST frames that have been transmitted. An excessive SEND.FILE.REQUEST frame count indicates that the LAN server is not responding after having been found.

RPL-ROM-SEQ: 01

Explanation: File Response Sequence Number. This value is displayed when the LAN server has responded to the SEND.FILE.REQUEST. It indicates how many times valid FILE.DATA.RESPONSE frames have been received.

RPL-ROM-ERR:

Explanation: Computer error. This field displays an error code indicating that the adapter has difficulty in functioning with the computer. In most cases, the panel will be frozen and this field will be highlighted because the adapter cannot continue. See “Troubleshooting RPL problems”.

Troubleshooting RPL problems

The following chart is helpful if you do not get the expected results when you use an RPL feature on a client computer.

If other computers on the network need problem determination, you might need one or more of the following documents:

- The operator’s guide for your computer
- The problem determination guide for network-related problems

Table 6. Failure indication messages

Failure Indication	Action
The computer’s BASIC panel appears, or the computer shows a diagram to insert a diskette into the diskette drive, or boots to the hard disk or diskette drive.	Perform the installation steps for your adapter.
The BU field on the client computer display panel is not X'0000'.	See “Bring-up error”.
The OP field on the client computer display panel is not X'0000'.	See “Open error” on page 29.
The Client computer display panel shows any response that has not been identified.	Contact your network administrator.

Bring-up error

The bring-up (BU) field is not X'0000'. The RPL feature is unable to initialize the adapter for use. The BU error codes and the action to take are listed here:

Table 7. Bring-up error codes

BU Error Code	Cause	Action
0020-002C	A module on the adapter is not responding correctly.	The adapter appears to be defective. Run the adapter diagnostics.
0048	Initialization timeout.	The adapter appears to be defective. Run the adapter diagnostics.
All others.	Adapter failure.	The adapter appears to be defective. Run the adapter diagnostics. Contact your network administrator if problems persist.

Open error

The open error (OP) field contains an error code. If the OP field is not X'0000', the RPL feature is trying to open the adapter after an unsuccessful attempt. If the problem persists, record the 4 digits of the OP field. Using Open Error and the Reason Code as the symptom, refer to the *IBM Token-Ring Network Problem Determination Guide* to resolve the problem.

Table 8. Open error codes

OP Error Code	Cause	Action
0011, 0010	No media attached.	Connect the cable to the adapter or to the token-ring concentrator or both.
002D	The adapter detected that it was the only adapter present in the ring during the open command it it has removed itself from the ring.	Start your RPL server. If the error persists, reboot the client computer.
002E	The adapter could not detect frames during the **open** command and has removed itself from the ring. This indicates that either the adapter is running at the wrong speed and does not have circuitry to detect it, or there is something wrong with the access unit or cabling to which the adapter is connected.	Connect the cable to the adapter or to the token-ring concentrator or both. Check if you are using the correct cable.
All Others	Adapter open failure.	Refer to the *IBM Token-Ring Network Problem Determination Guide*.

Chapter 3. IBM LAN Client

This chapter describes the IBM LAN Client features.

Supported environments

This section lists the adapters, software, and operating systems supported by the IBM LAN Client.

Supported IBM LAN adapters

IBM LAN Client provides support for the following adapters:

- IBM Token-Ring PCI Family Adapters
  - IBM 16/4 Token-Ring PCI Adapter 2
  - IBM 16/4 Token-Ring PCI Special
  - IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
  - IBM High-Speed 100/16/4 Token-Ring PCI Adapter
- IBM PCI Token-Ring Adapter
- IBM PCI Wake on LAN Token-Ring Adapter
- IBM Auto LANStreamer PCI Adapter
- IBM Auto 16/4 Token-Ring ISA Adapter
- IBM Token-Ring 16/4 ISA-16 Adapter
- IBM Token-Ring Auto 16/4 Credit Card Adapter (PCMCIA)
- IBM Auto 16/4 Token-Ring MC Adapter
- IBM Token-Ring 16/4 Adapter/A
- IBM Auto-Wake 16/4 Token-Ring ISA Adapter
- IBM Turbo 16/4 Token-Ring ISA Adapter
- IBM Turbo 16/4 Token-Ring PC Card (PCMCIA)
- IBM Turbo 16/4 Token-Ring PC Card 2

The device driver needed for the adapter to operate with the IBM LAN Client software is provided on the adapter product CD-ROM. The following drivers are provided:

- TOKEN.LAN — for ISA, Micro Channel®, and PCMCIA token-ring adapters
- IBMMPCO.LAN — for the IBM Auto LANStreamer PCI Adapter
- IBMTRPO.LAN — for the IBM Token-Ring PCI Family Adapters

The installation program will copy the driver to your workstation hard disk when you tell it which adapter you will be using. It will also provide the correct load statements in STARTNET.BAT.

Supported software

IBM LAN Client provides support for the following protocols and client applications:

For DOS 5.0 or later:

- IEEE 802.2
- NetBIOS
- DOS LAN Services 5.x (with IBM Warp Server)
- Novell IntranetWare Client for DOS and Windows 3.1 (with Novell NetWare 2.15c and later)
- PC3270 Version 4.x
- DCAF (Version 1.3 + CSDs)
- Artisoft LANtastic Version 6.0

- Attachmate 3270 Emulation
- LANDP® (If you are using Version 2, make sure that the service level of LAN.EXE is MS004 or later.)

For Windows 3.1, Windows 3.11, and Windows for Workgroups 3.11:

- IEEE 802.2
- NetBIOS
- DOS LAN Services 5.x (with IBM Warp Server)
- Novell IntranetWare Client for DOS and Windows® 3.1 (with Novell NetWare 4.x)
- AS/400® for Windows (Version 4.0, V3R1M0, and V3R1M1)
- TCP/IP using Winsock 1.1 or 1.2
- PC3270/Windows Version 4.x
- Artisoft LANtastic Version 6.0
- APPC/Windows

Note: IBM LAN Station Manager cannot be run in the same workstation as IBM LAN Client.

Supported operating systems

IBM LAN Client supports the following desktop operating systems:

- MS-DOS 5.x and 6.x
- PC-DOS 5.x, 6.x, and 7.0
- Windows 3.1 and 3.11, in enhanced mode
- Windows for Workgroups 3.11

Restrictions for this release

The following restrictions apply for this release of IBM LAN Client:

- IBM LAN Client will operate with only one adapter.
- IBM LAN Client does not support the RPL function.

Overview

IBM LAN Client provides program interfaces to support network application programs using selected IBM Token-Ring adapters. It allows a DOS/Windows client workstation to communicate with an IBM LAN Server at Version 3.0, 4.0, and Warp Server, or with a Novell NetWare Server at Version 2.15c or later, or to use TCP/IP applications in Windows. (The IBM and Novell client code is included with this package but, with the exception of PING, TCP/IP applications are not.) In addition, support is provided for programs written to the NetBIOS or IEEE 802.2 application programming interfaces.

Benefits

- Requires as little as 4 KB conventional memory. (See “DOS conventional memory usage reduction” on page 33 for more details.)
- Uses one common environment for concurrent multiple protocols.
- One or more of NetBIOS, IPX, TCP/IP, and IEEE 802.2.
- Does not require shim modules, such as ODINSUP and LANSUP.
- Includes client software for attachment to Novell NetWare Servers or IBM LAN Servers.
- Includes DOS LAN Services 5.x.

- Includes Novell IntranetWare Client for DOS and Windows 3.1.
- Provides full access to essential NetWare services such as NetWare Directory Services (NDS).
- Provides improved connection reliability, including the ability to auto-reconnect open files.
- Provides enhanced large Internet packet (LIP) and packet burst support.
- Includes an installation tool with a graphical user interface (GUI) for easy installation of client software.
- Includes a command-line version of the installation tool for use by network administrators who are installing on a large number of workstations.
- Allows the same adapter device driver to be used for client workstations and for Novell NetWare servers, reducing support complexity.

DOS conventional memory usage reduction

IBM LAN Client minimizes the use of DOS conventional memory for network communications. With LAN Client, the LAN adapter drivers and protocol stacks no longer require large amounts of DOS memory. Table 9 shows the memory requirements LAN Client, compared with existing implementations. This table shows how much DOS conventional memory is used by LAN Client for three popular communication protocols, compared with current usage.

Table 9. Memory reduction when using LAN Client

Protocol	Before IBM LAN Client	With IBM LAN Client
IPX	59 KB	5 KB
IEEE 802.2	95 KB	4 KB
NetBIOS	95 KB	4 KB

Installation and configuration

1. Run LCINST.EXE from the root directory of the CD-ROM if you have one of the IBM Token-Ring PCI Family Adapters or from the \lanclnt directory if you have the IBM Turbo 16/4 Token-Ring PC Card 2. You can also run it from the installed version of LCINST from the LAN Client diskettes or the self-extracting package file (LCPKG.EXE).

   Note: To install LCINST to a hard disk from the LAN Client diskettes, insert LAN Client diskette 1 in drive A and enter **install**.
2. Select your software environment from the first IBM LAN Client Installation panel (DOS, Windows, or Windows for Workgroups).
3. Select your adapter from the IBM LAN Client Adapter Selection panel.
4. Continue to the IBM LAN Client Application and Protocol Selection panel.
5. Select the protocols to install and click **OK**.
6. Select the tabs on the IBM LAN Client Configuration panel to configure each protocol.
7. Select **Install**.
8. Reboot your computer when prompted.

   Note: The command line version (LCINSTC.EXE) can also be used to install IBM LAN Client. For a list of valid parameters that can be used with the command line version, type **lcinstc /h** and press **Enter**.

Chapter 4. LAN Adapter Management Agent

This chapter describes the features of the IBM LAN Adapter Management Agent.

Supported environments

LAN adapters

The IBM LAN Adapter Management Agent supports any IBM LAN adapter with a device driver for the operating systems listed in the following section. The latest LAN adapter drivers provide the most manageability of the LAN adapter.

Operating systems

For Windows environments, the Agent requires that Windows NT Workstation or Windows NT Server Version 3.51 or later, Windows 95, Windows 98, or Windows 2000 be installed on the system. The Agent implements Desktop Management Interface (DMI) Version 2.0 on Windows NT, Windows 95, Windows 98, and Windows 2000. Windows environments support SNMP Version 1.

For OS/2 environments, the Agent requires that OS/2 Version 3.0 or later be installed on the system. The Agent implements DMI version 1.0 on OS/2. OS/2 environments support SNMP Version 2.

Overview

The IBM LAN Adapter Management Agent makes IBM LAN adapters visible to management applications using industry-standard management techniques. The Agent provides manageability using either the Simple Network Management Protocol (SNMP) or the DMI.

SNMP is the most common management-oriented protocol. The IBM LAN Adapter Management Agent can be coupled with IBM Nways® Management Applications to remotely manage IBM LAN adapters resident in the Agent's workstation. The Agent can generally be managed by any SNMP-compliant management application.

DMI is a programming interface developed by members of the PC industry to bring management and control to PC systems. DMI browsers, which are supplied in the Agent package, can also manage other systems using standard communications protocols. DMI is also used by many workgroup management applications.

The Agent runs on Microsoft Windows NT, Windows 95, Windows 98, Windows 2000, and IBM OS/2 workstations and provides an easy-to-use installation process for each environment. Management using SNMP and DMI is available for each operating environment. Some of the attributes provided by the Agent are:

- General: product name, bus information, functional state
- Resources: memory areas, I/O ports, interrupt levels
- Counters: packets and bytes transmitted/received, ring utilization
- Drivers: name, version, specification level
- Addresses: universally administered, locally administered, multicast/functional
- Capabilities: Wake on LAN, auto-sense, full-duplex
- Power management information: wake-up information, power states
- Class of Service: TCP and UDP port range information, priority transmit counters

- Route switching: current route switching mode, switched packet counter
- Redundant NIC information: status, failover notification, failover trigger

Benefits

The IBM LAN Adapter Management Agent allows you to manage the LAN adapters in PC systems.

System requirements

Windows NT, Windows 95, Windows 98, and Windows 2000 software requirements

Before you can install the SNMP function of the IBM LAN Adapter Management Agent on Windows platforms, the SNMP Service must already be installed at the Agent's station. This is because the Agent needs to add entries to the SNMP Service registry parameters. The SNMP Service enables a Windows end station to be administered remotely with an SNMP management tool. The DMI function of the Agent has no installation prerequisites for Windows NT, Windows 95, Windows 98, and Windows 2000.

OS/2 software requirements

The Agent requires that TCP/IP for OS/2 Version 3.0 or later be installed on the OS/2 system.

IBM Nways Management Applications

Web-based device management using Java® technology is provided by coupling the Agent and IBM Nways Management Applications. A LAN adapter management application is provided by:

- Nways Workgroup Manager for Windows NT, Version 1.1 or later
- Nways Manager for AIX®, Version 1.2 or later
- Nways Manager for HP-UX, Version 1.2 or later

Installation and configuration

Windows NT, Windows 95, Windows 98, and Windows 2000

To install the IBM LAN Adapter Management Agent, run the SETUP.EXE program from a diskette, or execute the appropriate self-extracting installation package. The following major components are installed:

- DMI service provider
- DMI instrumentation for IBM LAN adapters
- SNMP extension agent
- DMI browser application

The DMI service provider and the DMI instrumentation are installed as Windows Services. On Windows NT, they are originally given a Startup Type of Automatic. On Windows 95 and Windows 98, they are started in the RunServices registry key. The DMI service provider has the service name Win32sl. The SNMP extension agent is used in conjunction with Microsoft's SNMP extensible agent service to provide a mapping between SNMP and DMI. The DMI Browser application provided is the Intel DMI Explorer. The DMI browser application, this document, and a deinstall icon are contained in the IBM LAN Adapter Management Agent folder.

OS/2

To install the Agent, run the INSTALL.EXE program from the installation media. The following components are installed:

- DMI service provider
- DMI instrumentation for IBM LAN adapters
- DMI-to-SNMP mapper
- SNMP daemon
- DMI browser application

For OS/2 Version 3.0, the DMI service provider and the DMI instrumentation are started automatically by commands in CONFIG.SYS. The DMI-to-SNMP mapper (DMISA.EXE) and SNMP daemon (SNMPD.EXE) start automatically from the system's Startup folder. To start the DMI browser, double-click the icon in the IBM LAN Adapter Management Agent for OS/2 folder.

If you have previously installed the SystemView® Agent for OS/2 on your OS/2 Version 3.0 workstation, some of the SNMP and DMI management components will already exist. The DMI service provider is started automatically in CONFIG.SYS. The DMI-to-SNMP mapper (DMISA.EXE) and SNMP daemon (SNMPD.EXE) start automatically from the System Startup folder. To start the DMI browser, double-click the icon in the SystemView Agent for OS/2 folder. The DMI instrumentation for IBM LAN adapters is provided by the INSTALL program and configured to start automatically from CONFIG.SYS.

For OS/2 Version 4.0, some of the SNMP and DMI management components are already provided by the base operating system. The DMI service provider is always running. The DMI-to-SNMP mapper, SNMP daemon, and DMI browser are part of the System Management Agent folder, in the Utility program folder. The System Management Agent folder provides separate icons for startup and configuration of the System Management Agent. The DMI instrumentation for IBM LAN adapters is provided by the INSTALL program and is configured to start automatically from CONFIG.SYS.

The IBM LAN Adapter Management Agent for OS/2 folder will always include this document and a deinstall icon.

If you alter the adapter configuration in your OS/2 system, you can use the MPTS Configuration program to bind the IBM LAN Adapter Management Agent for OS/2 to the LAN adapters of your choice. Go into the Adapter and Protocol Configuration menu and add the IBM LAN Adapter Management Agent for OS/2 for the adapters that you want to manage.

Example scenarios

Remote DMI

Remote DMI allows the DMI Browser to manage IBM LAN adapters in other PC systems. Remote DMI exists only with DMI Version 2.0. The DMI Browser must be started with command line parameters for Remote DMI. The underlying distribution mechanism for Remote DMI is the Remote Procedure Call Network Service. The functionality of Remote DMI is contained in the DMI Browser (IDMIEX.EXE) and the DMI Service Provider (WIN32SL.EXE). To use Remote DMI, configure the Remote Procedure Call (RPC) Network Service and then start the DMI Browser with the appropriate command line parameters.

1. Configure RPC Network Services:

a. Click **Start → Settings → Control Panel**.
b. From the Control Panel, select **Network**.
c. Select **RPC Configuration** and select **Properties**.
   The Properties are:
   - Name Service Provider: Select **DCE Cell Directory Service**.
   - Network Address: Provide the host name or IP address of the remote PC system to be managed.
   - Security Service Provider: This can remain Windows NT Security Service.

d. Select **OK** and then close the Network Panel.

2. Start the DMI Browser and direct it to manage a remote PC system:
   a. From a command prompt change to the Agent installation directory.
   b. Change to the \bin subdirectory within the Agent install directory.
   c. Start a DMI Browser instance. The general syntax of the command is:

```
idmiex /path "dce|tcpip|hostname"
```

   Some specific examples are:

```
idmiex /path "dce|tcpip|9.37.233.1"
idmiex /path "dce|tcpip|server99"
```

   Note: The DMI Browser in the Agent pulldown menu will manage the local system.

MIB browsing

When you use an SNMP-based manager and its MIB browser, the general steps are:

1. Copy the MACDMI.MIB file from the <install dir>\SNMPMGRS path, to the appropriate directory on the manager station. The destination directory is most likely the same location where all the other *.MIB files are located. For example, when you use NetView® for AIX, this is the /usr/OV/snmp_mibs directory.
2. Load/Install the MACDMI.MIB file into the manager's MIB database. If you are using NetView for AIX, start NetView for AIX, select **OPTIONS** and then the **LOAD/UNLOAD** option.
3. View the information provided by the IBM LAN Adapter Management Agent by traversing the MIB tree and browsing to:

```
iso.org.dod.internet.private.enterprises.ibm.ibmArchitecture.ibmDmi.
     mibsFromMifs.ibmLanAdapter.dmtfGroups
```

   or

```
1.3.6.1.4.1.2.5.11.1.8.1
```

Chapter 5. Route Switching

This chapter describes the Route Switching feature of the IBM token-ring adapters.

Supported environments

	Windows NT 3.51, 4.0	Windows 95, 98, 2000	Windows 3.x	OS/2 Warp 3.0 and later	Novell NetWare Server
IBM 16/4 Token-Ring CardBus Adapter	Supported (Windows NT 4.0 only)	Supported	Not supported	Supported	Not supported
IBM 16/4 Token-Ring Low Profile PCI Management Adapter	Supported (Windows NT 4.0 only)	Supported (Windows 98 and Windows 2000 only)	Not supported	Not supported	Not supported
IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter IBM 16/4 Token-Ring PCI Management Adapter	Supported	Supported	Not supported	Supported	Supported
IBM High-Speed 100/16/4 Token-Ring PCI Adapter IBM 16/4 Token-Ring PCI Adapter 2 IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN IBM PCI Token-Ring Adapter IBM PCI Wake on LAN Token-Ring Adapter	Supported	Supported	Supported (using LAN Client)	Supported	Supported
IBM Turbo 16/4 Token-Ring ISA Adapter IBM Auto-Wake 16/4 Token-Ring ISA Adapter	Supported (client mode only)	Not supported	Not supported	Not Supported	Supported (client mode only)
IBM Turbo 16/4 Token-Ring PC Card IBM Turbo 16/4 Token-Ring PC Card 2	Supported	Supported	Not supported	Not supported	Supported

History

Before the explosive growth in the use of Internet-based protocols, the 80/20 rule was followed when designing and deploying an IP-based network. This rule stated that the network should be designed on the assumption that 80% of network traffic would remain within the same subnet while 20% of network traffic would cross subnet boundaries. Maintaining the 80/20 rule allowed routers of that time to keep

up with traffic flowing between subnets. With the explosive growth of the use of HTTP, that is, Web-based intranets and the Internet, the 80/20 rule can no longer be maintained.

As users jump from server to server on the Web they might jump from subnet to subnet, requiring almost all network activity to traverse the routers dividing the subnets. In addition, as network backbone technologies increase in speed, such as the move to 100-Mbps Token-Ring, the router bottleneck problem becomes even more of an issue.

Campus network architectures have been moving in two fundamental directions. The first is a continuation of a core networking architecture, with routers moving data between subnets, and the second is an edge networking architecture such as the IBM Switched Virtual Networking framework. In the area of performance improvements, efforts in the core networking model center around improving router performance, for example the recent interest in media-speed routers. By contrast, one of the main interests of the edge networking model is based on improving networking performance by distributing function away from a centralized, single-point-of-failure device.

Overview

Route Switching is IBM's approach to IP switching, or Layer 3 switching, that is actually a hybrid of both models. Route Switching still requires a centralized routing function in the network in order to provide the many functions that a router provides, except for the movement of traffic between subnets. With Route Switching, the traffic movement more closely follows the edge networking model.

The Route Switching feature of the IBM Token-Ring Adapters has been integrated within the device driver making installation and configuration as simple as upgrading the device driver. There are two modes of operation for Route Switching: client mode or peer mode. Client mode is the preferred mode. Route Switching is based on the Next Hop Routing Protocol (NHRP) standard from the Internet Engineering Task Force (IETF) and makes use of this standard when operating in either client or peer mode.

When Route Switching is operating in client mode an IBM Multiprotocol Switching Services (MSS) Server is required to perform the Route Switching server function. When in client mode, the enabled IP host issues requests to the IBM MSS Server for shortcut information for a remote IP host to which it is attempting to communicate. Once the shortcut information is received by the requesting client, subsequent traffic to the remote IP host is sent through the shortcut path instead of through the routed path. When Route Switching is operating in peer mode, the same request for shortcut information is sent directly through the routers to the remote IP host. If you install and configure Route Switching for peer mode on the remote host, the remote host sends a shortcut reply back to the requesting host. In either case, until the reply is received, the IP traffic will continue to be sent on the routed path.

In both situations, access control maintained by the router is not compromised. In the case of client mode, the MSS is also performing the routing function and will ensure that shortcut information is not supplied for a remote host that is not allowed to be reached. When in peer mode, the shortcut request goes through the router to the remote host. Therefore, if the requesting host is not permitted to communicate with the remote host, the request for a shortcut path will never be received by the remote host.

Route Switching can also be set to automatic mode. When in automatic mode Route Switching will initially operate in both client and peer mode. The first reply to a shortcut request that the host receives will determine the permanent mode of operation. For example, as soon as the adapter opens, Route Switching will begin attempting to discover the MSS Servers that exist in the network. At the same time, if IP traffic is being transmitted that is destined to a remote host not in this subnet, Route Switching will also begin sending shortcut requests to these remote IP hosts. If the requesting host receives a server discovery reply from an MSS Server, Route Switching will transition into client mode. If it receives a reply from a remote IP host, it will transition into peer mode.

Benefits

Route Switching can greatly improve performance of IP-based communications in networks with congested routers. The goal of Route Switching is to bypass the routing functions in an IP-based network without bypassing or undermining the other functions that a router provides, such as a firewall function and possibly broadcast containment. If the routers are creating a delay in the communication between IP hosts, Route Switching will eliminate that delay with just a simple upgrade of the LAN adapter device driver.

If a network currently has routing functions that are in need of performance improvements, Route Switching can add life to these routers and extend their usefulness indefinitely. In other words, with just the simple upgrade of device drivers for the IBM Token-Ring adapters, huge expenses for new higher performance routers can be deferred or completely eliminated.

Example scenarios

One-armed router

An environment in which Route Switching can be useful is a premise, or one-armed router, configuration. In this configuration there is one router at a location managing a multiple IP subnet network. All IP traffic between hosts on different subnets must go through this router. In this situation, two workstations might be on the same physical token ring, but from an IP perspective are configured to be on different IP subnets. This is very often the case when the two hosts belong to different business organizations or due simply to when they were installed. In this situation, traffic between these two workstations must leave one workstation, traverse the network all the way to the router, through the router, and then back across the network to the other workstation.

With Route Switching configured for peer mode, only the initial IP packets between these two hosts will be sent through the router. If in fact the two workstations are on the same ring, once the Route Switching function in the two workstations exchange their shortcut information, the traffic will only exist on that ring and will not be forwarded across any bridging functions. Suddenly, performance between these workstations is tremendously improved due to the removal of the router from the communications path. Also, the total number of packets flowing in the network is greatly reduced as well as the work load on the overburdened router.

Managing Route Switching with IBM LAN Adapter Management Agent

View the following values for the current configuration as well as the current status of Route Switching while using the IBM LAN Adapter Management Agent.

Route Switching Mode (Win32 only) Indicates the current state of the Route Switching function.

MSS Server Count Valid when Route Switching is operating in client mode. MSS Server count indicates the number of MSS Server interfaces that have responded to the request made by this computer to determine the Route Switching Servers in the network.

Maximum number of Cache Entries States the maximum number of cache entries available for use.

Current Number of Active Cache Entries Indicates the number of cache entries that are currently in use and contain valid shortcut information.

Switched Frame Count Count of the frames which have been sent using shortcut information when they otherwise would have been sent through a routed path. Observing this value changing over time indicates that Route Switching is operating.

Peer Holding Time (Win32 only) Valid when Route Switching is operating in peer or auto mode. Peer holding time indicates the cache entry holding time value which has been configured. This value is passed by this machine in replies to shortcut information.

System requirements

- Peer mode

  When Route Switching is operating in peer mode there are two requirements. First, IP hosts communicating with each other must have a Route Switching-enabled device driver installed and have Route Switching configured to either peer or auto mode. Second, there must be a Layer 2 path between the IP subnets.
- Client mode

  The client mode of operation is an asymmetric solution in terms of the two IP hosts communicating. This means that Route Switching Client can be configured on only one of the two hosts and benefits can be achieved. In order for Route Switching Client to operate, an IBM MSS properly configured for Route Switching is required.

  For more information about MSS, go to `http://www.ibm.com/networking`.

Installation and configuration

Installation and configuration information are particular to each adapter and are explained in the installation guide for your adapter. Go to `http://www.ibm.com/networking` and view the installation books for your adapter.

Route Switching parameters

The Route Switching function operates exactly the same way in every environment and accepts the same parameters in every environment. The following four parameters are used by the Route Switching function:

Route Switching mode

This parameter defines the mode in which the Route Switching function will operate. Route Switching can operate in client, peer, and auto modes, or it can be disabled.

In client mode, Route Switching will operate with an IBM MSS Server to provide the Route Switching function. In this mode of operation, the endstations will make requests of the server for shortcut information to remote IP hosts with which it is communicating.

In peer mode, Route Switching will operate without the existence of an IBM MSS Server. In this mode of operation, the end stations will make requests to the remote IP hosts to which it is communicating for its shortcut information. This mode of operation requires both IP host end stations involved in a conversation to have Route Switching Peer correctly installed and configured in order to operate. When in peer mode, the IP subnet mask must be passed to the Route Switching function.

In auto mode, Route Switching will initially operate in both modes. This means it will attempt to find an IBM MSS Server in the network as well as remote IP host end stations configured with Route Switching Peer. The first positive response it receives will determine the mode of operation of Route Switching for this end station.

For example, if an end station begins to operate in auto mode it will begin to attempt to discover IBM MSS Servers in the network. When IP traffic is transmitted to remote IP hosts residing on a different subnet, the Route Switching function will also send a shortcut request to the remote host in order to determine the shortcut information. If the remote host has configured Route Switching to peer or auto mode, it will respond to the request. If there are no IBM MSS Servers in the network, the end station will then enter into peer mode of operation. When in auto mode, the IP subnet mask must be passed to the Route Switching function.

If the machine is placed into a reduced-power state or is in some way suspended when configured in auto mode, it will return to auto mode when it returns to full power. This allows Route Switching to handle the changing of the network while an end station is not on the network.

Route Switching IP subnet mask

This parameter is required when Route Switching is operating in either peer or auto mode. It defines the IP subnet mask to which this adapter is connecting. This parameter is typically determined automatically. The Route Switching IP Subnet Mask must be in IP dotted-decimal address notation.

Route Switching peer holding time

This parameter is used when Route Switching is operating in either peer or auto mode. This value defines the amount of time that shortcut information is considered to be valid by the Route Switching function. When an end station provides its shortcut information to another requesting end station it includes this value along with the information. The requesting end station is allowed to use this shortcut information for this specified amount of time.

Route Switching cache table size

This parameter specifies the maximum number of entries that the Route Switching function can maintain at any given moment in time.

Each of the following installation and configuration sections assumes that your adapter is already installed and configured. The following sections define the steps required to enable Route Switching. If the adapter is not yet installed, refer to the Installation and Configuration manual for the adapter being used.

Windows 95, Windows 98, Windows NT, and Windows 2000

If you are using a Token-Ring PCI adapter on Windows 95 OSR2, Windows 98, Windows NT, or Windows 2000, use the instructions in "Token-Ring PCI adapters (on Windows 95 OSR2, Windows 98, Windows NT, and Windows 2000)" to set Route Switching parameters.

If you are using the IBM Turbo 16/4 Token-Ring PC Card 2, use the instructions in "IBM Turbo 16/4 Token-Ring PC Card 2" on page 45 to set Route Switching parameters.

Otherwise, use the instructions in this section.

To set the Route Switching parameters, perform the following steps:

1. Click **Start → Settings → Control Panel**.
2. Double-click **IBM Token-Ring Adapter**.
3. Select the adapter to be configured with Route Switching from the pull-down window at the top.
4. Click **Route Switching**.
5. Select **Route Switch Mode of Operation** in the upper box.
6. If you select either Peer Mode or Auto Mode, the IP Subnet (Network) Number parameter must be defined. If the Microsoft TCP/IP support is being used, the correct value for this parameter is automatically calculated and placed in the value field for this parameter. If this is not the case, then select the value field for this parameter and type the IP subnet mask for the subnet to which this adapter is connecting. You must enter this parameter in IP dotted-decimal notation.
7. Optionally, set the Peer Holding Time and the Cache Table Size to appropriate values based on the above descriptions.
8. Click **OK**.
9. Click **Close**.
10. Reboot the computer to apply the changes.

Token-Ring PCI adapters (on Windows 95 OSR2, Windows 98, Windows NT, and Windows 2000)

To set the Route Switching parameters, perform the following steps:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Network**.
3. Select **Adapters**, then **IBM Token-Ring PCI Family Adapter**, and **Properties**.
4. Click the **Route Switching** tab.
5. If you select either Peer Mode or Auto Mode, the IP Subnet (Network) Number parameter must be defined. If the Microsoft TCP/IP support is being used, the correct value for this parameter is automatically calculated and placed in the value field for this parameter. If this is not the case, then select the value field for this parameter and type the IP subnet mask for the subnet to which this adapter is connecting. You must enter this parameter in IP dotted-decimal notation.
6. Optionally, set the Peer Holding Time and the Cache Table Size to appropriate values based on the above descriptions.
7. Click **OK**.
8. Click **Close**.
9. Reboot the computer to apply the changes.

IBM Turbo 16/4 Token-Ring PC Card 2

To set the Route Switching parameters, perform the following steps:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Network**.
3. Select **Adapters**, then **IBM Turbo 16/4 Token-Ring PC Card 2**, and **Properties**.
4. Click the **Route Switching** tab.
5. If you select either Peer Mode or Auto Mode, the IP Subnet (Network) Number parameter must be defined. If the Microsoft TCP/IP support is being used, the correct value for this parameter is automatically calculated and placed in the value field for this parameter. If this is not the case, then select the value field for this parameter and type the IP subnet mask for the subnet to which this adapter is connecting. You must enter this parameter in IP dotted-decimal notation.
6. Optionally, set the Peer Holding Time and the Cache Table Size to appropriate values based on the above descriptions.
7. Click **OK**.
8. Click **Close**.
9. Reboot the computer to apply the changes.

Novell NetWare server

To set the Route Switching parameters, perform the following steps:

1. From the NetWare server console, type **load install**.
2. Select **Driver Options**.
3. Select **Configure Network Drivers**.
4. Select **Select a driver**.
5. Select the appropriate driver from the list of available drivers and press **Enter**.
6. Select **Select/Modify driver parameters and protocols** and press **Enter**.

For Route Switching configuration:

1. Using the arrow keys, move to the Parameters section, select **Route Switching Mode**, and press **Enter**.
2. Select either **Client**, **Peer**, or **Auto** for the parameter value and press **Enter**. You will see other Route Switching parameters in the parameter list.
3. Using the arrow keys, select **Route Switching Table Size** and enter a value from 16 to 1024.
4. If you selected Auto or Peer in step 2, use the arrow keys to select **Route Switching Holding Time** and enter a value from 2 to 20.
5. If you selected Auto or Peer in step 2, use the arrow keys to select **Route Switching Subnet Mask** and enter a valid IP subnet address for your network.

IBM LAN Client

To set the Route Switching parameters, perform the following steps:

1. Take ***one*** of the following actions:
   - If you have a token-ring PCI adapter that supports IBM LAN Client, run **LCINST.EXE** from the root directory of the adapter CD-ROM.
   - If you have the IBM Turbo 16/4 Token-Ring PC Card 2, run **LCINST.EXE** from the \LANCLNT directory of the adapter CD-ROM.

- Run **LCINST.EXE** from the LAN Client diskettes or the self-extracting package file (LCPKG.EXE).

  Note: To install LCINST.EXE to a hard disk from the LAN Client diskettes, insert LAN Client diskette 1 in drive A and enter **install**.

2. Select the environment from the first IBM LAN Client Installation panel (Windows or Windows for Workgroups).
3. Select your adapter from the IBM LAN Client Adapter Selection panel.
4. Continue to the IBM LAN Client Application and Protocol Selection panel.
5. Select **TCP/IP** as one of the protocols to install and click **OK**.
6. Select the **Route Switch** tab on the IBM LAN Client Configuration panel.
7. Check **Enable**.
8. Select **Auto**, **Peer**, or **Client** mode.

   Note: If you select Auto or Peer, then you must enter an IP Address and a Subnet Mask on the TCP/IP configuration panel. You cannot enable DHCP.

9. Select **Table Size** and **Holding Time** values.

   Note: Holding Time is not valid if you selected client mode.

10. Click **Install**.

OS/2

To set the Route Switching parameters perform the following steps:

1. Double-click **MPTS** on the desktop.
2. Click **OK**.
3. Select **LAN Adapters and Protocols** and click **Configure**.
4. Select the name of the adapter in the current configuration section of the window and click **Edit**.
5. Scroll down through the configuration parameters until Route Switch Mode is displayed.
6. Make sure that the cursor is in the data entry portion of this parameter by either scrolling up or down or by clicking the data entry area.
7. To set the mode of Route Switching, type one of the following values: **Client**, **Peer**, or **Auto**.
8. Move the cursor to the data entry field for the IP Subnet Mask parameter.
9. Make sure that the cursor is in the data entry portion of this parameter by either scrolling up or down or by clicking the data entry area.
10. Enter the IP dotted-decimal value for the IP subnet network number to which this adapter is going to attach.
11. Click **OK**.
12. Click **OK** on the right side of the window.
13. Follow the instructions on the panels to exit MPTS.

Chapter 6. Class of Service

This chapter describes the Class of Service (CoS) for IP feature.

Supported environments

CoS for IP is supported for the adapters and operating systems listed in the following table.

	Windows NT 3.51, 4.0	Windows 95, 98, 2000	Windows 3.x (using IBM LAN Client)	OS/2 Warp 3.0 and later	Novell NetWare Server (4.11 and higher)
IBM 16/4 Token-Ring CardBus Adapter	Supported (Windows NT 4.0 only)	Supported	Not supported	Supported	Not supported
IBM 16/4 Token-Ring Low Profile PCI Management Adapter	Supported (Windows NT 4.0 only)	Supported (Windows 98 and Windows 2000 only)	Not supported	Not supported	Not supported
IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter IBM 16/4 Token-Ring PCI Management Adapter	Supported	Supported	Not supported	Supported	Supported
IBM High-Speed 100/16/4 Token-Ring PCI Adapter IBM 16/4 Token-Ring PCI Adapter 2 IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN IBM PCI Token-Ring Adapter IBM PCI Wake on LAN Token-Ring Adapter	Supported	Supported	Supported	Supported	Supported
IBM Turbo 16/4 Token-Ring PC Card IBM Turbo 16/4 Token-Ring PC Card 2	Supported	Supported	Not supported	Not supported	Supported

Special note regarding token-ring PCI adapters

The IBM token-ring PCI adapters are enabled with advanced technology that lets higher-priority traffic expedite through the adapter, thus preventing this traffic from being held up behind lower-priority traffic.

The adapter includes multiple transmit paths for use by the device drivers. This multiple transmit path capability lets the driver pass a high-priority frame to the adapter and have this frame transmitted before a previously queued normal priority

frame. This eliminates any traffic delays for the high-priority traffic from the moment the traffic is deemed to be high-priority in the device driver.

This advanced function exists in all IBM token-ring PCI adapters.

Overview

The ability to assign relative priorities, or degrees of importance, to traffic as it traverses a network has existed in token-ring networks since the inception of the token-ring standard. Unfortunately, there has never been a method to assign the priorities to the traffic as the frames were transmitted. CoS for IP solves this problem by allowing network managers to assign priorities to IP traffic transmitted by an IP host.

Benefits

With the use of CoS for IP, you can categorize your IP traffic on the network and assign a degree of importance in the network to certain types of IP traffic. This prevents traffic considered to be of low importance from taking valuable network bandwidth away from important traffic. The backing up of a server farm or a session of a computer game will no longer adversely impact the streaming of an educational video session or a real-time video conference.

CoS for IP makes use of a traffic prioritization mechanism that has always existed in the token-ring architecture but has never been exploited by higher-layer protocols and applications. CoS for IP does not rely on any special enablement to the infrastructure of the network. That is, the switches and bridges of the network do not necessarily need to know that CoS for IP is being used. Even though the network is not aware of this traffic prioritization mechanism, CoS for IP allows the traffic that has been assigned a high priority to maintain this high-priority status from the time that the traffic enters the network to its final destination.

In addition, CoS for IP does not require new protocol stacks and applications that are aware of traffic prioritization. In fact, the traffic being treated as high priority is up to the network manager and does not even have to be multimedia related. If performing a backup of a server is considered a high priority then this traffic can be deemed more important by the network manager than other traffic on the network.

Because CoS for IP uses a token-ring mechanism for implementing traffic prioritization, the best results occur when the traffic that has been given a priority status is sent through a Layer 2 switched, or bridged, path and travels entirely on token-ring networks. IBM's Route Switching function solves this requirement by establishing the Layer 2 path even when the two end stations reside on different subnets. With the advent of Web-based networking and intranet-based IP networks, intersubnet communications is becoming more the normal situation. Route Switching and CoS for IP work together to resolve growing network performance problems not just for high-priority traffic but for all traffic in the network.

Example scenarios

CoS for IP can be used to ensure that time-sensitive traffic, such as streaming audio or video, arrives at the destination computer within the required time. To make use of CoS for IP, a network manager would determine the protocol and the port range being used by the server application and configure CoS for IP with these values on the server. For example, a network manager might have a server running a RealNetworks streaming audio server application that is sending audio traffic to

clients using UDP port ranges, 26992 through 29040. The network manager would configure CoS for IP for these values and assign a priority level for this range.

CoS for IP can be managed using LAN Adapter Management Agent. The following values can be displayed:.

Win32 and OS/2 environments

LAN Adapter Transmit Priority Information Displays the general transmit priority capabilities of the adapter. For example, this attribute displays the number of physical transmit channels supported by the adapter hardware.

LAN Adapter Transmit Priority Distribution Shows the frame count and byte count for each priority level. Displaying these values will indicate the priority at which traffic is being sent.

Win32 environments

LAN Adapter Class of Service Information Displays the number of port ranges defined for each protocol.

LAN Adapter Class of Service TCP Port Ranges Displays each of the defined port ranges for the TCP protocol. Displaying these values will confirm that the port ranges configured have been accepted and are being used by the CoS for IP support.

LAN Adapter Class of Service UDP Port Ranges Displays each of the defined port ranges for the UDP protocol. Displaying these values will confirm that the port ranges configured have been accepted and are being used by the CoS for IP support.

System requirements

There are no special requirements for the machines that will make use of CoS for IP other than having a supported IBM adapter and the correct level of device driver.

CoS for IP makes use of the priority bits defined by the token-ring architecture. Because of the use of these Layer 2 bit fields, traffic being assigned a higher-than-normal priority should be traversing only a Layer 2 path in order to achieve the full effects of CoS for IP. Route Switching complements CoS for IP by attempting to establish a Layer 2 connection for all IP traffic that would otherwise traverse Layer 3 devices.

Installation and configuration

Installation and configuration information are particular to each adapter and are explained in the installation guide for your adapter. Go to `http://www.ibm.com/networking` and view the installation books for your adapter.

CoS for IP uses the destination port number of outbound TCP and UDP traffic to determine the Class of Service, or priority, of the traffic. Once the range of port numbers used for a particular TCP- or UDP-based application has been determined, this port range is simply passed to the CoS for IP function within the device driver through the following configuration parameters.

CoS for IP parameters

CoS for IP is enabled in the device drivers by simply defining one or more TCP or UDP port ranges. A port range is defined by a starting port value and an ending port value. Each of these values is inclusive, meaning the port values that make up a port range include the starting and ending values. For each port range defined, you must select a priority value from 1 to 6. You can define a maximum of 15 port ranges for each of the two protocols. When configuring CoS for IP in either the OS/2 or Novell Server environments, define these port range parameters in the following format:

- There are a total of five port range parameters, each defining three port ranges for each of the two protocols.
- The name of each parameter is in the format: `TCPPortRange<1..5>` or `UDPPortRange<1..5>`
- The value of each of these 10 parameters is a character string having the following format:

```
ParmValue := <PortRange>[<PortRange><PortRange>]
PortRange := <PortNumber><PortNumber><PriorityValue>
PortNumber := a 4-character hexadecimal value.
PriorityValue := a 1-character value from 1 to 6.
```

A bridging device in a token-ring network will forward traffic at a priority of 4 when necessary. If CoS for IP is being used in a network made up of bridges this fact must be taken into account. It might be necessary to make use of only priorities 5 and 6 when defining port ranges in order to keep the traffic at a higher priority than the bridged traffic. When the higher-priority traffic travels across a bridging function the bridge should maintain the frame priority. For example, a network manager has defined certain UDP traffic to be priority 6 and this traffic is to flow across a number of bridges as it travels from a server to a client. When this traffic is forwarded onto subsequent rings by the bridges, the bridges will now forward it with a priority of 6 instead of 4.

Each of the following installation and configuration sections assumes that the adapter is already installed and configured. The following sections define only the steps required to enable CoS for IP. If the adapter is not installed, refer to the installation manual for the adapter you are using.

Windows 95, Windows 98, Windows NT, and Windows 2000

If you are using a token-ring PCI adapter on Windows 95 OSR2, Windows 98, Windows NT, or Windows 2000, use the instructions in “Token-ring PCI adapters (on Windows 95 OSR2, Windows 98, Windows NT, and Windows 2000)” on page 51 to set CoS for IP parameters.

If you are using the IBM Turbo 16/4 Token-Ring PC Card 2, use the instructions in “IBM Turbo 16/4 Token-Ring PC Card 2” on page 51 to set CoS for IP parameters.

Otherwise, use the instructions in this section.

To set the CoS for IP parameters, perform the following steps:

1. Select **Start → Settings → Control Panel**.
2. Double-click **IBM Token-Ring Adapter**.
3. Select the adapter to be configured from the pull-down window at the top.
4. Select **Class of Service for IP**.
5. Select **Add** on the right side of the window.

6. Select the appropriate protocol by clicking either **TCP** or **UDP**.
7. Select the value field for the Start port value and enter the starting port value for the port range in decimal notation.
8. Select the value field for the End port value and enter the ending port value for the port range in decimal notation.
9. Select the priority for this port range by dragging the slider on the right side of the window.
10. Select **OK**.
11. Repeat steps 5 through 10 for each port range to be defined.

    Note: Class of Service for IP supports a maximum of 15 defined port ranges for each protocol.
12. Select **OK** at the bottom of the window.
13. Select **Close** at the bottom of the window.
14. Reboot your computer to apply the changes.

Token-ring PCI adapters (on Windows 95 OSR2, Windows 98, Windows NT, and Windows 2000)

To set the CoS for IP parameters, perform the following steps:

1. Select **Start → Settings → Control Panel**.
2. Double-click **Network**.
3. Select **Adapters**, then **IBM Token-Ring PCI Family Adapter**, and **Properties**.
4. Select **Class of Service** tab.
5. Select **Add**.
6. Select the appropriate protocol by clicking either **TCP** or **UDP**.
7. Select the value field for the Start port value and enter the starting port value for the port range in decimal notation.
8. Select the value field for the End port value and enter the ending port value for the port range in decimal notation.
9. Select the value field for port range and enter the priority in decimal notation.
10. Select **OK**.
11. Repeat steps 5 through 10 for each port range to be defined.

    Note: Class of Service for IP supports a maximum of 15 defined port ranges for each protocol.
12. Select **OK** at the bottom of the window.
13. Select **Close** at the bottom of the window.
14. Reboot your computer to apply the changes.

IBM Turbo 16/4 Token-Ring PC Card 2

To set the CoS for IP parameters, perform the following steps:

1. Select **Start → Settings → Control Panel**.
2. Double-click **Network**.
3. Select **Adapters**, then **IBM Turbo 16/4 Token-Ring PC Card 2**, and **Properties**.
4. Select **Class of Service** tab.
5. Select **Add**.
6. Select the appropriate protocol by clicking either **TCP** or **UDP**.

7. Select the value field for the Start port value and enter the starting port value for the port range in decimal notation.
8. Select the value field for the End port value and enter the ending port value for the port range in decimal notation.
9. Select the value field for port range and enter the priority in decimal notation.
10. Select **OK**.
11. Repeat steps 5 through 10 for each port range to be defined.

    Note: Class of Service for IP supports a maximum of 15 defined port ranges for each protocol.
12. Select **OK** at the bottom of the window.
13. Select **Close** at the bottom of the window.
14. Reboot your computer to apply the changes.

Novell NetWare Server

To set the CoS for IP parameters, perform the following steps:

1. From the NetWare Server console, enter **load install**.
2. Select **Driver Options**.
3. Select **Configure Network Drivers**.
4. Select **Select a driver**.
5. Select the appropriate driver from the list of available drivers and press **Enter**.
6. Select **Select/Modify driver parameters and protocols** and press **Enter**.

For Class of Service configuration:

1. Using the arrow keys, move to the Parameters section, select **Class of Service**, and press **Enter**.
2. Select **Enabled** from the list and press **Enter**. You will see another Class of Service parameter in the parameter list.
3. Using the arrow keys, select **Class of Service Set Number** and enter a number from 1 to 16. This will create an indirect reference to a file named IBMCOS*x*.CFG, where *x* is the number you entered. This file contains the Class of Service keywords and values as defined above. This file can be used by different adapters in the system.

LAN Client

To set the CoS for IP parameters, perform the following steps:

1. Run **LCINST.EXE** from the root directory of the CD-ROM if you have one of the IBM Token-Ring PCI Family Adapters or from the \LANCLNT directory if you have the IBM Turbo 16/4 Token-Ring PC Card 2. You can also run it from the LAN Client diskettes or the self-extracting package file (LCPKG.EXE).

   Note: To install LCINST.EXE to a hard disk from the LAN Client diskettes, insert LAN Client diskette 1 in drive A and enter **install**.
2. Select the environment from the first IBM LAN Client Installation panel (Windows or Windows for Workgroups).
3. Select your adapter from the IBM LAN Client Adapter Selection panel.
4. Continue to the IBM LAN Client Application and Protocol Selection panel.
5. Select **TCP/IP** as one of the protocols to install and click **OK**.
6. Select the **Class of Srv** tab on the IBM LAN Client Configuration panel.

7. Fill in the UDP and TCP Port Ranges to be configured along with the appropriate Priority value. You can enter a total of 4 port ranges between UDP and TCP.
8. Click **Install**.

OS/2

To set the CoS for IP parameters, perform the following steps:

1. Double-click **MTPS** on the desktop.
2. Click **OK**.
3. Make sure that LAN Adapters and Protocols is selected and click **Configure**.
4. Select the Name of the adapter in the current configuration section of the window and click **Edit**.
5. Scroll down through the configuration parameters until the TCP or UDP Class of Service port range parameters are displayed.
6. Make sure that the cursor is in the data entry portion of any one of these parameters by scrolling up or down or by clicking the data entry area.
7. Define a port range by typing a string that is in the format defined in “CoS for IP parameters” on page 50.
8. Continue to define any additional port range parameters in the same manner.
9. Click **OK**.
10. Click **OK** on the right side of the window.
11. Follow the instructions on the panels to exit MPTS.

Chapter 7. Redundant NIC

This chapter describes the Redundant NIC feature.

Supported environments

Redundant NIC is currently supported on the following adapters:

- IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Management Adapter
- IBM 16/4 Token-Ring PCI Adapter 2
- IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN
- IBM High-Speed 100/16/4 Token-Ring PCI Adapter
- IBM PCI Token-Ring Adapter
- IBM PCI Wake on LAN Token-Ring Adapter

The following operating environments are supported:

- Windows NT Server 3.51 and 4.0
- NetWare 4.11, 4.2, and 5.0

Quick Failover, an extension to Redundant NIC, is available for the following adapter and microcode combinations on Windows NT 4.0 SP5, NetWare 4.11 and 4.2 with IWSP6A and NetWare 5.0 with NW5SP2A.

Adapter	Microcode
IBM High-Speed 100/16/4 Token-Ring PCI Management Adapter	any
IBM 16/4 Token-Ring PCI Management Adapter	any
IBM 16/4 Token-Ring PCI Adapter 2	PX15C0CT or later
IBM 16/4 Token-Ring PCI Adapter 2 with Wake on LAN	AL15DAAA or later
IBM High-Speed 100/16/4 Token-Ring PCI Adapter	HSS2DAB4 or later
IBM PCI Wake on LAN Token-Ring Adapter	PX14D0CS or later

For more information about Quick Failover, see “Quick Failover” on page 56.

Overview

The Redundant NIC function provides a high-availability solution for your Windows NT Server 3.51 and 4.0 or NetWare 4.11, 4.2 and 5.0 server. This function maintains network connectivity in the event of an adapter- or lobe-related failure. You can assign a backup adapter to take control of the network connection if the active adapter fails.

The Redundant NIC function will initiate a failover when a cable fault or a hard error occurs on the adapter. A failover causes the driver to switch traffic from the active adapter to the backup adapter. The active and backup roles are traded between the adapters of the redundant pair.

In many cases, the failover to the backup adapter will occur seamlessly. Due to the failover latency involved in opening the backup adapter onto the ring, some protocols might require that sessions be reestablished. In either case, network connectivity is maintained and server downtime is avoided.

Benefits

The Redundant NIC function provides a high-availability solution for your token-ring connected servers. The goal of Redundant NIC is to maintain network connectivity in the event of an adapter- or lobe-related failure.

Example scenarios

Managing a Redundant NIC NT server with the Agent

During driver configuration, users can define a Redundant NIC pair. The pair consists of an active adapter and a backup adapter. The backup adapter will take over in the event of a failure on the active adapter. These failovers can occur continually as long as the backup adapter is operational. Redundant NIC is offered on Windows NT and NetWare server systems. The LAN Adapter Management Agent can be used to complement the Redundant NIC function on Windows NT.

The Agent will send a DMI indication and SNMP trap upon detecting the completion of a Redundant NIC failover. The Agent also allows a failover to be initiated via DMI or SNMP. The Agent also provides the addresses of the active and backup adapters, a running count of failovers and the status of the backup adapter. The Nways Management Applications format the contents of the failover SNMP trap into a clear message.

The combined Redundant NIC and Agent functions should be used on mission-critical servers, and the Nways Management Applications should be used to monitor those servers. Redundant NIC provides the continual network connectivity necessary for the clients using the Windows NT Server. The Agent sends the failover SNMP trap to the Nways Management Application, or any other SNMP-based network management application. Once notified of the server failover, the network administrator can correct the error. For example, the error might be an accidentally disconnected cable. Once the cable has been reconnected, the network administrator can then force a failover from the management application and restore the server's original adapter configuration.

Quick Failover

Quick Failover (QFO) is an extension to original Redundant NIC. QFO reduces the failover time from around 30 seconds to less than 10 seconds, and it allows the primary and secondary adapter pair to be in any PCI slot in the system. QFO is supported on Windows NT 4.0 SP 5, NetWare (4.11, 4.2) with IWSP6A and NetWare 5.0 with NW5SP2A.QFO for NetWare also has an enhanced user interface from the original RNIC for NetWare release. You can find additional information on NetWare Quick Failover device driver parameters in the ″Novell NetWare Server driver parameters″ section of the User's Guide for your adapter.

In addition to having an adapter that supports this feature, you must also have the proper device driver and microcode. See "Supported environments" on page 55 for a list of the device drivers and microcode. On Windows NT, if your adapter or microcode level is different from those listed, the device driver automatically defaults to the regular Redundant NIC functions.

Installation and configuration

Windows NT

Follow these instructions when setting up a Redundant NIC pair.

1. Ensure that both adapters of a redundant pair are cabled to the same network.
2. Select **Control → Panel Network → Adapters** and your adapter. Use the Redundant NIC tab located in Properties for the primary adapters to control your redundant pairs.
3. You must specify a Locally Administered Address (LAA) for the primary adapter. The LAA is located in the Basic tab of Properties for the primary adapter.

Redundant NIC usage tips

- It is strongly recommended that you specify a Ring Speed parameter of 16 Mbps or 4 Mbps instead of Automatic. This will reduce the amount of time needed to perform a failover.
- Once a redundant pair has been defined, the secondary adapter is not configurable until the redundancy has been disabled.
- Once a redundant pair has been defined, neither the primary nor the secondary adapter can be removed until the redundancy has been disabled.
- When a failover occurs, check the cabling of the failed adapter. If it has been disconnected, reconnect it as soon as possible so that it is ready to function as a backup.
- The Redundant NIC function is not supported on the Auto LANStreamer PCI adapter.

Managing Redundant NIC

The LAN Adapter Management Agent Version 1.40 or later allows you to manage the Redundant NIC operation. In the event of a failover, the Agent sends an SNMP trap to notify that a failover has occurred. The user can also initiate a failover through the Agent. For more information about the Agent, see “Chapter 4. LAN Adapter Management Agent” on page 35. For an example of using the Agent and Redundant NIC, see “Example scenarios” on page 56.

NetWare

The Redundant NIC function is provided in two pieces: IBMRNIC.NLM and IBMTRPO.LAN. When a failover from the active to the backup adapter occurs, the only protocols that can be switched are IP and IPX. Any other protocol information that is bound to the active adapter will be lost.

Note: The only protocol information that is retained when a failover occurs is what is bound to the active adapter when the problem occurs. No conflicting protocols should be bound to the backup adapter. The only exception to this is when ROUTE.NLM is used. In that case, ROUTE.NLM should be bound to the active and backup adapters.

Failovers can occur from the active to the backup adapter, and also from the backup to the active until a good connection is made. If the backup adapter is not an IBM token-ring PCI adapter, only one automatic failover to the backup is supported. The Redundant NIC NLM can monitor four pairs at one time.

IBMRNIC.NLM Version 2.53 or later has some new features. Quick Failover, which allows failovers to occur much more quickly than normal failovers, is a significant new feature. To take advantage of Quick Failover you must have IBMTRPO.LAN

Version 2.46 or later. Additionally, your adapter must be using a microcode version specified in “Supported environments” on page 55 or later. Use the flash update tool available from your manufacturer if an adapter microcode update is necessary. Failback is an additional new feature. Failback causes failovers to occur automatically when the secondary adapter is active and when it can be determined that the primary adapter could be active instead. This feature requires you to use Quick Failover on the primary adapter. Failback is enabled by default, but can be disabled when a pair is created. In Versions 2.53 or later of IBMRNIC.NLM, a new user interface allows you to create pairs more easily. This user interface replaces many of the command line functions used in previous versions of the Redundant NIC NLM. The user interface provides functions that allow the user to get the current status of all pairs, cause manual failovers to occur, change the switching status, create, remove, save and load pairs

Installation of Redundant NIC software

Versions of IBMTRPO.LAN prior to Version 2.14 will not work with the Redundant NIC capability. To use Quick Failover you need IBMTRPO.LAN Version 2.46 or later along with an adapter using a microcode version specified in “Supported environments” on page 55 or later. Each adapter must be plugged into the same ring on the network for the failover to be completely transparent to the clients communicating with the server.

The driver communicates adapter failures or cable disconnects to the IBMRNIC. NLM via the NESL/NEB interface. If ODINEB.NLM loads after the LAN driver, these messages are never sent to the IBMRNIC NLM by the NESL/NEB subsystem. If the IBMRNIC.NLM does not failover after a cable disconnect or failure, verify that ODINEB.NLM is loading before the LAN driver. Make sure that you do not unload ODINEB.NLM while IBMRNIC.NLM is loaded. ODINEB.NLM lets you unload it at any time even if other NLMs depend on it to be loaded.

If you use INETCFG.NLM to configure your system, follow the steps in “Installation using INETCFG.NLM” on page 59 instead of the following INSTALL.NLM section.

Installation using INSTALL.NLM or NWCONFIG.NLM:

1. Install the latest support pack from Novell on your NetWare 4.11, 4.2, or 5.0 Server if the latest support pack is not already installed on your system.

   Support packs are available at `http://support.novell.com`.
2. Install the adapters you would like to pair into a NetWare 4.11, 4.2 or 5.0 Server.
3. Copy IBMRNIC.NLM from the \NOVELL\NETWARE directory on the driver diskette to SYS:\SYSTEM on the server.
4. Load INSTALL.NLM or NWCONFIG.NLM on the server and proceed to the section where you install network adapters.
5. Set up the primary adapter. In the Load Software panel, perform the following steps:
   a. Make sure the path for the driver is A:\NOVELL\NETWARE.
   b. Copy the new driver (IBMTRPO.LAN) and IBMTRPO.LDI from the diskette.
   c. Select protocols. In the Parameters panel, select **Standard Failover** for IBMRNIC Failover Mode and make sure the Standby Mode is set to DISABLED, unless using the ″-backup″ parameter. If your adapter supports Quick Failover, select **Quick Failover** and specify the IBMRNIC Failover Address in the next field. If your adapter does not support Quick Failover, use the Node Address field to specify the LAA. Set other parameters as needed.

d. If you do not require failback, make sure it is disabled.
e. Save and load the driver. While it is processing, press **Alt+Esc** to get to the Console panel. Choose the slot of the primary adapter.
f. Choose a network number to bind to.

6. Set up the secondary adapter:
   a. Choose to load an additional network driver.
   b. Do not copy the driver again.
   c. Select the same protocols you chose to use with the primary adapter. If you chose TCP/IP, use a temporary IP address for the secondary adapter. You must use the same locally administered Node Address specified with the primary adapter. Set Standby to ENABLED if the secondary adapter is an IBM Token-Ring PCI Family Adapter and both adapters in the pair are using Standard Failover mode. If using the IBMRNIC ″-backup″ parameter with a non IBM token-ring PCI adapter, Standby does not apply. Save and load the driver.
   d. While it is processing, press **Alt+Esc** to get to the Console panel. When asked to load another frame type, answer NO.
   e. Choose the slot of the secondary adapter.
   f. Choose a temporary network number to bind to.
   g. Do not load an additional network driver.
7. Exit back to the Console.
8. Edit the AUTOEXEC.NCF file:
   a. Before all of the LOAD IBMTRPO statements, insert `LOAD ODINEB` on a new line.
   b. After all of the BIND statements, add `LOAD IBMRNIC PAIR <pairname> -p<slot#> -s<slot#>` and any additional parameters.

      See “Setting up a Redundant NIC pair” on page 60 for more information on IBMRNIC command line parameters.

      Note: If the secondary adapter is not an IBM token-ring PCI adapter, the -backup parameter must be used on the pair line. Also, because the secondary adapter probably will not support the standby keyword, the primary adapter must be loaded with the standby keyword.
   c. Delete all BIND statements for the secondary adapter.
9. Restart the server to apply the changes.

Note: Double-check your AUTOEXEC.NCF every time that you use the INSTALL.NLM program. It is possible that the INSTALL.NLM will move or remove ODINEB.NLM. Make sure that it loads before the network driver (IBMTRPO.LAN) and that IBMRNIC loads after the network driver.

Installation using INETCFG.NLM:

1. Install the ODI33F.EXE or later patch from Novell if you have a NetWare 4.11 Server.
2. Install the adapters you want to pair into a NetWare 4.11 or 5.0 Server.
3. Copy IBMRNIC.NLM and TOKENTSM.NLM from the \NOVELL\NETWARE directory on the driver diskette to SYS:\SYSTEM on the server.
4. Load INETCFG.NLM on the server and proceed to the section where you add a new board. If you are asked whether to use the fast setup method, select **No, use the standard setup method.**

5. Set up the primary adapter. In the New Board panel, perform the following steps:
   a. Make sure the path for the driver is A:\NOVELL\NETWARE.
   b. Choose IBMTRPO from the list.
   c. In the Configuration Panel, name the Board, fill in the slot number, and the node. Standby Mode must be set to DISABLED unless the ″-backup″ parameter is specified. Set other parameters as needed.
   d. Save the changes.
6. Set up the secondary adapter:
   a. Select IBMTRPO from the list unless a non IBM token-ring PCI adapter is being used as the secondary adapter. In that case, use the appropriate driver for the secondary adapter.
   b. In the Configuration panel, name the Board (the name must be different from that of the primary adapter), fill in the slot number, and enter the node or rnicopen address (must be the same as that of the primary adapter). Set Standby to ENABLED if the secondary adapter is an IBM token-ring PCI adapter and both adapters in the pair are using Standard Failover mode. If using the IBMRNIC ″-backup″ parameter with a non IBM token-ring PCI adapter, Standby does not apply. Set other parameters as needed.
   c. Save the changes.
7. In the Protocols section, select User-specified Protocols, create and name a temporary protocol and save that information.
8. In the Bindings section, choose binding parameters for the primary adapter as needed. Bind the User-specified Protocol that you defined in the previous step to all appropriate frame types of the secondary adapter.

   Since the User-specified Protocol that you created does not exist, no protocols will actually be bound to the secondary adapter. You might notice error messages that point this out when the server is starting up. These messages are for information only; no action is required.
9. Exit back to the Console.
10. Edit the AUTOEXEC.NCF file:
    - Before the INITSYS.NCF command, add LOAD ODINEB.
    - After the INITSYS.NCF command, add LOAD IBMRNIC PAIR <pairname> -p<slot#> -s<slot#> and any additional parameters.

      See “Setting up a Redundant NIC pair”.

      Note: If the secondary adapter is not an IBM token-ring PCI adapter, the -backup parameter must be used on the IBMRNIC pair line. The primary adapter must also be loaded with the standby keyword.
11. Restart the server to apply the changes.

    Note: Double-check your AUTOEXEC.NCF every time you use the INETCFG.NLM program. It is possible that the INETCFG.NLM will move or remove ODINEB.NLM. Make sure that it loads before the network driver (IBMTRPO.LAN) and that IBMRNIC loads after the network driver.

Setting up a Redundant NIC pair

Follow these instructions to prepare IBMRNIC.NLM to monitor your adapter pair.

The Redundant NIC NLM requires that several options be specified in order to create a pair. You can specify the options to IBMRNIC.NLM when you load the nlm

or on the command line after IBMRNIC.NLM is loaded. To automate the commands on reboot, add them to your AUTOEXEC.NCF.

To complete the setup, you need the following information:

- The slot number assigned to each adapter. If the secondary adapter is not a PCI adapter, you need to know the hexadecimal value of the secondary adapter's I/O Port or Memory Mapped base I/O address.
- If TCP/IP is bound to your adapter, you need to know your default router's IP address.
- You need to select a name for your adapter pair.
- You need to know if Quick Failover is supported and being used on each adapter and if IBMTRPO.LAN supports it.

Note: If the IBM token-ring PCI adapter driver (IBMTRPO.LAN) is loaded with the option to enable Quick Failover, the adapter will not become active until a Redundant NIC pair is made with that adapter. You will not be able to use that adapter until a pair is made.

To set up a pair when you load the NLM, use the following format:

```
load ibmrnic pair <pairname> -p<slot#> -s<slot#> | -x<base address>
     [-r<ip_address>] [-backup]
```

If IBMRNIC is already loaded you can set up a pair by using the IBMRNIC keyword on the system console. Its format is:

```
ibmrnic pair <pairname> -p<slot#> -s|x<slot#> -r<ip_address>
     [-backup]
```

A description of each parameter follows:

<pairname>
This parameter is required and identifies the Redundant NIC pair. The pair name must be 12 characters or less. It is case-sensitive. All ASCII characters are accepted.

-p<slot#>
This parameter is required and tells the NLM the slot number of the IBM token-ring PCI adapter that you want to be the active adapter initially.

-s<slot#>
This parameter is required if the secondary adapter can be identified by a slot number. It tells the NLM the slot number of the IBM token-ring PCI adapter that you want to be the backup adapter initially.

-x<base address>
This parameter is only needed when the -backup keyword is used and you cannot specify a slot for the secondary adapter. This parameter specifies the I/O port or the memory mapped address of the secondary adapter (in hex).

-r<ip_address>
This parameter is optional. It might be needed if you are using TCP/IP on your active adapter. If you do not load the TOKEN-RING_SNAP frame type then you do not need this parameter. If you load the TOKEN-RING_SNAP frame type, you only need this parameter if you have IP bound and you have a default IP router. If this parameter is not specified, IP will not know what the default router is after an adapter failover.

-backup

This parameter is optional. It should only be used if your backup adapter is not an IBM token-ring PCI adapter. If this parameter is used the primary adapter must load with the standby keyword.

Using Redundant NIC software

The user interface

As stated previously, the **ibmrnic** command can be used on the system console after IBMRNIC.NLM is loaded. This command can be used to create a pair and to get help on creating pairs. A user interface is started on a panel separate from the System Console that is used to modify your pairs. In versions of the Redundant NIC NLM prior to Version 2.50 all redundant NIC operations were performed on the command line. Now, only the pair and help commands are supported. The new user interface provides all of the other functions along with some extra functions. The user interface allows you to create, remove, save, and load pairs. You can also perform manual failovers and change the switching mode. The most recent status of all configured pairs is always shown on the screen.

Command line functions

ibmrnic help

Enter **ibmrnic help** to show the valid options for the **ibmrnic** command.

ibmrnic pair

This command is described in “Setting up a Redundant NIC pair” on page 60.

Redundant NIC utility functions

Create

Press the **Insert** key to display a form that helps you create a pair. Fill in all of the fields of the form and select **create**. The fields are the pair name, the primary slot, the secondary slot/port, the IP router and failback enable/disable.

Delete

Press the **Delete** key to remove a pair. A list box with all configured pair names appears. Select the name of the pair you would like to remove. If more than one pair exists, there is an entry that you can select to remove all pairs.

Failover

Press the **F8** key to cause a failover to occur on a pair that you select. A list box with all configured pairs appears. When you select a pair from the list, a failover occurs from the active to the backup on that pair.

Mode

Press the **F9** key to change the switching mode of an adapter. Select the pair name for which you want to change the mode. Then select the new mode for that pair.

Normally the Redundant NIC pair will automatically failover from the active to the backup if a cable fault or adapter failure is detected. Use this command to change the mode of the pair so that an automatic failover will not occur. To prevent automatic failovers from occurring, set the pair to manual mode. In manual mode,

the **ibmrnic switch** command is the only way to failover from the active to the backup adapter. Disabled mode will not allow failovers. You can use disabled mode when performing maintenance on the backup adapter.

Save

Press the **F4** key to save the configuration of all of the current pairs to a file. You must save the configuration to one of the files that is specified in the list box that appears.

Load

Press the **F5** key to load the configuration from a previously saved file and then select the file you want to use to restore your configuration.

The configuration can also be restored from one of the saved files when IBMRNIC.NLM initially loads. To do this, specify the number of the file your configuration was saved to. For example, if the file name is IBMRNIC0.DAT, then to load IBMRNIC with the configuration stored in IBMRNIC0.DAT you would enter:

```
load ibmrnic 0
```

The files operated on by the Save and Load options are located in the sys:/system directory of the server.

Pair information and adapter information

The status of all pairs is shown in the main portal of the IBMRNIC window. If a pair is configured the following information will be displayed: the pair name and LAA (locally administered address), the slots that the primary and secondary adapters are using, the switching mode of the pair (manual, automatic, or disabled), the current state of the primary adapter, the current state of the secondary adapter, the number of failovers that have occurred, and the time the last failover occurred. Because all of this information can not be shown at one time, you must press the **F1** key to toggle between the pair information and the adapter information.

Note: The terms primary and secondary do not refer to which adapter is currently active. The primary adapter is initially the active adapter and was configured by using the `-p<<slot#>` option on the command line. The secondary adapter is initially the backup adapter and was referred to by `-s<<slot#>` or `-x<<hex port#>` on the command line.

There are several possible states that apply to an adapter. The possible states are:

operating
: This adapter is open and operating. This is the active adapter

standby ready
: This adapter is ready for failover if the active adapter fails. This is the backup adapter.

cable disconnected
: The cable was disconnected from this adapter.

error detected
: There might be an adapter check error.

opening
: The adapter is trying to open.

unloaded
One or more logical boards can no longer be located for this adapter.

adapter removed
This adapter was removed from the system.

Using Redundant NIC on a Hot-Plug server

The Redundant NIC NLM can be used in a server that supports PCI Hot-Plug, but some manual intervention is required to maintain its proper operation. If an adapter is removed that is part of an IBMRNIC pair, then failovers will no longer occur. If the active adapter in a pair is removed, then a failover will occur. After a hot-plug operation has been completed, the adapter driver must be loaded manually. Do not let HWDETECT.NLM attempt to automatically load the driver for the adapter. HWDETECT.NLM will not load the driver with the correct parameters needed to get the Redundant NIC pair operational again.

To perform a failover, perform the following procedure:

1. Make sure that the adapter is not active.
2. Perform the hot-plug operation.
3. Load the driver with the same parameters in which the pair was created.

Note: If the secondary adapter is not an IBM token-ring PCI adapter ,and you are trying to reload its driver, you might have problems if the driver does not have an equivalent of the `standby` parameter.

Examples (taken from a NetWare 4.11 server):

1. AUTOEXEC.NCF of a simple Quick Failover Redundant NIC configuration after using INSTALL.NLM:

```
set Time Zone = EST5EDT
set Daylight Savings Time Offset = 1:00:00
set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST  2:00:00 AM)
set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST  2:00:00 AM)
set Default Time Server Type = SINGLE

# Note: The Time zone information mentioned above
# should always precede the SERVER name.
set Bindery Context = O=workgroup
file server name NWSRV1
ipx internal net 60990060

# The network environment for this server consists
# of a Token-Ring LAN with only one Frame Type
load tcpip
load odineb

# Primary adapter
LOAD IBMTRPO SLOT=3 RNICOPEN=400010203182 FRAME=TOKEN-RING NAME=IBMTRPO_1_TOK
BIND IPX IBMTRPO_1_TOK NET=ABCD1
# Secondary adapter loaded with the same frame type as the Primary
LOAD IBMTRPO SLOT=2 RNICOPEN=400010203182 FRAME=TOKEN-RING
     NAME=IBMTRPO_2_TOK

# Create the Redundant NIC pair with Primary slot=3, and Secondary Slot=2
load ibmrnic pair mypair -p3 -s2

mount all
```

2. AUTOEXEC.NCF of a complex Redundant NIC configuration after using INSTALL.NLM:

```
set Time Zone = EST5EDT
   set Daylight Savings Time Offset = 1:00:00
   set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST  2:00:00 AM)
   set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST  2:00:00 AM)
   set Default Time Server Type = SINGLE

   # Note: The Time zone information mentioned above
   # should always precede the SERVER name.
   set Bindery Context = O=workgroup
   file server name NWSRV1
   ipx internal net 60990060

   # The network environment for this server includes both Token-Ring frame
   # types, utilizes Source Routing, has an IP network with a default IP gateway,
   # and utilizes Route Switching via the IBM 8210
   LOAD IPXRTR routing=NLSP
   load tcpip
   load odineb

   # Primary Adapter
   LOAD IBMTRPO SLOT=3 NODE=400010203182 RT=C FRAME=TOKEN-RING
        NAME=IBMTRPO_1_TOK
   BIND IPX IBMTRPO_1_TOK NET=ABCD1
   LOAD IBMTRPO SLOT=3 NODE=400010203182 RT=C FRAME=TOKEN-RING_SNAP
        NAME=IBMTRPO_1_TSP
   BIND IPX IBMTRPO_1_TSP NET=FF1
   BIND IP IBMTRPO_1_TSP ADDR=10.20.31.82 MASK=ff.ff.ff.0 GATE=10.20.31.254

   # Secondary Adapter with the same frame types as Primary loaded, but no
   # bindings
   LOAD IBMTRPO SLOT=2 NODE=400010203182 STANDBY RT=C
        FRAME=TOKEN-RING  NAME=IBMTRPO_2_TOK
   LOAD IBMTRPO SLOT=2 NODE=400010203182 STANDBY RT=C
        FRAME=TOKEN-RING_SNAP  NAME=IBMTRPO_2_TSP

   # Create the Redundant NIC pair with the Primary slot=3, the Secondary
   # slot=2, and the Default IP gateway=10.20.31.254
   load ibmrnic pair mypair -p3 -s2 -r10.20.31.254

   # If Source Routing is needed, then route.nlm must be loaded for
   # all the logical boards of both the primary and secondary adapter
   load route name=ibmtrpo_1_tok rsp=ar time=10
   load route name=ibmtrpo_1_tsp rsp=ar time=10
   load route name=ibmtrpo_2_tok rsp=ar time=10
   load route name=ibmtrpo_2_tsp rsp=ar time=10

   mount all
```

3. AUTOEXEC.NCF of installs with INETCFG (it is the same for both complex and simple installs):

```
 set Time Zone = EST5EDT
   set Daylight Savings Time Offset = 1:00:00
   set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST  2:00:00 AM)
   set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST  2:00:00 AM)
   set Default Time Server Type = SINGLE
   # Note: The Time zone information mentioned above
   # should always precede the SERVER name.
   set Bindery Context = O=workgroup
   file server name NWSRV2
   ipx internal net 35083DE8

   ; Network driver LOADs and BINDs are initiated via
   ; INITSYS.NCF. The actual LOAD and BIND commands
   ; are contained in INITSYS.NCF and NETINFO.CFG.
   ; These files are in SYS:ETC.
   load odineb
```

```
   sys:etc\initsys.ncf
   load ibmrnic pair mypair -p7 -s6

   mount all
```

4. What is displayed if you select **View All Commands** from INETCFG after a simple installation:

```
# The network environment for this server consists
   # of a Token-Ring LAN with only one Frame Type
   LOAD SNMP
   LOAD IBMTRPO NAME=TOK1_TOK FRAME=TOKEN-RING SLOT=7 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES
   RTSWENABLE=NO
   LOAD IBMTRPO NAME=TOK2_TOK FRAME=TOKEN-RING SLOT=6 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES STANDBY
   RTSWENABLE=NO
   BIND IPX TOK1_TOK net=abcd1 seq=1
   LOAD DUMMY
   BIND DUMMY TOK2_TOK
```

5. What is displayed if you select **View All Commands** from INETCFG after a complex installation:

```
# The network environment for this server includes both Token-Ring frame
   # types, utilizes Source Routing, has an IP network with a default IP gateway,
   # and utilizes Route Switching via the IBM 8210
   LOAD SNMP
   LOAD IBMTRPO NAME=TOK1_TOK FRAME=TOKEN-RING SLOT=7 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES
   RT=C RTTS=1024
   LOAD IBMTRPO NAME=TOK1_TSP FRAME=TOKEN-RING_SNAP SLOT=7 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES
   RT=C RTTS=1024
   LOAD IBMTRPO NAME=TOK2_TOK FRAME=TOKEN-RING SLOT=6 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES STANDBY
   RT=C RTTS=1024
   LOAD IBMTRPO NAME=TOK2_TSP FRAME=TOKEN-RING_SNAP SLOT=6 NODE=400010203181
        RXBUFFERS=32 TXBUFFERS=16 DATARATE=AUTO FULLDUPLEX=YES
   STANDBY RT=C RTTS=1024
   LOAD IPXRTR ROUTING=NLSP
   BIND IPX TOK1_TOK net=abcd1 seq=1
   BIND IPX TOK1_TSP net=ff1 seq=2
   LOAD ROUTE NAME=TOK1_TOK RSP=AR TIME=10
   LOAD ROUTE NAME=TOK1_TSP RSP=AR TIME=10
   LOAD ROUTE NAME=TOK2_TOK RSP=AR TIME=10
   LOAD ROUTE NAME=TOK2_TSP RSP=AR TIME=10
   LOAD Tcpip RIP=Yes Forward=No
   BIND IP TOK1_TSP ARP=Yes Mask=ff.ff.ff.0 Address=10.20.31.81
   LOAD DUMMY
   BIND DUMMY TOK2_TOK
   BIND DUMMY TOK2_TSP
```

6. AUTOEXEC.NCF of a simple Redundant NIC configuration after using INSTALL.NLM to configure two pairs (one using a non IBM token-ring PCI adapter as the secondary adapter):

```
set Time Zone = EST5EDT
   set Daylight Savings Time Offset = 1:00:00
   set Start Of Daylight Savings Time = (APRIL SUNDAY FIRST 2:00:00 AM)
   set End Of Daylight Savings Time = (OCTOBER SUNDAY LAST 2:00:00 AM)
   set Default Time Server Type = SINGLE

   # Note: The Time zone information mentioned above
   # should always precede the SERVER name.
   set Bindery Context = O=workgroup
   file server name NWSRV1
   ipx internal net 60990060

   # The network environment for this server consists
```

```
# of a Token-Ring LAN with only one Frame Type
load tcpip
load odineb

# Primary adapter 1
LOAD IBMTRPO SLOT=4 NODE=400000000004 DATARATE=M16 STANDBY FRAME=TOKEN-RING
     NAME=IBMTRPO_4_TOK
BIND IPX IBMTRPO_4_TOK NET=1234
#Secondary adapter 1 (notice this adapter is not an IBM PCI Token-Ring
     adapter)
LOAD IBMMPCO SLOT=5 NODE=400000000004 DATARATE=16 ENABLEFDX FRAME=TOKEN-RING
     NAME=IBMMPCO_5_TOK

# Primary adapter 2
LOAD IBMTRPO SLOT=3 NODE=400010203182 FRAME=TOKEN-RING  NAME=IBMTRPO_1_TOK
BIND IPX IBMTRPO_1_TOK NET=ABCD1
# Secondary adapter loaded with the same frame type as the Primary 2
LOAD IBMTRPO SLOT=2 NODE=400010203182 STANDBY FRAME=TOKEN-RING
     NAME=IBMTRPO_2_TOK

# Create the Redundant NIC pair with Primary slot=4, and Secondary
# Slot=5 (this pair uses the -backup parameter because the Secondary
# adapter is not an IBM PCI Token-Ring adapter)
load ibmrnic pair bkpair -p4 -s5 -backup
# Create the Redundant NIC pair with Primary slot=3, and Secondary Slot=2
ibmrnic pair mypair -p3 -s2

mount all
```

Messages

RNIC-100: FAILED TO ALLOCATE MEMORY FOR LAN BOARDS

Explanation: Your server is not able to allocate memory for IBMRNIC.NLM

User Action: Try unloading NLMs that are not needed or add more memory to the server.

RNIC-101: FAILED TO REGISTER FOR ONE OR MORE NESL EVENTS.

Explanation: The Redundant NIC NLM was unable to register for some NESL/NEB events. This could prevent the Redundant NIC pairs from functioning correctly.

User Action: Update MSM.NLM to the latest available level.

RNIC-102: PAIRING SUCCEEDED

Explanation: A Redundant NIC pair was created successfully and will be monitored for events from the adapters that make up the pair.

User Action: None.

RNIC-103: MUST SPECIFY -P AND -S OR -X TO CREATE A REDUNDANT NIC PAIR

Explanation: The Redundant NIC NLM must be told the slot for the primary and secondary adapters when a pair is created.

User Action: See “Setting up a Redundant NIC pair” on page 60 for information about creating a pair.

RNIC-104: MUST SPECIFY A NAME FOR A REDUNDANT NIC PAIR

Explanation: Redundant NIC pairs must be given a name for the pairing to be completed.

User Action: Try to create the pair again and specify a pair name.

RNIC-105: PAIR NAME IN USE. CHOOSE ANOTHER NAME.

Explanation: You tried to use an existing pair name for another pair.

User Action: None.

RNIC-106: THE DEFAULT IP ROUTER ADDRESS THAT WAS SPECIFIED IS INVALID.

Explanation: The default IP router address format that you specified was incorrect.

User Action: Verify the IP address of your router.

RNIC-107: UNABLE TO GET OPTIONS STRUCTURE MEMORY.

Explanation: There was a problem allocating memory. The server could be out of memory or there could be a problem with CLIB.NLM.

User Action: Try unloading NLMs that are not needed or add more memory to the server.

RNIC-108: NO REDUNDANT NIC PAIRS LOADED

Explanation: There are no configured pairs to show at this time.

User Action: None.

RNIC-109: ERROR READING PAIR INFORMATION FROM FILE

Explanation: Redundant NIC was unable to load one or more pairs from a saved configuration file.

User Action: Try recreating the pairs and resaving the file.

RNIC-110: ALL PAIRS WERE REMOVED.

Explanation: All Redundant NIC pairings were successfully removed.

User Action: None.

RNIC-111: INVALID REDUNDANT NIC PAIR NAME

Explanation: The pair name specified with the **ibmrnic switch** command does not exist.

User Action: Use **ibmrnic show** to determine the correct name.

RNIC-112: MANUAL ADAPTER FAILOVER SUCCEEDED

Explanation: An **ibmrnic switch** command was issued to a Redundant NIC pair and the failover completed successfully.

User Action: None.

RNIC-113: INVALID IBMRNIC SWITCH COMMAND

Explanation: The **ibmrnic switch** command that you specified was not correct.

User Action: Enter **ibmrnic help** to get help with the **ibmrnic** command.

RNIC-114: SWITCH MODE SET TO <MODE>

Explanation: The Redundant NIC switch mode was successfully set to the specified mode.

User Action: None.

RNIC-115: COULD NOT START THREAD TO HANDLE KEYBOARD REQUESTS

Explanation: A new thread failed to start.

User Action: Unload the NLM and reload it. Some memory may need to be freed.

RNIC-116: <PAIRNAME> UNPAIRED SUCCESSFULLY

Explanation: The Redundant NIC pair *<pairname>* was removed successfully.

User Action: None.

RNIC-117: UNKNOWN OR MALFORMED COMMAND

Explanation: You typed in a command that was not valid.

User Action: Type **ibmrnic help** to get help with the **ibmrnic** command.

RNIC-118: ERROR SAVING PAIR INFORMATION TO THE FILE

Explanation: The configuration for the pairs could not be saved.

User Action: Verify that there is space available for new files.

RNIC-119: THE SETTINGS WERE SAVED TO THE FILE SUCCESSFULLY

Explanation: The current configuration was correctly saved to a file.

User Action: None.

RNIC-120: USE THE IBMRNIC UTILITY SCREEN TO PERFORM THIS OPERATION

Explanation: Instead of using the console command line, use the NWSNUT interface.

User Action: Try performing the command using the NWSNUT utility.

RNIC-121: INVALID FILE NUMBER SPECIFIED

Explanation: The file number specified on the command line is invalid.

User Action: Choose a file number from that is valid.

RNIC-122: THE FAIL BACK FUNCTION COULD NOT BE STARTED

Explanation: The thread that performs the fail back function did not start.

User Action: Unload and then reload IBMRNIC.NLM.

RNIC-123: THE GRAPHICAL INTERFACE WAS NOT INITIALIZED

Explanation: There was a problem starting the NWSNUT utility for Redundant NIC.

User Action: Try unloading and then reloading IBMRNIC.NLM.

RNIC-124: CREATING DEFAULT INI FILE

Explanation: A default INI file is being created because the current INI file cannot be found.

User Action: None.

RNIC-125: INVALID FILE FORMAT, USING BUILT IN DEFAULTS

Explanation: The INI file is invalid and will not be used.

User Action: Correct the problem introduced to the INI file or delete it so IBMRNIC can recreate the default file.

RNIC-126: INVALID VALUE IN INI FILE

Explanation: An entry in the INI file was found to be incorrect.

User Action: Correct any problems in the INI file.

RNIC-127: COULD NOT START THREAD TO HANDLE COMMAND LINE

Explanation: The thread that processes the IBMRNIC command line did not get started.

User Action: Try unloading and reloading IBMRNIC.NLM.

RNIC-128: PROBLEM ALLOCATING RESOURCE TAGS

Explanation: There was not enough memory to allocate resource tags for IBMRNIC.NLM.

User Action: Unload and reload IBMRNIC.NLM.

RNIC-200: UNABLE TO GET PARAMETER STRUCTURE MEMORY

Explanation: Your server is not able to allocate memory for IBMRNIC.NLM.

User Action: Try unloading NLMs that are not needed or add more memory to the server.

RNIC-201: SETUP FAILED: INVALID COMMAND LINE FORMAT

Explanation: You typed an ibmrnic pair parameter that was not valid.

User Action: Enter **ibmrnic help** to get help with the **ibmrnic** command.

RNIC-202: SETUP FAILED: UNABLE TO GET MEMORY FOR RNIC PROFILE

Explanation: Your server is not able to allocate memory for IBMRNIC.NLM.

User Action: Try unloading NLMs that are not needed or add more memory to the server.

RNIC-203: SETUP FAILED: PROBLEM INITIALIZING THE ADAPTER PAIR

Explanation: The initialization routine for the pair failed.

User Action: Try creating the pair again.

RNIC-204: SETUP FAILED: PARAMETERS STRUCTURE IS MISSING

Explanation: There was a problem accessing the parameters structure.

User Action: Try setting up the pair again.

RNIC-205: SETUP FAILED: FAILED TO FIND ANY LOADED IBM TOKEN-RING BOARDS.

Explanation: The Redundant NIC NLM was not able to find any IBM token-ring boards loaded at this time.

User Action: Load token-ring boards for the primary and secondary adapters.

RNIC-206: SETUP FAILED: PRIMARY ADAPTER NOT FOUND

Explanation: There is no adapter in the slot that you specified as primary.

User Action: Specify the correct slot.

RNIC-207: SETUP FAILED: COULD NOT ALLOCATE SPACE TO READ THE MSM CONFIG TABLE

Explanation: Problem allocating memory. It is possible that the machine is low on RAM.

User Action: Try unloading NLMs that are not needed or add more memory to the server.

RNIC-208: SETUP FAILED: PROBLEM READING THE MSM CONFIG TABLE

Explanation: The Config table for the adapter could not be read.

User Action: Make sure that you are using the correct LAN driver.

RNIC-209: SETUP FAILED: INCORRECT LAN DRIVER VERSION

Explanation: Your LAN driver is too old.

User Action: Use the one that came with the IBMRNIC.NLM diskette or a newer version if one is available.

RNIC-210: SETUP FAILED: SECONDARY ADAPTER NOT FOUND

Explanation: There is no adapter in the slot that you specified as secondary.

User Action: Specify the correct slot.

RNIC-211: SETUP FAILED: PRIMARY AND SECONDARY LOGICAL BOARDS DO NOT MATCH

Explanation: The logical boards on the primary adapter do not match the logical boards on the secondary adapter.

User Action: Check the frame types for the primary and secondary adapters. They should match.

RNIC-212: SETUP FAILED: PRIMARY AND SECONDARY MAC ADDRESSES DO NOT MATCH

Explanation: The same Locally Administered Address must be assigned to each adapter using the **node address=**<*LAA*> command line keyword.

User Action: Set the Locally Administered Address on the primary and secondary adapters to the same address.

RNIC-213: SETUP FAILED: COULD NOT FIND MLID CONFIG TABLE TO PERFORM ADAPTER STATUS CHECK

Explanation: There is a problem reading the adapter Config table.

User Action: Try setting up the pair again.

RNIC-214: SETUP FAILED: THE PRIMARY ADAPTER MUST NOT BE SHUT DOWN

Explanation: The primary adapter must be open in order for Redundant NIC to initialize correctly.

User Action: Specify a primary adapter that is not shut down.

RNIC-215: SETUP FAILED: THE SECONDARY ADAPTER MUST NOT BE OPEN

Explanation: The secondary adapter must be closed when Redundant NIC is being initialized.

User Action: Specify an adapter that was loaded with the standby keyword.

RNIC-216: SETUP FAILED: THE PRIMARY ADAPTER COULD NOT ACCEPT THE LAA

Explanation: There was a problem setting up the adapter with the Quick Failover feature.

User Action: Make sure the correct level of microcode is on the adapter.

RNIC-217: SETUP FAILED: COULD NOT SHUT DOWN THE SECONDARY ADAPTER

Explanation: The secondary adapter did not respond to a request to shut down.

User Action: Try setting up the pair again.

RNIC-218: SETUP FAILED: THE PRIMARY ADAPTER SPECIFIED IS PART OF ANOTHER PAIR

Explanation: The primary adapter you specified is part of another Redundant NIC pair.

User Action: Specify a primary adapter that is not part of a Redundant NIC pair.

RNIC-219: SETUP FAILED: THE SECONDARY ADAPTER SPECIFIED IS PART OF ANOTHER PAIR

Explanation: The secondary adapter you specified is part of another Redundant NIC pair.

User Action: Specify a secondary adapter that is not part of a Redundant NIC pair.

RNIC-220: SETUP FAILED: FAILED TO RESET THE PRIMARY ADAPTER

Explanation: The primary adapter could not be reset.

User Action: Attempt to create the pair again.

RNIC-221: SETUP FAILED: THE PRIMARY ADAPTER DOES NOT SUPPORT QUICK FAILOVER

Explanation: The primary adapter must have newer microcode to support Quick Failover.

User Action: Update the microcode on the adapter or do not load the adapters driver with the RNICOPEN keyword.

RNIC-222: SETUP FAILED: THE SECONDARY ADAPTER DOES NOT SUPPORT QUICK FAILOVER

Explanation: The secondary adapter must have newer microcode to support Quick Failover.

User Action: Update the microcode on the adapter or do not load the adapters driver with the RNICOPEN keyword.

RNIC-223: SETUP FAILED: THE PRIMARY AND SECONDARY ADAPTERS MUST NOT BE THE SAME

Explanation: The primary and secondary adapters specified were the same adapter.

User Action: Attempt to create the pair again with two adapters.

RNIC-300: UNPAIR FAILED: INVALID IBMRNIC PAIR NAME

Explanation: The pair that you tried to remove does not exist.

User Action: Enter **ibmrnic show** to find the correct pair name of the adapters that you would like to remove.

RNIC-301: UNPAIR FAILED: COULD NOT REMOVE LINK FROM LIST OF PAIRS

Explanation: There was a problem unpairing the adapters.

User Action: Try to remove the pair again.

RNIC-400: MANUAL ADAPTER FAILOVER UNSUCCESSFUL: THE SWITCHING MODE IS DISABLED.

Explanation: When the switching mode is disabled you cannot initiate a manual failover.

User Action: Set the switching mode to manual or auto.

RNIC-401: MANUAL ADAPTER FAILOVER UNSUCCESSFUL: THE BACKUP ADAPTER IS NOT ABLE TO BECOME ACTIVE AT THIS TIME.

Explanation: An attempt was made to failover to the backup adapter. The state of the backup adapter is preventing it from becoming an active adapter.

User Action: Make sure that the backup adapter is not open.

RNIC-402: MANUAL ADAPTER FAILOVER UNSUCCESSFUL: SHUTDOWN OF ACTIVE ADAPTER FAILED

Explanation: The active adapter could not be shut down.

User Action: Try issuing a manual failover from the command line.

RNIC-403: MANUAL ADAPTER FAILOVER UNSUCCESSFUL: FAILED TO ACTIVATE BACKUP ADAPTER.

Explanation: The backup adapter could not be reset.

User Action: Try issuing a manual failover from the command line.

Chapter 8. Tivoli Management Agent

This chapter describes the Tivoli® Management Agent (TMA).

Supported environments

The TMA executes independent of the LAN adapter. As long as the adapter has a device driver for a supported operating system, the TMA will be able to try to connect to a server.

The TMA packages are provided to support the following operating systems:
- Windows NT
- Windows 95 and Windows 98
- NetWare 3.x
- NetWare 4.x and 5.x
- OS/2
- Windows 3.x

Overview

The Tivoli Management Agent gives you the framework necessary to perform management operations such as software distribution, inventory, user administration and distributed monitoring. Instead of software applications sitting on top of the desktop, the Tivoli Management Agent automatically determines what is needed to perform a given management operation. If that capability already resides on the computer, it immediately proceeds with the operation. If not, the Agent downloads the appropriate software from the server to the desktop with no operator intervention.

In addition, the Agent downloads newer versions as updates are loaded on the server.You can gain significant productivity advances with these management features because Tivoli Management Software is installed only once on the server with updates performed automatically thereafter.

For more information about Tivoli Systems and Tivoli-Ready™ initiatives, visit the Tivoli Web site at `http://www.tivoli.com`

Installation and configuration

To begin the installation, you must first get the installation package. See “Downloads” on page 1. After you have downloaded the package, execute the package to expand the files.

Note: NetWare installations must be done from a NetWare client.

Use the procedures in the following sections to configure the TMA.

Windows NT

1. Execute the batch file NTINS.BAT to install TMA.
2. A check will be done for a previously installed TMA.

- If an existing TMA is installed on the target machine, NTINS.BAT will abort without installing. The TMA has a “live upgrade” feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
- If an existing TMA is not found, NTINS.BAT will automatically install TMA in the directory c:\tivoli.

3. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to “Windows NT” on page 77 for instructions to activate your Tivoli Management Agent.

Windows 95 and Windows 98

1. Execute the batch file WIN9XINS.BAT to install TMA.
2. A check will be done for a previously installed TMA.
   - If an existing TMA is installed on the target machine, WIN9XINS.BAT will abort without installing. The TMA has a live upgrade feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
   - If an existing TMA is not found, WIN9XINS.BAT will automatically install TMA in the directory c:\tivoli.
3. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to “Windows 95 and Windows 98” on page 78 for instructions to activate your Tivoli Management Agent.

NetWare 3.x

1. Log in to the NetWare server drive (referred to here as drive *x*).
2. Execute the batch file NW3XINS.BAT to install TMA. Enter the NetWare server drive letter as a parameter. For example, if *x* is the server drive letter, at a DOS prompt, enter the following:

   ```
   nw3xins x
   ```

3. A check will be done for a previously installed TMA.
   - If an existing TMA is installed on the target machine, NW3XINS.BAT will abort without installing. The TMA has a live upgrade feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
   - If an existing TMA is not found, NW3XINS.BAT will automatically install TMA in the directory *x*:\tivoli (where *x* is your drive letter).
4. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to “NetWare 3.x” on page 79 for instructions to activate your Tivoli Management Agent.

NetWare 4.x and 5.x

1. Log in to the NetWare server drive (referred to here as *x*).
2. Execute the batch file NW4_5INS.BAT to install TMA. Enter the NetWare server drive letter as a parameter. For example, if *x* is the server drive letter, at a DOS prompt, enter the following:

   ```
   nw4_5ins x
   ```

3. A check will be done for a previously installed TMA.

- If an existing TMA is installed on the target machine, NW4_5INS.BAT will abort without installing. The TMA has a live upgrade feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
- If an existing TMA is not found, NW4_5INS.BAT will automatically install TMA in the directory *x*:\Tivoli.

4. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to "NetWare 4.x and 5.x" on page 80 for instructions to activate your Tivoli Management Agent.

OS/2

1. Execute the command file OS2INS.CMD from an OS/2 window to install TMA.
2. A check will be done for a previously installed TMA.
   - If an existing TMA is installed on the target machine, os2ins.cmd will abort without installing. The TMA has a live upgrade feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
   - If an existing TMA is not found, OS2INS.CMD will automatically install TMA in the directory *x*:\Tivoli.
3. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to "OS/2" on page 81 for instructions to activate your Tivoli Management Agent.

Windows 3.x

1. Execute the batch file WIN3XINS.BAT to install TMA.
2. A check will be done for a previously installed TMA.
   - If an existing TMA is installed on the target machine, WIN3XINS.BAT will abort without installing. The TMA has a live upgrade feature so that any version of a TMA can join the Tivoli Enterprise and will be automatically upgraded to the latest version.
   - If an existing TMA is not found, WIN3XINS.BAT will automatically install TMA in the directory *x*:\Tivoli.
3. After the TMA has been installed, use your Web browser to open the file *x*:\Tivoli\TivReady\readme.html (where *x* is your CD-ROM drive) or proceed to "Windows 3.x" on page 82 for instructions to activate your Tivoli Management Agent.

Activating the Tivoli Management Agent

Windows NT

This machine has the Tivoli Management Agent installed in an inactive state.

If you want this machine to become part of your Tivoli Enterprise you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway that the TMA will need to log in to. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed once. After this activation, the TMA is running on the machine and is configured to start and log in to the TMR every time the machine starts.

Your installation includes a logon script that can be used to automate the one-time setup process described in this section. See c:\tivoli\lcf\generic\logontma.bat

The steps in this section can be performed in any order. The first two steps are not necessary to start the TMA, but are necessary for running of Tivoli methods once the endpoint joins the TMR.

Start TAP

Activate the Tivoli Authentication Process (TAP): `run c:\tivoli\lcf\bin\w32-ix86\mrt\wlcftap.exe -a` Reboot your computer.

Add Tivoli user and group

Add the Tivoli reserved user (nobody): `run c:\tivoli\lcf\bin\w32-ix86\mrt\ntconfig.exe -e`

Start the Tivoli Management Agent: `c:\tivoli\lcf\bin\w32-ix86\mrt\lcfd.exe` with the following options:

Note: Options are case-sensitive.

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
-i	Installs the TMA as an NT service. This also configures the TMA for autostart when the computer boots.
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

To view a Usage statement and see all the options that can be used in starting the endpoint, `run C:\Tivoli\lcf\bin\w32-ix86\mrt\lcfd.exe -s -D?`

Add the taskbar icon

Type `C:\Tivoli\lcf\bin\w32-ix86\mrt\lcfep.exe -x -i` to install the taskbar icon. To remove, use the -s option.

Windows 95 and Windows 98

This computer has the Tivoli Management Agent installed in an inactive state.

If you want this computer to become part of your Tivoli Enterprise, you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway where this TMA will log in. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed

once. After this activation, the TMA is running on the computer and is configured to start and log in to the TMR every time the computer starts.

Your installation includes a logon script that can be used to automate the one-time setup process described in this section. See `c:\Tivoli\lcf\generic\logontma.bat`

Start the TMA

To activate the TMA, start LCFD.EXE from the command line using options to identify the correct gateway (Tivoli Management Gateway). For example, some companies have one gateway that the whole company logs into, others have many different choices. The Tivoli Administrator will provide this information.

Start the Tivoli Management Agent

`C:\Tivoli\lcf\bin\win95\mrt\lcfd.exe` with the following options:

Note: Options are case-sensitive.

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

To view a Usage statement and see all the options that can be used in starting the endpoint, `run C:\Tivoli\lcf\bn\win95\mrt\lcfd.exe -s -D?`

Start the taskbar icon

To activate the taskbar icon you need to start `lcfep.exe -x -i`

NetWare 3.x

This computer has the Tivoli Management Agent installed in an inactive state.

If you want this computer to become part of your Tivoli Enterprise, you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway where this TMA will log in. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed once. After this activation, the TMA is running on the computer and is configured to start and log in to the TMR every time the computer starts.

Note: Even though the steps in this section are in a certain order, the first step can be performed at any time. The next step must be performed before the third.

Autostart of the TMA
Add the line `sys\system\lcf.ncf` to your AUTOEXEC.NCF file.

Add command line parameters to lcf.ncf
Add command line parameters to the line that loads LCFD.NLM in sys:\system\lcf.ncf and sys:\system\tivoli\lcf\1\lcf.ncf. They should include options to identify the correct gateway (Tivoli Management Gateway). For example, some companies have one gateway that the whole company logs into. Others have many different choices. The Tivoli Administrator will provide this information.

Note: Options are case-sensitive.

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

Start the TMA
Type `lcf` This will load LCFUTILS.NLM and LCFD.NLM.

Stopping TMA
Type `unload lcfd` then `unload lcfutils`

To view a usage statement and see all of the options that can be used in starting the endpoint, `run load sys:\system\Tivoli\lcf\bin\nw3\mrt\lcfd.exe -s -D?`

NetWare 4.x and 5.x
This computer has the Tivoli Management Agent installed in an inactive state.

If you want this computer to become part of your Tivoli Enterprise, you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway where this TMA will log in. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed once. After this activation, the TMA is running on the computer and is configured to start and log in to the TMR every time the computer starts.

Note: Even though the steps in this section are in a certain order, the first step can be performed at any time. The next step must be performed before the third.

Autostart of the TMA
Add the line `sys\system\lcf.ncf` to your autoexec.ncf file.

Add command line parameters to lcf.ncf

Add command line parameters to the line that loads LCFD.NLM in sys:\system\lcf.ncf and sys:\system\tivoli\lcf\1\lcf.ncf. They should include options to identify the correct gateway (Tivoli Management Gateway). For example, some companies have one gateway that the whole company logs into. Others have many different choices. The Tivoli Administrator will provide this information.

Note: Options are case-sensitive.

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

Start the TMA

Type `lcf` This will load LCFUTILS.NLM and LCFD.NLM.

Stopping TMA

Type `unload lcfd` then `unload lcfutils`

To view a usage statement and see all of the options that can be used in starting the endpoint, `run load sys:\system\Tivoli\lcf\bin\nw4\mrt\lcfd.exe -s -D?`

OS/2

This computer has the Tivoli Management Agent installed in an inactive state.

If you want this computer to become part of your Tivoli Enterprise, you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway where this TMA will log in. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed once. After this activation, the TMA is running on the computer and is configured to start and log in to the TMR every time the computer starts.

Note: Even though the steps in this section are in a certain order, they can be performed in any order. The first step is not necessary to start the TMA, but it is necessary for running the TMA after a reboot.

Autostart of the TMA

Add an entry to the Startup Folder to run `c:\tivoli\lcf\dat\1\startlcf.exe`

Start the TMA

Start the LCFD.EXE program from the command line using options to identify the correct gateway (Tivoli Management Gateway). For example, some companies have one gateway that the whole company logs into. Others have many different choices. The Tivoli Administrator will provide this information.

Start the Tivoli Management Agent: `C:\Tivoli\lcf\bin\os2-ix86\mrt\lcfd.exe` with the following options:

Note: Options are case-sensitive

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

To view a Usage statement and see all of the options that can be used in starting the endpoint, `run C:\Tivoli\lcf\bin\os2-ix86\mrt\lcfd.exe -s -D?`

Windows 3.x

This computer has the Tivoli Management Agent installed in an inactive state.

If you want this computer to become part of your Tivoli Enterprise, you will need to activate or wake up the agent. The Tivoli Enterprise includes a computer with a gateway where this TMA will log in. As user or system administrator, you can ensure that the TMA is activated correctly and joins the Tivoli Enterprise by following the instructions in this section. This process only needs to be performed once. After this activation, the TMA is running on the computer and is configured to start and log in to the TMR every time the computer starts.

win32s is required to run the TMA

Note: Even though the steps in this section are in a certain order, they can be performed in any order. The first step is not necessary to start the TMA but is necessary for running of Tivoli methods once the endpoint joins the TMR.

Autostart of the TMA

Add an entry to the `run=` entry in the WIN.INI file:
`run=c:\tivoli\lcf\dat\1\startlcf.exe`

Start the TMA

Start LCFD.EXE from the command line using options to identify the correct gateway (Tivoli Management Gateway). For example, some companies have one

gateway that the whole company logs into, others have many different choices. The Tivoli Administrator will provide this information.

Start the Tivoli Management Agent:

`C:\Tivoli\lcf\bin\win3x\mrt\lcfd.exe` with the following options:

Note: Options are case-sensitive.

Option	Function
-C working directory	(Uppercase C) This causes the TMA to change the working directory to `working directory` when starting. The value should always be C:\Tivoli\lcf\dat\1
If the TMA is started without the `-g` option the endpoint will immediately broadcast a message in search of a Tivoli Management Gateway on its subnet. This is not recommended for most customers. Therefore, please use the following options to specify a Tivoli Management Gateway.	
-g gateway+port	Contacts the specified Tivoli Management Gateway for initial login. `gateway_address` is the hostname or IP address of the Tivoli Management Gateway that the endpoint will log into. `port` is the listening port of the gateway.
-p port	Contacts the gateway on the specified port. `port` is the listening port of the gateway.
-P port	(Uppercase P) Specifies a local port for use by the TMA. `port` is the listening port of the TMA.

To view a Usage statement and see all of the options that can be used in starting the endpoint, `run C:\Tivoli\lcf\bin\win3x\mrt\lcfd.exe -s -D?`

Chapter 9. Network adapter performance tuning

Obtaining the very best performance from a network adapter is not always a simple task. IBM adapters and their device drivers undergo extensive performance analysis in order to derive the best default configuration for the majority of possible configurations in which they are going to be placed. However, each environment introduces specific characteristics that affect the ability of the adapters and device driver to achieve the highest performance. IBM adapters and their device drivers are engineered to allow the user a great amount of flexibility to tune the performance in their specific environment. This includes not only many performance-based configuration parameters but also enhanced functions whose sole purpose is to achieve the highest performance possible, such as Route Switching and Class of Service for IP.

Tuning network adapters for the very highest performance is such a large topic that it is best addressed in a separate document. The following URL will take you to an IBM white paper explaining steps to achieve the best performance from your IBM adapters for your specific networking environment:

`http://www.ibm.com/networking/per/per10.html`

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance,

compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
AIX
AS/400
CallPath
CICS
LANDP
LANStreamer
Micro Channel
Nways
Operating System/2
OS/2
RS/6000
SystemView
System/370
VTAM
Wake on LAN

Tivoli, NetView, and Tivoli Ready are trademarks of Tivoli Systems Inc. in the United States, other countries, or both.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

NetWare Network Computing Products from IBM

The following additional license terms apply to the Novell IntranetWare Client for DOS and Windows 3.1 code, included with IBM's LAN Client program. In the event of any inconsistency between the following terms and the terms of the IBM License Agreement for Productivity Aids, the following terms shall prevail.

IF YOU DOWNLOAD OR USE THIS PROGRAM YOU AGREE TO THESE TERMS.

The IBM program you have licensed may be designed to run in a single computer system only, or it may contain modules designed to run in multiple computer system environments. The type of environment that applies is limited by the definitions that follow:

SINGLE USER PROGRAM means a program which operates on an intelligent single-user device by which the device acts as a standalone system or a peer system on a Communications Network

COMMUNICATIONS NETWORK means a computer system which allows a number of independent computing devices to communicate with each other

NETWORK HOST OR NETWORK SERVER means a single machine on which a Host program or NLM or VAP operates to provide the host or server resources to the other machines in a network

HOST PROGRAM means that portion of the NetWare network operating system that executes on the Network Host or Network Server

CLIENT PROGRAM means that portion of the NetWare network operating system that executes on the personal workstation

NLM PROGRAM OR VAP PROGRAM means an application program that executes under control of the NetWare network operating system on the Network Host or Network Server

DOCUMENTATION means the manual(s) and other printed material packaged by IBM with the Program

If you have licensed a Host Program, an NLM Program or a VAP Program, and/or Client Program, you are authorized to 1) use one copy of the Host Program on a single Network Host or Network Server; 2) use a single copy of an NLM Program or a VAP Program on a single Network Host or Network Server; and 3) use the Client Program, and to, without additional charge, reproduce and use copies, subject to the limitation identified in the Program Documentation, of the Client Program, in support of the Host Program.

Glossary

The following symbols are used in this glossary:

- The symbol (A) identifies definitions from the *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018.
- The symbol (I) identifies definitions from published parts of the *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1).
- The symbol (T) identifies definitions from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1.

The following cross-references are used in this glossary:

Contrast with:
This refers to a term that has an opposed or substantively different meaning.

Synonym for:
This indicates that the term has the same meaning as a preferred term, which was defined in its correct place in the glossary.

Synonymous with:
This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:
This refers the reader to related terms that have a related, but not synonymous, meaning.

A

active. (1) Able to communicate on the network. (2) Operational. (3) Pertaining to a node or device that is connected or is available for connection to another node or device. (4) Currently transmitting or receiving.

actual data transfer rate. The average number of bits, characters, or blocks per unit of time transferred from a data source and received by a data sink.

adapter. In a communicating device, a circuit card that, with its associated software and/or microcode, enables the device to communicate over the network.

adapter address. The hexadecimal digits that identify an adapter.

address. (1) A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination. (A) (2) To refer to a device or an item of data by its address. (I) (3) In word processing, the location, identified by an address code, of a specific section of the recording medium or storage. (T) (4) A name, label, or number identifying a location in storage, a device in a system or network, or any other data source. (5) In data communication, the unique code assigned to each device or workstation connected to a network.

Address Resolution Protocol (ARP). A protocol that dynamically maps between Internet addresses, baseband adapter addresses, X.25 addresses, and token-ring adapter addresses on a local area network.

Advanced Program-to-Program Communication (APPC). (1) The general facility characterizing the LU 6.2 architecture and its various implementations in products. (2) Sometimes used to refer to the LU 6.2 architecture and its product implementations as a whole, or to an LU 6.2 product feature in particular, such as an APPC application program interface.

agent. (1) In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. See also *client-server model* and *network management station (NMS).* (2) A customer-service person whose job is to handle outgoing or incoming telephone calls (for example, an agent in an ACD group).

AIX. Advanced Interactive Executive. See *AIX operating system.*

AIX operating system. IBM's implementation of the UNIX® operating system. The RS/6000® system, among others, runs the AIX operating system. See *UNIX operating system.*

alert. (1) A message sent to a management services focal point in a network to identify a problem or an impending problem. (2) In the NetView and NETCENTER programs, a high priority event that warrants immediate attention.

API. Application program interface.

APPC. Advanced Program-to-Program Communication.

application. (1) The use to which an information processing system is put; for example, a payroll application, an airline reservation application, a network application. (2) A collection of software components used to perform specific types of user-oriented work on a computer. (3) In the AS/400 system, the collection of CSP/AE objects that together can be run on the system. An application consists of a program object, up to five map group objects (depending on how many different devices are supported), and any number of table objects.

application program. (1) A program that is specific to the solution of an application problem. Synonymous with *application software*. (T) (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities. (4) In SDF/CICS®, the program using the physical maps and symbolic description maps generated from a source map set.

Note:
Do not use the term *application* in place of *application program.*

application program interface (API). (1) A functional interface supplied by the operating system or by a separately orderable licensed program that allows an application program written in a high-level language to use specific data or functions of the operating system or the licensed program. (2) The interface through which an application program interacts with an access method. In VTAM® programs, it is the language structure used in control blocks so that application programs can reference them and be identified to VTAM.

architecture. A logical structure that encompasses operating principles including services, functions, and protocols. See *computer architecture, network architecture, Systems Application Architecture (SAA), Systems Network Architecture (SNA)*.

ARP. Address Resolution Protocol.

attach. To make a device a part of a network logically.

Note:
Not to be confused with *connect,* which implies physically connecting a device to a network.

attaching device. Any device that is physically connected to a network and can communicate over the network. See *ring attaching device*.

attachment. A port or a pair of ports, optionally including an associated optical bypass, that are managed as a functional unit. A dual attachment includes two ports: a port A, and a port B. A single attachment includes a Port S.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone can be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

bandwidth. (1) The difference, expressed in hertz, between the highest and the lowest frequencies of a range of frequencies. For example, analog transmission by recognizable voice telephone requires a bandwidth of about 3000 hertz (3 kHz). (2) The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

Basic Input/Output System (BIOS). Code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

binary digit. Synonym for *bit.*

BIOS. Basic Input/Output System.

bit. Either of the digits 0 or 1 when used in the binary numeration system. Synonymous with *binary digit*. (T) See also *byte*.

block. A string of data elements recorded or transmitted as a unit. The element may be characters, words, or physical records. (T)

bridge. (1) An attaching device that connects two LAN segments to allow the transfer of information from one LAN segment to the other. A bridge can connect the LAN segments directly by network adapters and software in a single device, or it can connect network adapters in two separate devices through software and use of a telecommunications link between the two adapters. (2) A functional unit that connects two LANs that use the same logical link control (LLC) procedures but may use the same or different medium access control (MAC) procedures. (T) Contrast with *gateway* and *router*.

Note: A bridge connects networks or systems of the same or similar architectures, whereas a gateway connects networks or systems of different architectures.

bridging. The forwarding of a frame from one local area network segment to another. The destination is

based upon the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadband local area network. A local area network (LAN) in which information is encoded, multiplexed, and transmitted through modulation of carriers. (T)

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of the same data to more than one destination. A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Broadcast can be implemented in hardware (Ethernet, for example) or software. Contrast with *multicast.*

bus. (1) A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) (2) A computer configuration in which processors are interconnected in series. See also *hypercube*. (3) A network configuration in which nodes are interconnected through a bidirectional transmission medium. (4) One or more conductors used for transmitting signals or power. (A)

bypass. (1) To eliminate a station or an access unit from a ring network by allowing the data to flow in a path around it. (2) The ability of a station to be optically isolated from the network while maintaining the integrity of the ring. (3) The ability of a node to optically isolate itself from the FDDI network while maintaining the continuity of the cable plant.

byte. (1) A string that consists of a number of bits, treated as a unit, and representing a character.(T) (2) A binary character operated upon as a unit and usually shorter than a computer word.(A) (3) A group of 8 adjacent binary digits that represent one EBCDIC character. (4) See *n-bit byte*. See also *bit*.

C

cable segment. A section of cable between components or devices on a network. A segment can consist of a single patch cable, multiple patch cables connected together, or a combination of building cable and patch cables connected together. See *LAN segment*, *ring segment*.

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor.(T) (2) To place, hide, or store in a cache. An optional part of the directory database in network nodes where frequently used directory information can be stored to speed directory searches.

carrier. (1) On broadband networks, a continuous frequency signal that can be modulated with an information-carrying signal. (2) An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system.(T)

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) The portion of a storage medium that is accessible to a given reading or writing station; for example, track, band. (A) (3) The portion of a storage medium that is accessible to a given reading or writing station. (4) In broadband transmission, a designation of a frequency band 6 MH wide.

channel-attached. (1) Pertaining to the connection of devices directly by data channels (I/O channels) to a computer. (2) Pertaining to devices connected to a controlling unit by cables rather than by telecommunication lines. See also *local*. Contrast with *telecommunication-attached*.

claim token. A process whereby one or more stations bid for the right to initialize the ring.

class of service (CoS). A designation of the transport network characteristics, such as route security, transmission priority, and bandwidth, needed for a particular session. The class of service is derived from a *mode name* specified in the Bind by the initiator of a session.

client. (1) A user. (2) A functional unit that receives shared services from a server. (T)

client-server. In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

client-server model. A common way to describe network services and the model user processes (programs) of those services.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network. (3) The task of defining the hardware and software characteristics of a system or subsystem. (4) See also *system configuration*.

configuration parameters. Variables in a configuration definition, the values of which characterize the relationship of a product, such as a bridge, to other products in the same network.

connect. In a LAN, to physically join a cable from a station to an access unit or network connection point. Contrast with *attach*.

connection. (1) In data communication, an association established between functional units for conveying information (I) (A) A logical association between a call

participant (party) and a switch. (2) In Open Systems Interconnection architecture, an association established by a given layer between two or more entities of the next higher layer for the purpose of data transfer. (T) (3) In SNA, the network path that links two logical units (LUs) in different nodes to enable them to establish communications. (4) In X.25 communication, a virtual circuit between two data terminal equipments (DTEs). A switched virtual circuit (SVC) connection lasts for the duration of a call; a permanent virtual circuit (PVC) is a permanent connection between the DTEs. (5) In TCP/IP, the path between two protocol applications that provides reliable data stream delivery service. (6) In Internet, a connection extends from a TCP application on one system to a TCP application on another system. (7) The path between two protocol functions, usually located in different machines, that provides reliable data delivery service. (8) A party's connection represents that party's participation in a telephone call.

connectivity. (1) The capability of a system or device to be attached to other systems or devices without modification. (T) (2) The capability to attach a variety of functional units without modifying them.

D

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE can be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE can perform other functions that are usually performed at the network end of the line.

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. (1) In SNA or Open Systems Interconnection (OSI), the layer that schedules data transfer over a link between two nodes and performs error control for the link. Examples of DLC are synchronous data link control (SDLC) for serial-by-bit connection and DLC for the System/370® channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reach the higher layers.
(2) See *Systems Network Architecture (SNA)*. (3) See also *logical link control (LLC) sublayer*, *medium access control (MAC) sublayer*.

data link control (DLC) protocol. The LAN protocol used to attach a device to and remove a device from the network. The DLC protocol is also used to send information onto and receive information from the network, exchange data, and control information with network higher level protocols and interfaces.

data rate. See *data transfer rate, line data rate*.

data segment. A control section of a program which contains only data. It is usually addressed with its own hardware segment and offset.

data transfer rate. The average number of bits, characters, or blocks, per unit time passing between corresponding equipment in a data transmission system. (I) See *actual data transfer rate, effective transfer rate*. The rate is expressed in bits, characters, or blocks per second, minute, or hour.

DCE. Data circuit-terminating equipment.

device driver. The code needed to attach and use a device on a computer or a network.

device identifier (ID). An 8-bit identifier that uniquely identifies a physical I/O device.

diagnostics. The process of investigating the cause or the nature of a condition or problem in a product or system.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line. (3) Nonoperational or nonfunctional.

disk. A round, flat, data medium that is rotated in order to read or write data. (T) See also *diskette*.

diskette. (1) A small magnetic disk enclosed in a jacket. (T) (2) A thin, flexible magnetic disk and a semi-rigid protective jacket, in which the disk is permanently enclosed.

diskette drive. The mechanism used to seek, read, and write data on a diskette.

DLC. Data link control.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It represents IP addresses in the Internet.

duplex. Pertaining to communication in which data can be sent and received at the same time. Synonymous with *full-duplex*. Contrast with *half-duplex*.

E

enable. To make functional.

enabled. (1) On a LAN, pertaining to an adapter or device that is active, operational, and able to receive frames from the network. (2) Pertaining to the state in which a transmission control unit or an audio response unit can accept incoming calls on a line.

execute. To perform the actions specified by a program or a portion of a program. (T)

F

feature. A part of an IBM product that can be ordered separately by the customer. See *switch feature*.

field. On a data medium or a storage, a specified area used for a particular class of data; for example, a group of character positions used to enter or display wage rates on a screen. (T)

file. A named set of records stored or processed as a unit. (T)

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. Synonymous with *schema*. (T) (2) A data structure that consists of fields, predetermined by a protocol, for the transmission of user data and control data. The composition of a frame, especially the number and types of fields, may vary according to the type of protocol. Synonymous with *transmission frame*. (T) (3) The unit of transmission in some local area networks, including the IBM Token-Ring Network; it includes delimiters, control characters, information, and checking characters. (4) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures. (5) A packet that is transmitted over a serial line or LANs. See also *packet*. (6) In FDDI, a PDU transmitted between co-operating MAC entities on a ring, and consisting of a variable number of octets and control symbols.

full-duplex. Synonym for *duplex*.

function. (1) A specific purpose of an entity, or its characteristic action. (A) (2) In data communications, a machine action such as carriage return or line feed. (A) (3) In NetView DM, a function is the specification of a transmission activity on a resource or group of resources. Functions are grouped into phases. In CSCM, resources are known as data objects.

H

half-duplex (HDX). In data communication, pertaining to transmission in only one direction at a time. Contrast with *duplex*.

hard disk. (1) A rigid magnetic disk such as the internal disks used in the system units of personal computers and in external hard disk drives. Synonymous with *fixed disk*. (2) A rigid disk used in a hard disk drive.

Note: The term hard disk is also used loosely in the industry for boards and cartridges containing microchips or bubble memory that simulate the operations of a hard disk drive.

hard error. (1) An error condition on a network that requires that the network be reconfigured or that the source of the error be removed before the network can resume reliable operation. Contrast with *soft error*. (2) Synonym for *hard failure*. (T)

hard failure. An error condition on a network that requires that the network be reconfigured or that the source of the error be removed before the network can resume reliable operation. Synonymous with *hard error*. (T)

hardware. All or part of the physical components of an information processing system, such as computers or peripheral devices. (T) (A)

hexadecimal. (1) Pertaining to a selection, choice, or condition that has 16 possible different values or states. (I) (2) Pertaining to a fixed-radix numeration system, with radix of 16. (I) (3) Pertaining to a system of numbers to the base 16; hexadecimal digits range from 0 through 9 and A through F, where A represents 10 and F represents 15.

host. (1) In Internet terminology, an end system. (2) In interpretive execution mode, the real machine as opposed to the virtual or interpreted machine (the guest).

I

I/O. Input/output.

IBM Token-Ring Network. A baseband local area network with a ring topology that passes tokens from Token-Ring adapter to Token-Ring adapter.

IEEE. Institute of Electrical and Electronics Engineers.

initialize. In a LAN, to prepare the adapter (and adapter support code, if used) for use by an application program.

input/output (I/O). (1) Pertaining to a device whose parts can perform an input process and an output process at the same time. (I) (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process.

Note: The phrase input/output may be used in place of input/output data, input/output signals, and input/output process when such a usage is clear in context.
(3) Pertaining to input, output, or both. (A) (4) Pertaining to a device, process, or channel involved in data input, data output, or both.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

Internet. A worldwide network connecting users through autonomous networks in industry, education, government, and research. The Internet network uses Internet Protocol (IP). The major Internet services include electronic mail, FTP, telnet, World Wide Web, and electronic bulletin boards (Usenet). For network interconnection and routing, and Transmission Control Protocol (TCP) for end-to-end control. (A)

Internet address. A 32-bit address assigned to hosts using TCP/IP. See also *TCP/IP*.

Internet Engineering Task Force (IETF). One of the task forces of the Internet Architecture Board (IAB) responsible for solving short-term engineering needs of the Internet.

Internet Packet Exchange (IPX). The routing protocol used to connect Novell's servers or any workstation or router that implements IPX with other workstations. Although similar to TCP/IP, it uses different packet formats and terminology. See also *TCP/IP* and *Xerox Network Services (XNS).*

Internet Protocol (IP). (1) A protocol that routes data through a network or interconnected networks. IP acts as an interface between the higher logical layers and the physical network. However, this protocol does not provide error recovery, flow control, or guarantee the reliability of the physical network. IP is a connectionless protocol. (2) A protocol used to route data from its source to its destination in an Internet environment.

interrupt. (1) A suspension of a process, such as execution of a computer program caused by an external event, and performed in such a way that the process can be resumed. (A) (2) To stop a process in such a way that it can be resumed. (3) In data communication, to take an action at a receiving station that causes the sending station to end a transmission. (4) A means of passing processing control from one software or microcode module or routine to another, or of requesting a particular software, microcode, or hardware function.

IP. Internet Protocol.

IP address. A 32-bit address assigned to devices or hosts in an IP internet that maps to a physical address. The IP address is composed of a network and host portion.

IPX. Internet Packet Exchange.

ISO. International Organization for Standardization.

K

KB. (1) For processor storage and real and virtual memory, 1024 bytes. (2) For disk storage capacity and transmission rates, 1000 bytes.

Kb. Kilobit.

kilobit (Kb). 1000 binary digits.

L

LAN. Local area network.

LAN adapter. The circuit card within a communicating device (such as a personal computer) that, together with its associated software, enables the device to be attached to a LAN.

LAN segment. (1) Any portion of a LAN (for example, a single bus or ring) that can operate independently but is connected to other parts of the establishment network via bridges. (2) An entire ring or bus network without bridges. See *cable segment*, *ring segment*.

line data rate. The rate of data transmission over a telecommunications link.

local area network (LAN). (1) Physical network technology that transfers data at high speed over short distances. (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also *token ring* and *Ethernet.* (3) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) Contrast with *wide area network (WAN)* and *metropolitan area network (MAN)*.

logical link control (LLC). (1) The data link control (DLC) LAN sublayer that provides two types of (DLC) operation. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform

error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires the establishment of a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery. (2) A sublayer of the OSI link layer that defines formats and protocols for exchanging frames between LLC sublayers attached to a local area network. It has provisions that ensure that error-free, nonduplicated, properly ordered frames are delivered to the appropriate data-link user. See also *bridge* and *medium access control (MAC).*

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP) address, a source service access point (SSAP), a control field, and user data. See *logical link control (LLC)*.

logical link control (LLC) sublayer. One of two sublayers of the ISO Open Systems Interconnection data link layer (which corresponds to the SNA data link control layer), proposed for LANs by the IEEE Project 802 Committee on Local Area Networks and the European Computer Manufacturers Association (ECMA). It includes those functions unique to the particular link control procedures that are associated with the attached node and are independent of the medium; this allows different logical link protocols to coexist on the same network without interfering with each other. The LLC sublayer uses services provided by the medium access control (MAC) sublayer and provides services to the network layer.

M

MAC. Medium access control.

management information base (MIB). A collection of objects that can be accessed by means of a network management protocol.

MB. (1) For processor storage and real and virtual memory, 1,048,576 bytes. (2) For disk storage capacity and transmission rates, 1,000,000 bytes.

Mb. Megabit.

media access control (MAC). In FDDI, the portion of the data link layer responsible for scheduling and routing data transmissions on a shared medium local area network, for example, an FDDI ring.

medium access control (MAC). (1) The sublayer of the data link control layer that supports media-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. The MAC sublayer includes the medium-access port. See *logical link control (LLC).* (2) For local area networks, the method of determining which device has access to the transmission medium at any time.

medium access control (MAC) frame. (1) In the IBM Token-Ring Network: An address resolution request frame that has the unique part of a destination address and an “all rings” address. A sender issues this request to determine the ring where the destination station is located and whether the node is active. (2) Response from an active destination node to the requesting source node, providing the source node with the complete address and ring number of the destination node.

medium access control (MAC) procedure. In a local area network, the part of the protocol that governs access to the transmission medium independently of the physical characteristics of the medium, but takes into account the topological aspects of the network, in order to enable the exchange of data between data stations.

medium access control (MAC) protocol. (1) In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T) See also *logical link control protocol*. (2) The LAN protocol sublayer of data link control (DLC) protocol that includes functions for adapter address recognition, copying of message units from the physical network, and message unit format recognition, error detection, and routing within the processor.

medium access control (MAC) segment. An individual LAN communicating through the medium access control (MAC) layer within this network.

medium access control (MAC) service data unit (MSDU). In a medium access control (MAC) frame, the logical link control protocol data unit (LPDU) and the routing information field (if the destination station is located on a different ring).

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

medium access control (MAC) subvector. A group of related fields within a medium access control (MAC) major vector.

medium access control (MAC) vector. The medium access control (MAC) frame information field.

memory. All of the addressable storage space in a processing unit and other internal storages that is used to execute instructions. (T)

MIB. (1) Management information base. (2) MIB module.

N

NetBIOS. Network Basic Input/Output System. An operating system interface for application programs used on IBM personal computers that are attached to the IBM Token-Ring Network. See also *BIOS*.

network. (1) An arrangement of nodes and connecting branches. (T) (2) A configuration of data processing devices and software connected for information interchange. (3) A signal path connecting input/output devices to a system. A network can consist of multiple LAN segments connected together with bridging products. See ring (network). (4) The interconnection of two or more subnets. See also *Fiber Distributed Data Interface (FDDI) LAN*.

network address. See *Internet address.*

network administrator. A person who manages the use and maintenance of a network.

network architecture. The logical structure and operating principles of a computer network. (T) See also *systems network architecture (SNA)* and *Open Systems Interconnection (OSI) architecture*.

Note: The operating principles of a network include those of services, functions, and protocols.

network identifier (ID). A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

network management. The process of planning, organizing, and controlling a communications-oriented system.

network management station (NMS). The system responsible for managing a network or a portion of a network. The NMS talks to network management agents, that reside in the managed nodes, by means of a network management protocol. See also *agent.*

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network operator. (1) A person or program responsible for controlling the operation of all or part of a network. (2) In a multiple-domain network, a person or program responsible for controlling all domains.

O

operating system (OS). Software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible. (T)

Operating System/2® (OS/2). A set of programs that control the operation of high-speed large-memory IBM personal computers (such as the IBM Personal System/2 computer, Models 50 and above), providing multitasking and the ability to address up to 16 MB of memory. Contrast with *IBM Disk Operating System (DOS)*.

option. (1) A specification in a statement that can be used to influence the execution of the statement. (2) A hardware or software function that can be selected or enabled as part of a configuration process. (3) A piece of hardware (such as a network adapter) that can be installed in a device to modify or enhance device function.

OS. Operating system.

P

packet. (1) In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. (I) (2) Synonymous with *data frame*. Contrast with *frame*.

panel. A formatted display of information that appears on a display screen.

parameter. (1) A variable that is given a constant value for a specified application and that may denote the application. (I) (A) (2) An item in a menu or for which the user specifies a value or for which the system provides a value when the menu is interpreted. (3) Data passed between programs or procedures.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The route traversed by the information exchanged between two attaching devices in a network. (3) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units (NAUs). A path consists of a virtual route and its route extension, if any. See also *explicit route (ER)*, *route extension (REX)* and *virtual route (VR).*

personal computer (PC). (1) A microcomputer primarily intended for stand-alone use by an individual. (T) (2) A desk-top, floor-standing, or portable microcomputer that usually consists of a system unit, a display monitor, a keyboard, one or more diskette drives, internal fixed-disk storage, and an optional

printer. PCs are designed primarily to give independent computing power to a single user and are inexpensively priced for purchase by individuals or small businesses.

pointer. (1) An identifier that indicates the location of an item of data. (A) (2) A data element that indicates the location of another data element. (T) (3) A physical or symbolic identifier of a unique target.

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. Synonymous with *socket*. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter, however, there can be more than one port on an adapter. A single DLC process can control one or more ports. (4) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (5) In FDDI, a PHY entity and a PMD entity in a node, together creating a PHY/PMD pair, that can connect to the fiber media and provide one end of a physical connection with another node.

port number. The identification of an application entity to the transport service in IP.

POST. Power-on self-test.

power-on self-test (POST). A series of diagnostic tests that are run automatically by a device when the power is switched on.

problem determination. The process of determining the source of a problem; for example, a program component, a machine failure, telecommunication facilities, user or contractor-installed programs or equipment, an environment failure such as a power loss, or user error.

procedure. A set of instructions that gives a service representative a step-by-step procedure for tracing a symptom to the cause of failure.

protocol. (1) A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components.

R

read-only memory (ROM). (1) A storage device in which data, under normal conditions, can only be read. (T). (2) Memory in which stored data cannot be modified by the user except under special conditions.

remote. Pertaining to a system, program, or device that is accessed through a telecommunication line. Contrast with *local*. Synonym for *link-attached*.

remote program load. A function provided by adapter hardware components and software that enables one computer to load programs and operating systems into the memory of another computer, without requiring the use of a diskette or fixed disk at the receiving computer.

return code. (1) A value (usually hexadecimal) provided by an adapter or a program to indicate the result of an action, command, or operation. (2) A code used to influence the execution of succeeding instructions. (A)

ring attaching device. In a ring network, any device equipped with an adapter that is physically attached to the ring.

ring network. (1) A network configuration in which devices are connected by unidirectional transmission links to form a closed path. (2) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) See also *star/ring network, Token-Ring network.*

ring segment. A ring segment is any section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. A segment can consist of a single lobe, the cable between access units, or a combination of cables, lobes, and/or access units. See *cable segment*, *LAN segment*.

ring status. The condition of the ring.

ROM. Read-only memory. (A)

router. (1) A computer that determines that path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. Contrast with *bridge* and *gateway.* (3) In OSI terminology, a router is a network layer intermediate system.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing protocol. A technique for each router to find another router and to keep up to date about the best way to get to every network. Examples of routing protocols are: Routing Information Protocol (RIP), Hello, and Open Shortest Path First (OSPF).

S

segment. (1) In the IBM Token-Ring Network, a section of cable between components or devices. A segment can consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) The unit of transfer between TCP functions in different machines. Each segment contains control and data fields whereby the current byte stream position and actual data bytes are identified along with a checksum to validate received data. (3) In an OS/2 program, a variable-length area of contiguous storage addresses not exceeding 64 KB. See also *data segment*, *cable segment*, *LAN segment*, *ring segment*.

select. The process of choosing a single symbol or menu item by placing the cursor on it and clicking the mouse button. To select multiple symbols simultaneously, press and hold the Shift key down while clicking on the symbols you want to select.

server. (1) A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T) (2) In a network, a data station that provides facilities to other stations; for example, a file server, a print server, a mail server. (A) (3) A class of adapter in a network node that performs local processing and does not have any physical connections to other devices (as do port adapters and trunk adapters). (4) A device, program, or code module on a network dedicated to providing a specific service to a network.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session. (3) The period of time during which a user of a terminal can communicate with an interactive system, usually, elapsed time between logon and logoff.

Simple Network Management Protocol (SNMP). (1) An IP network management protocol that is used to monitor routers and attached networks. (2) A TCP/IP-based protocol for exchanging network management information and outlining the structure for communications among network devices. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

socket. (1) In the AIX operating system: (a) A unique host identifier created by the concatenation of a port identifier with a transmission control protocol/Internet protocol (TCP/IP) address. (b) A port identifier. (c) A 16-bit port number. (d) A port on a specific host; a communications end point that is accessible through a protocol family's addressing mechanism. A socket is identified by a socket address. See also *socket address*. (2) An IP address and port number pairing. (3) In TCP/IP, the Internet address of the host computer on which the application runs, and the port number it uses. A TCP/IP application is identified by its socket. (4) Synonym for *port (2)*.

switch. (1) On an adapter, a mechanism used to select a value to enable or disable a configurable option or feature. (2) In CallPath®, equipment that makes, breaks, or changes the connections between telephone lines to establish, terminate, or change a telephone call. Private branch exchange switches reside on a customer's premises, while central office switches reside within the telephone service provider's network.

switch feature. A service provided by the switch that can be invoked by a program or by manual phoneset activity. "Do not disturb" is an example of a switch feature.

system. In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions. (I) (A)

system configuration. A process that specifies the devices and programs that form a particular data processing system.

T

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

telecommunication-attached. Pertaining to the attachment of devices by teleprocessing lines to a host processor. Synonym for *remote*. Contrast with *channel-attached*.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) A sequence of bits passed from one device to another along the token ring. When the token has data appended to it, it becomes a frame.

token ring. (1) A network with a ring topology that passes tokens from one attaching device to another; for example, the IBM Token-Ring Network. See also *local area network (LAN)*. (2) A group of interconnected Token Rings.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations,

by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a sequence from node to node. A node that is ready to send can capture the token and insert data for transmission. (3) A group of interconnected token rings.

Transmission Control Protocol (TCP). (1) A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for inter-network protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol. (2) A transport protocol in the Internet suite of protocols that provides reliable, connection-oriented, full-duplex data stream service.

Transmission Control Protocol/Internet Protocol (TCP/IP). (1) A set of protocols that allow cooperating computers to share resources across a heterogeneous network. (2) A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission frame. (1) In data transmission, data transported from one node to another in a particular format that can be recognized by the receiving node. In addition to a data or information field, a frame has some kind of delimiter that marks its beginning and end and usually control fields, address information that identifies the source and destination, and one or more check bits that allow the receiver to detect any errors that occur after the sender has transmitted the frame. (2) In synchronous data link control (SDLC), the vehicle for every command, every response, and all information that is transmitted using SDLC procedures. Each frame begins and ends with a flag. (3) In high level data link control (HDLC), the sequence of contiguous bits bracketed by and including opening and closing flag (01111110) sequences. (4) In a Token-Ring network, a bit pattern containing data that a station has inserted for transmission after capturing a token.

transmit. To send information from one place for reception elsewhere. (A)

U

UDP. User Datagram Protocol.

UNIX operating system. An operating system developed by Bell Laboratories that features multiprogramming in a multiuser environment. The UNIX operating system was originally developed for use on minicomputers, but has been adapted for mainframes and microcomputers.

Note: The AIX operating system is IBM's implementation of the UNIX operating system.

User Datagram Protocol (UDP). (1) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. UDP is used for application-to-application programs between TCP/IP host systems. (2) A transport protocol in the Internet suite of protocols that provides unreliable, connectionless datagram service. (3) The Internet Protocol that enables an application programmer on one machine or process to send a datagram to an application program on another machine or process. UDP uses the internet protocol (IP) to deliver datagrams.

V

version. A separately licensed program, based on an existing licensed program, that usually has significant new code or new function.

W

WAN. Wide area network.

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks and national telephone networks. Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

window. (1) In computer graphics, a predetermined part of a virtual space. (2) A division of a screen in which one of several programs being executed concurrently can display information. (3) One or more parts of a display screen with visible boundaries in which information is displayed. (4) See also *help window*.

wrap test. A test that checks attachment or control unit circuitry without checking the mechanism itself by returning the output of the mechanism as input; for example, when unrecoverable communication adapter or machine errors occur, a wrap test can transmit a specific character pattern to or through the modem in a loop and then compare the character pattern received with the pattern transmitted. See also *optical wrap*.

Index

C

client setup, RPL/PXE 4
CONFIG.SYS for RPL 10

D

DOS 31
  LAN Services 31
  memory usage reduction 33

E

enabling RPL/PXE 4

I

IBM LAN Client 31
  installation 31
  restrictions 32

L

LAN adapter management agent 35
LAN Client installation 33

M

messages
  PXE 17
  RPL 15, 27

N

Novell NetWare Server 10
  RPL, setting up 10

O

OS/2 LAN server
  support for RPL 9

Q

Quick Failover
  description 56
  supported environments 55

R

Redundant NIC
  benefits 56
  description 55
  installation 57
  supported environments 55
related publications vii
Remote Program Load (RPL)
  client setup 4
  description 3
  messages 15, 27
  overview 3
  setting up for OS/2 LAN server 9
  troubleshooting 19, 28
Route Switching, configuring 39
RPL/PXE, enabling 4

T

troubleshooting RPL problems 28

W

Windows NT 4.0 Server 12
  RPL, setting up 12