Transcend™ LinkBuilder® FDDI SmartAgent™ Software User's Guide

A member of the LinkBuilder FDDI family

For 3Com User Group Information
1-800-NET-3Com
or your local 3Com office

Manual Part No. 09-0537-000
Published April 1994. Printed in the U.S.A.

3Com Corporation
5400 Bayfront Plaza
Santa Clara
California, USA
95052-8145

3Com Corporation reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this guide without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this manual at any time.

If you are a government agency, then this software and documentation is provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software Clause at 48 C.F.R. 52.227-7013. 3Com Corporation, 5400 Bayfront Plaza, Santa Clara, California 95052-8145.

For civilian agencies:
Restricted Rights Legend: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software – Restricted Rights clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com's standard commercial agreement for the Software. Unpublished rights reserved under the copyright laws of the United States.

Manual written by John Jeter. Edited by Nancy Kurahashi. Technical illustrations by Tim Buckreus. Production by Becky Whitmer.

LIMITED WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	One year
Network adapters	Lifetime
Ethernet stackable hubs and Unmanaged Ethernet fixed port repeaters (One year if not registered)	Lifetime*
*Power supply and fans in these stackable hubs and unmanaged repeaters	One year
Other hardware products	One year
Spare parts and spares kits	90 days

If a product does not operate as warranted during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com pursuant to any warranty.

SOFTWARE: 3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the magnetic media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation hereunder shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt by 3Com.

WARRANTIES EXCLUSIVE: IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES

OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) SHALL 3COM BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

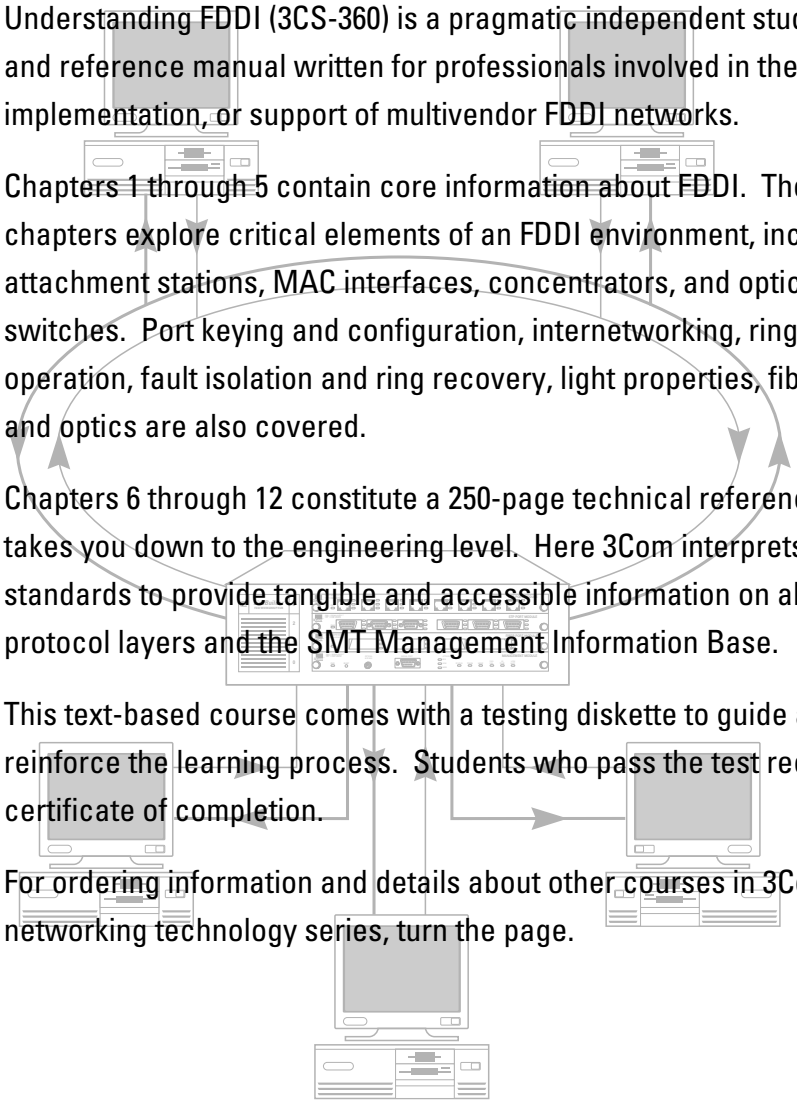
Some states do not allow the exclusion of implied warranties or the limitation of incidental or consequential damages for consumer products, so the above limitations and exclusions may not apply to you. This warranty gives you specific legal rights which may vary from state to state.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

Contents

Figure

3Com's FDDI Training and Reference Manual



Understanding FDDI (3CS-360) is a pragmatic independent study course and reference manual written for professionals involved in the design, implementation, or support of multivendor FDDI networks.

Chapters 1 through 5 contain core information about FDDI. These chapters explore critical elements of an FDDI environment, including attachment stations, MAC interfaces, concentrators, and optical bypass switches. Port keying and configuration, internetworking, ring startup, operation, fault isolation and ring recovery, light properties, fiber media, and optics are also covered.

Chapters 6 through 12 constitute a 250-page technical reference that takes you down to the engineering level. Here 3Com interprets the FDDI standards to provide tangible and accessible information on all four FDDI protocol layers and the SMT Management Information Base.

This text-based course comes with a testing diskette to guide and reinforce the learning process. Students who pass the test receive a certificate of completion.

For ordering information and details about other courses in 3Com's data networking technology series, turn the page.

Additional 3Com Data Networking Courses

3Com's practical self-paced training on the networking industry's prevailing standards and architectures provides a cost-effective way for professionals to keep pace with the complex planning and support demands of a multivendor data network. Each course contains supplementary technical materials organized for easy future reference.

These courses come in text format, with an interactive testing diskette to guide and reinforce the learning process. Students who pass the final test receive a certificate of completion.

Introduction to Bridging and Routing (3CS-011)

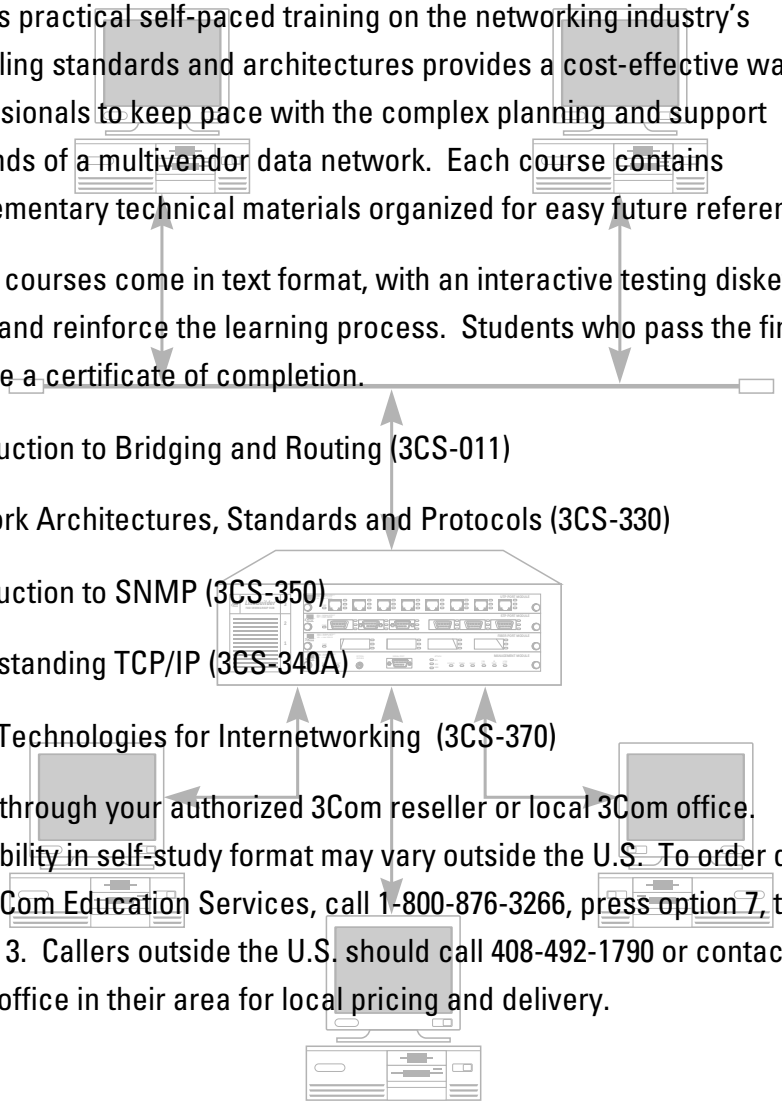
Network Architectures, Standards and Protocols (3CS-330)

Introduction to SNMP (3CS-350)

Understanding TCP/IP (3CS-340A)

WAN Technologies for Internetworking (3CS-370)

Order through your authorized 3Com reseller or local 3Com office. Availability in self-study format may vary outside the U.S. To order directly from 3Com Education Services, call 1-800-876-3266, press option 7, then option 3. Callers outside the U.S. should call 408-492-1790 or contact the 3Com office in their area for local pricing and delivery.



Chapter 1
Overview of Hub Management

Introduction to Hub Management

The 3Com® LinkBuilder® FDDI Workgroup Hub supports Simple Network Management Protocol (SNMP) manageability through standard and 3Com proprietary Management Information Bases (MIBs). (Throughout this guide, the LinkBuilder FDDI Workgroup Hub will be referred to as "the hub.") The hub functions in conjunction with an SNMP management station to support SNMP management services. This includes providing a proxy agent to translate SNMP requests for Station Management (SMT) 7.3 stations on the ring.

NOTE: *The LinkBuilder FDDI Workgroup Hub implements the FDDI standard SMT 7.3.*

The Transcend™ LinkBuilder FDDI SmartAgent™ software running on the hub is a member of 3Com's Transcend SmartAgent family. SmartAgent network management software supports network management and communications protocols, including SNMP and SMT.

With an SNMP network management application running on a management station, you will be able to:

- Monitor the performance of manageable devices
- Read performance statistics from managed devices
- Configure managed devices
- Detect and correct problems on the network
- Maintain an inventory of network devices
- Graphically illustrate the topology of the network

Check the application guide to determine the specific capabilities of your management application.

By using the console attached to the hub or by using the Telnet protocol to access the hub, you can invoke a small set of hub-specific SNMP commands to do the following:

- Specify device access using the community string relationship
- Specify the trap receiver's IP address, community relationship, and trap period
- Set the system's contact, name, and location

These functions are described in Chapter 3, "Using Hub-Specific SNMP Commands."

SNMP MIB Files

The hub supports two subsets of the standard MIB, as agreed upon by the Internet Engineering Task Force (IETF): SNMP MIB II and FDDI MIB. It also supports a 3Com proprietary MIB defining the hub's trap- and product-specific MIBs.

The base SNMP MIB II specifications are defined in *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II Request for Comments (RFC) 1213, March 1991*. The FDDI MIB specifications are defined in *FDDI Management Information Base Request for Comments (RFC) 1512, September 1993*.

The proprietary MIB specifications are defined in *3Com LinkBuilder FDDI Workgroup Hub's Trap- and Product-Specific MIB Revision, November 5, 1993.* For a list and definitions of the LinkBuilder FDDI Workgroup Hub MIB, refer to Appendix A in this manual.

MIB II specifications are also published in the 3Com self-study course *Introduction to SNMP (3CS-350)*. This course explores the architecture and governing principles of the SNMP protocol, as well as the differentiation between the SMI, the MIB, and ASN.1, and their implementation in vendors' SNMP network management products.

SNMP Management

SNMP supports management functions by enabling communication between a network management station and network elements, such as the devices on the ring that are attached to the hub. The management station runs the network management protocol and management applications that monitor and control the network elements. The hub supports the agents that perform network management functions as requested by the network management station.

The SmartAgent software running on the hub provides a proxy agent for SNMP requests for SMT 7.3 stations on the ring. The proxy agent acts on behalf of devices that have not implemented SNMP but have implemented SMT 7.3. This proxy function running on the hub translates SNMP packets into SMT packets and vice versa.

To establish a proxy relationship with an SMT device, you include its MAC (Media Access Control) address with the hub's community string when accessing the device from the management station. The community string is followed by an @ sign and the ASCII-coded MAC address (in noncanonical order) of the proxied device. For example, type:

```
private@026601352203
```

where "private" is the hub's community string and "026601352203" is the SMT device's MAC address.

For additional information, refer to the documentation supporting the management software running on your management station.

Establishing the Management Environment

The SmartAgent management software is supplied on a diskette labeled *Transcend LinkBuilder FDDI SmartAgent*, version 1.1. You must copy the software to a Trivial File Transfer Protocol (TFTP) server, which may or may not also function as the management station on which the SNMP management application is running.

The network management applications listed below represent a sample of those that support network management:

- ISOVIEW® Network Manager (3Com)
- SunNet Manager™ (Sun® Microsystems, Inc.)
- NetView®/6000 (IBM®)
- Open View® (Hewlett-Packard®)
- NMS™ (NetWare® Management System, Novell®, Inc.)

The management station must be accessible to the hub across the network. Figure 1-1 shows an example of a network setup that facilitates network management.

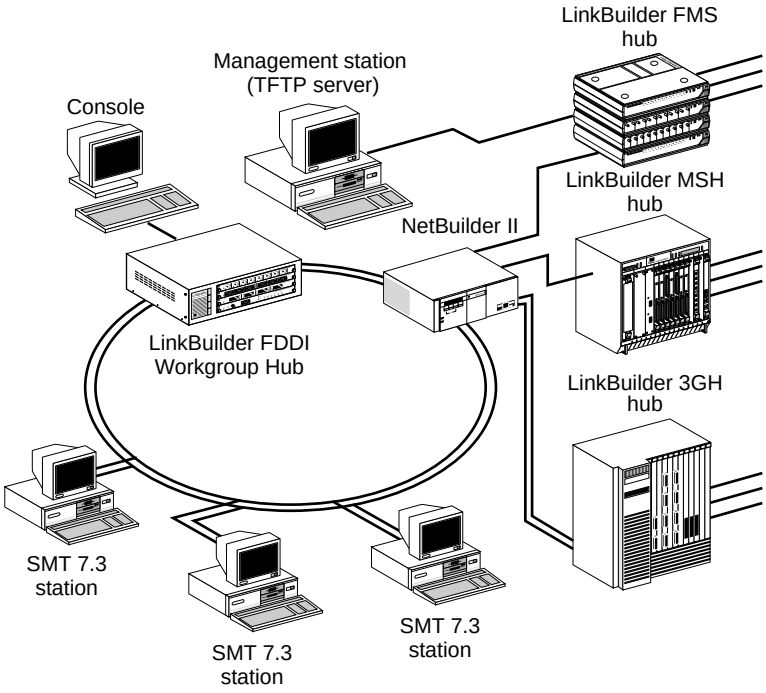


Figure 1-1. LinkBuilder FDDI Workgroup Hub Management Environment

Follow the major steps below to install the LinkBuilder FDDI Workgroup Hub management software.

1. Copy the management software image to a TFTP server.
2. Ping the server from the hub to verify connectivity (optional).
3. Set the boot method and download the image to the hub.
4. Compile the MIBs on the management station.

Detailed information on these steps is provided in Chapter 2. Once you have performed each of these procedures, you can set the hub's community string, designate devices as trap receivers, and enter system device information, as described in Chapter 3.

Chapter 2
Installing Hub Management Software

This chapter describes how to:

- Copy the management software image to the TFTP server. The TFTP server may also function as the management station.
- Ping the TFTP server.
- Download the management image into the hub's flash EPROM.
- Compile the MIBs on the management station.

Selecting a Management Station

Many platforms can function as a network management station. Select a platform that is capable of providing enough memory to support the user-selected management software and to store and compile the SNMP MIBs.

The selected platform may also function as the TFTP server.

Copying the Image to the TFTP Server

To copy the hub SmartAgent software image from the *Transcend LinkBuilder FDDI SmartAgent* diskette, version 1.1, into the TFTP server, follow these steps:

1. **On the TFTP server, create a directory to hold the software image. For example, type:**

   ```
   mkdir lbfddi.hub
   ```

2. **Insert the *Transcend LinkBuilder FDDI SmartAgent* diskette into the diskette drive on the TFTP server.**

3. **Copy the diskette's contents to the newly created directory. For example, type:**

   ```
   copy A:\*.* C:\lbfddi.hub
   ```

   The copied files contain the MIBs that you need to compile and the flash image for the hub.

Pinging the TFTP Server

To verify the connection between the hub and the TFTP server, and to prepare for downloading the image to the hub, ping the TFTP server.

At the console attached to the hub, enter the *ping* command, followed by the IP address of the TFTP server in the format *XXX.XXX.XXX.XXX*. For example, at the prompt, type:

```
ping 123.44.55.66
```

where *123.44.55.66* is the IP address. (If you do not know the server's IP address, ask your system administrator.)

If the server is operational, this answer will be displayed:

```
123.44.55.66 is alive
```

You can now set up the download parameters and begin to download the image to the hub.

Downloading the Image to the Hub

To download the image from the server to the hub, you must enter certain variables individually. This process is described below.

NOTE: *You cannot download the flash image over the serial link via a modem.*

To download an image from the TFTP server, follow these steps:

1. **At the console connected to the hub, set the boot method for the software to be downloaded. Type:**

   ```
   set boot method [Enter]
   ```

   This selection prompt appears:

   ```
   Select one of the following:
     1. LOCAL
     2. TFTP
   Boot Method?
   ```

2. **Select the TFTP option. Type:**

   ```
   2 [Enter]
   ```

   This display appears, confirming your selection and showing that you also need to enter the TFTP server's IP address and the image filename.

   ```
   Boot parameters
     Method   :TFTP
     Server   :
     Filename :
   ```

3. **Set the TFTP server's IP address. Type:**

   ```
   set boot server [Enter]
   ```

   This prompt appears:

   ```
   Enter server IP address in dot notation?
   ```

4. **Enter the server's IP address. For example, type:**

   ```
   123.44.55.66 [Enter]
   ```

   This confirmation appears:

   ```
   Boot parameters
     Method      : TFTP
     Server      : 123.44.55.66
     Filename    :
   ```

5. **Set the image filename to be used. Type:**

   ```
   set boot filename [Enter]
   ```

   The filename prompt appears:

   ```
   Enter filename?
   ```

6. **Type the name of the image file after the question mark. Type:**

   ```
   3C779_11.img [Enter]
   ```

NOTE: *The name of the image file that you enter here (*3C779_11.img *in this example) must be the same filename used for the file that you copied to the management station.*

   This display appears, showing your entries:

```
Boot parameters
  Method     : TFTP
  Server     : 123.44.55.66
  Filename   : 3C779_11.img
```

7. **Reset the hub.**

   Press the hub's RESET button or type the *reset* command from the console.

   You are asked to confirm the *reset* command, which activates the download sequence. If you confirm the *reset* command by typing "y", this message appears:

   ```
   Done.
   ```

   A series of messages then appears, followed by this line:

   ```
   TFTP download requested.
   ```

   Additional messages appear, followed by a line of dots indicating that the download is in progress.

   When the download is complete, this message appears:

   ```
   TFTP download completed successfully.
   ```

The new image is now downloaded and stored in the hub's flash EPROM. If no errors are encountered, the hub is reset and the new image is executed.

If a problem with the download is encountered, an error message will appear. Refer to Appendix C for a list of error messages and their explanations.

You can now specify the hub's community strings, designate devices to be trap receivers, and enter system device information, as detailed in Chapter 3.

Solving Downloading Problems

Two possible downloading problems with recommended solutions are discussed in this section.

Simultaneous Downloads

When running multiple downloads, you should not run downloads simultaneously. If you attempt to do so, the disruptive nature of downloading will break the ring and could isolate stations on the ring from the boot (TFTP) server. This may cause a download to fail.

To avoid this problem, run downloads one at a time.

Network Connections

A download may fail if the image coming from the TFTP server must pass through a bridge to which the hub is directly connected. When you invoke the *reset* command to start the download, the disruptive nature of downloading causes the bridge to wait 30 seconds before processing the download request. By that time, the hub has finished its retry and can no longer find the TFTP server. This problem does not occur if you use a router instead of a bridge for this particular connection.

To avoid this problem when using a bridge, set up your network in one of these ways:

- Connect an FDDILink adapter (in a PC) to the other bridge port.
- Connect one or more active devices to the ring.

This work-around permits the bridge to continue forwarding packets without closing down for the download.

Compiling the MIBs

After downloading the image to the hub, you can compile the hub's trap- and product-specific MIB. For information and instructions on compiling the MIBs, refer to the documentation provided by the specific management software application that you are running on the management station.

Chapter 3
Using Hub-Specific SNMP Commands

This chapter describes how to use the hub-specific SNMP commands to support management functions on the hub. Refer to Appendix B for a complete listing and usage syntax of the SNMP commands. These commands are invoked from the console attached to the hub or over the network via Telnet.

Community Strings

After you have downloaded the SmartAgent image to the hub, its community string displays its default value—"public"—with the corresponding access capability being "RO" (read-only). This setting allows other devices that have the same community string to communicate with the hub. Devices with a community string of "public" can only read messages transmitted to and from the hub. You can set up to eight community strings on the hub. You can designate either "RO" (read-only) or "RW" (read-write) access capabilities for each community string.

To display, add, or change community string values, follow these steps:

1. **Enter an *snmp show community* command. Type:**

```
snmp sh comm
```

This display appears:

```
    Community  Capability
1.  public     RO
 .
 .
 .
 .
 .
8.
```

2. Enter an *snmp add community* command. For example, type:

```
snmp add comm supervisor RW
```

where “supervisor” is the name of the community string being added and “RW” indicates read-write access capability.

3. To confirm the add, enter an *snmp show community* command. Type:

```
snmp sh comm
```

This display appears:

```
    Community   Capability
1.  public      RO
2.  supervisor  RW
 .
 .
 .
 .
8.
```

4. To change the access capability of the added string, first delete the community string and then add the community string with the new access capability.

a. Enter the *snmp delete* command. Type:

```
snmp del comm supervisor
```

This deletes both the community string and the access level.

b. Enter the *snmp add* command. Type:

```
snmp add comm supervisor RO
```

5. **To confirm the change, type:**

```
snmp sh comm
```

This display appears:

```
    Community  Capability
1.  public     RO
2.  supervisor RO
 .
 .
 .
 .
8.
```

If you want to delete all current community strings, type the *snmp clear* command. For example:

```
snmp cl comm
```

This deletes all entries in the community string table, including the community strings and the access capability fields.

Trap Receivers

You can specify which network devices will receive trap reports and the frequency of traps sent for persistent trap conditions. For example, to specify a device with an IP address of 123.44.55.66 and a community string of "public" for the trap receivers table, enter the *snmp add* command. Type:

```
snmp add trap 123.44.55.66 public
```

If you want the same device to receive the notifications of persistent trap conditions every 60 seconds, first delete the trap receiver and its community string. Type:

```
snmp del trap 123.44.55.66 public
```

Then enter the *snmp add* command, followed by the IP address, the community string, and the trap period. Type:

```
snmp add trap 123.44.55.66 public 60
```

NOTE: *If you specify a time period for trap notification, it must be at least 30 seconds or more.*

To delete this trap receiver from the trap receivers table, enter the *snmp delete* command. Type:

```
snmp del trap 123.44.55.66
```

To display all entries in the trap receivers table, enter the *snmp show* command. Type:

```
snmp sh trap
```

To delete all entries in the trap receivers table, enter the *snmp clear* command. Type:

```
snmp cl trap
```

System Information

The SNMP system commands allow you to specify a system contact (a person to contact if system problems occur), a system name (a unique designation for the system), and a system location (the location of the device on the system). Once this information has been specified, you can display it.

Specify system information from the console attached to the hub, as illustrated below:

- **To specify the system contact, enter the *snmp set syscontact* command. Type:**

  ```
  snmp set syscon
  ```

  You will be prompted for the contact string:

  ```
  Enter the system contact:
  ```

  You can type up to 255 characters for the contact string.

- **To specify the system name, enter the *snmp set sysname* command. Type:**

  ```
  snmp set sysnam
  ```

  You will be prompted for the name string:

  ```
  Enter the system name:
  ```

  You can type up to 255 characters for the name string.

- **To specify the system location, enter the *snmp set syslocation* command. Type:**

  ```
  snmp set sysloc
  ```

  You will be prompted for the location string:

  ```
  Enter the system location:
  ```

  You can type up to 255 characters for the location string.

To verify the system information that you have entered, invoke the *snmp show* commands, as shown below:

`snmp sh syscon`	Displays the system contact string
`snmp sh sysnam`	Displays the system name string
`snmp sh sysloc`	Displays the system location string
`snmp sh sysall`	Displays the system contact, name, and location strings

Appendix A
LinkBuilder FDDI Workgroup Hub MIB Descriptions

This appendix defines the LinkBuilder FDDI Workgroup Hub MIBs. The object identifiers for the MIBs can be found in the LBFDDI.MIB file in the *Transcend LinkBuilder FDDI SmartAgent* diskette. These MIBs support two types of traps and one trap-related type of MIB for the hub, as listed below:

- Generic traps
- Enterprise-specific traps
- Workgroup-specific MIBs

Generic Traps

coldStart	The sending hub is reinitializing itself.
authenticationFailure	The sending hub is the addressee of a protocol message that is not properly authenticated.

Enterprise-Specific Traps

a3comLowBattery	The sending hub's battery is low.
a3comHighTemp	The sending hub's temperature is high.
a3comFanFailed	The sending hub's fan failed.
a3comBadTelnetPasswd	Someone tried the Telnet login to the sending hub three consecutive times and failed.
a3comBadConsolePasswd	Someone tried the console login to the sending hub three consecutive times and failed.

LinkBuilder FDDI Workgroup Hub-Specific MIBs

hubLowBattery	Shows the current status of the hub's battery. If the variable changed from false to true, the enterprise-specific trap *a3comLowBattery* will be sent to the configured SNMP management stations.
hubHighTemp	Shows the current temperature status of the hub. If the variable changed from false to true, the enterprise-specific trap *a3comHighTemp* will be sent to the configured SNMP management stations.
hubFanFailed	Shows the current fan fail status of the hub. If the variable changed from false to true, the enterprise-specific trap *a3comFanFailed* will be sent to the configured SNMP management stations.
hubLowBatteryCount	Shows the number of times the *hubLowBattery* variable has changed from false to true.
hubHighTempCount	Shows the number of times the *hubHighTemp* variable has changed from false to true. This variable is also saved in nonvolatile RAM.
hubFanFailedCount	Shows the number of times the *hubFanFailedCount* variable has changed from false to true.
hubBadTelnetPasswdCount	This variable is incremented by 1 after three consecutive Telnet login attempts fail. This variable is also saved in nonvolatile RAM.
hubBadConsolePasswdCount	This variable is incremented by 1 after three consecutive console login attempts fail. This variable is also saved in nonvolatile RAM.

Appendix B
LinkBuilder FDDI Workgroup Hub Commands

Commands

The commands supported by the hub management console command mode and the primitive console command mode enable you to set and display the basic parameters needed to configure, operate, and manage the hub.

Basic LinkBuilder FDDI Workgroup Hub Commands

To display the basic list of commands, type:

`help` or `?`

The command definitions appear, as shown below:

```
help | ?      ->  Display this message.
set           ->  Set, use set help for more information.
show          ->  Show, use show help for more information.
clear         ->  Clear, use clear help for more information.
connect       ->  Connect station to ring.
disconnect    ->  Disconnect station from ring.
ping          ->  Send echo packets to a host, use ping help for usage.
arp           ->  Configure arp table, use arp help for usage.
route         ->  Add/Delete/Dump IP routes, use route help for usage.
logout        ->  Logout console or telnet connection.
reset         ->  Reset the hub.
snmp          ->  SNMP commands, use snmp help for more information.
!!            ->  Repeat last command.
```

Hub-Specific SNMP Commands

To display the hub-specific SNMP commands, type:

```
snmp
```

The hub-specific SNMP command definitions appear, as shown below:

```
snmp add          -> Add an SNMP community or trap receiver.
snmp clear        -> Clear all SNMP communities or trap receivers.
snmp del          -> Delete an SNMP community or trap receiver.
snmp help | ?     -> Display this message.
snmp set          -> Set SNMP parameters.
snmp show         -> Show SNMP parameters.
```

Hub-specific SNMP command usage is illustrated below:

```
snmp add
Usage:      snmp add community COMMUNITY [RO|RW]
            snmp add traprcvr IP_ADDRESS [COMMUNITY] [PERIOD]

snmp clear
Usage:      snmp clear communities
            snmp clear traprcvrs
snmp del
Usage:      snmp delete community COMMUNITY
            snmp delete traprcvr IP_ADDRESS

snmp set
Usage:      snmp set syscontact
            snmp set sysname
            snmp set syslocation

snmp show
Usage:      snmp show communities
            snmp show traprcvrs
            snmp show syscontact
            snmp show sysname
            snmp show syslocation
            snmp show sysall
```

Addition to the LinkBuilder FDDI Workgroup Hub Commands

The command set detailed in the *LinkBuilder FDDI Workgroup Hub User Guide* has been augmented by one new command.

The *repeat* command, invoked by two exclamation points (!!), repeats the last command you entered and can save keystrokes. For example, immediately after specifying the SNMP system contact, you may want to specify the SNMP system name. If you enter the *snmp set syscontact* command by typing:

```
snmp set syscon
```

you can redisplay the command by typing:

```
!! <Return>
```

The command appears again:

```
snmp set syscon
```

Now you can backspace to remove “con” and type “nam,” with this result:

```
snmp set sysnam
```

This saves input time and may help to reduce input errors.

Hub-Specific SNMP Command Descriptions

The hub-specific SNMP command descriptions fall into three categories: community, trap receiver, and system.

Command abbreviations are allowed. These are indicated by the underlined letters.

Community String Commands

snmp add community

Syntax
snmp add community *community* [RO|RW]

Description
The *snmp add community* command adds the specified string (*community*) to the communities table with access set to RO (read-only) or RW (read-write). If you do not specify an access argument, it defaults to RO.

You can specify up to eight communities for the hub, but duplicate communities are not allowed. Community strings are limited to 16 characters.

snmp delete community

Syntax
snmp del community *community*

Description
The *snmp del community* command deletes the specified string (*community*) from the communities table.

snmp show communities

Syntax
snmp show communities

Description
The *snmp show communities* command displays the communities table.

snmp clear communities

Syntax
snmp clear communities

Description
The *snmp clear communities* command deletes all entries in the communities table.

Trap Receiver Commands

snmp add traprcvr

Syntax
snmp add traprcvr *ipaddress*
snmp add traprcvr *ipaddress* [community]
snmp add traprcvr *ipaddress* [community][period]

Description
The *snmp add traprcvr* command specifies the IP address of the network device that will receive trap reports. You must enter an IP address; optionally, you may specify a community string and trap period.

The community defaults to “public” if not specified.

The trap period (in seconds) controls the frequency of traps sent for persistent trap conditions. The trap period defaults to zero (0) if not specified, which indicates that a single trap is to be sent each time the trap condition occurs, regardless of its persistence.

If the setting is other than zero, a trap will be sent at the interval specified by “period” as long as the trap condition persists. If specified, the trap period must be 30 seconds or more. If you specify a trap period of less than 30 seconds, an error message will be displayed. You cannot specify a trap period without specifying a community string.

You can specify up to eight trap receivers, but duplicate trap receivers are not allowed.

snmp delete traprcvr

Syntax
snmp del traprcvr *ipaddress*

Description
The *snmp del traprcvr* command deletes the specified trap receiver from the trap receivers table.

snmp show traprcvr

Syntax
snmp show traprcvr

Description
The *snmp show traprcvr* command displays the contents of the trap receivers table.

snmp clear traprcvr

Syntax
snmp clear traprcvr

Description
The *snmp clear traprcvr* command deletes all entries in the trap receivers table.

System Commands

snmp set syscontact

Syntax
snmp set syscontact

Description
The *snmp set syscontact* command allows you to set the system contact string (MIB object: *sysContact*). When you invoke the command, you are prompted for the system contact. The system contact string is limited to 255 characters.

snmp set sysname

Syntax
snmp set sysname

Description
The *snmp set sysname* command allows you to set the system name string (MIB object: *sysName*). When you invoke the command, you are prompted for the system name. The system name string is limited to 255 characters.

snmp set syslocation

Syntax
snmp set syslocation

Description
The *snmp set syslocation* command allows you to set the system location string (MIB object: *sysLocation*). When you invoke the command, you are prompted for the system location. The system location string is limited to 255 characters.

snmp show syscontact

Syntax
snmp show syscontact

Description
The *snmp show syscontact* command displays the system contact string.

snmp show sysname

Syntax
snmp show sysname

Description
The *snmp show sysname* command displays the system name string.

snmp show syslocation

Syntax
snmp show syslocation

Description
The *snmp show syslocation* command displays the system location string.

snmp show sysall

Syntax
snmp show sysall

Description
The *snmp show sysall* command displays the system name, contact, and location strings.

Appendix C
Error Messages

This appendix lists the error messages that may be displayed on the terminal console attached to the hub. These messages are in addition to the system messages listed in Appendix A of the *LinkBuilder FDDI Workgroup Hub User Guide*. The messages are listed alphabetically. Each message includes a brief explanation and suggested action.

Community already exists

Meaning: You attempted to assign a community string with a duplicate name.

Action: Reenter the community string with a unique name.

Community strings are limited to 16 characters

Meaning: You entered a community string longer than 16 characters.

Action: Reenter the community string with no more than 16 characters.

Error: Invalid IP address

Meaning: You entered an IP address that was invalid.

Action: Reenter a valid IP address.

No free entries left in table

Meaning: You attempted to specify more than eight trap receivers or community strings. No more than eight trap receivers or community strings can be specified in the trap table or community table, respectively.

Action: Use the *snmp del traprcvr* command to delete unneeded trap receivers or the *snmp del community* command to delete unneeded community strings.

No match found in table

Meaning: You entered an incorrect community string or trap receiver IP address when attempting to delete a community string or trap receiver IP address.

Action: Use the *snmp show communities* command or the *snmp show traprcvr* command to verify the community string or trap receiver IP address that you are trying to delete.

Trap period must be expressed as a number

Meaning: You attempted to designate a trap period with a nonnumeric character.

Action: Reenter the trap period with a numeric character.

Trap period must be 30 seconds or greater

Meaning: You entered a trap period of less than 30 seconds.

Action: Reenter a trap period of at least 30 seconds.

Trap receiver already exists

Meaning: You attempted to designate as a trap receiver a device that has already been specified.

Action: Reenter an IP address for a device that has not been previously specified as a trap receiver.

Appendix D
Technical Support

This appendix explains how to obtain worldwide support for 3Com adapters and software.

On-line Product Support

3Com offers worldwide product support 24 hours a day, seven days a week, through automated on-line systems.

3Com Bulletin Board Service

3Com's menu-driven bulletin board service contains the most current product information in downloadable files. This service provides:

- Bug reports
- Technical tips
- Product information
- Diagnostic programs
- Software drivers, patches, and fixes

These files are easy to access through a modem connection set at 8 data bits, no parity, 1 stop bit. Call the telephone number nearest you:

Australia	(61) (2) 955 2073 – up to 2400 baud
France	(33) (1) 69 86 69 54 – up to 9600 baud
Germany	(49) 89 62732-188/189 – up to 9600 baud
Hong Kong	(852) 537 5601 – up to 9600 baud
Italy	(39) (2) 27 30 06 80 – up to 9600 baud
Japan	(81) (3) 3243 9245 – up to 14400 baud
Singapore	(65) 543 5693 – up to 9600 baud
Taiwan	(886) (2) 5776160 – up to 14400 baud
U.K.	(44) (44) 2 278278 – up to 14400 baud
U.S.	(1) (408) 980-8204 – up to 14400 baud

For information on international access numbers added since this manual was published, contact your local 3Com office. Refer to the list of international sales offices later in this appendix.

3ComFacts℠ Automated Fax Service

3Com's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, seven days a week. Within this service you may choose to access CardFacts℠ for adapter information or NetFacts℠ for network system product information.

- **CardFacts** provides adapter installation diagrams, configuration drawings, troubleshooting instructions, and technical articles. Document 9999 provides you with an index of adapter documents.

- **NetFacts** provides data sheets and technical articles on 3Com's hub, bridge, router, terminal server, and software products. Document 8888 provides you with an index of system product documents.

Call 3ComFacts using your touch-tone telephone. International calling numbers are:

Hong Kong	(852) 537 5610
U.K.	(44) (44) 227 8279
U.S.	(1) (408) 727 7021

Local access to 3Com's fax system is available within the following countries using the numbers listed below:

Australia	1 800 123853
Denmark	800 17319
Finland	98 001 4444
France	05 90 81 58
Germany	0130 81 80 63
Italy	1678 99085
Netherlands	06 0228049
Norway	05 01 1062
Sweden	020 792954
U.K.	0800 626403

Ask3Com℠ On-line Service

Ask3Com is an on-line service, located on CompuServe℠. This service is accessible worldwide. Ask3Com contains extensive technical and marketing information on all 3Com products. To use Ask3Com, you must first obtain a CompuServe account. To open an account, contact your local CompuServe office.

To use Ask3Com, log into CompuServe, type:

```
GO THREECOM
```

and press [Enter] to see the Ask3Com main menu.

3Com Documentation on CD-ROM

An extensive library of 3Com product documentation is available in CD-ROM format through Support on Site™ for Networks subscription service. This multivendor CD-ROM service, offered by Computer Library™, a division of Ziff Communications Company, contains technical information and documentation from major data networking hardware and software manufacturers. Stand-alone and concurrent user network subscriptions are available. To order, call Computer Library at (800) 827-7889, extension 515. Outside the U.S. call (212) 503-4400 or use fax number (212) 503-4487.

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

U.S. and Canada

Call the following number to locate your local 3Com sales office:

U.S. (1) (800) NET-3Com

The 3Com sales office will refer you to the nearest 3Com authorized service partner.

Outside the U.S. and Canada

To locate a 3Com authorized service partner near you, contact your local 3Com sales office.

Australia	(61) 2 959 3020
Belgium/Netherlands	(31) 3402 55033
Brazil	55 11 530 2318
France	(33) 1 698 66800
Germany	(49) 89 627320
Hong Kong	(852) 868 9111
Italy	(39) 22 7302041
Japan	(81) 3 3243-9234
Mexico	525 531 0591
Middle East	971 4 317173
Nordic	(46) 8 703 4870
Singapore	(65) 538 9368
Taiwan	(886) 2 577 4352
U.K.	(44) 628 890 670

When you contact a 3Com authorized service partner for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Detail on recent configuration changes, if applicable

3Com's service partner will determine what action needs to be taken to resolve the problem. 3Com service partners can verify hardware failures and advise you when it is more cost-effective to replace, rather than repair, a product.

Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization number (RMA). A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

When you call for an RMA number, be prepared to provide the product name, serial number, and diagnostic error messages. Payment, shipping instructions, and turnaround time will be confirmed when the RMA number is assigned.

To obtain an RMA number, call or fax:

Europe	*Phone*	(44) (44) 2 278000
	Fax	(44) (44) 2 236824
U.S.	*Phone*	(800) 876-3266, press option 2
	Fax	(408) 764-7290
Outside Europe and the U.S.		
	Phone	(408) 492-1790
	Fax	(408) 764-7290

NOTE: *RMA forms (except Europe) are available on CardFacts. Dial (408) 727-7021 and request document 9014.*

Glossary

Agent	A software-based subsystem that is used by SNMP applications to monitor and control network elements. Agents only manage a specific set of resources on a given network device. These resources are described by MIB objects. The data generated by the agent is stored in its MIB and made available to the network management application.
Community	The relationship between an SNMP agent and one or more SNMP management systems. All members of a given community are given the same access privileges. The agent can be configured so that only managers that are members of a known community can send requests and receive responses.
Community string	A specification that determines who has access to MIB objects and what type of access is allowed, such as read-only or read-write. Each SNMP command has an associated community string, which is set by the network manager. The strings provide a measure of security for the information contained in the objects, but they are not passwords. SNMP packets are transmitted in textural format. Therefore, a device's community string allows the device to ignore what is transmitted if the community strings do not match.
Management station	A network device on which an SNMP management application is running. The management station runs the network management protocol and applications that monitor and control network devices.

MIB

Management Information Base. A set of managed objects (for example, a set of FDDI-managed objects). The MIB defines the data that a network manager can receive about a managed device. It defines the access permissions for each data item, and the size, type, and semantics of each data item. Transcend LinkBuilder FDDI SmartAgent software supports a portion of the standard MIB II, FDDI MIB, and 3Com proprietary MIB specifications. MIB II specifications are based on the *Management Information Base for Network Management of TCP/IP based Internets: MIB-II Request for Comments (RFC) 1213, DDN Network Information Center, SRI International, March 1991*. FDDI MIB specifications are based on RFC 1512, September 1993.

Object

A definition of the actual resource(s) being managed in the SNMP environment. Many objects are stored in the MIB. Objects contain values that describe the status, statistics, and general operating parameters of the device. Many objects are available in SNMP. They are defined according to a specific format known as the Structure of Management Information (SMI). An agent collects object information that is pertinent to the management of that device.

PDUs

Protocol Data Units. A set of messages used by SNMP to provide management capability across a diverse set of networks and systems.

Protocol

A formalized set of rules that computers use to communicate. Because of the complexity of communications between systems and the need for different communication requirements, protocols have been divided into modular layers, in which each layer performs a specific function for the layer above.

Proxy agent

A translator between SNMP and different management systems. Proxy agents receive SNMP directives from the management process, translate the directives into proprietary operations, collect information, and respond to the management process with standard SNMP messages and traps.

SmartAgent	Intelligent management agent in devices and logical connectivity systems. The SmartAgent software reduces the computational load on the network management station and alleviates management-oriented traffic on the network while performing automated functions for a network manager system or 3Com application.
SNMP	Simple Network Management Protocol. A network monitoring protocol for TCP/IP-based networks. It is a simple request/response protocol used to communicate management information between the network management station and the agent residing in network elements. The protocol does not define the objects that can be managed. (The MIB defines manageable objects.) SNMP can be used with any network management variable that can be inspected and altered.
TFTP server	A network device that supports the Trivial File Transfer Protocol. The primary function of the TFTP server is downloading files and images from a source location to a specified destination. The management station can also function as a TFTP server.
Transcend	A 3Com integrated network management solution based on groups of logically related devices with integrated sets of management tools.
Trap	An error condition. A type of SNMP Protocol Data Unit (PDU) that is issued by an agent to report certain conditions and changes of state to the management process. The traps supported by SNMP include Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, and EGP Neighbor Loss.
Trap receiver	A network device designated to receive reports of trap conditions.