Setup Guide

D-Link®

Network Adapter Load Balancing and Failover

Table of Contents

Setup Guide

Introduction

This software provides dynamic fail over and allows customers to load balance network traffic across multiple network adapters in the server. This is an elegantly simple yet extremely effective solution for increasing server availability and performance. The software allows easy integration into any NT 4.0 server environment, making it ideal for mission-critical database servers, electronic commerce, web servers and file servers.

This eliminates the network interface as a single point of failure by providing redundancy across multiple network ports in a array. This ensures that users maintain non-stop access to key resources on the network, even if one or more of the network interface connections goes down. If a connection to a port is lost, it 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.

This can eliminate network interface performance bottlenecks by distributing traffic among multiple Ethernet ports on the server. The software instantly routes connections to different ports as users access the server. This process effectively increases network interface bandwidth by a factor equal to the number of ports on the server. To the server, these multiple 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

- **Increases performance with network traffic load balancing.**
- **Load balances incoming as well as outgoing traffic for greatest performance.**
- **Enhances fault tolerance with failover across multiple ports.**
- **Provides instant failover without loss of connections or data.**
- **Works with all native NT protocols: IP, IPX, NetBEUI .**
- **Completely hardware independent. Works with any DFE570TX Server card and does not require special switching hardware.**
- **Generates SNMP alerts based on any of 5 port states.**

Important Information

The following sections cover important information you need to successfully install it. 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

This is an NDIS Intermediate driver that performs all of its functions in the Kernel mode of NT 4.0 . Because this operates in kernel mode, it should work well with almost any server configuration and application. A few specific requirements, however, should be met before this can successfully operate on your server.

- *Platforms:* Network server, or workstation with Intel Single Pentium or higher processor (Dual Pentium or higher recommended for high traffic loads)
- *Operating Systems*: Microsoft Windows NT 4.0 (with Service Pack 4 or Service Pack 3 + NDIS Hot Fix) .
- *Miscellaneous:* 32 MB RAM; 2 MB hard disk space; 3.5" high-density disk drive; VGA video adapter; mouse or compatible pointing device

Windows NT 4.0 Intel Versions

This is designed around the NDIS 4.0 Intermediate driver specification and therefore cannot work with older versions of NT.

Service Pack 4.0

Like most applications, This requires Service Pack 4.0 to operate correctly.

Note: It's unnecessary to install NDIS Hot Fix if Service Pack 4.0 was installed.

Service Pack 3.0

Like most applications, This requires Service Pack 3.0 to operate correctly.

Remember: Service Pack 3.0 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.

NDIS Hot Fix

NDISFIXI for Intel Systems solve a memory-leak problem in Microsoft's NDIS driver that leads to a "Blue Screen of Death." This update, released after Service Pack 3.0, MUST be applied before this 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

Note: Traditional Chinese:

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

Simple Chinese:

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

Remember: Any time Service Pack 3.0 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.

SNMP Services

This 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 spec. 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. This operates differently depending on the types of lower-level drivers used.

NDIS 4.0 Drivers

This takes advantage of NDIS 4.0 compatible drivers to provide instant failover (less than < 500 ms) because NDIS 4.0 drivers notify Intermediate drivers like This instantly of any failures or changes in status through “Status Indications." When an adapter fails, a Status Indication is sent to 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, This will instantaneously add the adapter into the array and redistribute the traffic.

Recommended:	**Always check with your D-Link’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 to this.**

Before You Install - a Checklist

Use this checklist to make sure your environment is set up correctly for This 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.
- Please make sure that Port No.1 of Server card is properly connected to a network device (ex: Switch) and checked for proper operation.
- All protocols, drivers, and network services especially SNMP Service are installed in NT and operate correctly.
- Service Pack 3.0 has been installed.
- The NDIS Hot fix has 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 it 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

Step 1
Insert diskette into floppy drive .

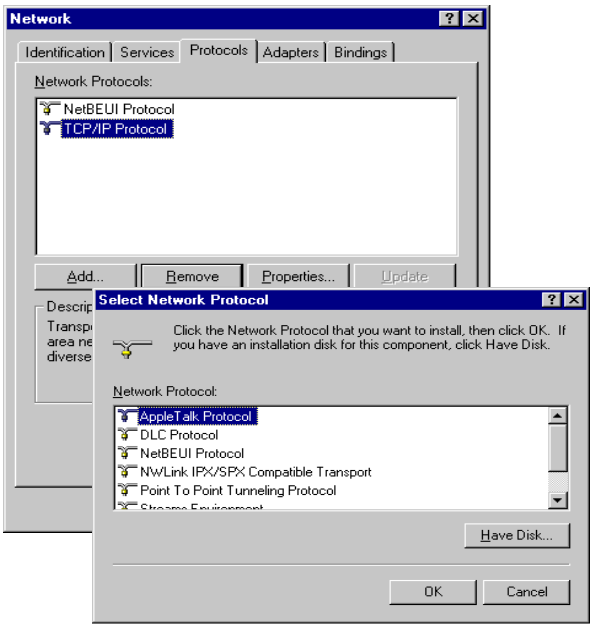
Step 2
Open Control Panel.

Step 3
Click on Networking.

Step 4
Click on Protocols tab.

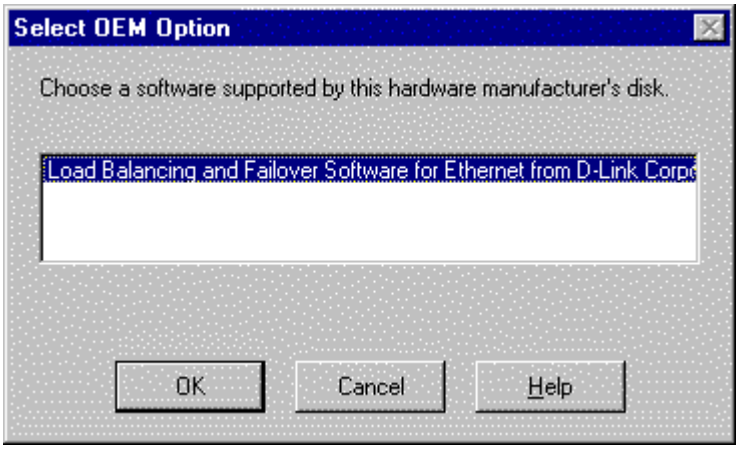
Step 5
Select **Add..** to add a new Protocol Service.

Step 6
Choose **Have Disk…** and the path to the drive or directory containing the software files.



installs as Protocol Service in NT's Network Control Panel

Step 7
The option " Load Balancing and Failover Software for Ethernet from D-Link Corporation" should appear. Select the appropriate option based on the type of adapter that are installed on the system 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...**

Step 9

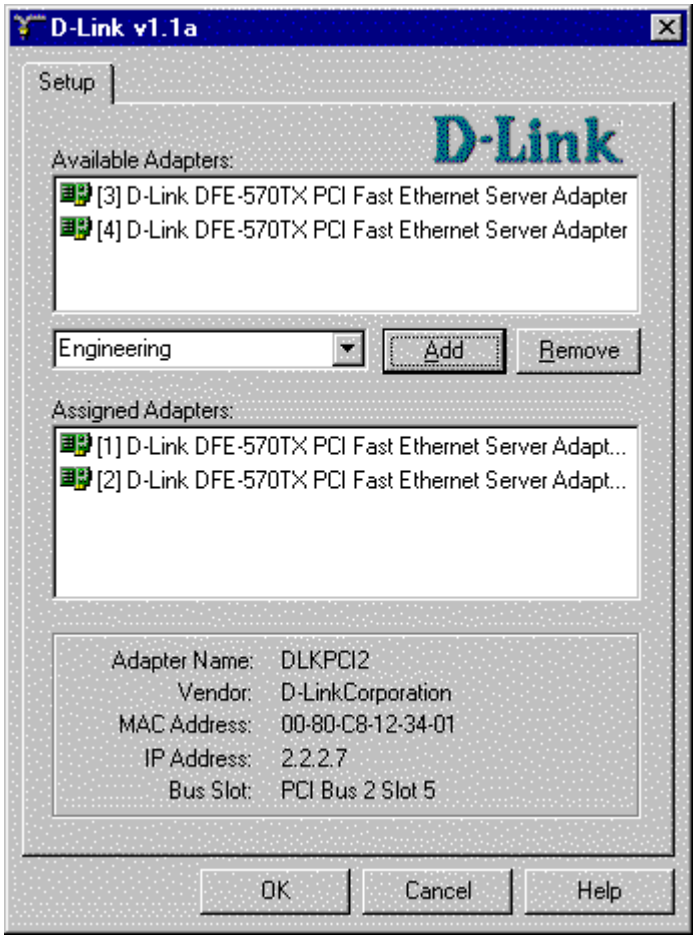
You will be prompted to give the new array a name. This dialog will appear the first time only when you add an adapter to an array. If you will add more than one array, you may want to give each array segment a name such as “Engineering” or “Accounting."

Step 10

The next prompt asks if you want to use this adapter’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 adapters to the array. You can change the IP address of the array later**.** When finished, click **OK.**

Step 11

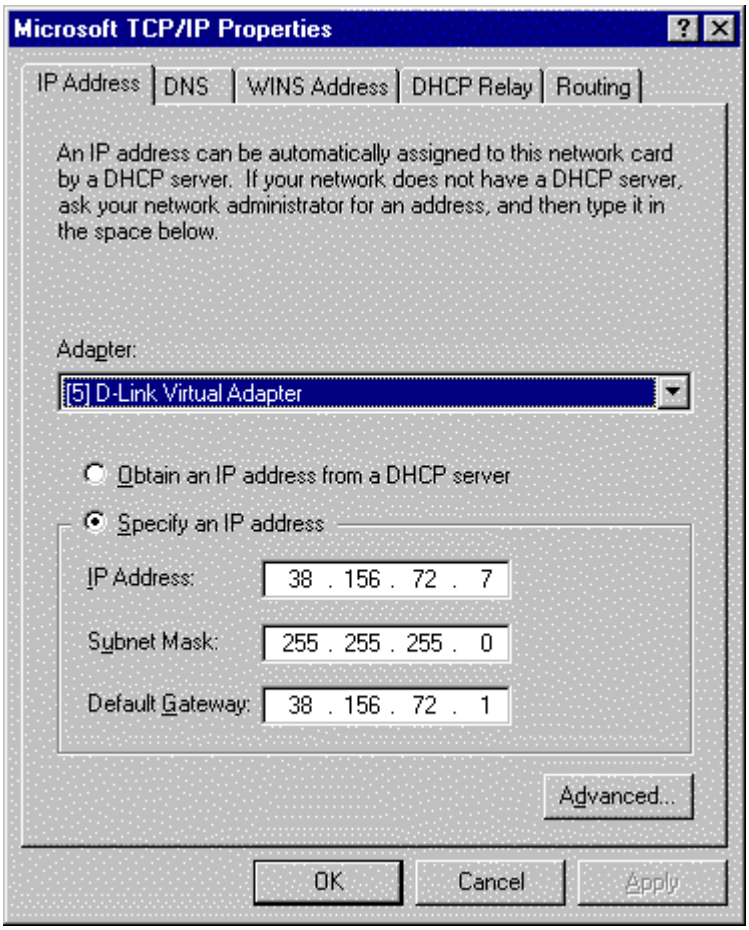
Close the Networking Control Panel applet. When prompted, reboot your machine for the new settings to take effect.



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 D-Link 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, you may have multiple clients to ping the address for the D-Link Virtual Adapter.

Reviewing Status and Statistics

At any time, you can instantly gauge the status of any port in a array and review 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 Protocol Transport following the steps below.

Step 1

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

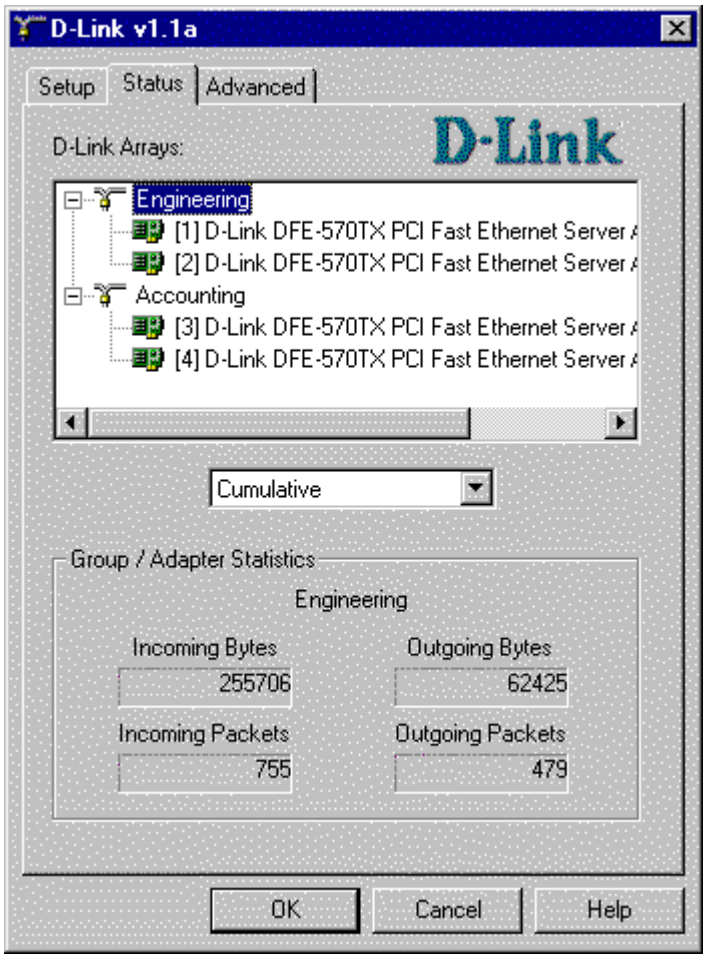
Step 2

Select the D-Link v1.1a and click on the Properties button. The dialog 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.



Viewing Ports Status and Alerts

Within the Status dialog box. you can also view the status of each port instantly. This keeps track of five different states for each port in an array. These states are represented using different color icons for the ports 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. Softeware 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 it has pulled the adapter from the array. This state prevents it from constantly failing over on faulty adapters that should be replaced.

NOTE:	This will permanently remove a port if it determines that the 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 adapter 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 port.

Whenever a card 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 Tap in the softeware interface allows for reactivation of permanently removed ports and updates to default parameters used in it .

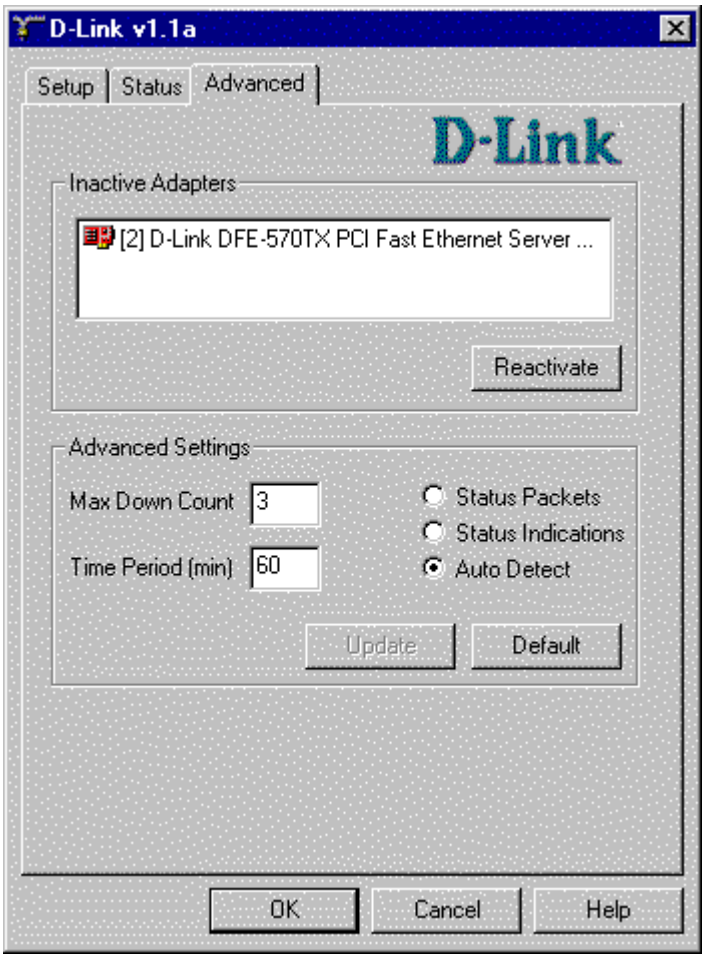
Inactive Ports

Normally, if an port fails but later indicates it is online again, This will automatically add the port back into the array. However, if the port fails three times within one hour (default), this will permanently remove the port from the array. These thresholds can be modified under the Advanced Settings (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 port . If the port has failed several times, the port may be experiencing intermittent hardware problems and may need to be replaced. A port with hardware problems may cause other network problems to occur on the network.

Advanced Settings

There are two groups of advanced settings that alter the operation of this. The first group of settings defines when to permanently remove an port from the array. The setting for **Max Down Count** is the number of times an port 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 port 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 a port is permanently removed. The default value for this field is 60 minutes (1 hour).

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

The **Status Indication** method uses NDIS 4.0 functionality to have an port inform this that an port has failed or is functioning properly again.

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 ports.

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.

Configuring SNMP

You can configure the software SNMP agent to send traps to your SNMP Management Console to notify you when an port fails or is brought back online. The software SMP 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 installed this, you can easily perform an update to install the software SNMP Agent.

Configuring Softeware SNMP Agent after an Earlier Installation

Step 1
If the softeware agent 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 Service Pack 3 and the NDIS Hot Fix.

Step 4
Update your SNMP workstation with the softeware MIBs. Softeware' two MIB files (Dlink.MIB and Dlink.MIP) are located in the root directory of your CD or diskette.

SNMP Traps

This generates SNMP traps to alert administrators of any changes in the state of a array.

- Port Down (Port Name and Array Name)
- Port Up (Port Name and Array Name)
- Down to one Port (Array Name)
- All ports in array are down (Array Name)

Windows NT Event Log Messages

This will report all port 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 by sofetware 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.
```