COMPAQ

Enterprise-Wide Contingency Planning

TechNote

Includes information on:

- The overview of enterprise storage management solutions
- The explanations of the process of developing, implementing and maintaining an enterprise-wide contingency plan
- Network risks and potential threats to enterprise operations
- Measures to counter potential enterprise network risks
- Using backup technology as an enterprise storage solution
- Methods for countering potential threats to enterprise operations

First Edition (January 1998)
Part Number ECG044/1097
Compaq Computer Corporation

Notice

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL. THIS INFORMATION IS PROVIDED “AS IS” AND COMPAQ COMPUTER CORPORATION DISCLAIMS ANY WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AND EXPRESSLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, GOOD TITLE AND AGAINST INFRINGEMENT.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state, or local requirements. Compaq does not warrant products other than its own strictly as stated in Compaq product warranties.

Enterprise-Wide Contingency Planning

First Edition (January 1998)
Part Number ECG044/1097

Contents

Chapter 1
About This TechNote
Chapter Organization 1-1
Notational Conventions 1-2
Additional Resources to Use 1-3

Chapter 2
Introduction
Enterprise Storage Management Solutions 2-2
Data Protection 2-3
Developing a Contingency Plan 2-3

Chapter 3
Contingency Planning
Risk Analysis 3-2
Security Planning 3-3
Disaster Recovery 3-5
Benefits of a Contingency Plan 3-6
Summary 3-6

Chapter 4
Identifying Risks
Identifying Potential Threats 4-2
IS Staff 4-2
Undocumented Policies and Procedures 4-3
Users 4-4
Virus 4-5
Theft 4-6
Hardware Failure 4-6
Managing Disk Space 4-6
Software Failure 4-7
Catastrophe 4-8

Chapter 5
Assurance Measures

Security Policy 5-2
User Training 5-3
Server Options 5-4
Server Fault Tolerance 5-4
RAID Technology 5-5
Compaq Technology 5-8
Physical Security 5-10
Network Operating System 5-11
Server Configuration 5-11
Novell Replication Services 5-11
Novell Storage Services 5-13
Audit Trails 5-14
Backup Strategy 5-15
Assessing the Network 5-15
Software Applications 5-16
Planning for Disaster Recovery 5-17
Developing a Contingency Plan 5-18

Chapter 6
Using Backup Technology

Network Environment 6-1
Cheyenne ARCserve 6 6-2
Cheyenne JETserve 6-3
Tape Server Requirements 6-4
Server Configuration 6-5
Remote Backup 6-7
Backup Media 6-8
Backup Frequency 6-9
Managing the Backup Window 6-10
Open Files 6-10
Updates and Patches 6-11
Poor Planning and Execution 6-12
Data Verification 6-12
Developing the Backup Plan 6-13
Selecting Backup Data 6-13
JETserve 6-21
Backup Frequency 6-23

Summary 6-24

Chapter 7
Testing and Maintenance
Verifying Data Integrity 7-2
Real-Time Data Verification 7-2
Off-Site Media Storage 7-2
Preparation 7-3
Assembling a Recovery Team 7-3
Replacing Equipment 7-4
Testing 7-4
Test Plans 7-4
Frequency 7-5
Data Recovery 7-6
Maintenance 7-9

Appendix A
Enterprise Example
Acme Group - Background Information A-1
Server Configurations and Software A-3
Existing Policies and Procedures A-4
Risk Analysis A-5
Undocumented Policies and Procedures A-5
Users A-5
Theft A-6
Server Management A-6
Hardware/Software Failure A-6
Assurance Measures A-6
User Training A-7
Backup Software A-7
Conclusion A-8

Appendix B
NetWare 4 Server Memory Worksheet

Index

Chapter 1
About This TechNote

This TechNote provides suggestions for developing, implementing, and maintaining an enterprise-wide Contingency Plan. This document is intended for network administrators with a knowledge of Compaq server products and intraNetWare/NetWare.

This TechNote:

- Describes solutions for enterprise storage management
- Proposes steps for developing a Contingency Plan
- Identifies potential threats to enterprise operations
- Suggests measures to counter network risks
- Provides tips to aid in developing a backup solution

Chapter Organization

The chapters in this Compaq TechNote contain the following information:

- **Chapter 1:** Gives a brief summary of each chapter and general information about notations used.
- **Chapter 2:** Provides an overview of enterprise storage management solutions.
- **Chapter 3:** Gives an explanation of the process of developing, implementing, and maintaining an enterprise-wide Contingency Plan.
- **Chapter 4:** Addresses network risks and potential threats to enterprise operations.
- **Chapter 5:** Discusses measures to counter potential enterprise network risks.
- **Chapter 6:** Presents information for using backing technology as an enterprise storage solution.
- **Chapter 7:** Suggests methods for countering potential threats to enterprise operations.

Notational Conventions

Table 1-1 defines the text conventions used within this TechNote.

Table 1-1
Notational Conventions

Convention	Use
Enter	When instructed to enter information, type in the information using your keyboard.
FILENAMES	Names of files appear in uppercase italic in the DOS and other environments.
items of importance	Presents important or specific points of information. These items appear in italics in all chapters of this TechNote.
Key + **Key**	When you see a plus sign between two keys, hold down the first key while you simultaneously press the second key. For example, "Press the **Ctrl** + **Z** keys" means to press the **Ctrl** key while you simultaneously press and release the **Z** key.
Keys	Keys on your keyboard appear in boldface.
"new terms" and "prompts"	The first occurrence of a technical term, prompt, or reference to a word other than a command appears in quotes.
PROGRAMS, COMMANDS, UTILITIES, DIRECTORY NAMES, and DRIVE NAMES	These items appear in uppercase in the DOS and other environments.
Select *item* → *item*	Items separated by arrows indicate items you select in a sequence.

continued

Notational Conventions *continued*

Set, Get	Screen button labels appear in bold initial caps.
screen selections and *variables*	These items appear in italics in all chapters of this TechNote.
user input and screen display	Information you type exactly as it appears on the screen.
USER INPUT	Information you type exactly as it appears is shown in uppercase.

CAUTION: Indicates that failure to follow directions could result in damage to equipment or loss of information

IMPORTANT: Presents clarifying or specific points of information

NOTE: Presents commentary, sidelines, or interesting points of information

Additional Resources to Use

Use the following list of resources for more information on the various topics mentioned in this TechNote:

Binomial Disaster Recovery Web-Letter, Vol. 3, Issue 1, 9/6/95, editor: Jeff Williams, letter@binomial.com, http://www.binomial.com/news_01.html

Compaq White Paper: *ARCserve 6 for NetWare, The Complete Solution for Enterprise Backup/Recovery*

META Group, “Enterprise Backup Selection Criteria”, research note, 11/27/95.

“Bulletproofing your server”. Chernicoff, David P., PC Week: Oct. 4 1993.

“Cheyenne Brings DLT to NetWare Backup”. InfoWorld: Aug. 28, 1995

Homer, Blaine. “NetWare 4.1 Backup: Protect Your Network from Disaster”. NetWare Connection, July 1996.

“Managing Backups on a NetWare LAN”. PC User: Mar. 20, 1996 EMAP (UK)

"ARCserve Rallies". LAN Times: Mar 18, 1996. McGraw-Hill Inc.

"Storage Management Metamorphosis". LAN Magazine: Feb. 1996. Miller Freeman, Inc. 1996

"Network VAR Solutions: Backup, Part II". Network VAR: Feb. 1996 Miller Freeman, Inc. 1996

"Defusing the Backup Bomb: NetWare Backup Software". InfoWorld: Dec. 11, 1995. InfoWorld Publishing Company 1995

"Backing up the Enterprise". InformationWeek: Apr. 1, 1996. CMP Publications Inc. 1996

"Backup Exec: A Family Line". LAN Magazine: Apr. 1996. Miller Freeman, Inc. 1996

"A Question of NetWare Server LANtegrity". Network Computing: Apr. 1, 1996. CMP Publications Inc. 1996

"LAND-5's TA400 Maximizes RAID Tape-Backup Speeds". LAN Times: Mar 4, 1996.

"Internet Firewalls and Security". Enterprise Systems Journal: Jul. 1996 Cardinal Business Media, Inc. 1996

"Above and Beyond Firewalls". INTERNETWORK: Jul. 1996 Cardinal Business Media Inc. 1996

"Virus Crisis Intensifying: Study". Computing Canada: Jul. 4, 1996. Plesman Publications Ltd. (Canada) 1996

Chapter 2
Introduction

As distributed computing and mission-critical heterogeneous client/server environments prevail, organizations strive to find the perfect enterprise storage management solution. Enterprises rely on data and applications to operate their businesses. Any length of downtime is critical and can result in significant revenue loss.

Environments with multiple systems, serving the needs of individual departments while sharing information, challenge the issue of storage management. Centralizing and consolidating servers aids in managing data and applications. However, outdated software and associated data must be automatically archived yet be available when needed. Archiving dated applications helps to manage disk space more efficiently. Nonetheless, if newly installed applications begin to hinder productivity (and profits) due to programming errors, reverting to an older version may prove to be more economical than waiting for patches or revisions.

Backing up applications and data is not enough. A strategy must include security guidelines and provisions to be followed during data recovery. This information considers user access levels to applications, disk volumes, and files.

When disaster strikes—whether the result of a catastrophe or hardware failure—there is no time for speculation. The recovery window should not be hindered by media limitations and, when possible, should restore applications and data in the order of importance to the mission of the enterprise.

Though the benefits of prudent disaster planning and recovery do not materialize until catastrophe strikes, no enterprise can risk ignoring disaster preparedness. Most companies directly affected by a catastrophe do not recover from the damage without a Contingency Plan in place. The readiness of a prudent Contingency Plan aids in managing unexpected calamities.

This document guides you through a step-by-step process to develop, implement, and maintain a Contingency Plan for Compaq Servers running intraNetWare/NetWare. Backup and recovery strategies, hardware options, and backup and recovery software performance are examined to provide you with a method to create a sound Contingency Plan.

Enterprise Storage Management Solutions

Networks have grown into multi-platform information banks comprised of a variety of file types. Data volumes continue to increase in size and have become crucial to the enterprise growth. Information has become the backbone upon which many enterprises are run. The primary networking challenge today is to share all resources and data throughout an enterprise.

Enterprise networks give individuals in an organization access to information, in order to put it to the best possible use. To serve this ambitious purpose requires heterogeneous systems running in parallel and, in most cases, sharing data and applications remotely. For example, if a manager in Atlanta needs up-to-date information from a system in Los Angeles, that information should be readily available as if it were on the manager's own desktop computer. For many enterprises, it is crucial that the manager succeed in obtaining information as needed. The cost of downtime or inaccessibility could possibly result in a loss of revenue for the company. Only a smooth-functioning enterprise network can make all the information available at all locations, all the time. An organization's ability to compete and survive may depend on its people's ability to find, share, and use information.

An enterprise storage management solution is necessary for anything from a single server to a heterogeneous distributed multi-server network. Considerations such as disaster recovery, risk analysis, and security are essential when developing a strategic plan for protecting the organizational network. Recovering from a catastrophic disruption of service must be not only possible, but expedient, even if a media or hardware failure has occurred. Restoration of mission-critical files that were either inadvertently or intentionally overwritten must be operable. An organization must have a strategy for data management and recovery in place that permits any key Information Systems (IS) staff member to get the company back on track if necessary. In addition, that solution must also limit users to recovering data files that relate to their own productivity.

The proper solution must accommodate the growth potential of data volumes, manage multiple storage devices, and maintain the integrity of mission-critical data. As data grows and storage needs change in the enterprise, a variety of tools must be implemented to ensure continued enterprise operations.

Data Protection

Even with fault tolerance protection available in Compaq servers, backup and recovery software alleviates the impact of disastrous or even intentional data loss. IS managers sometimes view the task of data protection and security as overwhelming. However, with a Compaq server that initiates hardware pre-failure alerts, a solid Contingency Plan, and automated backup, enterprise data protection is an achievable goal.

Developing a Contingency Plan

In addition to natural and man-made disasters that threaten the productivity of an enterprise, equipment failures, computer viruses, and human error can also disrupt the continuity of mission-critical applications. Whatever the case, development, implementation, and maintenance of a strategy to keep an enterprise operating is essential. Chapter 3, *Contingency Planning*, describes the groundwork for preparing for potential disasters.

Pinpointing the Problem

The process of developing a Contingency Plan entails pinpointing the critical elements for enterprise operations and identifying the potential threats to those elements. Chapter 4, *Identifying Risks*, describes the potential threats to enterprise operations. Once you have identified the risks that pertain to you, you can decide what measures to take in protecting enterprise data and applications using the strategies provided in Chapter 5, *Security Planning*.

Choosing a Solution

There are several methods you can employ to protect enterprise data and applications. One of the solutions, backup, is the least expensive and does not compromise reliability. This process, discussed in Chapter 6, *Using Backup Technology*, addresses tape server requirements and techniques for using backup technology.

Preparing for the Worst

Chapter 7, *Testing and Maintenance*, helps you identify and avoid hardware problems with maintenance, and counter potential software conflicts. Proactive maintenance prevents hardware failures. Server options, such as Compaq Insight Manager, automate this process with pre-failure alerts. In addition, backup applications can verify that all of the essential server requirements are functional and configured properly before the backup process begins. Log files as well as other real-time performance information, may be reviewed to ensure that the network is operational and data is protected.

Chapter 3
Contingency Planning

Disaster recovery and enterprise recovery are analogous issues that involve contingency planning. A Contingency Plan provides safeguards against the potential loss of the assets that are required to continue the operations of an enterprise. Contingency planning involves identifying risks, evaluating protective measures, implementation, testing, and maintenance.

In today's enterprises, networks link many users to different types of devices, applications and information. This distributed access, though necessary to maintain productivity, leaves systems and the organizations that depend on them vulnerable to many threats. Natural disasters, intentional acts like virus attacks, and incidents such as malfunctioning hardware or software can occur.

Studies have shown that more than half of all companies that suffer damages related to data loss and application downtime eventually go out of business.[i] Even with insurance policies that cover equipment loss, the cost of data loss and downtime of mission-critical applications can be insurmountable.

Given the relationship between system availability and business productivity, contingency planning should be an integral part of an organization's design. However, not enough attention is paid to data recovery after a calamity. With the control and management of each network within a conglomeration handled by different individuals, enterprises are even more vulnerable. Every workgroup is subject to different organizational goals and requirements. Viewed separately, the importance of each subset is not always clear. Nevertheless, the operation of the enterprise is contingent on the efficacy of each element. The slightest change in one area can affect the entire system.

The development of a Contingency Plan works in the same way. It begins with identifying mission-critical applications and data. In other words, information that is crucial to the ongoing productivity of the enterprise. For single server networks this task may seem trivial. However, every aspect of the enterprise must be considered—from the scheduler to the information database. A solid Contingency Plan identifies the elements that the enterprise must have. A Contingency Plan encompasses three major phases:

- risk analysis
- security planning

- disaster recovery

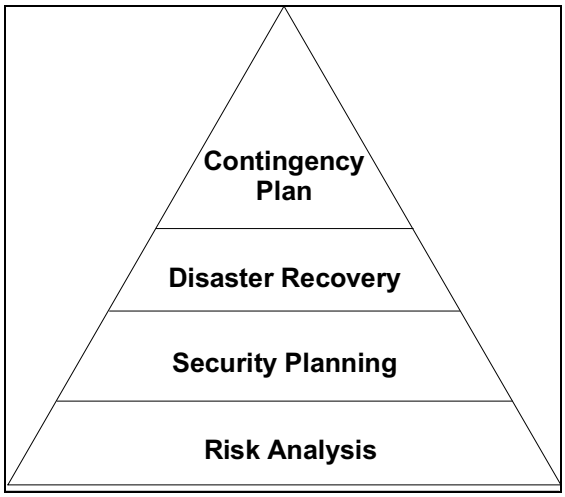

Figure 3-1. The Foundation of a Contingency Plan

The plan of action must take into consideration all possible scenarios. Most companies associate disaster recovery with natural or man-made disasters. However, it is the small-scale incidents enterprises face daily that pose the greatest risks. Computer viruses and security violations are prevalent problems in enterprise networks. These issues, in addition to other disasters, must be accounted for in a detailed document that can be comprehended by any key IS staff member in the organization.

Risk Analysis

The foundation of a Contingency Plan is a thorough risk analysis. A risk analysis is an organized process of identifying the vulnerabilities in enterprise operations. To find potential threats, you must know what you need to protect. This involves a detailed breakdown of business operations, beginning with analyzing *exactly* how the product or service is produced. This may seem trivial, but tracing business profits *backwards* can help to improve the business process and pinpoint the key assets in that process.

A risk analysis can identify undesirable events, measure the impact on operations, and estimate potential loss (whether monetary or market share). For example, one of the risks associated with inadequate user training of workstation security policies and procedures is leaving logged-in systems unattended: mission-critical data can be sabotaged or stolen. As a result, the business may lose profits and/or market share. Unlike an audit, which evaluates the current measures used to protect business assets, a risk analysis is a planning tool.

The National Computer Security Center (NCSC) coined the Risk Index[ii] to quantify a security metric to apply to networked systems. The Risk Index is the difference between the values assigned to data sensitivity level (x_1) and a user clearance level (x_2).

$$\text{Risk Index} = x_1 - x_2$$

These (x_1 and x_2) values are generally associated with document access (e.g. Confidential=1, Public=0, etc.). However, "access" should not be limited to data and applications, but should include hardware as well. Furthermore, values are defined according to the overall mission of the business.

Comparing the highest data sensitivity level of any component in the network to the lowest user clearance level yields the actual risk. This information is used in security planning for the enterprise network.

Security Planning

Security planning is, essentially, devising defense mechanisms for the vulnerabilities in the enterprise network. Using the information derived from a thorough risk analysis helps to create a complete security policy.

Security planning begins with management. It is a business decision that involves key managers minimizing profit loss due to any potential threat. The risk analysis identifies how profits will be affected should disaster strike. Managers can use this information to select countermeasures that are feasible.

The protective measures selected must collectively meet certain conditions. *Computer Security*[iii] outlines several performance stipulations such as:

- **Completeness:** There should be a strategy to counter every mission-critical risk.

- **Accuracy:** To maintain security, protective measures must be accurate and reliable. Each measure must fulfill its intended purpose yet avoid false alarms or deny access *only* to unauthorized users.
- **Simple:** The procedures for implementing the selected measures must be easy to use or well documented so key personnel can follow necessary steps to keep systems operational.
- **Maintainable:** The chosen measures should not require a level of maintenance that is not attainable by IS staff.
- **Continuity:** The protective measures must deliver the expected level of protection under the current operating conditions and include any anticipated changes.

- **Fail-safe:** Each measure must have an alternate or backup in case any type of malfunction occurs.
- **Cost-effective:** Expenditures must be justified in terms of the credible threats to be countered. You will have to get management approval and funding for your security plan. Without management involvement, it may be difficult to obtain funding for adequate protective measures.

No single method is sufficient to protect mission-critical information. You must employ a variety of methods to counter every threat to enterprise operations.

Disaster Recovery

Most people associate disaster with earthquakes, hurricanes, tornadoes, floods, or fires. However, a disaster is any event—whether unplanned or intentional—that causes damage. Catastrophes such as Hurricane Andrew, the Chicago flood, earthquakes, and the bombings of the World Trade Center and the federal building in Oklahoma are rare, frightening occurrences. However, catastrophes that impair enterprise operations happen nearly every day. The damage caused could result in data and/or equipment loss, which could inevitably result in revenue loss.

The horror stories that prevail vary in calamity, but all signify the same problem—inaccessibility of data. For example, despite a network administrator's efforts to mirror data on a primary server, unclear documentation followed by a critical user error rendered the data on the main server and the duplexed disk drive corrupted. This scenario illustrates "disaster" in relation to the enterprise network.

Disaster recovery refers to resuming business operations after any type of interruption. This includes:

- **Data Disaster:** Data is lost due to deletion or corruption
- **Hardware Failure:** Any component of the network has failed causing a halt in business operations
- **Site Disaster:** All vital components of the network must be replaced

Disaster recovery planning should vary according to the vulnerabilities of the organization. Contingencies based on equipment should be different for companies located in different regions of the country. For example, earthquakes would not be a concern for a Florida-based firm, while hurricanes would. On the other hand, disasters such as fire, flood, power-outages, equipment failure, and human error or sabotage, are vulnerabilities for every enterprise. With the exception of equipment failure[iv], nearly all disasters are unpredictable.

Benefits of a Contingency Plan

The utmost benefit of a thorough Contingency Plan is keeping a business in operation. More than one-third of the companies directly involved with the World Trade Center bombing were out of business within a year.[v] Revenue loss and missed business opportunities can have a tremendous affect on an enterprise during an extended period of system downtime. On the other hand, disaster resiliency can be a selling point. In fact, one of the brokerage firms in San Francisco that was able to keep functioning immediately after the 1989 earthquake is said to have gained market share.[vi]

Contingency planning also helps an enterprise re-examine how the integral elements of the company function. Determining what is necessary to resume productivity requires examining each stage in the business process, which can provide management with insight as to how productivity can be improved.

Having an established Contingency Plan in place when a situation arises eliminates guesswork and fumbling. This prevents lost time and productivity, which could result in lost revenues.

Summary

The primary goal of all contingency planning is to minimize unforeseen system downtime. A Contingency Plan is like an insurance policy because the actual cost of business downtime is not comprehended until disaster strikes.

Contingency planning should be an integral part of every enterprise. Components of the plan must be addressed as part of daily operations rather than during disaster recovery. Developing a Contingency Plan allows an enterprise to examine each integral unit and its contribution to overall operations. This examination exposes the organizational threats to productivity, and aids in identifying the types of measures that can be put into effect to counter them. In addition, should a disaster occur, an existing Contingency Plan can help expedite the process of returning the enterprise to normal operation.

With such a variety of issues to address, developing a contingency plan may seem overwhelming. Contingency planning is a business process that requires careful examination of the overall operation of the enterprise: the contribution of each unit to the continuity of productivity. This can be a penetrating issue that requires the propulsion and support of upper management.

---

[i] CommunicationsWeek. August 28, 1995. n572 p39(3). Liebmann, Lenny. Providing a safety net.
[ii] The NCSC publishes the "Yellow Book" which provides detailed information on the Risk Index.
[iii] Computer Security. Carroll, John M. 2d ed. Butterworth. 1987.
[iv] Compaq servers feature the Compaq Insight Manager, which includes pre-failure alerting for disks, memory, and processors.
[v] Liebmann, et al.
[vi] Liebmann, et al.

Chapter 4
Identifying Risks

No enterprise storage management solution stands alone: it is part of the organization's overall security policy that defines all aspects of its perimeter defense. To be successful, organizations must know what they are protecting. The Contingency Plan must be based on a carefully conducted network risk analysis and assessment. If an organization does not have a detailed Contingency Plan, the most carefully crafted protective measures can be circumvented to expose the entire network to unperceived risk.

The first step in developing a Contingency Plan requires a thorough examination of the network to pinpoint the entities that are critical to overall enterprise operations. This information helps to identify the potential threats and vulnerabilities associated with each element. The critical components of enterprise operations and their associated risks are listed below.

- **Host Server:** Exposed to the most risks due to links to other systems and workstations. On the other hand, network operating systems provide more built-in protection than most stand-alone systems and workstations.
- **Remote Server:** Exposed to the same risks as a host server, yet application of preventive and assurance measures for data integrity can be challenging if the server is located off site. Physical access to the equipment is difficult to monitor. Furthermore, any disaster could halt productivity if IS staff are nonresident.
- **Clients/Workstations:** Since security mechanisms are difficult to impose and manage, clients are exposed to a number of risks and can be a risk to the server. Even though mission-critical data should not reside on workstations, network and data access violations can still pose a threat without the proper network security controls.
- **Stand-alone Systems:** Like network clients and workstations, operating system software on stand-alone systems generally does not provide the same security mechanisms. However, under some circumstances, stand-alone systems can circumvent potential threats associated with transferring sensitive data over a network. As a result, these systems require a different set of standards and assurance measures for data security and integrity.

- **People:** IS staff, for example, also ‘store’ mission-critical information. Like clients/workstations, people are exposed to multiple risks and can be a risk to the entire network.

Identifying Potential Threats

Enterprises that do not prepare for potential threats put their businesses at risk. The value of the information processed by enterprise networks is directly related to the threat to the availability, integrity and confidentiality of that information.

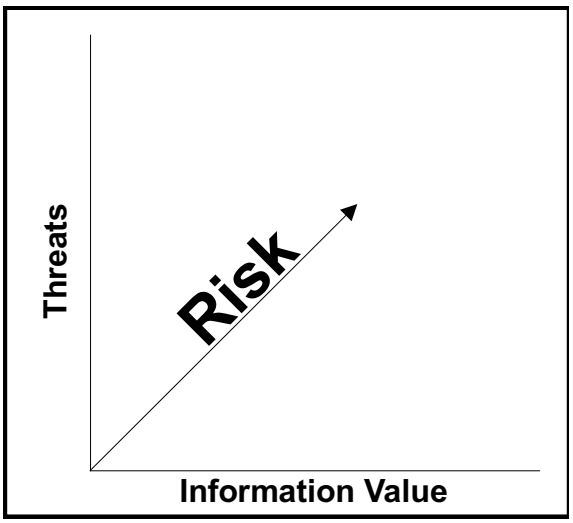

Figure 4-1. Relationship Between Information Value and Threats

Every identifiable threat is related to the potential access to the system. Most people consider intrusion to be the most harmful threat to the enterprise network. However, physical access to equipment and the denial of access can also be critical threats to enterprise operations.

IS Staff

The individuals who maintain the enterprise network can also cause complete disruption of mission-critical operations. Upgrading a server's operating system or mission-critical software can cause delays if not properly planned. Such critical changes should take place after normal work hours. Users should be informed of possible network downtime, should problems surface.

User interface changes also require communication to the end-user community, even if user login and data access have been verified. Any change in the environment can impede productivity and, as a result, affect profits.

Undocumented Policies and Procedures

Network security begins with clearly defined policies and procedures. This task involves a collaboration of IS staff, management, and auditors. IS staff have the background knowledge related to the capabilities and limitations of the network operating system and other software applications. Management has a clearer vision of the goals of the organization and the power to authorize funds to improve network security if necessary. Auditors have expertise in audit controls and risk analysis. Cooperation among these divisions can yield a comprehensive set of policies and procedures.

Network policies and procedures must be updated as hardware, software, or information sensitivity changes. These updates must be communicated to every employee in the organization and available through a variety of media. Some examples of these types of updates are:

- Formal training for new employees
- Ongoing newsletters circulated electronically and posted in each department reiterating policies and procedures for protecting critical information
- Electronic mail and hard-copy postings alerting employees of detected computer viruses

Employee training and awareness can limit the threat of undocumented policies and procedures. This imposes a certain amount of responsibility on the users who must bear the consequences of violating existing policies and procedures.

Users

Violating Rules and Procedures

Although network administrators cannot prevent users from sharing passwords, there are controls that can be administered to limit unauthorized access to data and networks. Network operating systems can be configured with login restrictions that limit multiple logins by a single user and require users to change their passwords periodically. In addition, audit trails can be used to monitor login locations if necessary. Inconsistencies may signal possible policy violations.

Leaving workstations and media with sensitive data unattended can also be a threat to enterprise operations. At the workstation level, utilities such as screen savers with password protection aid in safeguarding access. However, strict adherence to procedures is required for protecting media. Sensitive information should be stored on portable media only under special circumstances. Otherwise, mission-critical information should reside on the server where it is better protected by network operating system mechanisms and other security utilities.

Corrupting or Deleting Data

Sensitive data can be modified or deleted by users with proper access. Whether the act is intentional or accidental the result is the same: no access to mission-critical information. Network operating system mechanisms can be implemented to prevent such predicaments, but other assurance measures are required to counter these problems should they arise.

Inadequate Training

Saving mission-critical data on a workstation is a significant threat to enterprise operations not only for security reasons, but because responsibility for backup is often left up to the user. There are software applications that can backup workstation data, but user cooperation is still required. Without a thorough examination of enterprise operations, such as how data is processed, who processes it, and the affect the data has on profits, some users may unknowingly save mission-critical data on their workstations.

With clearly defined enterprise policies and procedures and mandatory training, users can better understand their role in overall enterprise operations and their responsibility for managing mission-critical data.

There may be some situations that require saving mission-critical data on a client desktop computer. This requires the user to consistently back up necessary data. If the user is not aware of backup procedures, this poses several risks:

- Data may not be backed up regularly
- The backup media may not be stored in a safe place
- The backup media could be mislabeled and inadvertently written over
- The backup media may not be accessible if that user cannot be located

Virus

Computer viruses range from benign to destructive and can have the same disruptive effect on network operations as hardware failure. With servers connected to the Internet, enterprise servers are even more susceptible to infection. A computer virus can originate from a variety of sources such as documents, electronic mail, and programs. The damage can range from the small annoyance of not being able to save a Microsoft Word document, to completely destroying data on a hard disk.

The National Computer Security Association (NCSA) conducted a study which revealed that the chance of a virus attack averages about one virus per 100 PCs every month.[i] The study, "1996 Virus Prevalence Survey" reported that over 90 percent of organizations that have 500 or more PCs experience a computer virus incident every month. The survey found the average downtime of an infected server to be 5.8 hours. The average recovery required an average 44 hours.

Statistics like those reported by the NCSA could cost some enterprises millions of dollars for server downtime. Any organization with a small and/or overloaded IS staff would be rendered helpless in trying to disinfect the network, contain the virus attack, and manage the daily operations of other systems.

Theft

Computer equipment theft can prove to be disastrous. Not only does the company have to deal with replacing equipment and settling insurance claims, but also with recovering lost data and software as well. Nonetheless, theft should not be solely equated with burglaries. Employee theft of hardware and software, as well as divulging company information, also account for a high percentage of technological larceny. In addition, software piracy exposes a company to additional profit loss. Violations can result in lawsuits and fines. This could seriously damage the business reputation and affect the market share of a company.

Security systems, off-site storage of backup media, and strict enforcement of enterprise policies and procedures are some of the preventive measures that can be used to counter the risk of theft.

Hardware Failure

Despite various forms of fault tolerance available today, hardware failure is still a possibility that plagues many network environments. Though some equipment failures are more serious than others (e.g. a network adapter versus the server fan), they both result in downtime. Data inaccessibility can cause a company to lose money every second there is a halt in productivity.

In addition to causing server downtime, hardware failures can also result in data corruption. A brownout, disk failure or tape drive failure can render files unrecoverable if the interruption occurred during a write operation.

Managing Disk Space

With mission-critical data, user files and electronic mail, server disk space must be managed closely. A server running out of disk space can deter saving a new or revised file on the server or prevent real-time database information from being updated.

Disk Compression

intraNetWare/NetWare is configured with disk compression enabled by default. Once a NetWare volume is created, the disk compression setting can not be changed without deleting the volume. With disk compression enabled, files that have not been accessed within a defined period of time, are compressed if there is a disk-space savings of at least 20 percent. This is the default setting that determines the minimum percentage a file must compress in order to remain compressed. The configuration parameter, Set Minimum Compression Gain, defines this value.

intraNetWare/NetWare Suballocation

Block suballocation regulates disk storage at the time a file is written to disk. Files that are larger than the volume block size are broken into the smallest segments possible and stored in preassigned blocks that only contain file fragments. With block suballocation enabled, there is hardly any wasted disk space and the server utilizes less RAM.

Before enabling block suballocation on a volume, make sure there is at least 10-20% of free space and at least 1000 free blocks. Otherwise, the lack of free disk space can result in suballocation "thrashing," which may eventually interrupt other processes and cause an increase in the Packet Receive Buffers and File Service Processes. When the server reaches the maximum Packet Receive Buffer, connections are lost and users are unable to login.

Software Failure

User productivity and enterprise operations can be greatly hindered by software failure. Mission-critical applications such as real-time databases are rendered inaccessible for data perusal or updates. In addition, software glitches can corrupt data or prevent data from being accurately updated.

Failure of commercial software is even more catastrophic because the problem cannot be readily fixed by on-site IS staff. This could require a complete change in information processing and a tremendous shift in business operations, which inevitably hinders productivity and affects profits.

Catastrophe

Catastrophes, whether natural (fire, flood, hurricane, or earthquake) or violent (terrorist acts), are rarely foreseeable and difficult to prevent. Some geographical regions are more prone to certain catastrophes than others, but every enterprise is vulnerable. Preventive mechanisms and forecasting helps, but the key to addressing any disaster is resiliency.

---

[i]Virus crisis intensifying: study. Computing Canada: Jul. 4, 1996 Plesman Publications Ltd. (Canada)

Chapter 5
Assurance Measures

When it comes to the design and deployment of a protective measure, there is no single "correct answer." Each organization is influenced by many different factors, such as its Contingency Plan, the technical background of its staff, cost factors, and the perceived threat of attack.

A comprehensive Contingency Plan consists of a variety of assurance measures. Each measure contributes to the overall effectiveness of the strategy. These measures include:

- Strict adherence to the existing security policy
- Mandated user training
- Use of available server options to forestall hardware failure
- Optimally configured Network Operating Systems (NOS)
- Adherence to a backup strategy

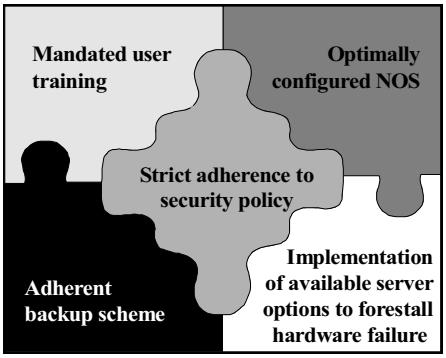

Figure 5-1. Pieces of a Comprehensive Contingency Plan

Enterprise operations' continuity is not accomplished through the technical expertise of the IS staff. In fact, effecting the Contingency Plan is primarily a management issue, so the security policy must be undertaken by management. Based on management's assessment of the importance of information and the systems in which the data is stored, IS staff can determine what controls are necessary at the operating system level. The amount of acceptable data loss in the event of a disaster is also management's decision. Once this business process is clearly defined, the measures to assure continuity can be explored and implemented.

Security Policy

Computer security consists of measures taken to protect data against unauthorized access to software applications and data. The biggest threats to data integrity are not natural disasters or terrorists, but are within the enterprise. Disgruntled employees and dishonest individuals account for the majority of breaches to network security.

The intraNetWare/NetWare operating system does incorporate security features to control data availability and impose network restrictions. However, NetWare alone cannot completely protect organizational servers from violations.

The purpose of planning network security is to reduce the likelihood of potential losses. Losses can come from hazards related to the environment, hardware and equipment failure, software application errors, accidents, or even intentional acts. The contingency plan implements controls to prevent such losses. These controls include establishing policies for authenticating users and maintaining procedures to follow under emergency conditions.

Security in a Contingency Plan entails:

- **User Login and Authentication:** A password/user ID scheme is recommended to avoid unauthorized access when users try to log onto applications and servers.
- **Workstation Security:** This involves ensuring that the right people use a PC to do authorized things. Elements of workstation security include screen locking when the machine is unoccupied for sustained periods of time, partitioned access to resources for multi-user machines, and anti-virus software.

- **Distributed Security:** This includes using Application Programming Interfaces to ensure data confidentiality and data integrity between application components in distributed applications. It also involves prepping the network for transmission of encryption keys and passwords.
- **Physical Security:** This area involves implementing rules for access control to electronic and physical networked resources.
- **Internet Security:** This includes firewalls, which are the barriers between private nets and the Internet.
- **Security Management:** Beyond hardware, technologies and tools, a well thought-out and explicit security policy should be disseminated and enforced. This entails identifying critical resources, performing a risk analysis, and defining rules and procedures relevant to your findings.

After defining the necessary controls for managing the enterprise computing operations in a security policy, you must communicate this information to the user community. A Contingency Plan is futile if users do not know that security policies and procedures exist. Users must also be informed of the value of the information they access and the potential harm they can cause due to carelessness, ignorance, or blatant disregard for policy and procedure.

User Training

Untrained users make mistakes that can cost the business money. These errors can include leaving media with sensitive data unattended, not securing a workstation, sharing passwords, or even engaging in casual conversation and revealing confidential company information. These mistakes tend to happen because users simply do not realize the value of the information to which they have access or the potential harm they can cause to the company as a result of disclosing that information.

Enterprise-wide training should explain policies and procedures for protecting company information. Employees must be informed of their responsibility to adhere to company policy and understand the consequences for failure to abide by the rules.

Training must occur regularly to accommodate new employees. On-going policy updates should be communicated through every medium available. In addition, there should always be hard-copy documentation available for perusal as well as postings in each department.

Computer security standards and guidelines provide for the effective integration of data recovery measures in an overall Contingency Plan. Having security training and awareness in place helps to ensure that the persons who must access computer resources are aware of proper contingency plan procedures and guidelines.

Some of the guidelines users should also be familiar are:

- Be familiar with information restrictions and enterprise procedures.
- Know the marking requirements for data, e.g. confidential.
- All storage media must be properly labeled.
- Know the actions to take in the event of a disaster.
- Know where to find information on how the system is configured and how it is intended to operate.

These measures not only aid in preventing unauthorized access, but can also limit accidental file deletions and the spread of computer viruses.

Server Options

Before putting a contingency plan in effect, consider the variety of server options available to safeguard data and applications. Compaq servers, for example, offer the Compaq Recovery Server Option Kit. This option kit switches operations of a primary server, if it fails, to either a standby or an on-line recovery server. Other options available are Server Fault Tolerance (SFT III) and RAID technology.

Applications that warn of potential hardware failure also aid in data protection. Compaq servers include a set of fault-management protection features. Finally, a backup and recovery system safeguards data if all other options fail.

Server Fault Tolerance

The goal of Server Fault Tolerance (SFT III) is to continue to operate even in the event of a hardware or software failure. This fault tolerance requires an on-line, real-time backup solution that uses data- and server-mirroring techniques. With data mirroring, data sent to a primary server is duplicated onto a secondary server. As files are updated or deleted on the primary server, the secondary server receives the same data.

Server fault tolerance is available with manual or automatic switch-over. Of course, manual switch-over does not indicate 100-percent uptime because the network manager must reassign all of the primary server tasks to the secondary server. Automatic switchover, which requires identical server hardware, is quite expensive, but a reliable way to keep enterprise operations going if a hardware failure occurs.

NetWare SFT III is a server fault-tolerance product that provides 100-percent uptime with a switch-over process that is transparent to the end-user community. NetWare SFT III does, however, require that two servers be identical in hard disk capacity, RAM, network adapters, and other options such as CD-ROM drives.

RAID Technology

RAID, which stands for Redundant Array of Inexpensive Disks, is a technology that incorporates fault-tolerance methods to protect data if one of the disks in the storage system fails. RAID technology can be implemented through a hardware, operating system, or third-party software solution. The hardware solution permits more of a variety of levels of fault tolerance and yields the best performance. Operating-system RAID solutions only offer disk-mirroring or disk-duplexing. The use of third-party software entails a RAID program that manages the multiple hard disks connected to your server. This implementation has revealed problems with stability and performance, especially for a heavily used server.[i]

A collection of hard disk drives grouped together form an array of physical drives. An array can also consist of one or more logical drives that are spread or ‘striped’ across the array of physical drives. Operating systems view the logical drives in an array as a single, contiguous storage space although it is made up of parts of several physical drives.

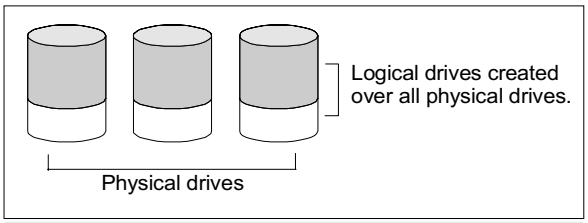

Figure 5-2. RAID 0 Drive Array with Three Physical Drives and Two Logical Drives

RAID technology embraces six levels: 0 through 5. RAID 0 only stripes data across multiple drives and does not provide data redundancy. Figure 5-2 is an example of RAID 0 technology.

RAID 1, disk-mirroring, requires two drives with the same amount of disk space. If a disk drive fails, data requests continue to be processed without data loss or downtime. The difference between disk-mirroring and disk-duplexing is the added redundancy that duplexing provides. With duplexing, each physical drive is located on a separate controller.

Disk-mirroring and disk-duplexing can be implemented through NetWare without any additional software. The main advantage of using drive array technology over disk-mirroring or -duplexing, however, is the ability to accommodate large amounts of data. Mirroring several gigabytes of data would prove to be an expensive data protection measure.

RAID 2, transfers bit-interleaved data across a group of disks and generates an error-correction code that is stored on a separate drive. However, significant computing power is required to perform this form of striping, which is not practical for most LAN applications.

RAID 3 distributes data across multiple disks. Data is striped at the byte level with one disk dedicated to storing parity information. In the event of a disk failure, the parity information is used to reconstruct the data. However, the dedicated parity drive reduces the amount of available storage. Furthermore, RAID 3 requires that all of disks in the array be rotationally synchronized, which affects performance.

RAID 4 also dedicates a single drive for parity information but stripes data at the block level. RAID 4 yields slightly better performance than RAID 3 because it does not necessitate synchronization of the disks.

Figure 5-3. RAID 4 Fault Tolerance

RAID 5 offers the best compromise between fault tolerance and price. This level of RAID technology not only stripes data across disk drives, but also distributes the parity or check data across drives. RAID 5 provides the ability to rebuild data immediately if a drive fails.

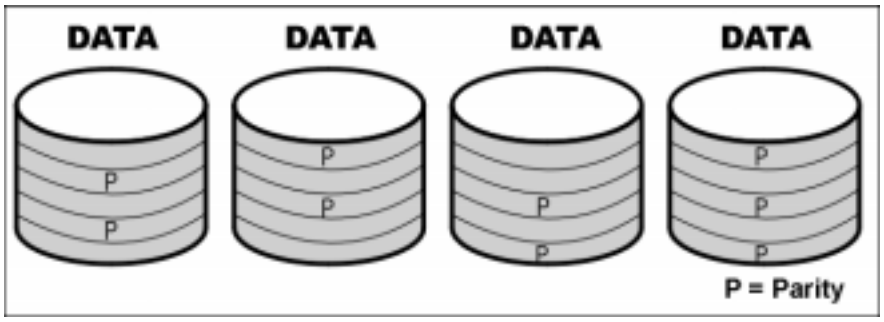

Figure 5-4. RAID 5 Distributed Data Guarding

The Compaq SMART SCSI Array Controller and the Compaq SMART SCSI-2 Array Controller, along with the Compaq Array Configuration Utility, support RAID levels 0, 1, 4 and 5. Further data protection can be achieved by assigning an on-line spare to any RAID-1, RAID-4, or RAID-5 configuration. The following table describes and compares the RAID level characteristics.

Table 5-1
RAID Level Characteristics

	Distributed Data Guarding (RAID 5)	Data Guarding (RAID 4)	Mirroring (RAID 1)	No Fault Tolerance (RAID 0)
Usable Disk Space*	67% to 93%	67% to 93%	50%	100%

Disk Space Formula (n = no. of drives)	(n-1)/n	(n-1)/n	n/2	n
Parity and Data Redundancy	Parity distributed over each drive	Parity distributed over each drive	Duplicate data	None

continued

RAID Level Characteristics *continued*

Minimum Number of Drives	4	3	2	1
Comments	Tolerant of single drive failures. Higher performance than RAID 4. Uses the least amount of storage capacity for fault tolerance.	Tolerant of single drive failures. Like RAID 5, uses the least amount of storage capacity for fault tolerance.	Tolerant of multiple, simultaneous drive failures. Higher performance than RAID 4 or 5. Uses the least amount of storage capacity for fault tolerance. Requires an even number of drives.	Best performance but data is lost if any drive in the logical drive fails. Uses no storage capacity for fault tolerance.

NOTE: All Drives are the same capacity

Compaq Technology

Server features such as Compaq Recovery Server Option, Automatic Server Recovery, Advanced Error Correcting Code (ECC) memory, Compaq Insight Manager and PCI Hot Plug are examples of server fault management provided by Compaq.

Compaq Recovery Server Option

The Compaq Recovery Server Option provides support for the standby recovery server. This server fault-tolerance option is more affordable than other implementations. With this configuration, two Compaq ProLiant Servers are attached to a common set of ProLiant Storage Systems, which stores a single copy of the operating system, applications, and data. If the primary server fails, the SCSI bus in the storage system is automatically switched from the primary to the standby server. The standby server then boots, and clients are back online without administrator intervention.

Automatic Server Recovery

Automatic Server Recovery (ASR) is a feature which allows the server to reboot to the operating system. ASR provides a cost-effective means of minimizing unplanned downtime since automatic reboot of the server brings users back on-line with minimal interruption of service.

Advanced Error Correcting Code

Compaq Fast-SCSI-2 drives use Error Correcting Code (ECC) logic to provide protection from data loss. During a write operation, ECC bytes are calculated and are written to the drive with the data. During a read operation, the data and the ECC bytes are read back. The ECC bytes are then recalculated on the data and are compared. If the ECC bytes match, the read is successful. If the ECC bytes do not match, the data can be reconstructed using the original ECC bytes. Faulty sectors, identified by mismatched ECC bytes, are remapped using Automatic Read/Write Reallocation. This ensures that the data is not written to the defective area.

The Compaq Health driver provides early warning and logging of impending component or subsystem failures. The Corrected Error Logging enables you to schedule maintenance down time to replace memory that is beginning to cause parity errors. With AECC memory, these errors are corrected without interrupting normal operation, and the memory module, which is generating the corrected errors, is logged in the Event Log. View this information using the Compaq Insight Manager while the server is running or the Compaq Diagnostics Utility after NetWare has been brought down.

Compaq Insight Manager

Compaq Insight Manager is a server management application that helps you identify potential hardware problems and manage the server locally or remotely. It provides fault prediction and tracking for storage and memory subsystems, DAT and DLT tape drives, and Uninterruptible Power Supplies. This enables it to receive Simple Network Management Protocol (SNMP) traps from backup and recovery applications such as ARCserve.

PCI Hot Plug

PCI Hot Plug technology permits hot swapping components and online capacity expansion of system components. These include power supplies, storage devices and, in some cases, hot swappable controllers through expensive proprietary buses and adapters. This eliminates the need to power down the system to replace a failed component. PCI Hot Plug technology not only reduces unplanned downtime, but can, in some cases, totally eliminate planned downtime. PCI Hot Plug technology has many features and benefits that include:

- **High Availability:** Particularly for enterprise environments, the ability to replace or upgrade a network or other I/O controller board while a system is operating is a substantial benefit. For instance, this allows replacement of a failed network controller board while the remaining network boards provide uninterrupted service.
- **Increased Storage Capacity:** Another benefit is the ability to add new network or I/O controller boards while a system is operating. For example, adding an array controller attached to an external storage chassis increases storage capacity without any down time.
- **Industry Standard:** Industry standard PCI Hot Plug has multiple benefits. Multiple system providers, operating system suppliers and adapter board vendors can implement hot plug. This gives you investment protection if the proposed implementation is compatible with existing PCI standards. Therefore, any changes made to system hardware, operating systems, or adapter drivers should not affect functionality in an existing system.
- **Backward Compatibility:** There is no need to overhaul entire systems just because certain components are hot plug capable. The technology is fully backward compatible.

Physical Security

The physical location of a server is another consideration. Hardware and software options are excellent means to counter threats, but these methods do very little to prevent destructive attacks or theft of equipment. Locking a server behind closed doors is the only way to protect the enterprise against nefarious attacks. This also applies to removable drives, tapes, printouts and sensitive documentation.

Network Operating System

The network operating system includes various utilities and controls to aid in protecting the network environment. However, these utilities serve little purpose if your server is not optimally configured.

The Compaq TechNote, *NetWare 4 Performance Management*, provides configuration and performance guidelines for NetWare 4.1 based on Compaq integration and performance testing. This TechNote also describes how different configuration options can affect the performance of your Compaq server, and provides you with a foundation for network performance analysis and management. This information can also apply to intraNetWare/NetWare 4.11.

Server Configuration

You must configure your server with an adequate amount of system memory to ensure optimum performance. NetWare 4.1x accommodates its memory protection schemes by using more cache than previous versions of NetWare. This results in more efficient memory allocation and a reduction in fragmentation. In addition, a large amount of system memory can compensate for an overworked hard drive subsystem.

The Appendix B provides formulas to calculate the system memory required for your server. These formulas include considerations for loading NetWare Loadable Modules (NLMs) that use CLIB.NLM and BTRIEVE.NLM, which are required by most third-party backup and recovery applications.

Novell Replication Services

One of the greatest challenges to managing a Wide Area Network (WAN) is transmission speed and bandwidth. WANs typically lease communications circuits, which generally provide transmission rates in the range of 56 kbps to 45 Mbps, or sometimes considerably less (e.g. 28.8 kbps or slower). Distributing critical data and applications across long distances can be expensive and time consuming. Furthermore, availability is susceptible to outages and WAN faults.

One solution to combat this problem is replication, in which information is duplicated from a source server to other locations to give local accessibility. This puts information closer to end users and results in faster access and less WAN traffic. Unfortunately, manually implementing this process is very time consuming for system administrators.

Novell Replication Services (NRS) automates the replication process. NRS replicates and synchronizes files and volumes from one server to any number of other servers on a local area network (LAN) or WAN. The scheduling facility provided by NRS allows administrators to schedule replica synchronization during off-peak hours, which reduces WAN traffic while rapidly delivering consistent information closer to users.

NRS requires a single NetWare Loadable Module (NLM) to be loaded on each server that is included in the replication process. The master server is the server from which objects are replicated, and the servers that file objects are replicated to are replica servers. A link server is a replica server that is configured as a master server with its own replicated servers linking two replicated regions.

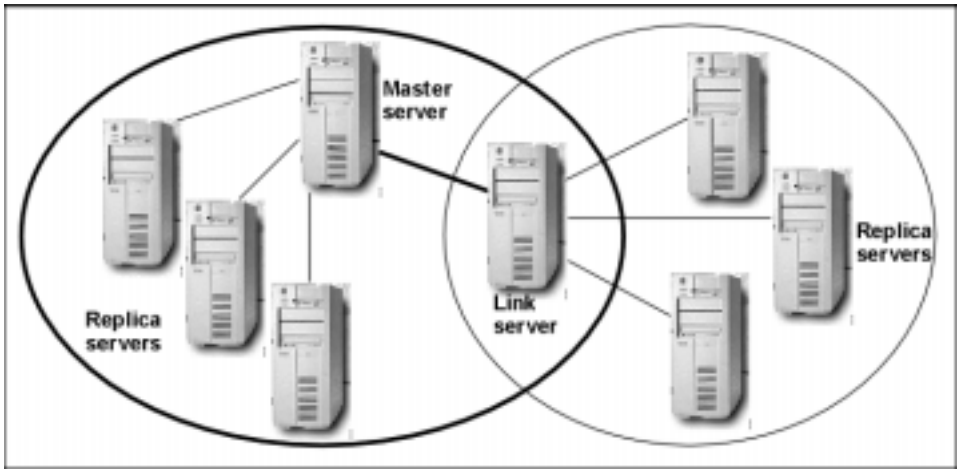

Figure 5-5. A Master Server Replicated to a Link Server that is Connected to Replica Servers

After NRS has been installed, the servers configured, the replication set defined, and the synchronization schedule set, no intervention of the network administrator is required. Like any other server application, a periodic review of the logs is necessary.

Replication operations are transactional to ensure against partial file updates if the network fails. If a network connection fails during synchronization, Novell Replication Services automatically continues synchronization, without re-sending files, when the connection becomes available. Auto restart after failure feature ensures that replication processes are completed even in the event of a failure.[ii]

Novell Replication Services works with Novell Directory Services (NDS) to synchronize the security rights along with the files. NDS ensures that only those users who have rights are permitted to access sensitive data, regardless of the user's login location or the location of the data. NRS is a Snap-In to the NWAdmin utility for easy administration.

This tool can help to counter the risks associated with WANs. With information closer to end users, data availability is improved and no longer subject to disruption due to WAN faults or performance constraints.[iii]

Novell Storage Services

Novell Storage Services (NSS) is the next-generation storage/access system being developed by Novell. At the time of this writing, NSS is in Alpha stage, and is scheduled to be delivered as part of the next intraNetWare release.[iv]

One of the three basic goals of NSS is to eliminate current NetWare file system limitations. The NetWare 4.11 design uses File Allocation Table (FAT) file system organization. With this implementation, the amount of memory required for a server is based on the number/size of files. NSS counters these memory and disk space restrictions by mounting any size volume with as little as 32 megabytes of memory. This feature will help to compensate for a restricted server hardware budget, faced by some companies, which necessitates accommodating a growing number of users and application requirements.

Another NetWare 4.11 file system drawback is the amount of time required to mount a volume. In general, the time required to mount a volume is linear to the volume size and the number of files. Furthermore, after a crash, NetWare 4.11 volumes must be scanned and repaired with the Novell VREPAIR utility. This process can take hours to complete, during which users are unable to access data. NSS permits rapid volume mount and repair times. Volumes are mounted in seconds regardless of their size, which can counter the potential hardware failure threat that every enterprise is vulnerable to.

Audit Trails

An audit trail (or activity log) provides a list of events that have transpired on the server. From user authentication to application usage, an audit trail can provide an administrator with a log of all server activity. This helps in regulating security policies and procedures to determine if adequate access controls are in place or if the current procedures require modification.

Like any other tool, the audit trail must be implemented carefully and tailored to meet the data and security requirements of the organization. Simply enabling all audit settings in NetWare 4.x can be overwhelming and defeat the purpose of using the tool in the first place. Because the NetWare AUDITCON can audit everything from login attempts to a document's complete history (e.g., access date and time, type of access, user name, etc.), the size of the activity log can grow rapidly. Reviewing the log could become cumbersome, which would persuade most network administrations to disable the feature.

There are several ways to manage auditing trails:

- Restrict individual audits. NetWare allows individuals to audit network transactions independently, that is, any action that changes NDS or a volume's content. This might seem ideal if there is a need to off-load some network security responsibilities to department or node administrators. However, the default size of an audit file is 1MB for any disk, regardless of the size of the disk or the available space. This file can grow extremely large if it monitors every transaction.
- The same security requirements for sensitive information should be imposed on activity log files. These files must be protected from any manual alterations.
- View logs daily to keep them down to a comprehensible size.
- Include activity logs as part of the backup set. This allows an administrator to view historical information to pinpoint specific occurrences.
- Use audit logs to track document modifications to files if sensitive information is stored on specific volumes.
- Avoid tracking every executable file, particularly with applications that run multiple executables. This can also generate a large activity log.
- Test audit trails to verify the transactions that are supposed to be tracked.

Audit trails can be used to justify needs for server improvements or funding for other tools needed to adequately manage network operations. If properly used, audit trails can either enhance or deter enterprise network operations.

Backup Strategy

Producing a backup strategy requires a thorough examination of network data, applications, and activity. Every entity within an enterprise makes a significant contribution to overall company operations and stability. As a result, determining data backup priorities can be difficult. Even with peak productivity times varying, tape backups should not hinder daily enterprise operations. On the other hand, information must be backed up based on the amount of risk that is involved if data loss occurs.

Assessing the Network

Planning for data recovery requires an extensive inventory and assessment of the network. To determine what data needs to be backed up (the backup set), you must identify what the critical resources are and where they reside.

Since applications required for company operations would have either been purchased or developed in-house, tracking what applications are being used should not be very difficult especially if centralized control of software installation and maintenance is exercised. However, if individual entities within the organization install and maintain software that is critical to overall company operations, this can make network assessment more challenging.

Commercial software that is critical to enterprise operations should be backed up at least once but need not be backed up daily unless the original media from which it was installed is not available. The exception occurs when options and preferences have been set within the software that are required for utilization. In that case, this information should exist in the form of a backup as well as a documented hard copy. Furthermore, every time preferences are changed the software application should be slated as part of the next backup and the changes documented.

Application usage and data access frequency also aid in pinpointing the backup set. Applications that are frequently accessed, that are relevant to business functions and/or profits, usually cannot stand to be out of commission for long periods of time.

Software Applications

The choice of backup and recovery software is critical to the stability of the enterprise network and the organization. Unlike backing up mainframes with a central data storage location, backing up LANs can sometimes be a difficult task. However, this task can be accomplished by most backup applications.

If a catastrophe occurs, such as server failure, data corruption, data deletion, or overwritten files, a backup turns a calamity into a minute setback. The backup and recovery software that is best suited for your enterprise depends on the backup and recovery window, amount of information, and the required backup frequency. With today's backup software, restoration of files or even an entire NetWare server can be achieved in a timely manner without extended downtime or prolonged non-productivity using either file-by-file or image-based technology.

File-by-File Backup

In the past, backup and restore on dissimilar networks was limited and complex. However, backup applications can now protect data on a variety of platform combinations. Applications that use file-by-file backup technology typically accommodate this feature. Other customizable features such as unattended automated backups, remote server and workstations backup, and on-line backup also aid in implementing a sound enterprise Contingency Plan.

Image-Based Backup

Image-based backup systems are high-speed applications targeted for single servers with large storage capacities (at least 8GB). Backup is not limited to data stored on NetWare volumes. Instead, the application creates an 'image' of the entire server, which includes all partitions. Restoration is just as fast at the volume level. However, single-file or directory restores are slower than restoration using a file-by-file application. Image-based applications are best suited for Contingency Plans that require a full backup in each session.

Virus

A computer virus existing on a backup media poses a serious threat to the network. If a virus is restored to the network during file restoration, it could affect every user on the network and infect client workstations.

Use virus scanning software either before or during backup, especially if workstations are included in the backup. Virus monitoring should be a routine part of network and client maintenance. However, most users rarely use such safeguards as anti-viral software. In addition, because word processing documents and electronic mail messages can now be infected with viruses, networks and the backup copies of information are always at risk. Some backup applications have the option to scan files during backup.

Hierarchical Storage Management

Hierarchical Storage Management (HSM) is a tool that frees up hard disk space by moving less frequently used files to inexpensive storage media. The primary goal of HSM is to save space on the server hard disk and free on-line storage space, thus lowering storage costs.

HSM is not a backup solution. Data is moved, not copied, to another media. Though software products are beginning to integrate HSM, backup and archiving, HSM alone does not directly address issues related to data loss. In fact, HSM can create a challenge during data recovery if HSM data consumes more disk space than what is available on the server. Some applications, however, allow you to restore specific files and/or directories, which would circumvent such problems.

Planning for Disaster Recovery

Server fault-tolerance does not guarantee 100-percent uptime at your place of business. If operations cannot continue at the home site, an alternate processing location or hot site must be previously designated in the Contingency Plan. This location must have the ability to support a system and network that can run your mission-critical applications and process required transactions on par with your production environment.

There are a wide range of options when selecting an alternate site for your processing. A hot site with a temporary system and network that are ready to go can be expensive to implement and maintain. On the other hand, if you plan on restoring service to another of your company’s sites with hardware obtained at the time of a disaster, the additional time it takes to restore your environment may have a far higher cost to your company than more expensive disaster recovery alternatives. The trade-off is the amount of profits that can be foregone with the system completely down until you can restore processing.

In preparing for the unexpected, a business needs to identify the critical components that could cause lost revenue and business opportunities in the event of a disaster.

Developing a Contingency Plan

Developing a Contingency Plan is a difficult process and can be very time consuming. However, when weighed against the potential business impact of a disaster, it is probably one of the most important tasks you can undertake. It is essential that it be closely tied to your business processes and take into account your company's processing needs.

The following procedure is a rough outline of the steps necessary to successfully design and implement a Contingency Plan for your business.

1. Identify your company's mission-critical applications. This requires discussing with each of your major customer groups how they use your systems and which of these functions are critical to their business processes. You can start this dialog with a list of the systems maintained by the IS department, but pay particular attention to where the data inputs originate and where outputs are routed. You might discover that there are systems, often developed by individual departments and not documented by the IS department, which are critical to your company's ability to continue business operations. Maintain a list of all critical systems and the business functions that would be damaged if the system were not available.
2. For each of the systems identified in Step 1, work with your customer to estimate the maximum amount of downtime each application can tolerate without materially affecting your business' ability to continue operation. At the same time, determine how current the data must be once the system is restored. Many business processes might permit you to take a week or more to restore processing, but at the same time mandate that once restored, the data be current to within 24 hours of when they ceased processing. Add this information to the list you started in Step 1.
3. For each of these systems, identify the location and amount of data. This information will assist you in designing a backup plan to facilitate disaster recovery. Add this information to the list started in Step 1.
4. Design a backup strategy to meet the requirements you have defined. Consider the following items in this process:

- ❑ Your customer's data currency requirements
- ❑ The amount of data to be backed up
- ❑ The length and frequency of backup windows available
- ❑ Backup technologies to be used

Chapter 6 contains more information on developing a backup strategy.

5. Designate an off-site location for backup media: This site should be a secure location away from your main business location but easily accessed by your key IS staff. Several vendors specialize in business records retention and archival. Many of these have made accommodations for the secure storage of magnetic media including scheduled transportation and rotation of media. Other possibilities for off-site storage include other business locations and even the homes of IS staff members.

6. Designate a location in which to restore processing. Possible alternatives include:

   - ❑ **Hot Site:** Multiple companies specialize in providing these services. A hot site has processing hardware and network facilities compatible with your production network installed and operating. In addition, these sites typically provide an enhanced environment that is "hardened" against most natural occurrences and have backup power available so you are not dependent on public utilities. This enables you to restore your environment and activate a temporary network between the hot site and your home site to restore processing. This is generally the quickest way to restore processing, but it is also likely to be the most expensive.
   - ❑ **Cold Site:** A cold site has appropriate utilities, network facilities and floor space to install hardware in and recreate your processing environment. Many of the same vendors that provide hot sites also can provide cold sites. Facilities provided by these vendors are comparable to those housing their hot site, but lack the running systems and networks. It is also reasonable to consider creating your own cold site if your company has floor space available in a location separate from your home site. Cold sites are much less expensive than hot sites, but since you must obtain hardware and software to recreate your environment, they generally require a significantly longer outage before processing can be restored.

- **Home Site:** Restoring processing at your home site is probably the least expensive option in terms of up-front costs. This option also requires acquiring hardware and software to recreate your processing environment. However, if you exercise this option, there is the potential that your home site could be significantly damaged or destroyed—rendering your plan inoperative. Following a disaster it is also highly probable that your home site could be without utilities such as electricity or water - making recovery difficult or impossible.

7. If you elect either of the latter two options, locate a reseller that can replace equipment and software if a disaster occurs. Discuss equipment availability with your vendor and consider asking the vendor to commit to a contract that would guarantee some level of equipment availability.

8. Document your server, network and client configurations in sufficient detail to re-create your environment accurately in the event of a disaster. In addition to specific hardware types and network diagrams, maintain records of specific hardware and software settings for each of these environments. The Compaq Insight Manager, the Compaq Survey Utility, and the ARCserve Disaster Recovery Utility can help you develop this documentation.

9. Establish the process for data recovery after a software failure or data loss, hardware failure, or server failure. This procedure should include:

   - Names and contact information for all IS staff and end users involved in the recovery.
   - Names and contact information for all vendors required to effect the recovery including your hot site or cold site vendor, off-site storage provider, and any computer resellers that have committed to provide hardware and software.
   - Location of any keys, combinations, or passwords necessary to access resources necessary for the recovery. This would include keys or combinations necessary to retrieve backup tapes and information on where to find the Administrator or Supervisor passwords for your servers.
   - All the information gathered and documented in the above steps.

- Specific assignments for recovery steps such as who will retrieve your tapes from off-site storage, how will they get to your alternate processing site, who will install any hardware or software required, who will actually restore the data, who will verify that the restores were successful, etc. Be sure to plan for backup personnel if your primary assignee is unavailable.

10. Make copies of this procedure for all individuals that will be involved. Encourage each of them to keep copies of the plan both at work and at home. Keep an additional copy with your backup tapes at your off-site storage location.
11. Conduct enterprise-wide training for disaster recovery
12. Test the plan at least annually. Be sure to test all facets of the plan from technical procedures, to the ability of your reseller to provide equipment to your ability to retrieve tapes from off-site storage. If you find problems with your original plan, update it and re-distribute copies to all participants.

Continuously update your plan based on testing, feedback, and server configuration, NDS changes, and changes in your business.

---

[i] Don't be afRAID of your storage problems. Network Computing: Jul. 15, 1996. CMP Publications Inc.
[ii] Novell Replication Services. Novell Developer Notes. August 1997.
[iii] Planning Replication. Novell Developer Notes. August 1997.
[iv] http://www.novell.com/products/nss/, NSS: Novell Storage Services Product Intro

Chapter 6
Using Backup Technology

When choosing and implementing a backup system, there are several factors you must consider.

- The backup system must meet the requirements of the backup and restore windows defined in the Contingency Plan.
- The software must accommodate the heterogeneous environments that are characteristic of enterprise networks.
- The application must backup remote servers and/or workstations if necessitated by the Contingency Plan.
- The host server must be optimally configured to run the backup application.
- The tape drives must be able to back up the data set in a fast, reliable manner.

Network Environment

In the past, backup and restore on dissimilar networks was limited and complex. However, backup applications from Cheyenne now provide the functionality that allows you to meet the requirements of the enterprise Contingency Plan.

Backup systems either perform file-by-file or image-based backups. Image-based backup systems are usually high-speed applications that back up data at the volume level. Individual file restoration can be achieved with either method. On the other hand, file-by-file backups are slower, but offer a variety of features to customize the backup process. Both methods have their benefits and drawbacks.

ARCserve 6 uses the file-by-file method. This application has many features to customize the backup process including a scheduler and rotation. JETserve performs image-based backups and is best suited for enterprises that require backup of at least 8GB. Refer to Table 6-1 to determine which system meets your backup needs.

Table 6-1
Feature Comparison

Requirement	ARCserve	JETserve
Tape rotation management	AUTOMATIC	MANUAL
Scheduling mechanism	CUSTOMIZABLE	LIMITED
RESTORATION		
File-by-file	SUPPORTED	LIMITED
Volume	SUPPORTED	SUPPORTED
Server	SUPPORTED	SUPPORTED
RAID	LIMITED	SUPPORTED
Drives supported	DAT & DLT	DLT only

Cheyenne ARCserve 6

Cheyenne ARCserve 6, a file-by-file backup software tool, safeguards data on enterprise servers and workstations in a NetWare network regardless of the local operating system running on the client machines. Backup and recovery with Cheyenne ARCserve 6 meets the needs of most organizations.

ARCserve 6 supports up to 32 tape drives attached to eight Small Computer System Interface (SCSI) boards. Performance and reliability are further enhanced with distributed processing, parallel streaming, and RAID 5 fault tolerance. The factor that makes ARCserve so powerful is its ability to customize the backup process. With ARCserve 6, you can automate backups of single or multiple servers. These and other ARCserve features aid in implementing and managing a solid Contingency Plan.

Protecting Servers

Every enterprise can take advantage of ARCserve's speed and simplified user interface. As part of any Contingency Plan, any key user should be able to restore mission-critical applications and files after a disaster. With the step-by-step guidelines provided by ARCserve 6 and a thorough Contingency Plan, practically any key IS member can restore data without sacrificing data security.

Protecting Workstation Data

Most people associate backup in an enterprise with network administrators backing up servers, leaving users responsible for backing up their workstation files regularly. The average user might back up their data on a weekly basis. Even so, this data is either backed up to a departmental server or to diskettes. The latter case involves a great amount of risk because the diskettes are usually in the same vicinity of the workstation. If the user's hard drive goes bad or a file is unintentionally overwritten, the diskettes provide a safety net for the data. However, if a fire or flood occurs, the diskettes fall prey to the same catastrophe. Given the effect a single user managing information can have on company operations, organizations cannot risk losing any mission-critical data.

A network administrator can handle individual user files in two ways: advising users to copy files to a server or allowing ARCserve to backup workstation files. Store mission-critical files on the network to safeguard against disaster and to safeguard company operations when that particular user is unavailable.

As part of the Contingency Plan, users designated as processing mission-critical information should have the Cheyenne Agents loaded on their workstations. Specific client files, directories or even the entire client hard drive can be included as part of the routine ARCserve backup.

Cheyenne JETserve

The JETserve Tape Backup system is an image-based backup and restoration application that is designed for single-server environments with storage capacities of 8 gigabytes (GB) or more. JETserve runs on Novell NetWare 3.x and 4.x file servers and is best suited for Contingency Plans that have a "fixed, finite, and inflexible backup and restore window."[i]

The JETserve solution is best suited for the enterprise that requires a daily, full-system backup. JETserve can protect mission-critical data and applications while staying within the limits of a pre-defined backup and recovery window. JETserve achieves high data transfer rates by reading from multiple disks simultaneously and writing to multiple tapes in parallel. This reduces the time required for a backup and provides quick and expedient data recovery after a disaster.

JETserve supports up to eight tape drives. The number of tape drives is the primary influence on the JETserve backup window. However, other factors such as the data transfer rate, data compression, and the read access time of the servers' disk drives also affect the speed of the JETserve backup and restore processes.

Before deciding on a backup application, make sure the designated tape server meets the configuration requirements of the software. Options such as additional RAM or a SCSI controller might be needed to take advantage of the performance expectations of the application and tape drives.

Tape Server Requirements

Performance is a very important consideration in a backup strategy. Hardware and software configurations must be manipulated according to their network environment to offer optimal performance. There is a trade-off in striving to achieve the optimal tape server configuration: capital. Careful initial assessment is necessary to establish what is reasonable and acceptable to protect mission-critical information sufficiently.

The Contingency Plan should include a record of every server hardware and software configuration. Include as much information as possible about each server in this record. Compaq servers are packaged with a Compaq SmartStart CD and a Compaq Support Software CD that include the necessary utilities to configure your server. They also enable you to create the support diskettes required for your network operating system to optimize the performance of your Compaq server.

If you configured your server using SmartStart 3.0 or later, a file named SUMMARY.TXT is written to the server's DOS partition. This file contains information about installed hardware, configuration options, operating system setup, NetWare volume configuration, and other pertinent details. Save both a hard and soft copy of this information. It speeds the data recovery process in the event of server failure or site disaster.

If you did not configure your server(s) using SmartStart, follow these steps to obtain server hardware configuration information:

1. Run the Compaq System Configuration Utility.
2. Select *System Configuration* from the main menu, then select *System Partition* from the System Configuration menu.
3. Select *Copy Files* from the System Partition menu, then scroll down to find the entry for the file, SYSTEM.CHL.
4. Press **Enter** to select SYSTEM.CHL, then select the destination drive and press **Enter**.
5. Press **Enter** again to confirm the drive selection. The file is copied to the destination drive.

Print this file to preserve a hard copy. Compaq also suggests that you designate this file as part of the next backup.

Update server modules and drivers with the most recent NetWare operating system patches and Novell Support Software Diskettes (NSSD). The latest NetWare patches and NSSD SoftPaq can be downloaded from the World Wide Web sites of Novell and Compaq respectively.

Compaq offers Insight Manager to manage network servers. Insight Manager delivers intelligent monitoring and alerting as well as visual control of your Compaq servers. Comprehensive fault management can be achieved for all major subsystems, including pre-failure alerting for disks, memory, and Pentium-Pro processors. When used in conjunction with SmartStart, Insight Manager allows you to deploy and manage configurations throughout the enterprise using the Compaq Integration Server and Insight Version Control.

Server Configuration

One key to optimal performance from a Compaq server is configuring the tape server with adequate memory. Novell published a NetWare 3 and 4 Server Memory Worksheet in the January 1995 issue of *Novell Application Notes*. Compaq tested the accuracy of the formula on a wide variety of Compaq server configurations and obtained significant server throughput improvements by increasing server memory to the value calculated with this formula.

To ensure that the servers in the enterprise network have the necessary hardware for optimal performance, apply this formula to every server on the network. This also aids in managing the backup and recovery windows.

NOTE: The worksheet is included in Appendix B of this document

SCSI Controller

Despite the performance provided tape drives, the native transfer rate can be impeded by the devices that share the SCSI controller. Ideally, for tape backup in particular, a server should be have at least one controller for every four tape drives. Furthermore, if high-performance is the goal, a 2:1 tape drive-SCSI controller ratio delivers maximum transfer rates using image-based backup and recovery software.

Data Compression

Enabling NetWare file compression, although saving disk space, can impede backup operations depending on the type of backup software you use. File-by-file backup software decompresses each compressed file before sending it to tape. However, since only files that are not accessed for an extended period of time are compressed, this does not affect incremental or differential backups. The backup window for full backups by applications that use the file-by-file method, however, could increase with NetWare file compression if turned on.

Because ARCserve uses the file-by-file method for backup, ARCserve's speed is improved when backing up NetWare volumes in which file compression is turned off. In local backup tests on a Compaq ProLiant Server, speed improved by nearly one third when NetWare file compression was turned off.

Table 6-2
Factors Affecting ARCserve Performance

Feature	Improvement/(Decline)
Writing to database	(2%)
Volume compression	(18%)
Tape compression	17%

Tape data compression improves speed as well as yields more storage capacity. Regardless of the software used for backup, transfer rates increase dramatically with tape compression enabled. On the other hand, image-based backups are not affected by NetWare file compression. Image-based backup and recovery applications perform backups on a volume basis eliminating the need to address file compression issues.

IMPORTANT: Compression could pose a potential problem when backing up large compressed files on server volumes that have disk space constraints, because file-by-file software decompresses each compressed file before sending it to tape.

ARCserve Database

ARCserve provides a database to track information related to every backup session. This information is especially useful during a restore. A single file restore, for example, could require traversing every tape used in the backup session. However, the ARCserve database can pinpoint the exact tape on which the backup file resides. In addition, you can use the ARCserve database to improve the backup process by viewing session information. The session information displays any errors or warnings that may have occurred during backup, such as skipped files.

There is a trade-off, however. Updating the ARCserve database during each backup session slightly increases the backup window (see Table 6-3). If you have a restricted backup window, disable writing to the ARCserve database. On the other hand, if you are performing incremental or differential backups, the ARCserve database can help keep media organized if a restore is required. Incremental/differential backups are much faster than full backups, but they take the longest to restore because you must have *every* tape used since the last full backup.

Remote Backup

The ability to manage backup jobs on multiple servers from one central console should not necessitate physically going from one server to another to manage backup media. ARCserve 6 can back up NetWare volumes from multiple remote servers. Managing tape drives is easier because each individual server does not require a dedicated tape drive.

Backing up data from remote systems, however, can be thwarted by throughput, bandwidth, and local configurations. ARCserve counters these obstacles with an optional High Performance Push Agent that loads on secondary servers that are not attached to a backup device. Instead of all processing being done on the host server, the push agent prepares jobs at the secondary server, and "pushes" the job at the primary server. This speeds up data transfer thus reducing the backup window.

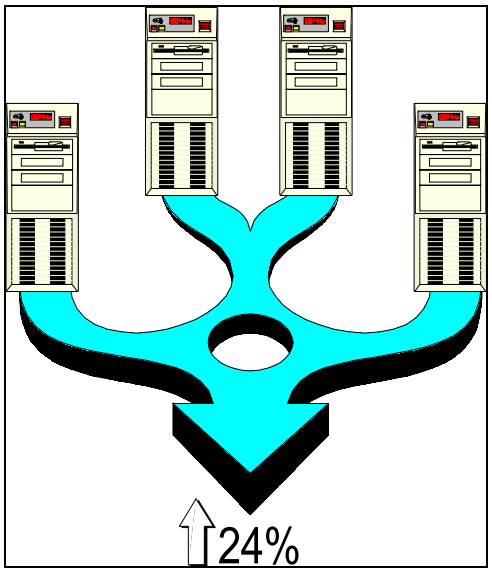

Figure 6-1. 1 Push Agent Data Transfer Rate Improvement

Because the Push Agent is loaded on the remote server, make sure that the remote server has adequate memory to accommodate the NLM. Refer to the worksheet in Appendix B to determine the amount of memory necessary for optimal performance.

Backup Media

Give careful consideration when choosing tape options. The tape backup option must be supported by the backup software and fully compatible with your current server hardware. Base your selection of backup devices on an assessment of the current data set that requires backup, the backup window and frequency, and an estimate of how much the data set will grow. All of these considerations must be examined before electing an option.

Compaq offers tape options ranging from DAT drives to DLT tape devices.

- The Compaq DAT Drive is best suited for enterprises that require backup of a relatively small data set along with a flexible backup window.
- The Compaq TurboDAT Drive can provide twice the capacity and four times the speed of a DAT drive. This competitively-priced tape drive is ideal for enterprises with a small data set and limited backup window.
- The Compaq Digital Linear Tape (DLT) tape devices are designed for enterprises requiring high-capacity, high-performance backup. The Compaq DLT models exceed the capacity limits of DAT technology while providing the performance and data integrity of advanced linear recording.

Compaq DAT and DLT Drives are compatible with a wide variety of operating systems. In addition, you can manage Compaq DLT Drives, via Compaq Insight Manager, to alert you if something goes wrong in preparation for backup or if predetermined reread/rewrite levels are exceeded. Extreme reread/rewrite activity might eventually cause drive failure.

The most important consideration with selecting a backup option is capacity. Though the backup window is also an important consideration, backup software can compensate for speed. Accommodating backup with drives of ample capacity decreases the backup window and requires fewer media. This also aids in managing the media in a rotation as well as duplicate tapes stored off site.

Backup Frequency

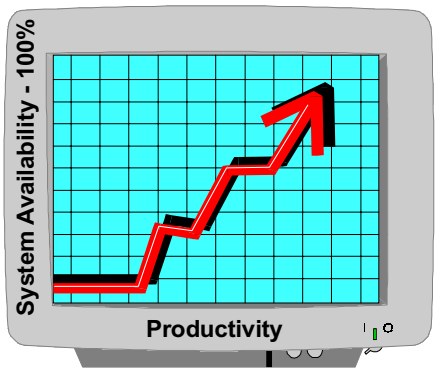

Figure 6-2. Ensure Backup Doesn't Effect Productivity

The maximum amount of downtime that the enterprise can stand is based on the results of the risk analysis. This information aids in determining the backup and recovery window—the time required to back up and restore crucial information without affecting productivity.

Every entity within an enterprise makes a significant contribution to overall company operations and stability. As a result, determining data backup priorities can be difficult. Even with peak productivity times varying, tape backups should not hinder daily enterprise operations. On the other hand, information must be backed up based on the amount of risk that is involved should data loss occur.

Perform backups as often as possible, depending on the amount of traffic on the server. Even though backups are important, network administrators still do not want to hinder productivity. If at all possible, perform backups when there is the least amount of traffic on the server. Unless the organization shuts down completely each day, no specific time will be convenient for every employee. Usually backup is done during off-hours or periods of low productivity such as lunch time. This avoids problems with open files and network performance. ARCserve has various backup options that allow you to tailor backup jobs to your backup strategy.

Managing the Backup Window

The backup window is the maximum amount of time allowed to back up information. This interval can be affected by a number of factors:

- Open files

- Problems with TSAs and supporting modules
- Poor planning
- Data verification

Open Files

Open files are a common problem that can hinder the backup process. Users have a tendency to depart the office leaving applications and files open. ARCserve now counters the open-file limitation with the Open File Agent. This is a separately purchased option that allows open files to be safely backed up without corruption.

Without the Open File Agent, ARCserve retries the open file as many as five times depending on settings in the Options screen. If during the retry period files remain open, ARCserve skips the files and notifies you via the Activity Log that the files were excluded.

Countering problems with open files begins with user awareness and compliance with network procedures. Again, inform users of backup schedules and restrict user access, if possible, during full backups. Monitor network productivity and try to avoid backup during peak usage.

Another alternative to deal with open files is JETserve. The JETserve image-based backup process reads blocks of raw data volume-by-volume. This permits backup of all files on nodes regardless of whether or not they are open. The only backup hindrance surfaces when write activity occurs, which causes the verify portion of the backup to fail. As with ARCserve, this can be countered by suspending or clearing user connections. Even though this may slightly affect productivity, JETserve compensates for this with high-speed performance.

Because JETserve is an image-based backup application, the backup window is based on volume size instead of the data set. This means that no matter how much data is stored on a NetWare volume, the backup window is the same. With the file-by-file method used by ARCserve, the backup window is based on the data set. If mission-critical data is restricted to certain volumes, JETserve is best suited for controlling the backup window. Otherwise, ARCserve delivers the best performance on a file-by-file basis.

Updates and Patches

It is important to keep track of the latest software updates. Compaq is always striving to improve its support products. NetWare Loadable Modules (NLMs) are constantly tested, enhanced, and updated if necessary. NLM updates are available on the Novell Support Software Diskettes (NSSD) via the Compaq web site (http://www.compaq.com), the CompuServe forum (GO COMPAQ), or SoftPaq files from ftp.compaq.com.

Always implement the latest NetWare patches. Even though you might not be experiencing any problems with ARCserve, JETserve, or NetWare, applying the latest patches can prevent potential problems from surfacing. Applying the latest patches can be time-consuming and difficult to manage especially if the entire network is the responsibility of one person. However, it helps to ensure that application modules are up-to-date and work properly with other software.

Poor Planning and Execution

If backups are not implemented using an automated method, it is crucial that manual backups be performed as planned. Inconsistencies can interfere with user productivity and access to data. A thorough backup requires suspension of logins and locking files included in the backup set. If mission-critical applications and data are not available when needed, the backup strategy impedes rather than facilitates company operations. Set realistic goals and perform a thorough assessment to determine the backup set and define the backup schedule.

Data Verification

A backup is only useful if it is a good representation of the data that was backed up. One way to ensure this is by setting one of the verification options during the backup process. The tradeoff, however, is that it increases the backup time because the backup application must compare the tape contents to the contents on the server(s). This, in turn, affects how long the servers are unavailable.

If possible, keep the default setting to Compare initial 10 MB. This only adds an average of two additional minutes per tape to the backup window. Here are some option settings to consider when deciding on a verification method:

- **Scan Media Contents:** Checking the header of each file offers some protection, but this method does not verify that the complete file was copied. The header may be correct, but there is a small chance there is a difference in file size.
- **Compare Media to Disk:** This is the most reliable method because ARCserve compares media byte-for-byte to ensure the integrity of the data on the tape. However, this method increases the backup window the most.
- **Compare Initial *n* Megabytes:** This is the fastest verification method. By default, the first ten megabytes of the tape are verified. If you are using tape compression, Compaq recommends that the amount of data verified represent at least ten percent of the total amount of data on the tape.
- **None:** This option reduces the backup window slightly, but Compaq strongly recommends using some form of data verification.

NOTE: JETserve automatically verifies data after the backup process

Developing the Backup Plan

Regardless of the backup application, you must identify the backup set, that is, what must be backed up. In LAN environments, all kinds of files that might be critical to business unit operations and individual productivity can reside in numerous locations. Planning the backup strategy requires an extensive inventory of where critical resources reside.

Selecting Backup Data

After a disaster, the primary task is to make the server and mission-critical applications and associated data accessible as quickly as possible. A minimal restore window begins with data storage procedures and an efficient backup.

Restrict file creation of data to certain volumes to avoid scattered mission-critical files. With mission-critical data identifiable, backup and restore jobs can run more efficiently by restoring information required to continue enterprise operations first.

ARCserve 6

ARCserve 6 provides utilities and options that can estimate the number of tapes required for backup and allow you to choose the order that nodes are processed. You can save this information in a script that can be used again. In addition, you can execute pre- and post-backup commands as part of the backup job. For example, you can unload specific software packages, or even NLMs, which conflict with ARCserve or impede backup operations.

At startup, ARCserve performs a “Pre-flight Check” to ensure it will run correctly on your network. The Pre-flight Check examines the version of each NLM, verifies the SCSI board, authenticates the ARCserve NDS job queue, and loads the ARCserve NLMs. If a compatibility problem is discovered with an NLM, ARCserve does not load. This gives you the opportunity to install the updated versions to ensure proper operation.

If restricting mission-critical data to certain nodes is not possible, you can take advantage of customizable backup options and utilities in ARCserve. The Count option can help you determine what data needs to be backed up and how many tapes will be required.

ARCserve also offers priority level grouping and file interleaving options that allow you to control the order in which backup sources are processed. Although use of these features is not mutually exclusive, the combination aids in minimizing the backup and restore window.

When you enable the File Interleaving (with Push Agent) option in the Global Backup Options window, ARCserve backs up each node (servers, clients, workstations, etc.) in the priority level order designated in the server options setting. Here are rules to keep in mind when grouping nodes for a file interleaving backup job:

- Assign the same priority at the server level as the volume on that server with the highest priority level. For example, if you assign a priority level of three to the VOL1 node of the ACCT server, you must assign the same priority level to the ACCT node.
- Set the maximum number of nodes allowed in a file interleaving session using the Configure ARCserve Server screen.

  NOTE: Nodes with a higher priority are backed up before any lower priority nodes. However, nodes with the same priority level are served in alphabetical order

The file interleaving and push agents work best when used together. With multiple nodes being backed up concurrently to the same tape drive and remote nodes preprocessing files to be backed up, these two features enable backup jobs to run much faster than normal.

ARCserve Backup Methods

A Custom/Full Backup is the default ARCserve backup method. However, ARCserve also offers other backup schemes to meet the needs of your Contingency Plan. After determining what data must be backed up, and estimating the number of tapes required for a full backup, the best initial approach is to perform Custom/Full Backups each day, verifying the contents of each backup tape. There is a tradeoff between the time it takes to perform the full backup and how much productivity is hindered if the backup is performed during normal work hours. This should help you determine whether a rotation or auto pilot option is employable.

Custom/Full Backups

This scheme is only for full or incremental backups that can be automatically run at designated daily or timed intervals. Use the Custom/Full backups method if:

- You have an unrestricted backup window
- You want to restore files as quickly as possible
- You have a limited number of media available for backup (since rotation and auto pilot backups require a different tape each day)
- You must back up applications as well as data
- You must augment your standard schedule with custom jobs and perform on-the-fly backups

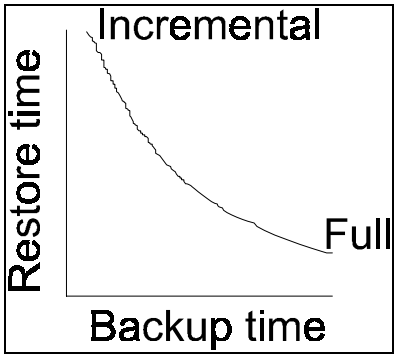

Figure 6-3. Compromise between ARCserve Backup Methods

If your Contingency Plan does not warrant a full backup each day, consider the incremental method. This method results in faster backups, but increases the restore window. For example, if you perform incremental backups Monday through Thursday and a full backup each Friday, a full restore requires media from the last full backup as well as tapes from each incremental backup since the last full backup. Furthermore, losing any media from any of the incremental backups will prohibit a full restore. Consequently, the highest level of verification and tape duplication are necessary to avoid potential problems if a full restore of server data is required.

Rotation

If your Contingency Plan requires a backup history of more than one day per week, the Rotation backup can aid the process by managing the tapes used in backup jobs. Use the Rotation backup scheme to designate the media to use for each backup job as well as define when you need to retire media. ARCserve enforces these media rules when it requests tapes during each backup job.

The ARCserve Rotation scheme automatically assigns a serial number to each media. It uses this information to inform you when to change media and which media to use. If the wrong media is in the drive during a backup operation, ARCserve automatically recognizes the problem and prompts you to put the correct media in the tape drive. This feature protects you from inadvertently overwriting the wrong tape in a rotation cycle, but it can increase the backup window and potentially hinder the completion of the backup job if left unattended. A backup job will not transpire if the wrong tape is in the drive and you select the Overwrite Same Media Name ...or Blank Media media rules option. Notification that the wrong tape is in the drive does not occur until the job starts.

With the priority to minimize the amount of time required for a backup, incremental backups in a Rotation scheme require fewer tapes because you can append the newly backed up files to the data that already exists on the tape. This is the quickest backup method, but it can also be the most risky if the media becomes damaged and no duplicate tapes are available.

Archiving Data

Server volumes that contain public files usually also consist of files that are rarely or never used. To help you manage server storage space, you can customize an ARCserve backup job that archives old files. This job can be designated to run cyclically. Use extra caution when selecting this backup option. One good rule of thumb is to archive files only after a full backup that includes the Compare Media to Disk verification method.

Archive data only after ARCserve reports zero data mismatches and successful tape duplication. In addition, document archiving procedures and inform users of the policy. After each archiving session save the ARCserve script so that all archiving jobs are performed in the same manner. For example, you could filter only files that were last accessed more than one year prior to the archiving job. Mark each archive tape clearly and check them periodically. Store each duplicate in different locations to avoid the vulnerability of succumbing to the same disaster.

CAUTION: When you select the Archive (Delete Source) as the backup type, be sure to set the filter in the source tab because the only method available is Full Backups option. As a result, if no filters are set, all data on the nodes included in that backup job will be deleted. The archived

files are listed in the Activity Log.

Auto Pilot

The ARCserve Auto Pilot method incorporates the Grandfather, Father, Son (GFS) tape-rotation method. The GFS scheme rotates tapes so that a tape is always available from yesterday (son), last Friday (father), and the last Friday of each of the last 12 months (grandfather). With the GFS scheme, you use at least 20 tapes.

	# tapes
Monday through Friday	5
1st Friday 2nd Friday 3rd Friday	3
Last Friday of each month	12
Total	20

Manipulate the GFS rotation to meet the requirements of your enterprise Contingency Plan. For example, if you need a backup on weekends, add an additional tape for each day.

AutoPilot encompasses a feature similar to the Archive method. The grooming option automatically frees disk space by moving rarely accessed files from the server to tape. Unlike the Archive method, you can specify the conditions in which files are removed. For example, you can require that files must be saved on at least three media copies and not accessed within the last six months. If duplicate grandfather tapes are stored off-site and tested for data integrity regularly, grooming is a viable option if disk space is a significant issue. Again, use careful planning and consideration to implement this procedure.

The Auto Pilot backup method can meet most enterprise backup needs. The only exceptions would be cases that require a customized backup each time. However, this would probably be due to an inadequately planned NDS tree or a lack of Contingency Planning. On the other hand, you can take advantage of the flexibility of the GFS backup rotation sequence that simple repeat interval backups do not offer.

The first requirement is for you to determine how often backups are needed. This entails determining whether incremental or differential backups can be implemented in the strategy. Refer to the following matrix to determine which method you should use:

Table 6-3
Auto Pilot Backup Options

	% change in Data	Backup Window	Restore Window	Tapes Required for Restore
Full Backup	>50	Unrestricted	Restrictive	Last full backup
Incremental Archive Bit	<=50	Restrictive	Unrestricted	Last full backup **and** all Inc. backups
Differential Archive Bit	<=25	Unrestricted	Restrictive	Last full backup **and** last Diff. backup

With the Auto Pilot GFS scheme, tapes are labeled intuitively, making it easy to locate an older tape if you need it to restore data. You can keep archived tapes as far back as you need with the GFS rotation sequence. The only limitation is the number of tapes required for testing and maintenance.

File Interleaving

File interleaving enables ARCserve to back up multiple nodes, of any type, simultaneously, to the same media. Given the fact that multiple nodes are being backed up, several factors can affect the backup window. The Network Interface Controller (NIC) and LAN implementation can have a significant effect on remote backups. 100VG have shown data transfer rates an average of 25-percent faster on remote backups than 10BASE-T.[ii] Faster data throughput can result in faster backups in environments that require backup of remote nodes.

Parallel Streaming

ARCserve parallel streaming enables backup of multiple nodes to multiple devices concurrently. Like file interleaving, NIC and LAN implementation also affect performance. However, because data from each remote server is streamed to a dedicated drive, transfer rates are slightly higher for parallel streaming.

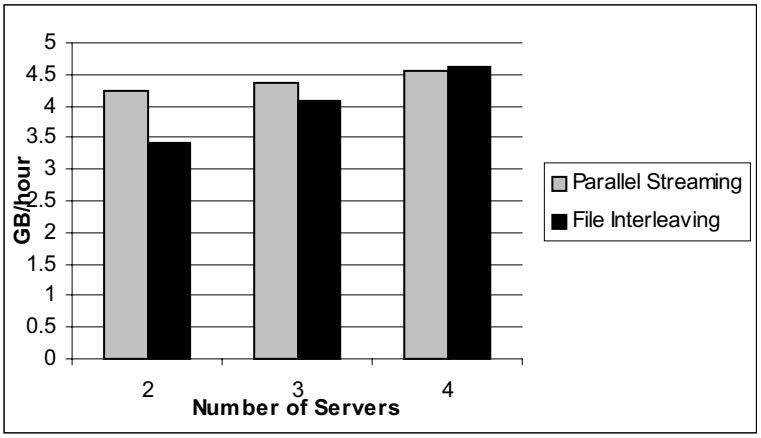

Figure 6-4. Data Transfer Rate Comparison

RAID Technology

ARCserve 6, when coupled with the RAID option, provides comprehensive hardware fault tolerance by redundantly storing your source data on multiple drives. RAID 1 enables ARCserve 6 to "see" two identical tape drives as a single logical device and stream data to that device. If one of the drives fails, the other drive continues the job, without having to reset and start from the beginning. Similarly, RAID 5 allows ARCserve 6 to "see" three or five identical drives as a single logical device. RAID 5 stripes data and parity information to the multiple drives. This permits data recovery if a drive fails or a tape is lost or corrupted.

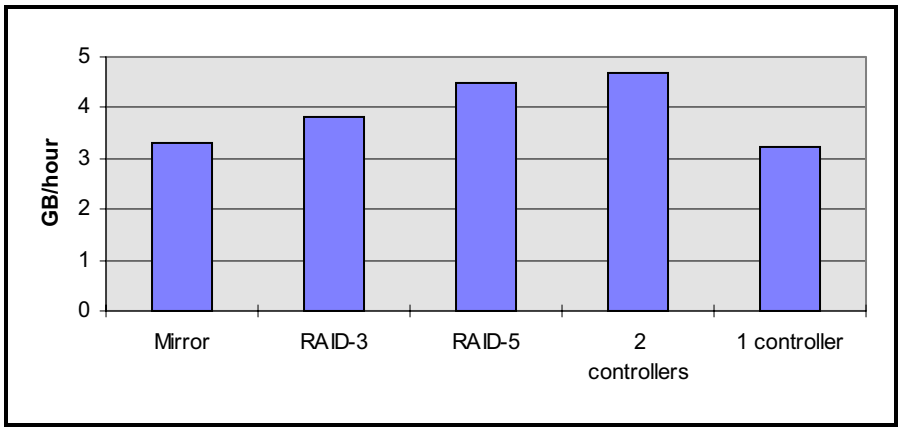

Figure 6-5. ARCserve Performance Using RAID Options

Performance increases because data is written to multiple drives at once. As stated before, performance is also directly related to the additional options implemented for tape backup (controllers, tape drives, RAID). However, there is a trade-off: expense. You must determine whether system downtime due to a longer backup window is more expensive than the initial costs associated with purchasing the necessary components for faster backup.

Preparing for Disaster

ARCserve 6 can capture server configuration information during backup. If the ARCserve host server fails, restoring the server only requires creating a DOS partition and installing NetWare. This eliminates guesswork as to which patches were running on the server before failure.

To create Disaster Recovery diskettes, run the Cheyenne Disaster Recovery Preparation module (CDRPREP). This module generates a report of the server's network operating system configuration. The file, CDR.DOC, contains the contents of the AUTOEXEC.NCF file, server and volume information, and a list of the NetWare modules and versions currently running on the server. CDRPREP copies these files onto the diskettes. Furthermore, you can choose additional files to be copied as part of the process. Keep this information with the copies of the Contingency Plan and any other information necessary to recover data.

Once a set of Disaster Recovery diskettes have been created following the instructions in the ARCserve Server guide, you need only continue the routine backup process. These diskettes only need to be updated when new patches are applied, new server components are installed, or any other changes are made to the AUTOEXEC.NCF.

In addition, as you prepare for disaster recovery, document all relevant network information: the kind of hubs you use, the way your wires run, client and printer setups, and so on. The more data you have on your setup, the less you have to rediscover during restoration.

JETserve

JETserve performs image backups at the volume level rather than the disk level. At the volume level, JETserve recognizes NetWare's hot fix and redirection areas. This avoids copying bad disk areas to the tape.

Traditional backup systems that use image technology for backups also require restoration of the entire disk image. This compromises file management despite increased backup speed. JETserve, on the other hand, surpasses this limitation by allowing individual file restoration.

With three or more drives, JETserve uses built-in RAID 5 fault tolerance to stream data across drives. Redundancy provides additional protection against drive or tape media failure. If a tape is corrupted, data on a bad tape can be re-created from other tapes in the array.

Despite JETserve's high-speed and high-performance, the customizable features are limited. However, the transfer rates that JETserve delivers can compensate for its simplicity.

Backup Options

JETserve permits automatic backups, but only one backup session can be scheduled per day. Any additional backups must be done manually. JETserve delivers the highest performance with RAID 5, which requires more than one tape drive. Even if your backup needs do not necessitate more than one tape drive (although Compaq recommends at least two drives for duplication purposes), JETserve is still faster than local backups using ARCserve.

Table 6-4
Comparison of Single Drive Backup

	GB/hour
ARCserve*	4.23
JETserve	4.26

* NetWare compression and writing to the database disabled

The foundation of JETserve is RAID technology. JETserve's high-speed transfer rates are best achieved with a RAID configuration. JETserve boasts speeds of up to 45 gigabytes per hour[iii]. However, such configurations are limited to enterprises that require hundreds of gigabytes of data to be backed up. Figure 6-6 shows data transfer rates achieved using four Compaq 20/40 DLT Drives with one SCSI controller.

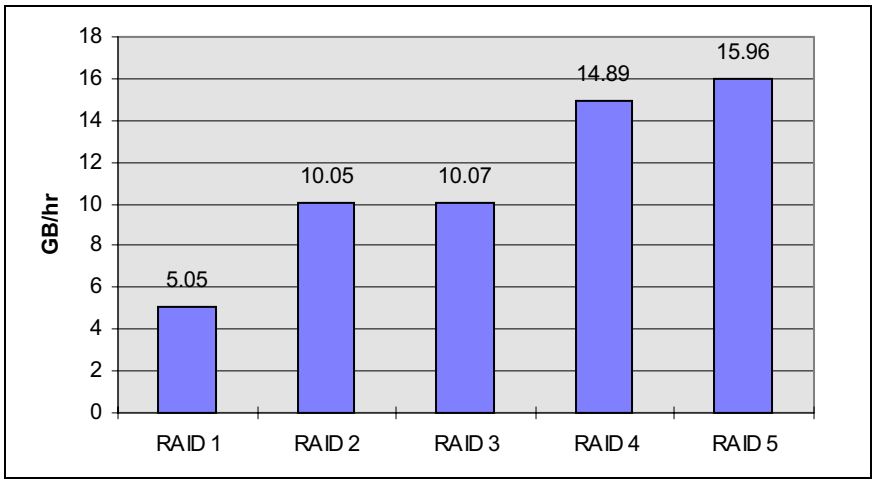

Figure 6-6. JETserve RAID Performance[iv]

JETserve is designed for full backups, but you can specify volumes for back up. The backup window is not based on the amount of data on the NetWare volume, but on the size of the volume. This can be perceived as a limitation because it would take the same amount of time to back up one gigabyte of data on a four-gigabyte capacity volume as it would take to back up three gigabytes of data.

IMPORTANT: Document all volume segment information. During a JETserve restore, the volume size and number of segments and blocks must match the volume on the media. Otherwise, you must perform a file-by-file restore which dramatically increases the restore window.

The restore options are not as limited as the backup options. If necessary, you can restore a single file, directory, or volume. See Chapter 7, *Testing and Maintenance*.

Backup Frequency

You can determine the backup frequency and schedule based on the backup set, the average time it takes to back up that data set, and the maximum time the server can be inaccessible without affecting enterprise profits. You can estimate the backup window by using the Count utility to determine the total amount of data (in megabytes) and the average time it takes to back up that amount of data. For example,

$$\text{backup window} = \frac{\text{backup set (GB)}}{\text{average speed (GB/hr)}}$$

where the average speed is based on server and tape drive performance.

Using the backup window can help you determine the:

- **Backup Method:** A small backup window and a requirement to perform a daily full backup might necessitate the use of an image-base backup system.
- **Backup Plan:** Given the amount of time available for backup, you can determine whether a full, incremental/differential, or a rotation that implements both plans, meets the requirements defined in your Contingency Plan.

Summary

Base your choice of assurance measures on the requirements outlined in your Contingency Plan. The amount of equipment and type of software you purchase is directly related to the value of the information required for enterprise operations. Another primary consideration in selecting assurance measures is the effect that implementing those measures will have on enterprise operations.

Backup is not a complete fault-tolerance solution. It is the final measure to return business operations to as close as possible to 'normal' if a data disaster occurs.

---

[i] JETserve Student Guide, Sept. 1995, Cheyenne Software, Inc. p.1-2.
[ii] Using a Compaq ProLiant with four Compaq 20/40 DLT drives and two SCSI controllers on the host server.
[iii] At the time of writing using eight Compaq 20/40 DLT drives and two SCSI controllers.
[iv] Using a Compaq ProLiant with five Compaq 20/40 DLT drives and two SCSI controllers.

Chapter 7
Testing and Maintenance

A Contingency Plan is never “written in stone”. You must regularly test and update it. Having a Contingency Plan in place does not completely protect the enterprise from data loss. A well thought-out Contingency Plan can prove to be useless in some cases. For example, server hardware fails and the only person who knows the correct configuration is on vacation in Aruba. Testing a Contingency Plan involves ensuring that data is recoverable in the defined restore window, regardless of the disaster.

The only way to make sure a Contingency Plan works is to test it. The last thing an enterprise needs is to flunk the Contingency Plan exam. Testing should entail everything from verifying backup media to replacing any network component. Testing and maintenance of your Contingency Plan ensures:

- The integrity of mission-critical information
- That a testing schedule is developed and followed
- The recovery team members are appointed and understand their roles in the recovery process
- Any network component can be replaced after a disaster or hardware failure
- Alternate methods of continuing business operations are readily available and can be implemented should systems become inoperable
- Test plans have defined goals and objectives
- Hardware and software applications are regularly updated
- The plan is updated appropriately when any problems or inconsistencies surface

These qualifying factors provide the assurance for the continuity of enterprise operations after a disaster.

Verifying Data Integrity

Data integrity is assumed as long as there are no user complaints. However, after receiving a Compaq pre-failure alert that a disk is about to fail there should be a way to verify the integrity of mission-critical information that was stored on that disk. If some form of fault-tolerance, such as a RAID-5 array configuration, were used for storing the information, data integrity should have been attained. On the other hand, a system configuration with limited fault-tolerance can result in a tainted backup as well.

Real-Time Data Verification

A backup is only useful if it is a good representation of the data that was backed up. Faithfully backing up mission-critical data and applications would prove to be useless if, when the information was needed for backup, the backup media were found to be faulty.

Image-based and file-by-file backup applications such as ARCserve and JETserve provide verification methods. Data verification increases the backup window regardless of the application. As mentioned in Chapter 6, *Backup Technology*, ARCserve offers three methods of verifying data. In essence, the amount of data integrity is proportional to the time required for verification: the greater the integrity, the larger the backup window.

Off-Site Media Storage

For businesses that are located in regions of the country that are prone to natural disasters, backup tapes should be stored a safe distance away. Backup tape sets stored in a safe deposit box at a local bank serve little purpose if the bank site is destroyed by the same natural disaster that hits the organization.

If a natural or man-made disaster strikes and destroys local equipment, vendors can replace systems and commercial software. Data replacement, on the other hand, is the ultimate responsibility of the IS staff. Enterprises that rely on timely data would find little use for week-old data that had been stored off site. In some cases, any form of data would be at least a starting point, but the goal is, again, to return operations to normal as quickly as possible.

The backup media stored off-site must meet the same requirements as local copies. Any tape rotation implemented on-site must be applied to off-site media as well. This might seem inconceivable, especially if daily backups are required. However, you must decide the risk in foregoing off-site daily backup media.

Preparation

Preparing for data recovery involves pinpointing key personnel and vendors. Individuals must be identified to perform the tests, observe the environment, and provide feedback after the testing. If possible, involve vendors and suppliers to examine the speed of the equipment replacement process.

Assembling a Recovery Team

Designate key personnel in advance for data recovery. This team should include not only IS staff, but also end users to communicate their expectations as well as provide feedback once systems are up and running.

Most companies do not have the resources to hire personnel specifically for these tasks. As a result, these responsibilities are added to team members' normal duties. However, attention to detail and commitment to the actualization of your Contingency Plan is even more significant.

Any changes to your Contingency Plan necessitate re-evaluation of the recovery team duties. If you must perform additional tasks, assign them to the appropriate team member(s). Likewise, if the additional tasks warrant more team members, communicate this information to management. This furnishes the support needed to draft and train the essential individuals prior to the next scheduled test. These new members require an integral understanding of their responsibilities *before* testing. Otherwise, their focus will tend to be more on comprehending their responsibilities rather than data recovery, which could lead to tainted observations.

Once you identify individuals who can effectively fulfill such responsibilities, another key determinant is ensuring their availability. The use of substitutes will suffice, but everyone requires the same training.

Replacing Equipment

With the number of computer system resellers available, replacing network equipment might not seem significant. However, you do not want to take the chance of equipment not being in stock or any other unforeseen issues. Choose a reliable vendor that can participate in annual testing.

A formal contract or agreement must be signed by both parties guaranteeing the equipment, supplies, services, and/or facilities necessary to resume enterprise operations. Be aware, however, that other organizations in your locale may also have the same type of agreement; and if you all suffer the same disaster, equipment will be distributed on a first-come, first-serve basis. If possible, try to maintain your own replacement parts off site.

Testing

The purpose of testing is twofold: to ensure the continuity of business operations and to ensure that the goals of the test plans are realistic and comprehensive. Develop a test plan for each critical business component if a single test plan is not practicable. Each test should provide the essential feedback to pinpoint any weaknesses so that some form of remedial action can be taken.

Test Plans

Development of a test plan should exploit the threats outlined in the risk analysis. A thorough test plan:

- Has clear goals
- Focuses on one component of the business operations
- Requires considerable analysis and skill to meet the goals realistically and economically

The test plan should meet the same criteria ascertained from the risk analysis. In essence, the test plan should challenge the assurance measures in place to counter the perceived risks. Most risks affect different facets of enterprise operations. As a result, the test plan can be segmented into a series of tests. Modularizing testing helps to minimize the disruption of normal operations and focus on a specific risk and associated assurance measure(s). Most of the critical systems and operations should be included in as many tests as possible.

Initial tests should use less critical applications and data to resolve minor issues. Subsequent tests should be conducted only after achieving errorless trials. A variety of comprehensive, discriminating tests can be examined to explore the activities from different angles.

If possible, create an environment separate from the production network that temporarily suspends user network activity. This enables users to give adequate feedback on the effects of server suspension on productivity.

Alternate site testing can be expensive especially if a vendor or external organization is involved. These tests must be carefully planned, and it is crucial that recovery procedures be followed according to plan. Any deviations should be documented detailing what was done and why the divergence occurred.

Testing Frequency

With computer operations in a continual state of flux, test your Contingency Plans as often as possible. Every organization should test their data recovery plan at least annually. Test your entire Contingency Plan to ensure that the procedures, media and equipment required for data recovery are operable. If possible, set up a small test environment to test your system’s backup and restore capabilities.

Testing frequency should not interfere with productivity, but individuals from the user community must participate to provide feedback after a simulated disaster. Like members of the recovery team, these individuals need the same level of commitment to ensure expedient and faultless data recovery.

Conduct your tests after any changes to system configurations or major software migrations or updates. Upgrading or changing mission-critical software applications results in new data sets. The procedures and time required to restore one type of software application might be different for another.

Integrate changes in server and/or client configurations into your Contingency Plan and test them. One rule of thumb to use is: The more complex the configuration and the more the enterprise relies on the technology, the more the plan should be tested.

On the other hand, if the same tests are performed too often, the tests could become too familiar. Observers and participants might overlook potential problems and weaknesses if the tasks involved are perceived as monotonous or formidable.

Data Recovery

Your Contingency Plan must also include the necessary steps to restore data during a crisis. Applications such as ARCserve and JETserve are completely menu driven and do not require tapes to be restored in order. However, during a full backup, both applications give you the option to create a summary file that includes information such as the media name, sequence number, and so on. Instructions detailing media information aid in minimizing the recovery window thus reducing the amount of system downtime.

After a disaster both ARCserve 6 and JETserve permit any user to run the software. However, the only information that an individual user can restore is information to which that user had access. Data on backup media can be protected further by specifying the password protection option when a backup is performed. This option prevents restoration of data, should backup media fall into the wrong hands. With a restore password safeguarding backup media, individual files cannot be restored to a different server. Procedures such as this must be in place and adhered to in order to avoid potential sabotage.

Recovering Individual Files

If a file is inadvertently deleted or is deemed unreadable as a result of corruption, the chances of it being restored are based on the backup history. If your backup strategy includes only a weekly full backup, the file might not have been included in the last backup depending on when the file was created. On the other hand, if your backup strategy includes more frequent backups, the last backup set should contain a copy of the file. Keep in mind, though, that any changes to the file since the last backup are lost.

The time it takes to restore a single file also depends on the backup method. Incremental and differential backups take longer to locate files for restore especially if each subsequent backup resides on a separate tape. ARCserve can generate reports on media sessions, which enables you to pinpoint the most recent backup. After that you can use the Media View of Restore to locate the file on tape.

File selection for file-by-file restoration is limited with JETserve. You can select a single file or a group of files or directories, but JETserve is designed for fast backup and restoration of entire volumes. As a result, it might take longer to restore a single file using JETserve than to restore an entire volume. Furthermore, a JETserve file-by-file restoration creates a temporary file. The size of this file is relative to the size of the volume in which it is being restored.

Temporary File Size = 10MB/GB on the NetWare Volume

For example, if you need to restore a single file on a four gigabyte volume, JETserve creates a 40 megabyte temporary file, regardless of the file size. This should not pose any significant problems to most NetWare environments, but these are issues that must be considered.

Restoring a Volume

Because ARCserve uses the file-by-file method, restoring a volume is not much different from restoring a single file. If you used file interleaving during an ARCserve backup job, you can use one of the ARCserve media reports to locate the session in the backup set, since multiple nodes could exist on the same tape.

With JETserve, a volume restore must be to the identical configuration. It is possible to restore files to a volume of a different configuration, but it must be done using the JETserve file-by-file restore feature. The volume restore is much faster than the file-by-file restore, but regardless of the volume's contents, a volume with a few files takes just as long to restore as a volume of the same size that is almost completely allocated.

Rebuilding a Server

When trying to restore the data on an entire server, the primary goal is speed. After a server failure, the first step is to replace the necessary equipment and reconfigure the server *exactly* as it was prior to failure. With ARCserve, you must restore the server boot disk, the NetWare operating system, and configure the NetWare volumes the same as before.

Running the Cheyenne Disaster Recovery Preparation (CDRPREP) utility can reduce the time required for restoring an entire server dramatically. The log file that CDRPREP generates provides you with information about the server startup files, NetWare modules, and the server configuration. In addition, the log file gives you step-by-step instructions to restore the server's data along with ARCserve.

It is crucial, however, that you update the server with the most recent NetWare patches regularly. During server recovery, the CDR process will not be completed unless the required support modules are compatible. If you encounter problems, abort the process and manually reinstall ARCserve. After that, you can still restore from media without problems.

ARCserve does not restrict NDS restoration to the volume or server level. You can restore NDS alone or with any combination of files. JETserve, however, restricts NDS restores to the volume level.

To recover a server using JETserve, you must install the JETserve software and create the NetWare volumes with the same size and number of segments. JETserve restores all of the selected NetWare volumes from media.

IMPORTANT: Document all volume segment information. During a JETserve restore, the volume size and number of segments and blocks must match the volume on the media. Otherwise, you must perform a file-by-file restore which dramatically increases the restore window.

Rebuilding the Network

If a catastrophe occurs, the NetWare LAN must be equipped with nearly identical equipment and software to guarantee a speedy recovery. As convenient as it may be, upgrading hardware and/or software following a catastrophe is not advisable. If the necessary equipment is obsolete, this should have been recognized during testing or when trying to pinpoint a vendor. In the latter case, this issue should have been addressed and the necessary measures identified. Otherwise, you pose the risk of incompatible hardware and software.

Regardless of the type of disaster, resuming business operations involves several phases:

- **Contact key personnel for data recovery** - Alert all IS staff and dispatch them to the recovery site. In addition, ensure that key personnel from departments who utilize mission-critical applications are present to verify data integrity.
- **Obtain backup media from off-site location** - Duplicate backup media must be easily retrieved at any time. If you store backup media at a location that does not have 24-hour access, you might not be able to get to your backup media in an emergency.
- **Configure server and clients according to documented procedures** - Server and client configurations must be available on hard and soft copy. If you install NetWare, apply the same patches and updates that existed before the disaster. Configuring the server *exactly* as documented speeds the data recovery process and avoids potential problems with software applications.
- **Begin the data recovery process** - NetWare 4.x necessitates restoring NDS information before file system data. Even though the goal is to restore data as fast as possible, security policies are still in effect. As a result, NDS must be in place to maintain access controls. Once NDS is restored, you can begin to restore critical applications and data.
- **Verify data integrity** - Once applications and data are restored, the usefulness of the data must be verified. Key users should login to the network and access critical applications before login is enabled for the general user community.

Maintenance

After testing or operational changes (system or application replacements or upgrades) the procedures for data recovery require modification. If your Contingency Plan is not adequately tested and the procedures for data recovery are not verified and updated appropriately, the plan can become obsolete. Most would consider the best method of maintaining the Contingency Plan to be updating it immediately after any observed problems or weakness. However, even maintenance efforts should be systematic because testing must occur again to ensure that the problem has been corrected or the new changes have not affected another component in the enterprise.

Problems that surface during testing might not always reflect a weakness in your Contingency Plan. You must also make sure the test adequately tests the plan. Furthermore, if you cannot comprehend what was learned from the test, then discard the test and develop a new one. Each test should reveal something about the risks and the assurance measure(s) used to counter the risk.

Update your Contingency Plan after each test if data recovery efforts fail. Signs of inadequacy include:

- The amount of time it takes to restore network activity is greater than the allotted restore window
- Storage media that contained mission-critical information is unreadable
- Fumbling through the recovery process
- Guesswork of server configurations
- Inability to contact key personnel

In addition, review your Contingency Plan and update it if any assurance measures are proven to be insufficient. For example:

- An intruder invades the network
- Confidential information is leaked to outsiders
- Equipment theft occurs

These issues warrant a scrupulous review of your current security measures to protect information, and the equipment in which the data is stored. Apply new measures and test them as soon as possible.

Even though testing may be modularized, notify all key IS staff of any plan updates. Changes in data recovery procedures for one component might infringe on the responsibilities of another component. In addition, as part of the Contingency Plan, any key IS staff member should be capable of resuming mission-critical operations. As a result, ensure that all circulated copies of the Contingency Plan are current.

Appendix A
Enterprise Example

This section examines issues in developing a Contingency Plan for a mid-size enterprise. Our mid-size enterprise is the Acme Group, an engineering firm that markets and distributes their products world wide.

Acme Group - Background Information

Corporate headquarters is located in Los Angeles. The MIS headquarters is also based in Los Angeles. Since this is the central political point within the organization, most of the people in this office tend to exercise their political clout. Consequently, organizational decisions are based on the specific needs of one component rather than a careful analysis to determine what is best for the entire organization.

The Dallas office is responsible for product marketing. It has an MIS staff that supports 1500 users. Despite supporting more users than any other city, the MIS staff feel that they are not included in significant decision-making processes spawned by the Los Angeles office. As a result, there is hostility between the Los Angeles and Dallas MIS departments.

All of the manufacturing facilities are located in Phoenix. The products that are developed in Los Angeles and Dallas are sent to Phoenix for production and distribution. Since most of the work in Phoenix is in a manufacturing facility, only 35 users access the LAN. However, there is a stand-alone computer system that runs the company's manufacturing and order fulfillment software.

The Los Angeles office feels that the Phoenix facility does not warrant a LAN administrator because of the number of users that access it. The Los Angeles MIS staff, however, is very helpful with any LAN problems, and there is a cordial relationship between the two cities.

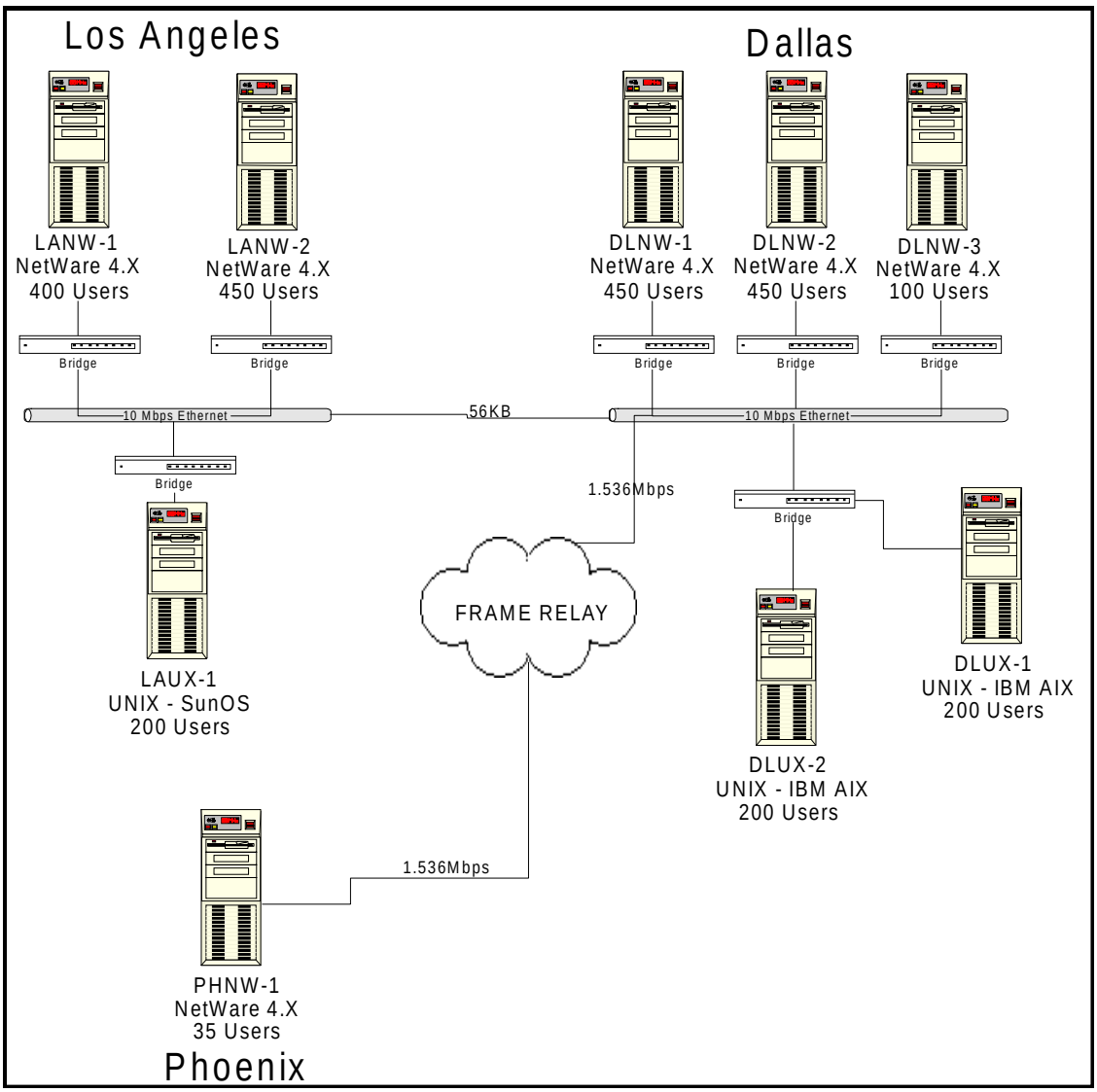

Figure A-1. The Acme Group Network

Server Configurations and Software

Table A-1
Server Information

Fileserver Name	Number of Users	Total Disk Space	Free Disk Space
LANW-1	50	10GB	325MB
LANW-2	450	40GB	1.31GB
LAUX-1	200	20GB	3GB
DLNW-1	450	40GB	4.4GB
DLNW-2	450	40GB	3GB
DLNW-3	100	20GB	5GB
DLUX-1	200	20GB	2.5
DLUX-2	200	20GB	1.5GB
PHNW-1	35	1.5GB	500MB

Servers are configured based on the network traffic and requirements at each location. Specific MIS staff members are responsible for server operation and maintenance.

The LANW-1 and DLNW-3 function as tape servers. The company's central database of designs is stored on LAUX-1. The volume on which the database exists is mirrored to the servers in the Dallas and Phoenix locations so that any new designs or changes to existing designs are immediately accessible to the production lines. This saves The Acme Group a great deal of time and money because none of the production lines have to wait to receive hard copies of designs.

The engineers use a Computer-Aided Design (CAD) application to create the designs. Licensed copies of the software are located on the LAUX-1 server in Los Angeles and the DLUX-1 server in Dallas. The Acme Group has relied on the CAD software to design its products, and has not drafted hard-copy designs since its engineers were formally trained and actively began using the CAD application.

The marketing group uses brainstorming and decision-making software to generation ideas and strategies for product campaigns. Several staff members provide input to make complex decisions and generate detailed reports and graphical presentations. These applications as well as other pertinent marketing information are stored on DLNW-1.

The Los Angeles servers are state-of-the-art systems. However, the DLNW-3 and PHNW-1 servers are older systems whose components are no longer supported by the manufacturer.

With the exception of the Phoenix location, all servers are located in climate-controlled areas in the MIS department that has limited physical access. The server at the manufacturing facility is located in the office of the production supervisor. Any staff member that has an office key can unlock his office. The master key is located in the supply room and can be accessed with any office key.

The Phoenix organization relies on a manufacturing application to track and analyze orders based on current facility production. The scheduling/dispatch information is generated hourly during facility operations to ensure that the work floor has current information that reflects schedule changes, production line problems and other delays. The proprietary system is located in a locked, temperature-controlled room and is maintained by the company that designed the application.

Existing Policies and Procedures

The Acme Group does not have a formal Contingency Plan in place. Physical security of servers is provided with keypad-access locks on the rooms in which the equipment is located. Access controls and limited audit trail information (i.e., login and logout times) are provided by the NetWare operating system.

There is no formal user training related to network security awareness and user responsibility. However, new employees are required to attend orientation in which company policies and procedures are explained as well as the rules governing intellectual property. The MIS departments routinely circulate information related to virus alerts and encourage regular scanning of floppy disks. A copy of the latest desktop virus protection and detection software may be installed from the network to any workstation.

Full backups are performed each night at the Los Angeles and Dallas locations. The Phoenix location is on a GFS rotation with Monday through Thursday incremental backups followed by a full backup each Friday. Alternate tapes are sent to an off-site storage facility on a weekly basis.

Risk Analysis

Undocumented Policies and Procedures

Given the tension between the MIS headquarters and the Dallas MIS staff, which supports most of the users in the entire company, relevant issues revealed by the Dallas MIS staff may be disregarded or underrated by MIS headquarters. This may pose a considerable threat to enterprise operations if adequate funding is not available to impose the necessary security measures to protect critical data.

Users

The Acme Group does not have formal network compliance training at any of its facilities. Software applications training is available to help users improve their skills, but no formal orientation exists to explain policies and procedures for protecting company information. When new employees begin work, someone from their department spends time with that individual explaining how to login to the network, access applications required to complete their tasks, and read electronic mail. This produces the possibility of miscommunication and entrusts the responsibility of protecting mission-critical applications and data entirely up to the integrity and competency of the employees.

Theft

Currently, equipment theft is not a problem with the Acme Group. However, the risk is always there. In the Phoenix office, anyone who has an office key, in effect, has access to the server. A drive loss or even complete system loss may not result in a loss of market share due to data loss, but would still hinder productivity, which is not insurable nor recoverable.

Server Management

Server configurations and maintenance are managed by each MIS department. Currently there are no standard guidelines or requirements for managing server configurations (e.g. application of patch kits, etc.). This could pose unnecessary problems if the MIS headquarters continues to make decisions without consulting the Phoenix group. For example, if LA mandates the use of a new third-party application for virus protection, the application may cause conflicts with existing applications or NLMs that run on the Phoenix servers. As a result, the company would have purchased licenses for software that can only be used by one-third of the overall servers while leaving other systems inadequately protected.

Hardware/Software Failure

The stand-alone system that the Phoenix facility relies on to manage orders and production schedules poses a great risk to manufacturing productivity. Unfortunately, the company that maintains the system is located out of state. Should a disaster (e.g., hardware or software failure) occur, production would be delayed and could remain at a standstill until the problem is resolved.

Assurance Measures

The situation between corporate headquarters and the Dallas office is a deterrent to the development of a sound company contingency plan. The Dallas office believes that management does not comprehend the importance of their role in the decision-making process and, as a result, the overall security of the company is affected.

The Dallas office might benefit from using audit trails to justify their need for server improvements or funding for other tools needed to adequately manage network operations. If adequate assurance measures are not in place for the Dallas office, or any component of The Acme Group, the entire enterprise is at risk of losing critical information.

User Training

With the widespread use of electronic mail and Internet access, formal training is a necessity. It is the company's responsibility to inform users of their responsibilities when using electronic mail as well as Internet services, such as the World Wide Web. Downloading large files can tie up bandwidth, software applications may be infected or cause other system problems, or employees may be perusing unauthorized web sites. In either case, business profits are affected because productivity is hindered.

Formal training also informs users of their duty to comply with existing policies and procedures. Training should not be limited to the technical aspects of protecting enterprise information (e.g. running virus detection applications and backing up data), but should also explain to employees the importance of data management as a business process. This is especially important because it will catch the attention of those individuals who could care less about backups and virus protection, but have a vested interest in the company losing market share due to an information disaster.

Backup Software

Because The Acme Group LAN encompasses dissimilar networks, an application that uses file-by-file backup technology might accommodate their needs. The company can take advantage of customizable features such as unattended automated backups, remote server and workstations backup, HSM, and virus protection.

Such features would allow either the Los Angeles group or the Dallas group to back up the server in Phoenix. This would eliminate the need for additional hardware and software components or a full-time network administrator at the Phoenix location.

Two servers in the network, LANW-1 and PHNW-1, are running out of disk space. The organization can either increase the amount of available disk space or incorporate HSM into the backup process to archive old data.

Despite the IS departments' efforts to combat virus attacks by circulating alerts and providing easy access to the latest anti-viral applications, users may not always take advantage of such safeguards.

An image-based backup system would be suitable for the stand-alone system that runs the manufacturing application. No single-file or directory restores would be required if a failure occurred. A full backup could be performed quickly and efficiently each session.

Conclusion

Before The Acme Group can develop and implement a sound Contingency Plan, several business issues must be resolved. A thorough network assessment at the Dallas office might reveal issues that will compel the LA headquarters to include the Dallas IS staff in the decision-making process.

Appendix B
NetWare 4 Server Memory Worksheet

The following worksheet demonstrates how to calculate the recommended system memory requirements that your Compaq server will require to run intraNetWare. The minimum memory to install intraNetWare is 20 MB. However, this worksheet allows you to either calculate a more efficient value for a new server, or double-check the memory requirements for an existing server. This worksheet replaces memory calculation formulas found in previous NetWare 3 and 4 documentation.

STEP 1: Calculate the Following Variables.

V1. Enter the *total* number of megabytes of disk connected to the server.

(For example: enter 1 for each MB, enter 1024 for each GB.)

V2. Calculate the number of megabytes of *useable* disk space connected to the server. _____MB

(If you are mirroring or duplexing multiply V1 * 0.5, otherwise copy V1.)

V3. Enter the server's volume block size (4, 8, 16, 32, or 64). _____KB

V4. Calculate the number of disk blocks per MB (divide 1024 / V3). _____Blocks/MB

V5. Calculate the total number of disk blocks (multiply V2 * V4). _____Blocks

V6. Enter the maximum number of clients (end-users) attached to the server. _____Clients

(For example: enter 24 for 24 end-users)

V7. Enter the maximum number of files that will reside on the server. _____Files

STEP 2: Calculate your Individual Memory Requirements.

Line 1. Enter the base memory requirement for the core OS and NDS. _____KB
(Enter 6144 for intraNetWare; 11,264 for SFT; or 12,288 for SMP.)

Line 2. Calculate the memory requirement for the Media Manager multiply _____KB
V1 * 0.1).

Line 3. Calculate the memory requirement for directory tables _____KB
(multiply V7 * .006, or if suballocation is enabled multiply V7 * .011).

Line 4. Calculate the memory requirement for additional Name Spaces _____KB

(multiply V7 * .006 * number of additional Name Spaces loaded on the server).

Line 5. Calculate the memory required to cache the FAT (multiply Line V5 * _____KB
.008).

Line 6. Calculate the memory requirement for file cache using the following table: _____KB

This calculation uses a 0.4-MB file cache per client memory requirement. The decrease as the user community size increases is based on assumptions regarding increased repetitive use of shared data (temporal and spatial locality) within cache.

Less than 100 clients	V6 * 400
Between 100 and 250 clients	40,000 + ((V6 - 100) * 200)
Between 250 and 500 clients	70,000 + ((V6 - 250) * 100)
Between 500 and 1000 clients	95,000 + ((V6 - 500) * 50)

Line 7. Enter the total memory (KB) required for support NLMs. _____KB
2,000KB is recommended for BTRIEVE(700), CLIB(500), INSTALL(600), and PSERVER(200)

Line 8. Enter the total memory (KB) required for other services. _____KB

Other services include GroupWise, ManageWise, NetWare for Macintosh, NetWare for SAA, and so on.

STEP 3: Calculate the Server's Total Memory Requirement.

Line 9. Total Lines 1–8 for your total memory requirement (in KB). _____KB

Line 10. Divide Line 9 by 1024 for a result in MB. _____MB

Using this result, round up to the server's nearest memory configuration. intraNetWare will enhance server performance by using all leftover memory for additional file cache.

The amount of memory reserved by intraNetWare for drivers and modules may depend on the type and number of server components as well as the amount of server memory. Observe the memory utilization statistics provided by MONITOR.NLM in the Resource Utilization option to see how server resources are utilizing available RAM.

Index

A

About this TechNote 1-1
Activity log *See* audit trail
Additonal resources 1-4
Alternate site testing 7-5
ARCserve 5-11, 6-2, 6-7, 6-8, 6-15, 6-21, 6-22, 7-6, 7-8
  activity log 6-12, 6-18, 6-19
  applying patches to 6-13
  backup methods 6-16, 6-17, 6-21
    archiving data 6-18
    auto pilot 6-19
    file interleaving 6-20
    parallel streaming 6-21
    RAID technology 6-21
    rotation 6-17
  data verification 7-2
  database 6-7
  feature comparison 6-2
  file interleaving 6-15
  Open-file Agent 6-12
  options and utilities 6-15
  performance 6-24
  performance factors 6-7
  pre-flight check 6-15
  Push Agent 6-8
Array
  configuration utility 5-7
Array controller 5-7
ASR 5-10
Assessing the network 5-17
Assurance measures 5-1
  backup strategy 5-16
  enterprise example A-6
  insufficient 7-11
  network operating system 5-12
  planning for disaster recovery 5-19
  security policy 5-2
  server options 5-4
  user training 5-3
Audit trails 5-15
AUDITCON 5-15
AUTOEXEC.NCF 6-22
Automatic
  read/write reallocation 5-10
Automatic Server Recovery *See* ASR

B

Backup
  assessing the network 5-17
  automated 6-2
  custom 6-16
  data selection 6-14
  feature comparison 6-2
  file-by-file 5-18, 6-1
  frequency 6-10, 6-25
  full 6-16
  Hierarchical Storage Management 5-19
  image-based 5-18, 6-1
  media 6-9
  methods 6-8
  off-site storage 7-2
  options 6-23
  remote 6-8
  security 7-6
  server configuration 6-4
  software applications 5-17, 6-3, 6-15, 7-2, A-7
    ARCserve 7-6
    JETserve 6-23
    performance 6-24
  software pplications
    JETserve 7-6

strategy 5-16, 5-20, 6-14, 6-16, 6-25
auto pilot 6-20
GFS scheme 6-19
tape system 6-3
virus detection 5-18
window 6-11, 6-13
management 6-13
open files 6-12
Backup technology 6-1
network environment 6-1
Backup window
formula 6-25
Backward compatability 5-11
BTRIEVE.NLM 5-12
Business operations 3-1, 3-2, 3-5, 4-7, 5-17, 5-19, 6-14, 6-26, 7-1, 7-4, 7-9
Business process 3-2, 3-3, 3-6, 3-7, 5-2, 5-20

C

CDRPREP 6-22, 7-9
Chapter
organization 1-1
summaries 1-1
Cheyenne Disaster Recovery Preparation *See* CDRPREP. *See* CDRPREP
CLIB.NLM 5-12
Client risks 4-1
Cold site 5-21
Compaq
web site 6-13
Compaq drivers
Health driver 5-10
Compaq products
array controller 5-7
Fast-SCSI-2 drives 5-10
Integration Server 6-5
tape devices 6-9
tape drives 6-24
Compaq server options
Recovery Server Option 5-4
Server Fault Tolerance 5-5
Compaq technology 5-9
Advanced Error Correcting Code 5-10
Automatic Server Recovery 5-10
Insight Manager 5-11
PCI Hot Plug 5-11
Recovery Server Option 5-10
Version Control 6-5
Compaq utilities
Array Configuration Utility 5-7
Compression 4-7
CompuServe forum 6-13
Contingency Plan 6-19, 7-1
maintenance 7-10
recovery team 7-3
Testing 7-4
testing frequency 7-5
Contingency planning 2-3, 3-1, 5-1, 5-2, 5-20, 7-11
benefits 3-6
development 2-3
disaster recovery 3-5
risk analysis 3-2
security 5-2, 5-3
security planning 3-3
summary 3-6
Controller
SCSI 6-6
Corrupting data 4-4

D

Data
- archiving 6-18
- compression 6-6
- mission-critical
  - on workstations 4-4
- off-site storage 7-2
- protection 2-3
  - server 6-2, 6-3
  - workstation 6-2, 6-3
- recovery 7-3, 7-6
  - individual files 7-6
  - locations 5-21
  - rebuilding a server 7-8
  - restoring a volume 7-8
  - team 7-3
  - the network 7-9
- risks of saving on desktop 4-5
- verification 6-13, 7-2

Deleting data 4-4
Developing a contingency plan 2-3
Disaster
- enterprise example A-6

Disaster recovery 3-5
- data disaster 3-5
- hardware failure 3-5
- planning 5-19
- site disaster 3-5

Disk duplexing 5-6
Disk mirroring 5-6
Disk space
- management 4-6

Disk storage 5-11, 5-15
- compression 4-7, 6-6
- management 4-7
- suballocation 4-7

Downtime 2-1, 2-2, 3-1, 3-6, 4-3, 4-5, 4-6, 5-6, 5-10, 5-11, 5-18, 5-20, 6-11, 6-22, 7-6

E

ECC 5-10
Enterprise
- example A-1, A-3
  - assurance measures A-6
  - network A-2
  - policies and procedures A-4
  - risk analysis A-5
  - server management A-6
  - theft A-6
  - user training A-7
  - users A-5
- mid-size A-1

Enterprise operations
- critical components 4-1

Enterprise storage management
- solutions *See* Management

Equipment
- replacement 7-4

Example enterprise *See* Enterprise

F

FAT 5-15
File
- restoration 7-6, 7-8

File Allocation Table 5-15
File interleaving 6-20

H

Hardware
- disaster A-6
- failure 3-5
- replacement 7-4

Hardware failure 4-6
Health driver 5-10
Hierarchical Storage Management 5-19
Home site 5-22
Host server risks 4-1
Hot site 5-21

I

Inadequacy
in training 4-4
Insight
Manager 6-5
Insight Manager 5-11
Integration Server 6-5
Internet security 5-3
intraNetWare
AUDITCON 5-15
disk compression 4-7
file system limitations 5-15
security features 5-2
SFT III 5-5
suballocation 4-7
Introduction 2-1
IS staff 4-3

J

JETserve 6-3, 6-12, 6-14, 6-23, 6-24, 6-25, 7-6, 7-8
applying patches to 6-13
backup options 6-23
data verification 7-2
feature comparison 6-2
performance 6-24
RAID performance 6-24

L

LAN 6-20, 7-9
administrator A-1
Login, user authentication 5-2

M

Maintenance 7-1, 7-10
Management
contingency planning 5-2
disk space 4-6
server A-6
Management solutions 2-2
data protection 2-3
developing a contingency plan 2-3
Identifying
risks 4-1
Media
policies and procedures 4-4
Memory 5-12
Mid-size enterprise A-1
MONITOR.NLM B-3
File service processes 4-7
Packet receive buffers 4-7

N

National Computer Security Association (NCSA) 4-5
NDS 5-14
restoration 7-9
NetWare
applying patches to 6-13
AUDITCON 5-15
disk compression 4-7
file system limitations 5-15
hot fix area 6-23
patches 7-9

redirection area 6-23
security features 5-2
server memory worksheet B-1
SFT III 5-5
suballocation 4-7
Network
downtime *See* downtime
operating system
Novell Replication Services 5-13
rebuilding 7-9
Network Interface Controller (NIC) 6-20
Network operating system 5-12
audit trails 5-15
NLM 6-13
accomodating the 6-9
Notational conventions 1-2
Novell Directory Services 5-14
Novell drivers
BTRIEVE. 5-12
CLIB.NLM 5-12
Novell Replication Services 5-13
Novell Storage Services 5-15
Novell Support Software Diskettes 6-5
NRS 5-13
NSS 5-15
NSSD 6-5, 6-13

O

operating System 5-12
Organization 1-1

P

Parallel streaming 6-21
Password 7-6
policies and procedures 4-4
PCI Hot Plug 5-11
People (associated risks) 4-2
Physical security 5-3, 5-12
Planning for disaster recovery 5-19
Policies and procedures 4-3, 4-4
enterprise example A-4
passwords 4-4
unattended media 4-4
workstation 4-4
Policy and procedures
updates 5-4
Potential threats *See* Threats
Pre-failure alerts 6-5
Pre-flight check (PFC) 6-15

R

RAID
RAID 0 5-6
RAID 1 6-21
RAID 5 6-2, 6-21
distributed data gaurding 5-7
RAID 5 6-23
RAID level characteristics 5-7
Reallocation
automatic read/write 5-10
Rebuilding
a server 7-8
Recovery
of data 7-6
Recovery Server Option 5-4, 5-10
Redundant Array of Inexpensive Disks (RAID) 5-5
Reference documents 1-4
Remote
server risks 4-1
Replication services 5-13
Resources 1-4

Restoration
file-by-file 7-6, 7-8
NDS 7-9
volume 7-8
Risk analysis 3-2
enterprise example A-5
Risk index 3-3
formula 3-3
Risks diagram 4-2
Rules and procedures
user violation Policies and procedures
Rules for node grouping 6-15

S

Sample enterprise *See* Enterprise
SCSI 6-2
controller 6-6
Security
contingency planning 5-3
physical 5-12
user guidelines 5-4
workstation 5-2
Security management 5-3
Security planning 3-3
perfomance stipulations 3-3
Security policy 5-2
Server
boot disk restoration 7-8
configuration 6-6
backup 6-4
enterprise example A-3
JETserve 6-4
SCSI controller 6-6
downtime *See* downtime
management
enterprise example A-6
memory worksheet 6-6
rebuilding a 7-8
Server configuration 5-12
Server Fault Tolerance 5-5
Server options 5-4
Server replication 5-14
SFT III 5-5
Simple Network Management Protocol 5-11
Small Computer System Interface 6-2
SmartStart 6-5
SNMP 5-11
Software
disaster A-6
failure 4-7
Software piracy 4-6
Solutions
data protection 2-3
developing a contingency plan 2-3
enterprise storage management 2-2
Stand-alone system risks 4-1
Suballocation 4-7
Summary
of chapters 1-1
SUMMARY.TXT 6-5

T

Tape
server configuration
optimal 6-4
Tape devices 6-9
TechNote
text conventions 1-2
Testing 7-1, 7-4
data recovery 7-6
frequency 7-5

test plan 7-4
Text conventions 1-2
Theft 4-6
enterprise example A-6
Thrashing 4-7
Threats
catastrophe 4-8
disk space management 4-6
hardware failure 4-6
IS staff 4-3
software failure 4-7
theft 4-6
undocumented policies and procedures 4-3
users 4-4
virus 4-5
Threats, Identifying 4-2
Training 5-3, A-7
employee 4-3
inadequate 4-4

U

User 4-4
enterprise example A-5
guidelines 5-4
training 5-3
User login 5-2

V

Virus 4-5
detection 5-18
Volume
restoration 7-8

W

WAN 5-13
Wide Area Network 5-13
Workstation
policies and procedures 4-4
saving data on 4-4
security 5-2
Workstation risks 4-1