

Introduction to LAN

TDC 363

Lecture 08

Course Outline

- Network Trouble Shooting Procedure (Chap. 12)
 - Case Studies of Network Trouble Shooting
 - Network Trouble Shooting Tools
 - Sniffer (ethereal)
- Integrity and Availability (Chap. 13)
- Network Management (Chap. 15)
 - Configuration Management
 - Performance Management

Troubleshooting Methodology

1. Identify the Symptoms
2. Identify the Scope of the Problem
3. Establish What Has Changed
4. Select the Most Probable Cause
5. Implement a Solution
6. Test the Solution
7. Recognize the Potential Effect of the Solution
8. Document the Problems and Solutions

Identify the Symptoms

- Is access to the network affected?
- Is network performance affected?
- Are data or programs (or both) affected?
 - Is this a client/server application or a local program?
- What are the network services affected?
- What are the error messages?
- Do the symptoms manifest themselves consistently?
 - An interim problem or a reproducible problem

Cf. Fig 12-1 & 12-2

02/28/08

TDC363-08

4

Identify the Scope of the Problem

- Identify the scope of the problem
 - How many users or network segments are affected?
 - When did the problem begin?
- If a problem is universal - affecting the entire LAN or WAN - you will naturally want to answer these questions very quickly

02/28/08

TDC363-08

5

Establish What Has Changed

- Did the operating system or configuration on a server, workstation, or connectivity device change?
- Were new components added to a server, workstation, or connectivity device?
- Were old components removed from a server, workstation, or connectivity device?

02/28/08

TDC363-08

6

Establish What Has Changed (cont.)

- Was a server, workstation, or connectivity device moved from its previous location to a new location?
- Was a server, workstation, or connectivity device replaced?
- Was new software installed on a server, workstations, or connectivity device?
- Was old software removed from a server, workstation, or connectivity device?

02/28/08

TDC363-08

7

Select the Most Probable Cause

- Verify user competency
- Re-create the problem
 - Can you make the symptoms recur every time?
 - Can you make the symptoms recur some of the time?
 - Do the symptoms happen only under certain circumstances?
 - Do the symptoms ever happen when you try to repeat them?

02/28/08

TDC363-08

8

Select the Most Probable Cause

Cast Study I

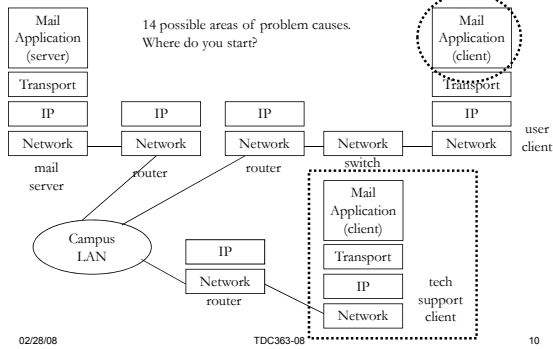
- A user calls the help desk that she cannot get her e-mail. The error message is that the mail server does not respond and the mail application times out. You are assigned to solve this problem.

02/28/08

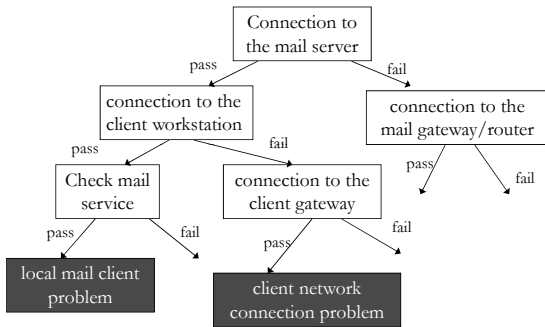
TDC363-08

9

Identify the Problem Cause



Case Study I (cont.)



Case Study I (cont.)

Client Network Connection Problem

- Verify physical connectivity
 - Is the device turned on?
 - Is the NIC properly inserted?
 - Is a device's network cable properly connected to both its NIC and the wall jack?
 - Do patch cables properly connect punch-down blocks to patch panels and patch panels to hubs or switches?

Implement a Solution

- Steps to help you implement a safe and reliable solution
 - Collect all the documentation you have about a problem's symptoms
 - If you are reinstalling software on a device, make a backup of the device's existing software installation
 - Perform the change, replacement, move or add that you believe will solve the problem
 - Test your solution

02/28/08

TDC363-08

13

Implement a Solution (cont.)

- Before leaving the area in which you were working, clean it up
- If the solution fixes the problem, record the details collected about the symptoms, the problem, and the solution in your organization's call tracking database
- If your solution solved a significant change or addressed a significant problem, revisit the solution a day or two later to verify the problem is fixed and hasn't caused other problems

02/28/08

TDC363-08

14

Test the Solution

- After implementing the solution, it must be tested to verify that it works properly
- Type of testing performed depends on the solution
- Often good to enlist the user who reported the problem in testing your solution, too

02/28/08

TDC363-08

15

Recognize the Potential Effects of the Solution

- When implementing a solutions, consider the:
 - Scope
 - Tradeoffs
 - Security
 - Scalability
 - Cost

02/28/08

TDC363-08

16

Document the Problems and Solutions

- Trouble Report and Tracking System (TRTS)
- What are the data fields in TRTS
 - Originator (Name, Phone, Organization, E-Mail)
 - Description (symptom) of the problem
 - Severity and Priority
 - Resolution of the problem
 - Problem Cause
 - Dates (open, assigned, resolved)
 - Location
 - Owner (Name, Phone, Organization, E-Mail)
 - Problem category (software, hardware, procedure, document)
 - Work Hours

02/28/08

TDC363-08

17

Case Study II

- This case study is from the book (p. 641)
- Scenario: a user loses his/her network connection. You happen to be in the area, and you have a laptop and a crossover cable with you.
- Do you agree with the trouble shooting procedure presented in the book?
- Do you have a better way of performing trouble shooting in this case?
- Network motto: if you have a hammer in your hand, **do not** see everything as nails.

02/28/08

TDC363-08

18

Case Study III

- This is a common problem for laptop users who have both wireless and wired Ethernet connection.
- John has been using wired connection in the office for a while, and everything works fine.
- He gets a wireless card. He installs it at home and everything works fine.
- When he comes back to the office, he cannot surf the Internet. He can ping his officemate's workstation.
- How do you do trouble shooting?

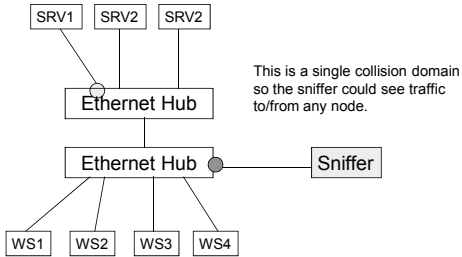
Tools for Network Trouble Shooting

Hardware Tools

- Crossover Cable
- Tone generator and tone locator
- Multimeter
- Cable continuity tester
- Cable performance tester
- Spectrum analyzer (wireless)

Sniffer/Protocol Analyzer (Hub)

- Investigate protocol/message contents
- Require in-depth knowledge of the protocol

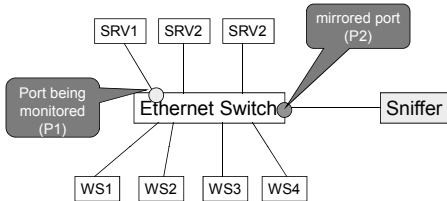


02/28/08

TDC363-08

22

Sniffer (Ethernet Switch)



The traffic to and from SRV1 (P1) is copied and forwarded to the sniffer (P2).
Not all Ethernet switches support mirror ports.
An advanced Ethernet switch can mirror multiple ports.
Reference: p. 635

02/28/08

TDC363-08

23

Sniffer Demonstration

- Windows – NetMon
- Linux – tcpdump
- Solaris – snoop
- Freeware– ethereal/wireshark

02/28/08

TDC363-08

24

More on Trouble Shooting

- Create an environment where you can reproduce the problem and test your solution.
- Learn from your mistakes
 - Document it
- Learn from others
 - Read their documents
 - If they do not have it, document it for them and for yourself.
- Avoid making the same mistake twice.

Course Outline

- Network Integrity and Availability
 - Availability calculation
- Fault tolerance network
 - Protection from power outage
 - Protection from network connections
 - Protection from server failure
 - Protection from storage failure
- Backup and disaster recovery plan

Integrity and Availability

Chapter 13

Integrity and Availability

- Integrity
 - Soundness of a network's programs, data, services, devices, and connections
- Availability
 - Refers to how consistently and reliably a file system to be accessed by authorized personnel
 - Percentage of time that the system/service is available to users.
- Reliability
 - Probability of failure-free operation for a given period of time. This is a function of time.
 - $R(0) = 1$
 - $R(\infty) = 0$ (why?)

02/28/08

TDC363-08

28

Availability Calculation

- Mean Time Between Failure (MTBF)
- Mean Time TO Repair (MTTR)
- System Downtime = MTTR
- Availability
 - Assumption: failures are detected immediately.
 - $\text{Availability} = \text{MTTR} \div (\text{MTBF} + \text{MTTR})$
- Example:
 - A server has a failure once a month
 - MTTR = 4 hours
 - $\text{Availability} = 1 - 4 \div (24 \times 30) = 99.4\%$

02/28/08

TDC363-08

29

Guidelines for Protecting Your Network

- Prevent anyone other than a network administrator from opening or changing the system files
- Monitor the network for unauthorized access or change
 - Process of monitoring a network for unauthorized access to its devices is known as **intrusion detection**

02/28/08

TDC363-08

30

Guidelines for Protecting Your Network (cont.)

- Record authorized system changes in a change management system
- Install redundant components
 - Situation in which more than one component is installed and ready to use for storing, processing, or transporting data is referred to as **redundancy**

02/28/08

TDC363-08

31

Guidelines for Protecting Your Network (cont.)

- Perform regular health checks (audits) on the network
- Monitor system performance, error logs, and the system log book regularly
- Keep backups, boot disks, and emergency repair disks current and available
- Implement and enforce security and disaster recovery policies
- Run anti-virus program regularly (e-mails, user files, system files, etc.)

02/28/08

TDC363-08

32

Viruses

- Program that replicates itself with the intent to infect more computers via networks, media, e-mails, etc.
 - Boot sector viruses
 - File-infected viruses – attach themselves to executables
 - Macro viruses
 - Network viruses
 - Worms – not a virus but could become a mechanism to carry virus (e-mail worms)
 - Trojan horse – programs do what they are not supposed to do. (Do not download software from unknown sources)
 - Bot – what is it? (ref. p. 673)

02/28/08

TDC363-08

33

Symptoms of Viruses

- Unexplained increases in file sizes
- Programs launching, running, or exiting more slowly than usual
- Unusual error messages appearing without probable cause
- Significant, unexpected loss of system memory
- Fluctuations in display quality

02/28/08

TDC363-08

34

Functions of Antivirus Software

- Signature scanning
 - Comparison of a file's content with known virus signatures in a signature database
- Integrity checking
 - Method of comparing current characteristics of files and disks against an archived version of these characteristics to discover any changes
- It should detect viruses by monitoring unexpected file changes or virus-like behaviors

02/28/08

TDC363-08

35

Functions of Antivirus Software (cont.)

- Receive regular updates and modifications from a centralized network console
- Consistently report only valid viruses, rather than reporting "false alarms"
 - Heuristic scanning
 - Attempt to identify viruses by discovering "virus-like" behavior

02/28/08

TDC363-08

36

Guideline for Antivirus Policy

- Every computer in an organization should be equipped with virus detection and cleaning software that regularly scans for viruses
- Users should not be allowed to alter or disable the antivirus software
- Users should know what to do in case their antivirus program detects a virus

Guideline for Antivirus Policy (cont.)

- Every organization should have an antivirus team that focuses on maintaining the antivirus measures in place
- Users should be prohibited from installing any unauthorized software on their systems
- Organizations should impose penalties on users who do not follow the antivirus policy

Fault Tolerance

- Capability for a system to continue performing (i.e., providing services) despite of an unexpected hardware or software malfunction
 - Performance may be affected but basic functionality is not affected.
 - Example 1, the response time may be slower, but you can get the response.
 - Example 2: You can process 50 transactions/sec, instead of 100 transactions/sec.
- Failure
 - Deviation from a specified level of system functions or performance
- Fault
 - Involves the malfunction of one component of a system
 - A fault may cause many failures.
 - A failure may be a manifestation of multiple faults.

Fault Tolerance

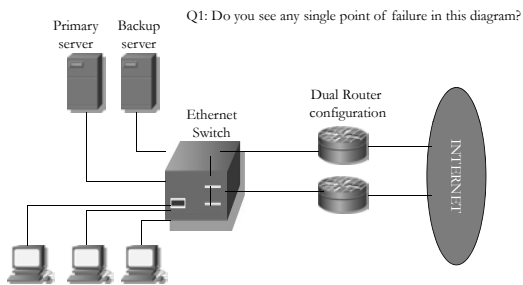
- Fail-over
 - Process of one component immediately assuming the duties of a failed component
- Hot swappable
 - You can change hardware components while the system is operational. (when it is hot)
 - Example, NIC cards on a fault tolerant server
- To assess the fault tolerance of your network, you must identify any **single point of failure**

02/28/08

TDC363-08

40

Example – Single Point of Failure



02/28/08

TDC363-08

41

Fault Tolerance of

- Power
- Network Connections
 - WAN
 - LAN
- Server
- Disk/Storage
 - RAID
 - NAS
 - SAN

02/28/08

TDC363-08

42

Environment and Power

- Environment
 - Analyze the physical environments in which your devices operate
- Power
 - Whatever the cause, networks cannot tolerate power loss or less than optimal power

02/28/08

TDC363-08

43

Uninterruptible Power Supply (UPS)

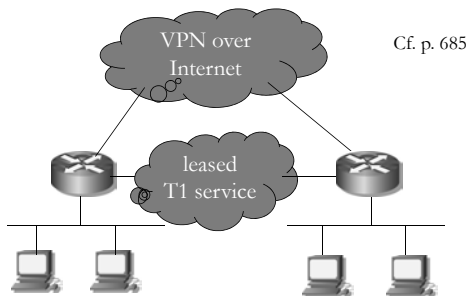
- Battery-operated power source directly attached to one or more devices and to a power supply
- Standby UPS
 - Switches instantaneously to the battery when it detects a loss of power from the wall outlet
- Online UPS
 - Uses the A/C power from the wall outlet to continuously charge its battery, while providing power to a network device through its battery
 - How long is your UPS?
 - 5, 10, 30, 90
- Generators

02/28/08

TDC363-08

44

Fault Tolerant WAN Connectivity

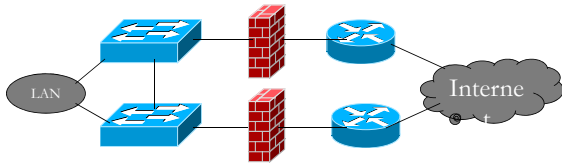


02/28/08

TDC363-08

45

Fault Tolerant Network Connectivity

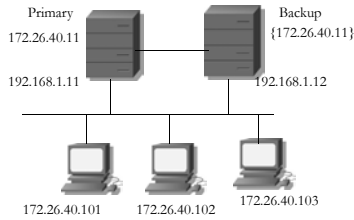


c.f. Fig 13-5

- Load balancing
 - Automatic distribution of traffic over multiple links or processors to optimize response
 - Redundancy does not imply load balancing, but load balancing usually imply redundancy. Why?
 - A routing protocol supports both redundancy and load balancing.

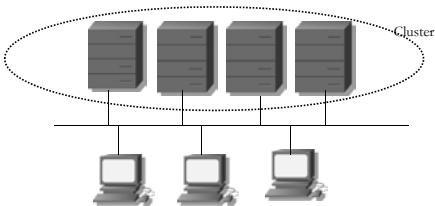
Server Mirroring

- Fault tolerance technique in which one server duplicates the transactions and data storage of another



Server Clustering

- Fault-tolerance technique that links multiple servers together to act as a single server
- Clustered servers share processing duties and appear as a single server to users
- Clustering is more cost-effective than mirroring



Storage - RAID

- Redundant Array of Inexpensive Disks (RAID)
 - A sophisticated means for dynamically replicating data over several physical hard drives
 - Collection of disks that provide fault tolerance for shared data and applications
 - A group of hard disks is called a disk **array**
 - The collection of disks working together in a RAID configuration is often referred to as the “RAID drive”

02/28/08

TDC363-08

49

RAID Level 0—Disk Striping

- Simple implementation of RAID in which data are written in 64 KB blocks equally across all disks in the array
- No redundancy in RAID Level 0

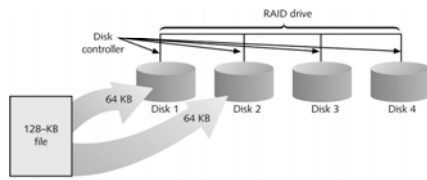


Figure 13-6 RAID Level 0—disk striping

02/28/08

TDC363-08

50

RAID Level 1—Disk Mirroring

- Data from one disk are copied to another disk automatically as the information is written
- 50% Disk utilization, most expensive (per MB)

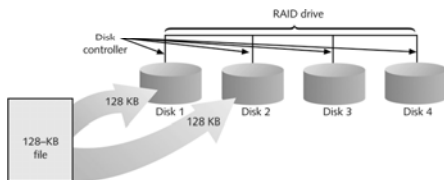


Figure 13-7 RAID Level 1—disk mirroring

02/28/08

TDC363-08

51

RAID Level 3—Disk Striping with Parity Error Correction Code (ECC)

- Disk striping with a special type of error correction code (ECC)
- Term **parity** refers to the mechanism used to verify the integrity of data by making the number of bits in a byte sum to either an odd or even number
- In the case of disk failure, **data can be reconstructed from the parity data** (error correction, not just error detection)

02/28/08

TDC363-08

52

RAID Level 3 (cont.)

- Parity error checking
 - Process of comparing the parity of data read from disk with the type of parity used by the system
 - Disk utilization: 75%

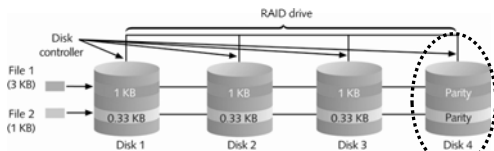


Figure 13-8 RAID Level 3—disk striping with parity ECC

02/28/08

TDC363-08

53

Parity Error Correction (example)

Example 1: 1 0 1 0 1 1



disk 1: odd bits

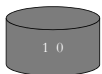


disk 2: even bits

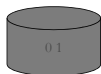


parity bits (even parity)

Example 2: 1 0 1 0 1 1



3k+1 bits



3k+2 bits



3k bits



parity bits (odd)

02/28/08

TDC363-08

54

RAID Level 5—Disk Striping with Distributed Parity

- Data are written in small blocks across several disks
- Better read but slower write than Mirrored Volume (RAID L1)
- Require more system resource (CPU and memory) for generating parity data
- Most commonly used.
- Minimum of three disks (why?)

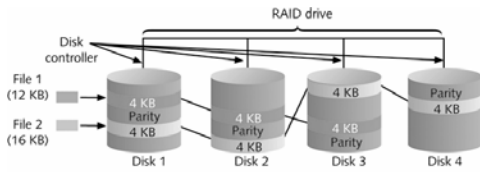


Figure 13-9 RAID Level 5—disk striping with distributed parity

02/28/08

TDC363-08

55

Network Attached Storage (NAS)

- Specialized storage device or group of storage devices providing centralized fault-tolerant data storage for a network

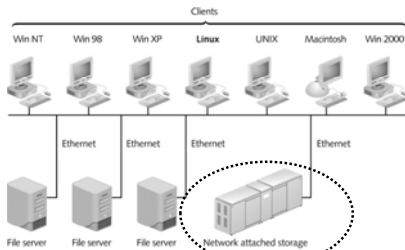


Figure 13-10 Network attached storage on a LAN

02/28/08

TDC363-08

56

NAS (cont.)

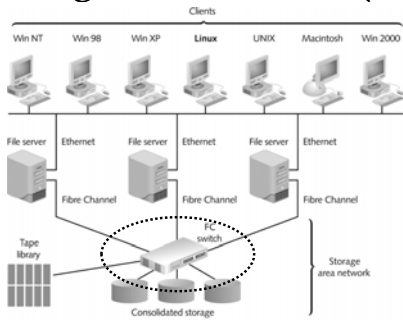
- NAS device is NOT a file server.
- Clients do not connect to the NAS device directly. Their requests still go through a file server.
- NAS device maintains its own interface to LAN
- It shares the network bandwidth with other applications.
- Advantages:
 - Optimized for file service
 - Scalability – no interruption of service by adding more disk space.

02/28/08

TDC363-08

57

Storage Area Networks (SANS)



02/28/08

TDC363-08

58

Storage Area Networks (SANS)

- Distinct networks of storage devices that communicate directly with each other and with other networks
- Extremely fault tolerant
- Extremely fast
 - Much of their speed can be attributed to **Fiber Channel**

02/28/08

TDC363-08

59

SAN (cont.)

- Can be distributed over multiple locations in a campus environment.
- Not like NAS, not part of the network
 - Does not affect network performance
- Like NAS, highly scalable.
- Disadvantage: too expensive
 - 10G Ethernet has its advantages and much cheaper.

02/28/08

TDC363-08

60

Data Backup

- Copy of data or program files created for archiving purposes
- Without backing up data and storing them off-site, you risk losing everything
- Note that backing up workstations or backing up servers and other host systems are different operations
- Tape or CD-RW

02/28/08

TDC363-08

61

Online Backups and Backup Strategy

- Online backups
 - Done over LAN/WAN
- Questions to ask in developing a backup strategy:
 - What kind of rotation schedule will backups follow?
 - At what time of day or night will the backups occur?
 - How will you verify the accuracy of the backups?

02/28/08

TDC363-08

62

Backup Strategy Methods

- Full backup
 - All data on all servers are copied to a storage medium
- Incremental backup
 - Only data that have changed since the last backup are copied to a storage medium
- Differential backup
 - Only data that have changed since the last backup are copied to a storage medium, and that information is then marked for subsequent backup

02/28/08

TDC363-08

63

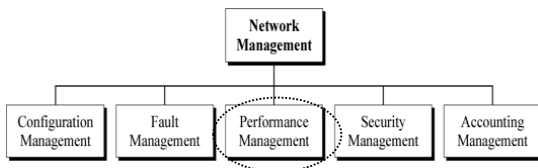
Disaster Recovery

- Process of restoring critical functionality and data after enterprise-wide outage that affects more than a single system or limited group of users
- Must take into account the possible extremes, rather than relatively minor situations

Network Management

Chapter 15

Five Areas of Network Management



F-C-A-P-S

Keeping Track

- Asset management
 - System of identifying and tracking the hardware and software on your network
- Change management
 - Use your change management system to record any changes resulting from network maintenance or upgrades

02/28/08

TDC363-08

67

Configuration Management

- Configuration: a state or an environment of your *network, hardware, and software*
- Configuration management:
 - Maintaining a set of *stable* configurations
 - When something goes wrong, you can easily and quickly *roll back* to the previous configurations (n-1).
 - If necessary, you can even roll back to n-2, or n-3 .. Configurations.

02/28/08

TDC363-08

68

Network Upgrade

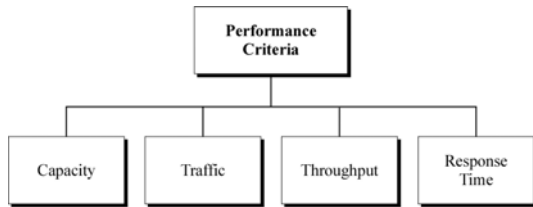
- Develop a plan, including a plan to roll it back
 - Before you do anything, make sure you know how to **undo** it.
- Review the plan and review it again
- Test it and test it again
- Schedule it.
 - Any scheduled downtime?
 - Double the estimate your engineers or vendors tell you.
- Inform your users
- Implement it
 - Make yourself (and others) ready and be prepared for any disaster
- Postmortem

02/28/08

TDC363-08

69

Performance Management



02/28/08

TDC363-08

70

Performance Measurements

- Round Trip Delay
 - One-way latency
- Jitter: variation of the delay
- Throughput (bps)
 - Transmission
 - Reception
 - Transmission + Reception
- Packet loss

02/28/08

TDC363-08

71

Review Questions

- Describe the 8-step trouble shooting procedure as recommended in the book.
- A user call the help desk that he cannot access a network drive. Illustrate your steps to do trouble shooting.
- Give 10 data fields to implement a trouble reporting system.
- What is network configuration management? Why do you need a plan for configuration management?
- What is **ping -f** on Linux?
- Identify delay and jitter in the Linux ping output.
- What is ethercal? What is a comparable tool on Linux?

02/28/08

TDC363-08

72

Review Questions (cont.)

- Calculate your average downtime per month for the system availability = 99.95%.
- How long is the power supply for a typical UPS during power outage? If it is not long enough, what is your solution?
- Design a network with redundant connections to the Internet.
- You have a single Frame Relay link between two offices. Give a cost-effective solution to create redundant links between the offices.
- List three items that you will put in an antivirus policy.
- Describe the difference between signature scanning and integrity checking of anti-virus program.
- Your vendor tells you that their NIC cards on their fault tolerant server are **hot swappable**, how do you verify it?

02/28/08

TDC363-08

73

Review Questions (cont.)

- What is the difference between server mirror and server cluster? Give one advantage of each.
- What are the three technologies to achieve fault tolerance in [disk] storage?
- **Given a bit stream and three disks, show the error correction code stored on the parity-bit disk (using odd parity bit).**
- Comparison of RAID5, disk efficiency, cost, and NOS support
- Draw a network diagram to illustrate NAS and SAN.
- Name one advantage of SAN over NAS, and one advantage of NAS over SAN.

02/28/08

TDC363-08

74
