Setup Guide

D-Link DFE-570TX

Network Adapter Load Balancing and Failover Driver

Table of Contents

D-link DFE-570TX

Load Balancing and Failover utility

Setup Guide

Introduction to the D-Link Load Balancing Utility

Your DFE-570 adapter includes a software utility that provides dynamic fail over and allows customers to load balance network traffic across the multiple ports on the adapter. This utility is an elegantly simple yet extremely effective solution for increasing server availability and performance. The software's protocol independence allow easy integration into any NT server environment, making it ideal for mission-critical database servers, electronic commerce, web servers and file servers.

This utility eliminates each network port as a single point of failure by providing redundancy across all the ports on the adapter. The software ensures that users maintain non-stop access to key resources on the network, even if one or more of the network interface connections go down. If a connection to an adapter is lost, the software will instantly take the port out of the array and balance the traffic across the remaining ports with no loss of data and, just as importantly, without loss of connection.

The software can eliminate network interface performance bottlenecks by distributing traffic among then four Ethernet ports on the adapter. The software instantly routes connections to different adapters as users access the server. This process effectively increases network interface bandwidth by a factor equal to the number of ports on the adapter. To the server, these ports appear as a single network interface. To the remote workstation or web surfer, the server appears immediately available without the delay caused by congestion during high-access periods.

Key Features

- **Increased performance with network traffic Load Balancing.**
- **Can more than triple your server's throughput.**
- **Instant failover across multiple ports without loss of data.**
- **Remote management with Web-based Enterprise Manager.**
- **Supports IP, IPX and NetBEUI and AppleTalk.**
- **SNMP alerts on failed adapters.**
- **Provides detailed throughput graphing and reporting.**

Important Information

The following sections cover important information you need to successfully install the load balancing utility. Please read this section carefully. This information is intended to help you get up and running quickly and minimize the "gotchas" that can waste hours of installation time.

Requirements

The load balancing software is an NDIS Intermediate driver that performs all of its functions in the Kernel mode of NT. Because the software operates in kernel mode, it should work well with almost any server configuration and application. A few specific requirements, however, should be met before the load-balancing driver can successfully operate on your server.

- ***Platforms:*** *NT Server, Workstation or Terminal Server Edition with Intel Pentium single or multiprocessor, DEC Alpha single or multiprocessor. (Dual processor or higher recommended for high traffic loads).*
- ***Operating Systems:***
  Microsoft Windows NT 4.0 with:
  Service Pack 5, Service Pack 4 and Roll-up Hot Fix, or Service Pack 3 and NDIS Hot Fix.
  Terminal Server Edition with *Service Pack 4.*
- ***Miscellaneous:*** *32 MB RAM; 2 MB hard disk space; 3.5" high-density disk drive; SVGA video adapter; mouse or compatible pointing device*

Note: For Windows 2000, please refer to the ***D-Link Load Balancing utility for Windows 2000*** documentation for information about installing load balancing and failover support in Windows 2000. (available XXX 2000).

Windows NT 4.0 Issues

As with most applications, it is recommended that you install the latest Service Pack from Microsoft prior to installing the load-balancing driver. The driver requires at least Service Pack 3 to operate correctly. In addition, Microsoft has provided several "Hot Fixes" that fix key problems that were discovered after each of the service packs were released. If you are not running the latest Service Pack, it is strongly recommended that you install the Hot Fixes listed below since they usually solve bugs within NT that can lead to the "Blue Screen of Death."

Remember: Service Pack 3 or Service Pack 4 must be reapplied any time you change or reconfigure Network Services or Protocols in the Network Control Panel. It is highly recommended that you add all protocols and devices that you will need before installing SP3 or SP4.

Service Pack 3 and NDIS Hot Fix

If Service Pack 3 is installed, it is important to install the NDIS Hot Fix from Microsoft. This Hot Fix is only required for SP3 because the problem has been fixed in SP4.

NDISFIXI for Intel Systems and NDISFIXA for Alpha solve a memory-leak problem in Microsoft's NDIS driver that leads to a "Blue Screen of Death." This update, released after Service Pack 3, MUST be applied before the load-balancing driver is loaded. You can find this fix at Microsoft's site at the following URL:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/ndis-fix

Remember: Any time Service Pack 3 is reapplied, the NDIS hot fix must also be reapplied. It is highly recommended that you first add all protocols and devices that you will need; then install SP3; and finally apply the NDIS hot fix.

Service Pack 4 and Roll-Up Hot Fix

If Service Pack 4 is installed on a multi-processor computer, the Roll-Up Hot Fix from Microsoft must be applied to the system. This Hot Fix is only required for SP4.

SP4HXI for Intel Systems and SP4HFXA for Alpha solve a synchronization problem in Microsoft's TCPIP driver that leads to a "Blue Screen of Death." This update, released after Service Pack 4, MUST be applied before the load-balancing driver is loaded. You can find this fix at Microsoft's site at the following URL:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4/roll-up/

Remember: Any time Service Pack 4 is reapplied, the Roll-Up Hot Fix must also be reapplied. It is highly recommended that you first add all protocols and devices that you will need; then install SP4; and finally apply the Roll-Up Hot Fix.

Service Pack 5

Service Pack 5 (SP5) is the recommended configuration for use with the D-Link Load balancing software running on Windows NT 4.0. If you are running the IPX protocol, SP5 provides the most reliable environment for failover performance. Also, as of release time there were no additional Hot Fixes that were required with SP5.

Terminal Server Edition and Service Pack 4

If Windows NT Terminal Server Edition (TSE) is installed, Service Pack 4 (SP4) for TSE from Microsoft must be applied to the system before the load balancing driver is installed. SP4 for TSE solves a memory-leak problem in Microsoft's NDIS driver that leads to a "Blue Screen of Death" among numerous other fixes.

Microsoft Cluster Server

If installing Microsoft Cluster Server with load balancing driver, the load-balancing driver must be installed first. After installing the driver, an advanced configuration option must be set to allow Microsoft Cluster Server to bind to the load balancer's virtual adapter that is. The *Clustering Support* option can be found on the Advanced Tab in the driver. For more detail on setting this option please refer to the Advanced Settings topic on page 12.

SNMP Services

The D-Link driver can send alarms and alerts to any SNMP Management Console based on various states and conditions of each network port. To utilize this feature, SNMP services must be installed on the server.

Hardware Driver Compatibility

Windows NT drivers are based on the NDIS specification. Starting with NT 4.0 the NDIS spec was updated to incorporate advanced features such as the use of Intermediate drivers which sit between the NT Protocol Stack and the lower-level hardware drivers. The 4.0 spec also outlines how the lower-level drivers communicate with Intermediate drivers. The load-balancing driver operates differently depending on the types of lower-level drivers used.

NDIS 4.0 Drivers

The load balancing software takes advantage of NDIS 4.0 compatible drivers to provide instant failover (less than < 500 ms) because NDIS 4.0 drivers notify Intermediate drivers instantly of any failures or changes in status through "Status Indications." When an adapter fails, a Status Indication is sent to the load-balancing driver and failover occurs instantly without losing a single packet in most cases. Also, when an adapter with an NDIS 4.0 driver is brought back online, the driver will instantaneously add the adapter into the array and redistribute the traffic.

Recommended: Always check with your NIC manufacturer's web site to make sure you have the latest driver—preferably an NDIS 4.0 version. NDIS 4.0 drivers provide instant failover capability with the load-balancing driver.

NDIS 3.x Drivers

Not all NIC manufacturers have released NDIS 4.0 versions of their drivers. However, the load-balancing driver can still provide a high level of failover performance with NIC drivers that do not send "Status Indications." For non-NDIS 4.0 drivers, the software utilizes "Status Packets" that are generated by load balancing software so each port can poll the other ports in the array to make sure they are still alive. This process generates a small amount of traffic on the network and introduces some latency in the failover process. However, even when using Status Packets, the software can provide failover within 1 or 2 seconds with only three to four packets lost on average.

Before You Install - a Checklist

Use this checklist to make sure your environment is set up correctly for the software to be installed properly. It is highly recommended you follow each of the steps in the order given.

- NT 4.0 is running properly.
- All NICs have been installed and checked for proper operation.
- All protocols, drivers, and network services are installed in NT and operate correctly.
- At least Service Pack 3 has been installed. Service Pack 5 recommended.
- The necessary Hot Fixes have been installed.
- All cables, switches and hubs are set up and working properly.

Network Environment Considerations

While testing failover functionality, your network should approach a "real-world" environment in terms of ambient background traffic. When the number of ports on the Server is reduced to two and no traffic is on the network, it is more difficult for load balancing software to detect when a failover situation has occurred (except with NDIS 4.0 drivers). If your test network consists of one or two clients and a server is connected on an isolated switch, try to avoid long periods of quiet time on your network. If adapters with non-NDIS 4.0 drivers do not receive a broadcast packet in over 2 minutes, determining which port is bad becomes difficult if only two ports are in use.

Quick Setup Guide

Installing the Load Balancing Driver

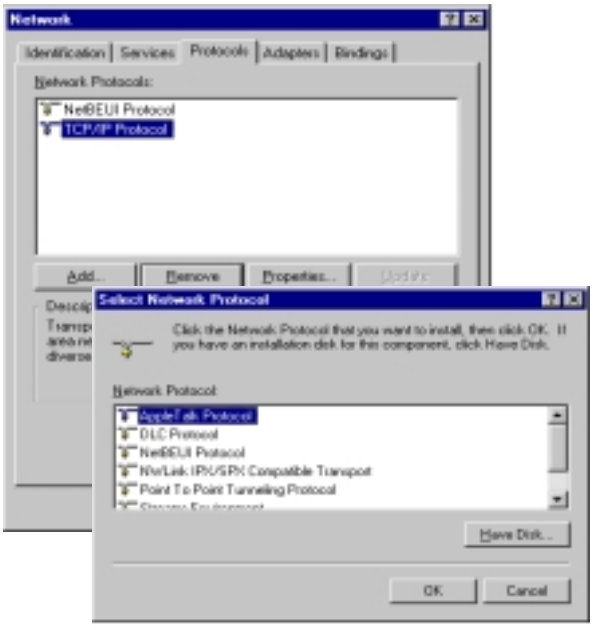
Step 1
Insert diskette into floppy drive or CD in the CD-ROM drive.

Step 2
Open Control Panel.

Step 3
Double-click on Networking.

Step 4
Click on Protocols tab.

Step 5
Select **Add..** to add a new Protocol Service.

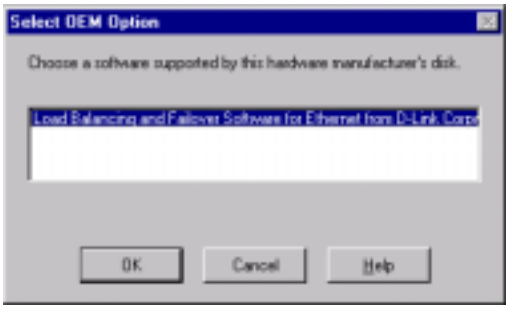


The driver installs as Protocol Service in NT's Network Control Panel

Step 6
Choose **Have Disk...** and the path to the drive or directory containing the D-Link installation files.

Step 7
The option "Load Balancing and Failover Software..." should appear. Select the option and click **OK**.

Step 8
The Setup dialog should be displayed. This dialog allows you to configure all of the ports that you want to add to the Array. Choose the first port in the "Available Adapters" list at the top of the dialog and select **Add...**



Adding the D-Link Protocol Transport

Step 9
You will be prompted to give the new array a name. This dialog will appear the first time only when you add an adapter to an array. If you will add more than one array, you may want to give each array segment a name such as "Engineering" or "Accounting."

Step 10

The next prompt asks if you want to use each port's protocol information as the primary address for the array. If this is the primary IP of the machine you want advertised to clients, select **Yes.** Otherwise, select **No** and continue adding the other ports to the array. You can change the IP address of the array later**.** When finished, click **OK.**

Using the setup dialog to add adapters to a new array.

Step 11

Close the Networking Control Panel applet. When prompted, reboot your machine for the new settings to take effect.

NOTE: All available ports or adapters must be assigned to an array. If you do not want load balancing or failover for a single port, assign it to a separate array by itself.

Verifying Protocol Information of the Array

Step 12

After rebooting, return to the Network Control Panel applet (repeat Steps 2 and 3) and select the Protocols tab.

Step 13

a) Select TCP/IP and click the Properties button.

b) Review the IP address configuration for the "D-Link Virtual Adapter."

The Virtual Adapter acts like a single adapter to NT but is actually the array of adapters. The IP address that is configured here is the server's IP address that will be advertised to the network.

c) Verify that the information is correct and click **OK** when finished.

d) To test that everything is set up properly, have multiple clients ping the address for the Virtual Adapter.

Using the Load Balancing Utility

Launching the Load Balancing Utility

At any time, you can instantly gauge the status of any port in an array and view performance statistics on each array or individual ports. To view the status information, open the Network Control Panel applet and view the properties of the D-Link Transport by following the steps below.

Step 1

Open the Network Control Panel applet and select the Protocols tab.

Step 2

Select D-Link Transport and click on the Properties button. The D-Link load balancing utility should be displayed with three tabs: Setup, Status, and Advanced.

Step 3

Select the Status tab to display the current condition of each port and throughput statistics for arrays or individual ports. Throughput statistics can be viewed on a per-second or cumulative basis. To toggle between these two modes, use the pull-down window in the center of the dialog.

Also, throughput can be viewed for individual ports or for the entire segment or array. Choose the Segment array name for which you wish to view statistics in the upper window or choose the individual NICs within the array.

With the Status Dialog, you can quickly gauge the status of each port.

Graph Details

In addition to the simple throughput statistics provided in the on the Status tab, detailed reports and graphs are provided in the Graph utility. To launch the graphing utility simply, click on the Graph Details button in the center of the Status tab. A complete overview of the D-Link Graph utility is provided in the section

Using the D-Link Graphing Utility on page 14.

Viewing NIC Card Status and Alerts

Within the Status dialog box, you can also view the status of each NIC instantly. The load balancing software keeps track of five different states for each NIC in an array. These states are represented using different color icons for the NICs in the tree view. The five states with explanations are shown below.

Green Adapter – Adapter's normal state. Adapter is working properly and has not failed since system start.

Green Adapter with Red X - Adapter is currently down and has failed for the first time.

Yellow Adapter - Adapter is currently working properly. However, yellow state indicates there has been a failure previously. The software will automatically reactivate adapters that indicate that they are working properly again.

Yellow Adapter with Red X - Adapter is currently down and has been down multiple times before.

Red Adapter - Adapter has failed more than three times in one hour (default) and the software has pulled the adapter from the array. This state prevents the load balancing software from constantly failing over on faulty adapters that should be replaced.

NOTE: The load balancing software will permanently remove a port if it determines that a port has failed more than three times in one hour (achieving the red state above). If you will be testing failover functionality, you may want to adjust this default. Otherwise, if you pull the wire on a port more than three times, you will have to reactivate the port from the Advanced Tab to add the port back into the array. Refer to the Advanced Configuration Options below to change these defaults or to learn how to reactivate a permanently inactivated adapter or port.

Whenever a port changes states, an SNMP alert is sent (assuming you have SNMP services loaded in NT) and an event is logged to the NT event log.

Advanced Configuration Options

The Advanced Tab in allows for advanced configuration options used by the failover and load balancing functions. There are three groups of advanced settings located on the Advanced Tab. The first section allows for reactivation of permanently removed adapters without rebooting the server. The next section provides settings for disabling load balancing and Microsoft Cluster Server support. Finally, the third section contains settings for the operation of the failover function. Each group of settings will be described in detail.

Inactive Adapters

Normally, if a port fails but later indicates it is online again, the load balancing software will automatically add the port back into the array. However, if the port fails three times within one hour (default), the software will permanently remove the adapter from the array. These thresholds can be modified under the Failover Settings section (see below).

To reactivate a permanently removed port, select the port and press the Reactivate button. If there are no problems inserting the port, the port will then be added back to its array without needing to reboot. Caution should be used when reactivating an adapter. If the adapter has failed several times, the adapter may be experiencing intermittent hardware problems and may need to be replaced. An adapter with hardware problems may cause other network problems to occur on the network.

Advanced Settings

The Advanced Settings section provides for the configuration of two optional settings. First, selecting the checkbox next to “Load Balancing Disabled” will disable the load balancing function. This setting will send data only through the primary adapter, but still provides for instantaneous failover. The Checkbox next to “Clustering Support” will change settings to the virtual driver so that Microsoft Cluster Server can be used with the load-balancing driver.

NOTE: Both of these settings require a reboot to take effect.

The Advanced Tab is used to reactivate adapters and modify advanced settings.

Failover Settings

The Failover Settings section provides options that control the failover function. Each setting is discussed below.

The first column of options set the conditions to permanently remove adapters from the array. The setting for **Max Down Count** is the number of times an adapter must go down (and comes back online) in the defined time period before being permanently removed. The default value for this field is 3. A value of zero (0) disables this feature so that an adapter can fail repeatedly without being permanently removed.

The setting for **Time Period** is the amount of time (in minutes) the **Max Down Count** setting must be exceeded before an adapter is permanently removed. The default value for this field is 60 minutes (1 hour).

The second column of settings control the method used to detect that an adapter has failed. The **Status Packets** method sends a status packet from one adapter to another in order to determine if the receiving adapter is available.

The **Status Indication** method uses NDIS 4.0 functionality to have an adapter inform the load balancing software that an adapter has failed or is functioning properly again. Not all adapters support this method but it does provide for faster failover.

The **Auto Detect** method determines at system startup which method (Status Packets or Status Indications) should be used to provide the best failover method for the installed adapters.

After any setting has been changed, the Update button will become active. Once all changes have been made, press the Update button for the settings to automatically go into effect. No reboot is required and all settings are saved for use after rebooting. To restore all settings back to their default values, press the Default button. Press the Update button to have these settings go into effect. If any changes have been made and the OK button is pressed, the new settings will then automatically be applied.

Using the D-Link Graphing Utility

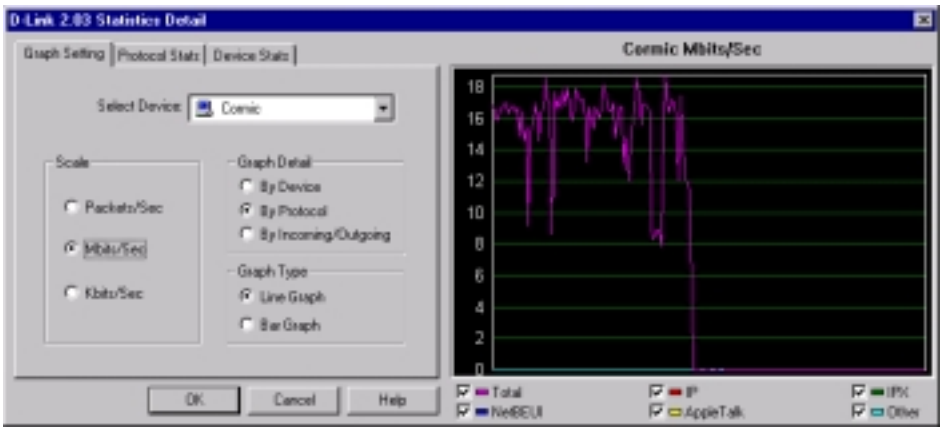
D-Link also provides a graphing utility to view detailed traffic statistics in real-time graphs and reports. The graphing utility offers two types of graph formats. First, the line graph is similar to the *Performance Monitor* in Windows NT and provides a detailed histogram of throughput data in real-time. The second option provides for real-time 3-D bar charts that provide throughput data for every component in a server or all of the protocol traffic.

To launch the D-Link Graph Utility, follow the steps outlined below.

Step 1
Open the D-Link Load balancing software and select the Status Tab. See Launching the Load Balancing Utility above.

Step 2
Select the *Graph Details* button in the middle of the Status Tab. The Graphing utility should be displayed with three tabs: *Graph Setting, Protocol Stats, and Device Stats*.

Step 3
Select the Graph Setting tab and select the device you wish to graph from the Select Device pull-down box located at the top of the tab. The following section explains each option on the Graph Settings tab.



The Graph Utility provides detailed statistics and graphs.

Graph Settings Tab

The “Graph Settings” tab allows you to customize how the software graphs and displays throughput data, as well as select which device to graph throughput data on. On this tab you can:

- **Change the scale to Packets/Sec, Mbits/Sec or Kbits/sec.**
- **Further breakout data by Incoming/Outgoing data, per adapter, or by protocol.**
- **Select between Bar Graph or Line Graph.**
- **Select the device to graph data for.**

Scale

To change the scale of any chart or graph, simply selected the appropriate option under Scale on the Graph Settings Tab. You can switch the scale from Packets per second, Megabits per second or Kbits per second.

Graph Detail

Graph Detail allows you to select how throughput totals are broken out for the currently selected device. You can choose to display breakout detail in three ways:

- **By Device**
  Allows you to view throughput from all of the sub-components that make up a device. For instance if the currently selected device is a Group (Array), then breakout totals will be displayed for each adapter that makes up that group.
- **By Protocol**
  This option allows you to view totals for each protocol running on the currently selected device in addition to the total throughput of the device.
- **By Incoming/Outgoing**
  This option allows you to view total incoming traffic to the device selected, total outgoing traffic in addition to the device's total overall throughput.

NOTE: This option is grayed out for Bar Chart type graphs since both Incoming and outgoing traffic detail is provided in the other two options for Bar graphs.

You can further customize the graph by selecting or unselecting each breakout component on the legend below the graph.

Graph Type

There are two ways to view throughput data in real time – Line Graphs or Bar Charts.

Line Graph

The line graph is similar to Performance Monitor in Windows NT. It gives you the ability to view data over time for total server throughput, by group, or adapter. Line graphs not only allow you to see total throughput for each device, but you can also view a variety of detailed statistics for each device including:

- **Incoming and outgoing data**
- **Traffic for each protocol**
- **Traffic for each sub-component (i.e. adapters that make up an array)**

Bar Graph
The bar graph option allows you to view throughput data for all components or protocols on the server at once as well as overall throughput for the server. The bars in the graph show both Incoming and outgoing data for each component. With the Bar graph option selected, you have the ability to see graph detail by Device or by protocol.

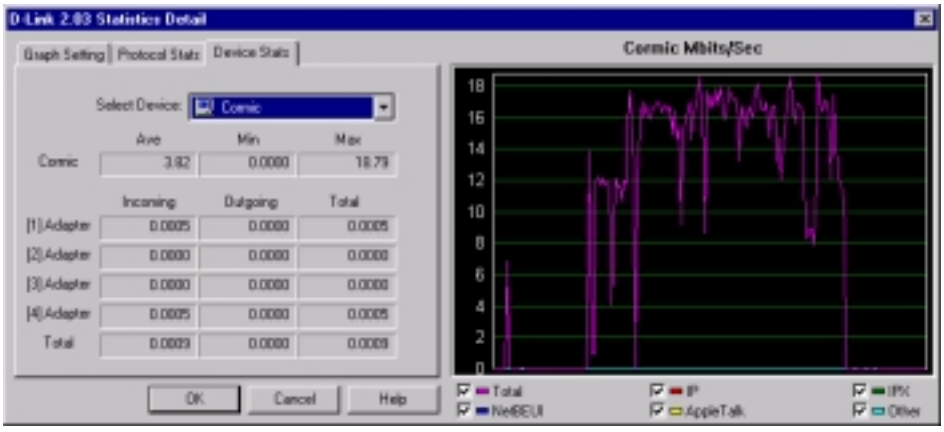
NOTE: With Bar chart selected, the Incoming/Outgoing option under graph detail will be grayed out since this data is already incorporated in the bar charts for both "By Device" and "By Protocol" options.

Protocol Stats Tab

The Protocol Stats Tab displays detailed statistics in tabular form for all protocols on the selected device. The device's total throughput statistics are shown as well as totals for IP, IPX, NetBEUI and AppleTalk protocols.

Device Stats Tab

The Device Stats tab shows detail statistics in tabular form broken out by sub-component. Average, minimum and maximum values are displayed in the first row of data for the selected device. Throughput data for each sub-component of the device along with the device total are also displayed.



The DeviceStats tab provides detailed statistics for each port.

Configuring SNMP

You can configure the D-Link SNMP agent to send traps to your SNMP Management Console to notify you when an adapter fails or is brought back online. The SNMP agent is automatically loaded if the following conditions are met on initial installation:

- TCP/IP is loaded.*
- SNMP Services are loaded.*

*See your NT Operating System manual for help with configuring TCP/IP and SNMP services.

If the above two conditions were not met when you first installed the software, you can easily perform an update to install the SNMP Agent.

Configuring SNMP Agent after an Earlier Installation

Step 1
If the load balancing software was installed previously, make sure you now have both TCP/IP and SNMP services properly installed.

Step 2
Open the Network Control Panel applet and select or highlight the D-Link Transport .

Step 3
Click the Update button in the lower left of the Setup tab.

NOTE: If you install any protocols or services such as TCP/IP or SNMP, you must reapply any Service Packs and Hot Fixes.

Step 4
Update your SNMP management console (CA Unicenter, Tivoli TNG, etc.) with the D-Link MIBs. D-Link's two MIB files (DLINK.MIB and DLINKARRAY.MIP) are located in the root directory of your CD or diskette. Please refer to your management consoles documentation for specific instructions.

SNMP Traps

The load balancing software generates SNMP traps to alert administrators of any changes in the state of an array.

- Adapter Down (Adapter Name and Array Name)
- Adapter Up (Adapter Name and Array Name)
- Down to one adapter (Array Name)
- All adapters in array are down (Array Name)

Windows NT Event Log Messages

The load balancing software will report all adapter errors and state changes to the NT Event Log. To view messages in the Event Log, use the Event Viewer supplied by NT. Examples of all the events generated are shown below:

Downed Adapter:

```
The adapter <Adapter Name> in <Array Name> has lost network
connectivity and has been removed from the Array.
```

Array has only one remaining Adapter:

```
There is only one functioning adapter in <Array Name> left.
```

All Adapters in Array are down:

```
All adapters in <Array Name> are down; therefore, users on
this segment can no longer communicate to this computer.
```

Failed Adapter comes online again:

```
The adapter <Adapter Name> in <Array Name> has regained
network connectivity and has been inserted back into the
Array.
```

Adapter has failed multiple times and is permanently removed:

```
The adapter <Adapter Name> in <Array Name> has lost network
connectivity and has been removed from the Array.  The adapter
has gone down <###> times in the past <###> minutes;
therefore, the adapter will not be put back into the array.
It is advisable that you investigate the cause of the lost
connections and possibly replace the adapter or cable.
```

Contacting D-Link

For technical assistance, you can reach us via e-mail, fax or phone.