Chapter 9

Disaster Recovery

One of the major issues that a network administrator must address is the possibility of system failure and associated downtime. The administrator must handle two major issues to guard against the danger of a failed server:

- Protecting data
- Reducing downtime

This chapter discusses both issues and examines how the use of fault-tolerant disk configurations and a backup strategy can help reduce the danger of lost time and data. This information falls under the "Choose a disaster recovery plan for various situations" job skill in the test preparation guide.

Chapter 9 targets the following objective in the Implementation section of the Networking Essentials exam:

Test Objectives

- Choose a disaster recovery plan for various situations

Test Yourself

Stop! Before reading this chapter, test yourself to determine how much study time you will need to devote to this section.

1. RAID 5 is a term that describes which of the following?
   A. A weekday backup strategy for enterprise networks
   B. A fault-tolerant disk configuration
   C. An NDIS-compatible SCSI controller
   D. Data backup through directory replication

2. The maximum number of disks in a stripe set is __________.
   A. 2
   B. 16
   C. 32
   D. Limited only by hardware

3. The maximum number of drives in a mirror set is __________.
   A. 2
   B. 4
   C. 16
   D. None of the above

Protecting Data

Natural disasters, equipment failures, power surges, and deliberate vandalism can cause the catastrophic loss of precious network data. Protecting the data is a primary responsibility of the network administrator. Microsoft highlights these important strategies for preventing data loss:

- Backup
- Uninterruptible Power Supply (UPS)

Both of these strategies are discussed in the following sections.

Backup

A backup schedule is an essential part of any data-protection strategy. You should design a backup system that is right for your situation and the data on your network.

A number of different strategies can be used in backing up files. One way is simply to copy a file to another drive. Operating systems, however, typically have special backup commands that help you with some of the bookkeeping required for maintaining a systematic backup schedule. Most backup commands mark the file with the date and time of the backup so that you (and the backup utility) will know when a copy of the file was saved last. This is the purpose of the FAT file system's Archive attribute. To determine whether this attribute exists, check the properties of any file on a FAT partition. If the Archive attribute is enabled, the file has changed since the last time a backup was done. In this chapter, you will see that some backup techniques reset this attribute, whereas others do not.

Although backups can be accomplished by saving files to a different drive, they typically are performed with some form of tape drive. Commonly called *DAT drives*, these devices are able to store many gigabytes of information quickly and economically. Moreover, the tapes are small and portable. Another important step in your backup plan, therefore, is deciding where to store these backup tapes. Many companies choose to make two copies of each backup tape and store one of the copies off-site, thereby guarding against a catastrophic event such as fire.

In addition to the various types of copy commands, Microsoft identifies the following backup types:

- **Full backup.** Backs up all specified files.
- **Incremental backup.** Backs up only those files that have changed since the last backup.
- **Differential backup.** Backs up the specified files if the files have changed since the last backup. This type doesn't mark the files as having been backed up, however. (A differential backup is somewhat like a copy command. Because the file is not marked as having been backed up, a later differential or incremental backup will back up the file again.)

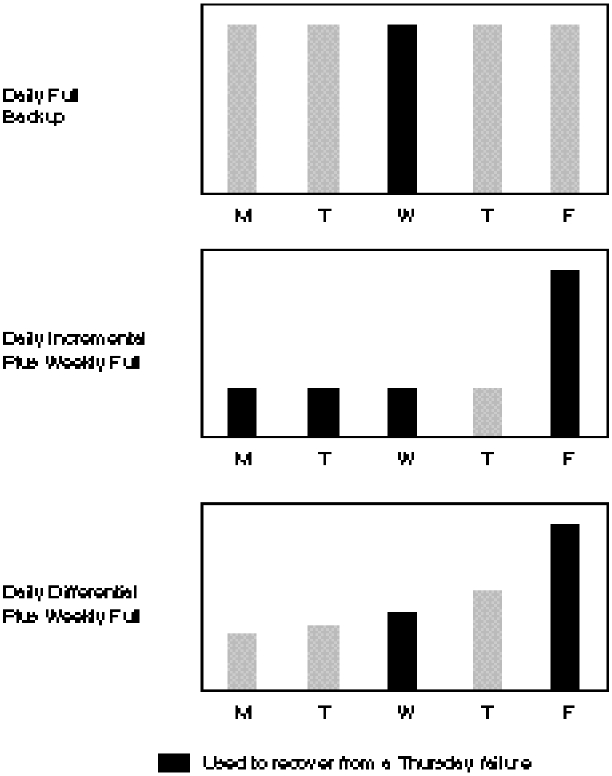
A typical backup plan includes some combination of these backup types performed at regular intervals. One common practice is to perform an incremental or differential backup each day and a full backup every week. Full backups make the restoration process easier because there is only one set of tapes; however, they also require a lengthy backup process each night, which often means that someone must physically change the tapes.

Incremental backups are much faster because they back up only those files that have been changed since the last backup. The Archive attribute switches on when a file is modified. An incremental backup backs up the file and then removes the attribute so that the file will not be backed up again unless it is changed the next day. A combination of incremental and full backups usually results in four to six incremental tape sets and one full tape set each week. If the drives fail, the administrator must restore the last full backup set, as well as all the incrementals performed since the drive failure. This process obviously is considerably slower than a backup scheme in which a full backup is performed every night.

Differential backups are similar to incrementals except that they do not reset the Archive attribute, which means that each backup during the week backs up all files changed since the last full backup. A full backup once a week (generally Friday or Saturday) and differentials every other day means that only two tapes will be needed in case of failure—the last full backup and the last differential (see fig. 9.1).

Figure 9.1

An ideal backup scheme implements a schedule of different backup types.



Keeping a log of all backups is important. Most backup utilities can generate a backup log. Microsoft recommends that you make two copies of the backup log—store one with the backup tapes and keep one at the computer site. Always test your backup system before you trust it. Perform a sample backup, restore the data, and check the data to be sure it is identical to the original.

You can attach a tape drive directly to a single server, or you can back up several servers across the network at once. Backups over the network are convenient for the administrator, but they can produce considerable network traffic. You can reduce the effects of this extra traffic if you place the computer attached to the tape drive on an isolated network segment and connect it directly to secondary network interface cards on each of the servers.

note

A number of other vendors also offer backup software—such as Arcada's BackupExec or Cheyenne's ArcServe—that include additional features, and in many cases, these are a very wise investment. For the test, though, remember that only the Microsoft Backup utility will be covered.

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is a special battery (or sometimes a generator) that supplies power to an electronic device in the event of a power failure. UPSs commonly are used with network servers to prevent a disorderly shutdown by warning users to log out. After a predetermined waiting period, the UPS software performs an orderly shutdown of the server. Many UPS units also regulate power distribution and serve as protection against power surges. Remember that a UPS generally does not provide for continued network functionality for longer than a few minutes. A UPS is not intended to keep the server running through a long power outage, but rather is designed to give the server time to do what it needs to before shutting down. This can prevent the data loss and system corruption that sometimes results from sudden shutdown.

When purchasing a UPS for a server, note that these come in many varieties (see fig. 9.2). As noted earlier, the UPS is really just a battery backup. Just like a car battery, the more powerful it is, the more expensive it is. Prices run from the hundreds to many thousands of dollars. Before you buy, know how many servers you will be running off the UPS and how much time they need to shutdown properly. One of the most popular UPS manufacturers is APC (American Power Conversion), a company that offers a full line of power supply and UPS products.

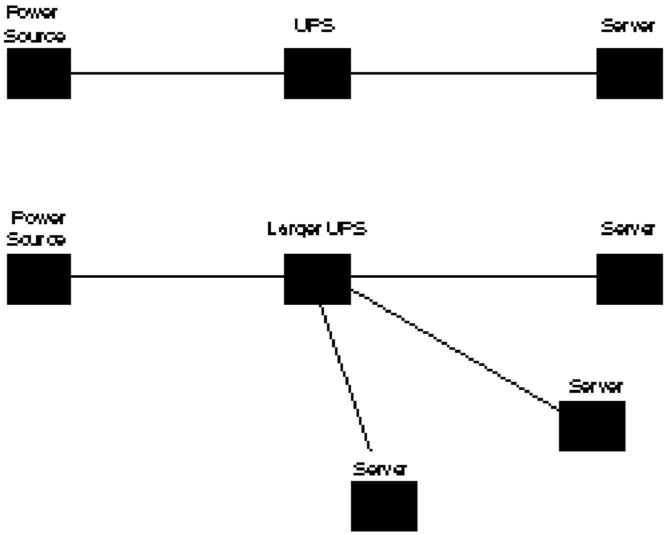


Figure 9.2

A large UPS can function in much the same way as a surge protector in that numerous components can be plugged into a single unit.

Backups mainly provide a quick method for system recovery. They require a long and tedious restoration process that can cost your company dearly in lost revenue and productivity. Because of this, the following sections examine some methods of minimizing—or even preventing—downtime in case of a drive failure.

Recovering from System Failure

Next to data security, keeping the network up and running properly is the most crucial day-to-day task of an administrator. The loss of a hard drive, even if not disastrous, can be a major inconvenience to your network users and may cost your organization in lost time and money. Procedures for lessening or preventing downtime from single hardware failures should be implemented. Disk configurations that enable this sort of protection are called *fault-tolerant* configurations.

Implementing a Fault-Tolerant Design

Connecting network components into a fault-tolerant configuration ensures that one hardware failure doesn't halt the network. You can achieve network fault-tolerance by providing redundant data paths, redundant hubs, and other such features. Generally, however, the data on the server itself—its hard drives—is the most crucial.

tip

> When developing a fault-tolerance scheme, remember that you must balance the need for rapid recovery from a failure against cost. The basic theory behind fault-tolerant design is hardware redundancy, which translates into additional hardware expenses. Also, remember that the greater the level of redundancy, the greater the complexity involved in the implementation.

Using RAID

A vital tool for protecting a network's data is the use of a *Redundant Array of Inexpensive Disks (RAID)*. Using a RAID system enables you to set up the best disk array design to protect your system. A RAID system combines two or more disks to create a large virtual disk structure that enables you to store redundant copies of the data. In a disk array, the drives are coordinated into different levels of RAID, to which the controller card distributes the data.

RAID uses a format of splitting data among drives at the bit, byte, or block level. The term *data striping* refers to the capability of arranging data in different sequences across drives. Demonstrations of data striping are shown in figure 9.3.

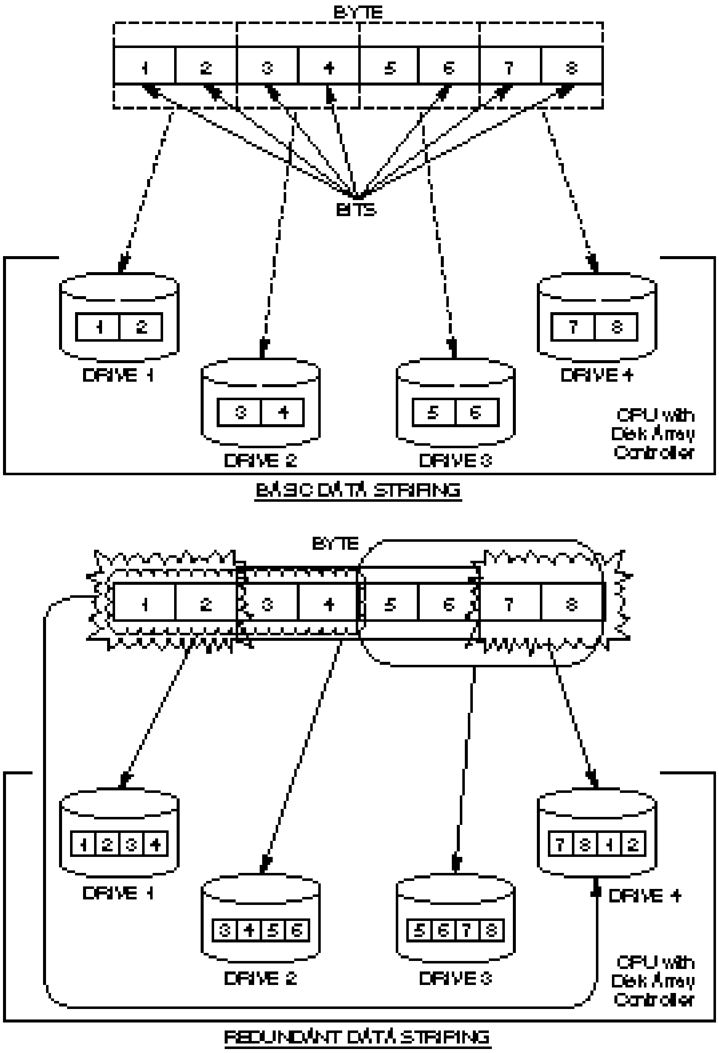


Figure 9.3

Data striping arranges data in different sequences across drives.

Your input in designing the most reliable drive setup for your network is an important responsibility. You must choose the best RAID implementation level to meet your users' requirements in data integrity and cost. Seven levels of RAID are available on the market today: 0, 1, 2, 3, 4, 5, and 10. A higher number isn't necessarily indicative of a better choice, so you must select the best level for your environment. The following paragraphs present a brief discussion of some of these available levels, notably RAID 0, 1, and 5, which Windows NT Server supports. Windows NT Workstation supports only RAID 0, and Windows 95 is not able to use any RAID levels at all.

warning

> A fault-tolerant disk scheme is used only to speed recovery time from a hardware fault. None of these RAID levels is intended to be a replacement for regular tape backups.

RAID 0

Level 0 uses data striping and *block interleaving*, a process that involves distributing the data block by block across the disk array in the same location across each disk. Data can be read or written to these same sectors from either disk, thus improving performance. RAID 0 requires at least two disks, and the striped partitions must be of the same size. Note that redundancy of data is *not* provided in RAID 0, which means that the failure of any single drive in the array can bring down the entire system and result in the loss of all data contained in the array. RAID 0 is supported in Windows NT Server and Windows NT Workstation, but not in Windows 95.

RAID 1

In level 1, drives are paired or mirrored with each byte of information being written to each identical drive. You can duplex these devices by adding a separate drive controller for each drive (duplexing is examined later in this chapter). *Disk mirroring* is defined as two hard drives—one primary, one secondary—that use the same disk channel (controller cards and cable), as illustrated in figure 9.4. Disk mirroring is most commonly configured by using disk drives contained in the server. Duplexing, which is covered later in this chapter, is a form of mirroring that enables you to configure a more robust hardware environment.

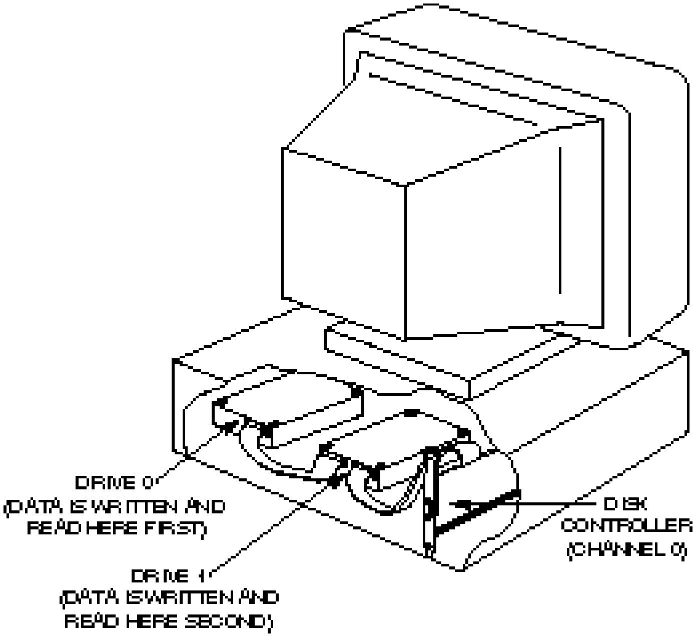


Figure 9.4

In disk mirroring, two hard drives use the same disk channel.

Mirroring does not provide a performance benefit such as RAID 0 provides. Use mirroring, however, to create two copies of the server's data and operating system, which enables either disk to boot and run the server. If one drive in the pair fails, for instance, the other drive can continue to operate. Disk mirroring can be expensive, though, because it requires 2 GB of disk space for every 1 GB you want to mirror. You also must make sure that your power source has enough wattage to handle the additional devices. Mirroring requires two drives, and the mirrored partitions must be of the same size. Windows NT Server supports mirroring, but Windows NT Workstation and Windows 95 do not.

Remember that mirroring is done for fault-tolerant, not performance reasons. With this said, it should be noted that an NT machine running a mirror set will run at about normal speed on writes to the mirror set, but can have marginal performance gains reading from the set. For the best of both worlds, though, we need to move on to RAID 5.

note

> RAID 2, 3, 4, and 5 are all versions of striping that incorporate similar fault-tolerant designs. Microsoft chose to support only level 5 striping in Windows NT Server. As the numbering scheme would imply, this is the newest revision of the four and is the most popular fault-tolerance scheme in use today. Level 5 requires less disk space than mirroring and has performance gains over other striping methods. As with mirroring, RAID level 5 is not available in Windows NT Workstation or Windows 95.

RAID 5

RAID 5 uses striping with parity information written across multiple drives to enable fault-tolerance with a minimum of wasted disk space. This level also offers the advantage of enabling relatively efficient performance on writes to the drives, as well as excellent read performance.

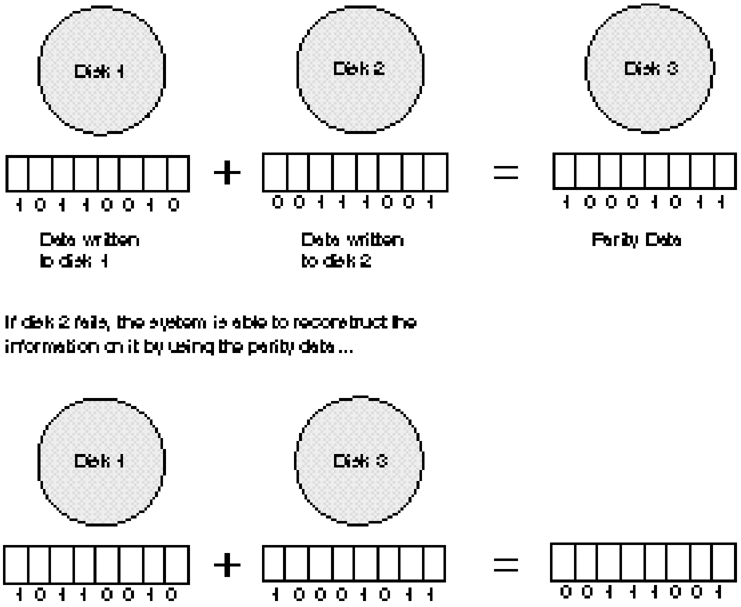
Striping with parity is based on the principle that all data is written to the hard drive in binary code (ones and zeros). RAID 5 requires at least three drives because this version writes data across two of them and then creates the parity block on the third. If the first byte is 00111000 and the second is 10101001, then the system computes the third by adding the digits together using this system:

1+1=0, 0+0=0, 0+1=1, 1+0=1

The sum of 00111000 and 10101001 is 10010001, which would be written to the third disk. If any of the disks fail, the process can be reversed and any disk can be reconstructed from the data on the other two. See figure 9.5 for an illustration of the process. Recovery includes replacing the bad disk and then regenerating its data through the Disk Administrator. A maximum of 32 disks can be connected in a RAID 5 array under Windows NT.

Figure 9.5

If Disk 2 fails, the system can reconstruct the information on it by using the parity data.



Choosing a RAID Level

When implementing a disk scheme, you have some options to consider. First, you must decide whether you are interested in performance gains (RAID 0) or data redundancy (RAID 1 or 5). Mirroring (RAID 1), for instance, enables the fastest recovery but results in a 50 percent loss of disk space. Likewise, striping with parity (RAID 5) is more economical but requires at least three physical disks and therefore provides more points of potential hardware failure.

Most network administrators prefer the RAID 5 solution, at least on larger servers with multiple drive bays. Because this level is a hybrid of striping and mirroring, it enables greater speed and more redundancy. Mirroring, however, offers the advantage of working well with non-SCSI hardware and is common as a fault-tolerant option on smaller, non-dedicated servers. Striping *without* parity should be reserved for workstations and servers on which speed considerations are paramount and possible downtime is an acceptable risk. See figure 9.6 for a graphical comparison.

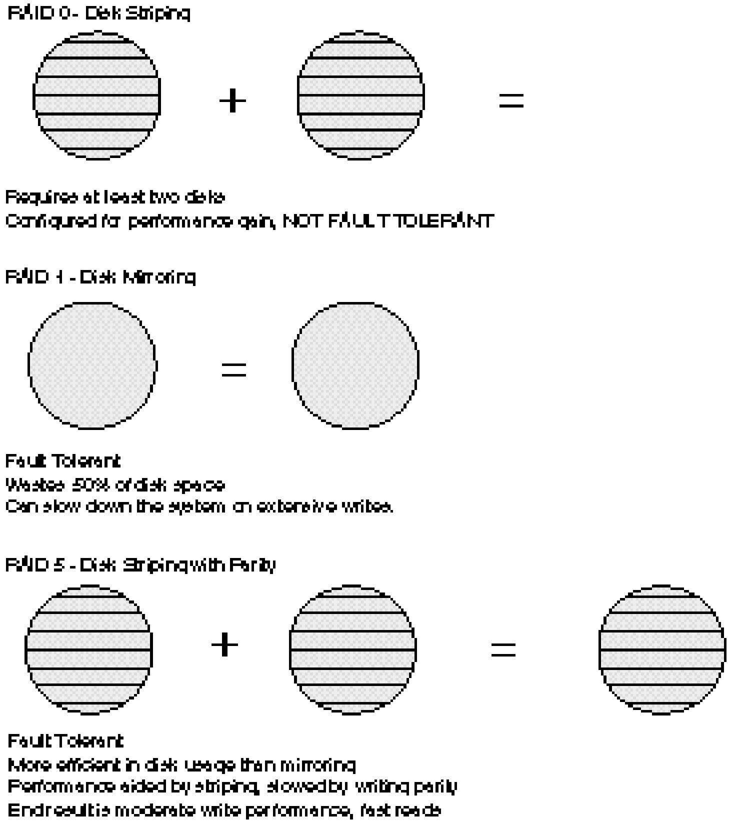

RAID 0- Disk Striping
+
=
Requires at least two disks
Configured for performance gain, NOT FAULT TOLERANT
RAID 1 - Disk Mirroring
=
Fault Tolerant
Wastes 50% of disk space
Can slow down the system on extensive writes.
RAID 5 - Disk Striping with Parity
+
=
Fault Tolerant
More efficient in disk usage than mirroring
Performance aided by striping, slowed by writing parity
End result is moderate write performance, fast reads

Figure 9.6

Different raid levels offer their own unique capabilities.

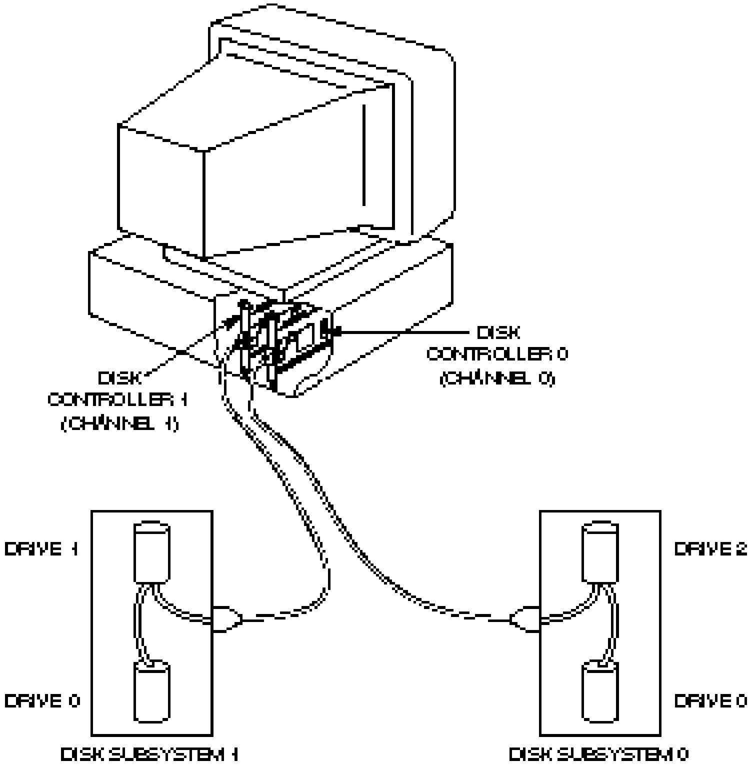
Disk Duplexing

In the event of disk channel failure (by a controller card or cable), access to all data on the channel stops and a message appears on the file server console screen (if your users don't let you know about it first). Even though drives can be mirrored, all disk activity on the mirrored pair ceases if the mirrored drives are connected to the same disk controller.

Disk duplexing performs the function of simultaneously writing data to disks located on different channels. As figure 9.7 illustrates, each hard disk in a duplexed pair connects to a separate hard disk controller. This figure shows a configuration in which the drives are housed in separate disk subsystems. Each subsystem also has a separate power supply. Disk duplexing offers a more reliable setup than is possible with mirroring because a failure of one disk drive's power supply doesn't disable the server. Instead, the server continues to work with the system that remains under power.

Figure 9.7

Disk duplexing simultaneously writes data to two disks located on different channels.



Working on the same channel is analogous to going to a baseball game when only one gate into the stadium is open. You can enter or exit through only one gate (channel) at the stadium (file server), and the crowd (data) can get backed up on both sides. If more than one gate (another channel) is open, though, the crowd (data) doesn't become backed up on both sides of the fence (file server or workstation).

Duplexing protects information at the hardware level with duplicate channels (controller cards and cables) and duplicate hard drives (refer to fig. 9.7).

Mirroring uses one controller card and two hard drives (refer to fig. 9.4). The point of failure for this setup is primarily the controller card or the cable connecting the drives to the controller card. Disk duplexing uses two controller cards and a minimum of one drive per controller card. The point of failure is reduced with duplicate hardware.

note

A number of different vendors also offer RAID protection at the hardware level on their server products. This protection is independent of the operating system, so if you really feel that RAID 5 on your Windows 95 workstation is a necessity, these software vendors might have a solution for you. Third-party products also permit the concept of redundancy to be taken to its logical extreme, resulting in the mirroring of entire Windows NT Server machines. This mirroring protects against the failure of virtually any single piece of hardware you can imagine, from a memory stick to a motherboard. Remember, though, that duplicate servers can get a bit expensive, so they are not recommended for everyone.

The previous sections examined a number of different disk configurations. Exercise 9.1 shows how you implement these RAID levels and other disk configuration options in Windows NT. The primary program for managing disk storage resources is the Disk Administrator, a tool that is usable only by members of the Administrators or Server Operators groups.

Summary

This chapter examined a number of options open to an administrator looking to provide data security and hardware redundancy for the network. Through the use of a regular backup plan, the installation of a UPS, and the implementation of a fault-tolerant disk scheme, you can help to ensure that your network will run as efficiently and safely as possible. Remember that there is no particular formula to use here; rather, you should follow a process of weighing costs against benefits. In the end, you want to provide the highest degree of safety for your critical data that you can achieve given your budget. Now test your knowledge of this chapter's topics by completing the exercise and answering some review questions.

Exercises

Remember that changes made to your disk configuration can have a serious effect on the system. Do not make anychanges in Disk Administrator unless you have carefullyplanned them previously!

Exercise 9.1: Exploring Windows NT's Disk Administrator

Objective: Explore the options available through Disk Administrator, such as establishing and breaking mirrored drives and creating or regenerating stripe sets with parity.

Estimated time: 10 minutes

To complete exercise 9.1, log on to a Windows NT 4.0 server or workstation with an account that has administrative authority. The server or workstation used can be a production machine—no changes will actually be made to the computer's configuration during this exercise.

1. Click Start, Programs, Administrative Tools. Then choose Disk Administrator.

2. Observe the Disk Administrator window and maximize it if it is not already in this state. The configuration of the disk or disks on your machine displays.

3. Click on one of the partitions on your screen. A dark black line appears around the partition, indicating that the partition is selected. Right-click on the partition and observe the available menu choices in the context-sensitive menu. Note that you can format the partition, change its logical drive letter, or examine its properties. If the disk is removable, the Eject option is also available.

4. Click on Partition in the Menu bar and examine the choices. Most of the choices are unavailable, but they include Create Volume Set and Create Stripe Set. You also can change your active partition in this Menu bar.

5. Click on Fault Tolerance on the Menu bar (Windows NT Server only) and observe that this menu enables you to establish and break mirrored drives, as well as to create or regenerate stripe sets with parity.

6. Feel free to explore further, and when you are finished examining the menus and options, close out of the Disk Administrator by clicking Partition, Exit.

Review Questions

The following questions test your knowledge of the information in this chapter. For additional exam help, visit Microsoft's site at www.microsoft.com/train_cert/cert/Mcpsteps.htm.

1. An incremental backup __________.

   A. backs up parts of the specified file that have changed since the last backup

   B. backs up and marks only those files that have changed since they were last backed up

   C. backs up the files that have changed since they were last backed up but doesn't mark them

   D. backs up the files that have changed over the course of a specified time period

2. A differential backup __________.

   A. backs up files that have changed since the last backup and doesn't mark the files as having been backed up

   B. backs up files that have changed since the last backup and marks the files as having been backed up

   C. copies all files that have been modified within a specific time period and marks them as having been backed up

   D. copies all files that have been modified within a specified time period and doesn't mark them as having been backed up

3. The best way to reduce the effects of extra traffic caused by a network backup is to __________.

   A. attach the tape drive directly to one of the servers

   B. back up each server to a nearby server

C. place the computer attached to the tape drive on an isolated network segment

D. back up the servers in ascending order of the size of the backup

4. UPS stands for __________.

   A. Unintentional Packet Switch
   B. Unfamiliar Password Sequence
   C. Unknown Polling Sequence
   D. Uninterruptible Power Supply

5. RAID level 5 __________.

   A. uses bit interleave data striping
   B. uses block interleave data striping
   C. doesn't use data striping
   D. provides parity-checking capabilities

6. RAID level 1 __________.

   A. uses bit interleave data striping
   B. uses block interleave data striping
   C. doesn't use data striping
   D. provides parity-checking capabilities

7. The difference between disk mirroring and disk duplexing is __________.

   A. disk mirroring is more reliable
   B. mirrored disks share the same disk channels
   C. duplexed disks share the same disk channels
   D. nonexistent

8. True or False: Implementing a RAID system eliminates the need for tape backup.

   A. True

   B. False

9. What is the minimum number of disks needed to configure a stripe set with parity on Windows NT Server?

   A. Two

   B. Three

   C. Four

   D. Seven

10. Network documentation should include which of the following?

    A. Hardware installation dates and specifications

    B. Copies of configuration files

    C. Software licensing information

    D. All of the above