

The Disaster Down the Hall

Jonathan L. Husni, MBA
President: Acendex

What exactly *is* a disaster?

- ◆ Anytime you're unable to access your data or process transactions for a period of time that affects your ability to conduct business due to a hardware or software failure, an environmental catastrophe, act of God, result of violence or other.

Why should you plan for such an eventuality?

- ◆ Maybe you shouldn't.
 - If you can carry on operations without access to your computer systems, you probably shouldn't waste your time or money.
 - Find out how dependent your business is on your information. Unplug your computers and carry on business as usual. You'll quickly discover if you need to plan for a disaster or not.

There are two separate but essential components of the Disaster Plan

◆ Human Behavior

- Where do they go?
- Who do they contact? And how? Where?
- What do they do?

◆ System Fault Tolerance

- How do we get our systems back online?
 - ◆ Who do we call?
 - ◆ How long does it take?
 - ◆ What is the procedure?
- How much data will be lost in the process? (time, orders, opportunity...)
- How do we do business?
 - ◆ Answer phones
 - ◆ Take orders
 - ◆ Process transactions

If you're still thinking that disaster planning is only for companies living in fear that their buildings will be bombed or burned to the ground, you're just not dealing with the facts.

There's lots of everyday things that can create business interruptions.

Sources of Trouble / Disasters

- ◆ Electrical Power
- ◆ Planned Obsolescence
- ◆ Acute failure of a critical component
- ◆ Central building trouble
- ◆ Telephone company outage
- ◆ Your Network Administrator
- ◆ The Janitor
- ◆ Hacker
- ◆ The Employee you fired last week
- ◆ Lack of planning

Electrical Power

- ◆ Blackouts
- ◆ Brownouts, sags, dips and their prolonged effects
- ◆ A/C Power Loss / Exposure to Heat
- ◆ Catastrophic Surge, Especially on the Ground Wire



Planned Obsolescence

Basically, if you're stuff's more than three years old, you're living on a prayer.



Acute failure of a critical component

- ◆ Motherboard
- ◆ Power Supply
- ◆ Disk
- ◆ RAM
- ◆ Controller
- ◆ NIC
- ◆ Router / Switch
- ◆ Etc.



Central building trouble

- ◆ A/C Failure
- ◆ Heat Failure
- ◆ Fire
- ◆ Sprinklers
- ◆ Building locked up
- ◆ Flood
- ◆ Power failure



Telephone Company or ISP Outage

- ◆ T1- or Internet-based order-entry systems
- ◆ Critical Web Site is Down
- ◆ Dial-up lines are out
 - C.O. Trouble
 - Backhoe



? Do any of these outages affect the way customers perceive the viability of your business ?

Your Network Administrator

- ◆ Deletes an important file which turns out not to be on any tapes
- ◆ New system being staged in the production environment causes malfunctions on the main network
- ◆ Vendor patches not applied, new updates not compatible
- ◆ Administrator testing features during production



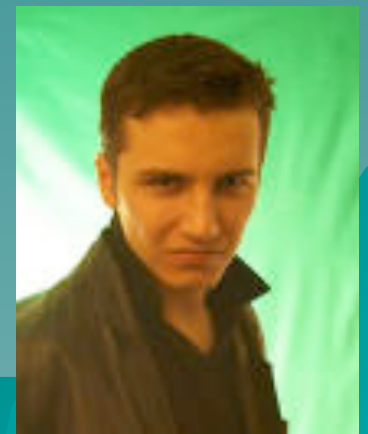
Lack of Planning

- ◆ Suddenly reaching a critical point where user demand wrecks performance
- ◆ Unexpectedly running out of disk space



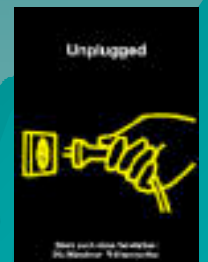
Hacker

- ◆ Hacker loads web site on your production servers wrecking performance.
- ◆ Hacker deletes data
- ◆ Security compromise (HIPAA, other)
- ◆ Virus or Worm



The Janitor

- ◆ Someone in your space, whether cleaning staff, maintenance, space planner, whatever unplugs your system
- ◆ Other unscheduled collateral but catastrophic damage introduced by accident (leaking air conditioner, sprinkler system, dust buildup, others)



Your Ex

Angry ex-employees are unpredictable at best, particularly if they ever had remote access to your systems.

I gave an hour lecture last year on a firm who fired their network administrator, failed to lock him out, and paid a very *very* dear price.



So, how do you plan for unplanned outages?

I recommend a *Weighted Scorecard* approach. Start with a checklist of the most common causes of unplanned system outages, indicate how likely each one is to happen at your organization, and how concerned you are about it; their product is your "*Need for Preparedness*" score. Work your way down the list from top to bottom until you're adequately prepared for any eventuality that concerns you. Since every firm is different, there are no right answers. *Your answers may also change based on actual experiences with any of these situations.*

Weighted Scorecard Sample

Brief	Effect Size	Probability Score	Need for Preparedness Score	Solutions	Cost of Preparedness (\$/hr)	Cost of Unpreparedness (hours)	Exceeded Hours of Downtime
Power Failure	100	0.95	95	UPS		\$300.00	
Brownouts, sags, dips	30	100	8000	Offline UPS		\$600.00	
Power Surges	30	100	8000	Offline UPS		\$600.00	
Air Conditioner outage	30	0.4	32	Two 1-ton auxiliary ventilation		\$5.000.00	
Acute failure of critical system component:	100	100	10000	Cluster Offline to mirrored Server		\$12.000.00	
Motherboard	100	30	3000	Cluster Offline to mirrored Server		\$12.000.00	
Power Supply	30	30	2400	Cluster Offline to mirrored Server In-line Power Supplies		\$15.000.00	
Disk	30	70	5600	Cluster Offline to mirrored Server RAID SAN		\$15.000.00	
RAM	35	10	900	Cluster Offline to mirrored Server		\$12.000.00	
Controller	35	10	900	Cluster Offline to mirrored Server		\$12.000.00	
Building Air Conditioning							
Failure	30	10	600	Business Continuity Plan, ventilation, Offline to mirrored Server		\$17.000.00	
Building Heat Failure	30	10	900	Business Continuity Plan to mirrored Server		\$15.000.00	
Fire	100	1	100	Offline to mirrored Server		\$10.000.00	
Sprinklers	30	5	450	Offline to mirrored Server		\$10.000.00	
Building locked up	100	5	500	Offline to mirrored Server		\$10.000.00	
Proximity to Federal Building	30	5	300	Offline to mirrored Server		\$10.000.00	
Flood	30	10	800	Offline to mirrored Server		\$10.000.00	
Power Failure	100	100	10000	Offline to mirrored Server		\$10.000.00	
TI or other remote connectivity	70	100	7000	Multiple Centers Backup Units		\$5.000.00	
WAN connectivity	35	100	5000	Multiple Centers Backup Units		\$5.000.00	
Disaster outage Central Office (CO)	40	65	3400	Telephone, Multiple Centers Backup Units, Cellular		\$5.000.00	
Trouse	35	10	900	Telephone, Multiple Centers Backup Units, Cellular		\$5.000.00	
Seismic	35	15	1425	Telephone, Multiple Centers Backup Units, Cellular		\$5.000.00	
Administrator deletes important file which is not on tape	75	90	6750	Backup Backup Procedures, Backup to Server		\$5.000.00	
New system being staged in production environment causes malfunctions	40	90	3600	Offline Testing Environment, Segmented network		\$5.000.00	
Vendor patches not applied, new updates not compatible	40	90	3600	Priority Maintenance		\$12.000.00	
Administrator testing features during production	40	100	4000	Offline Testing Environment, Segmented network		\$5.000.00	
Suddenly reaching critical point where user demand exceeds performance	30	95	7800	Priority Maintenance, Quarterly System Reviews		\$12.000.00	
Hacker	30	90	7200	Vulnerability Scan, Security Audit, Penetration, Password Policy, Priority Maintenance, Quarterly System Reviews		\$15.000.00	
Social Engineering	30	90	7200	Vulnerability Scan, Security Audit, Penetration, Password Policy, Priority Maintenance, Quarterly System Reviews, Employee Awareness and Education		\$15.000.00	
Virus Attack	30	100	6000	Vulnerability Scan, Security Audit, Penetration, Antivirus Software Suite with T&A Automated updates, Priority Maintenance, Quarterly System Reviews, Employee Awareness and Education		\$15.000.00	
Sabotage by employee: Ex-Employee	35	25	2375	Vulnerability Scan, Security Audit, Penetration, Password Policy, Lockdown Procedure for Terminations, Priority Maintenance, Quarterly System Reviews, Employee Awareness and Education		\$17.000.00	
Out of Disk Space	100	95	9500	Priority Maintenance, Quarterly System Reviews		\$12.000.00	
Janitor / Cleaning Person	30	100	8000	Secure Server, Restricted Environment		\$1.000.00	



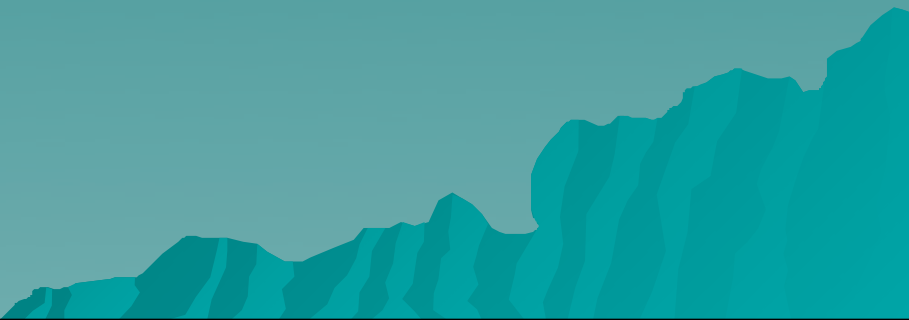
Beginning Your Plan

Once you've completed the weighted scorecard, complete these two simple steps to get you on your way:

1. Attach rough dollar amounts to your highest priorities and use the total to create a preliminary budget in accordance with your tolerance for scheduled downtime.
2. Solicit targeted recommendations from trusted sources who you believe have the experience to help you.

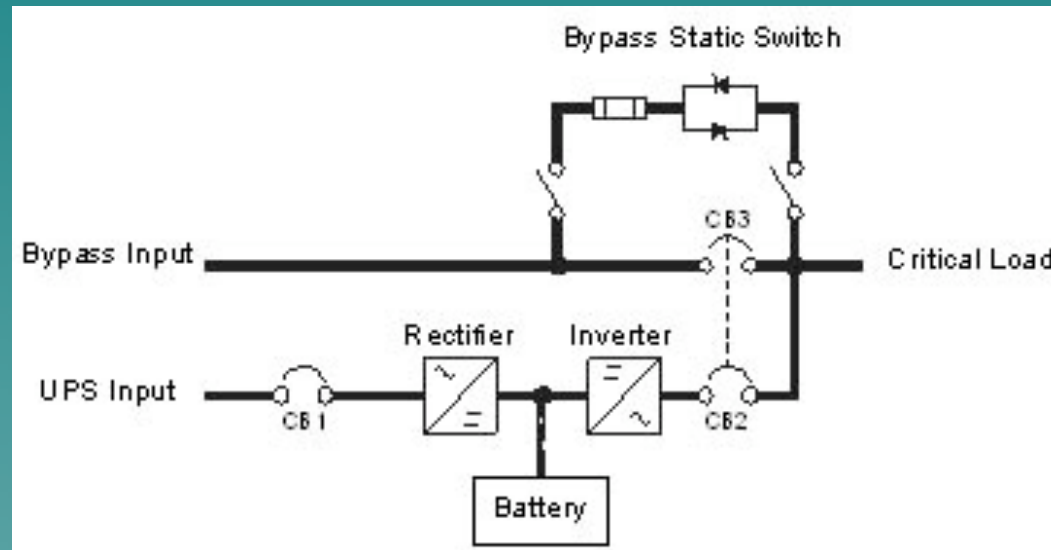
PROVEN SOLUTIONS:

Here are some proven solutions to the most prevalent sources of unscheduled system outages, why they are effective, and how they work:



PROVEN SOLUTIONS

◆ Online UPS



PROVEN SOLUTIONS

- ◆ Air Conditioner



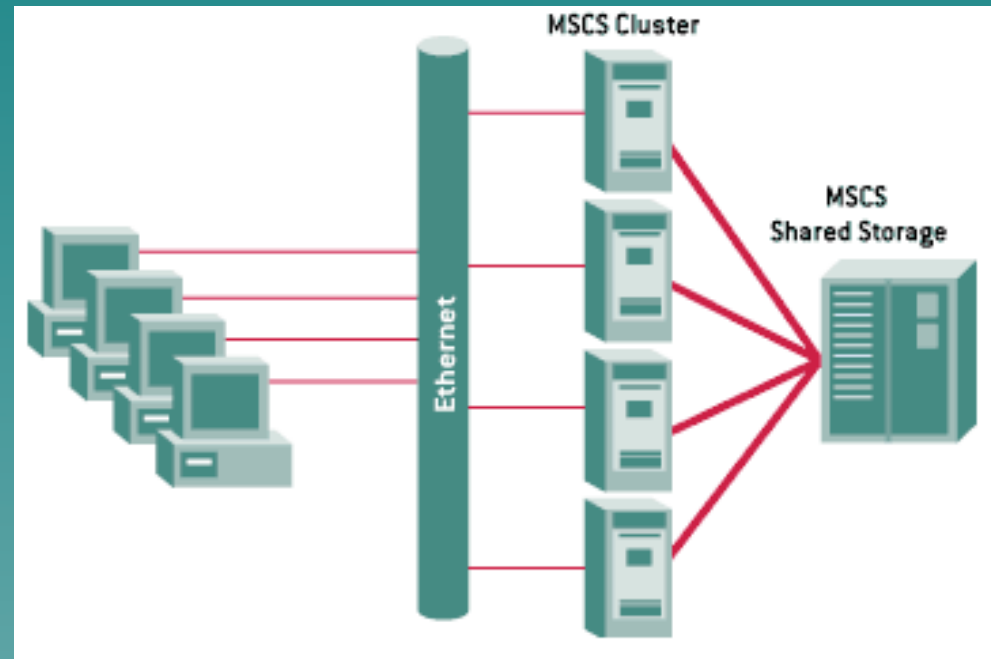
PROVEN SOLUTIONS

- ◆ Auxiliary Ventilation



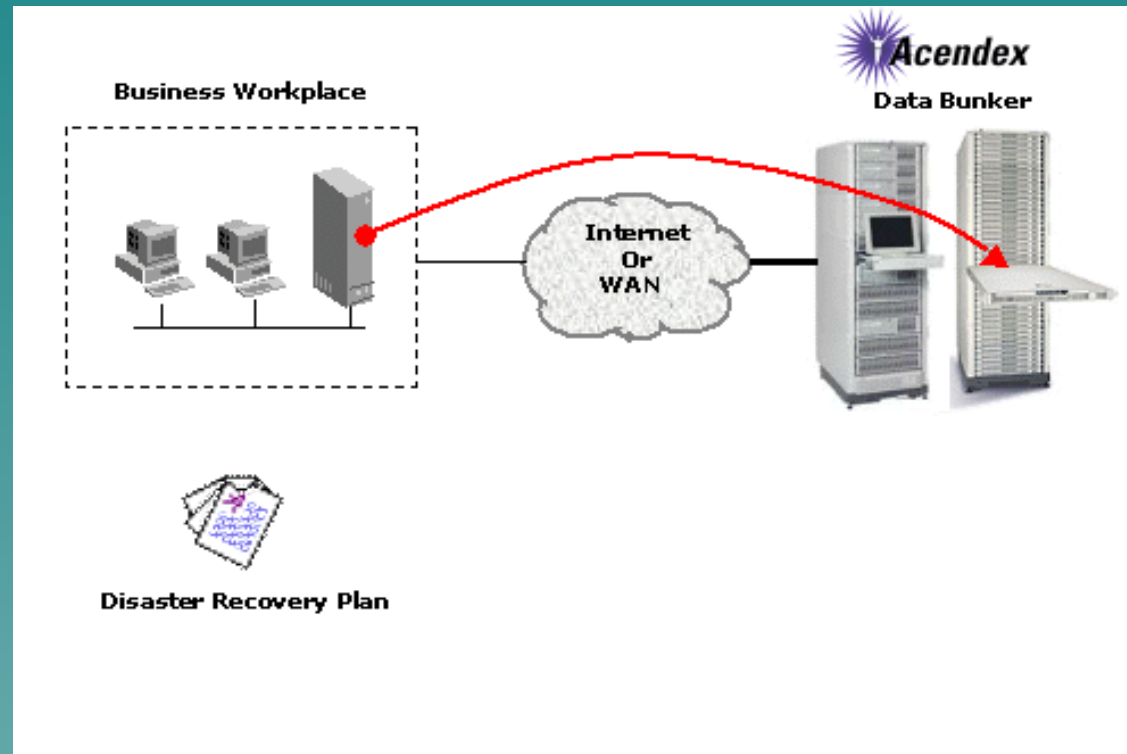
PROVEN SOLUTIONS

◆ Cluster



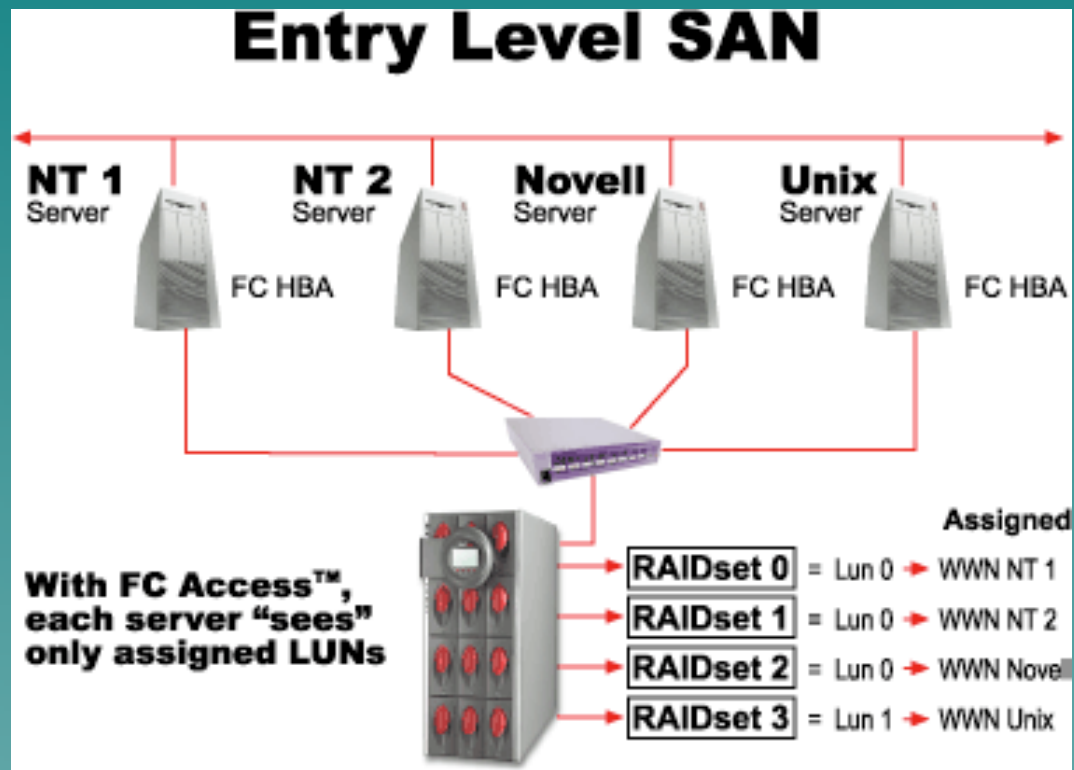
PROVEN SOLUTIONS

- ◆ Offsite Mirrored Server



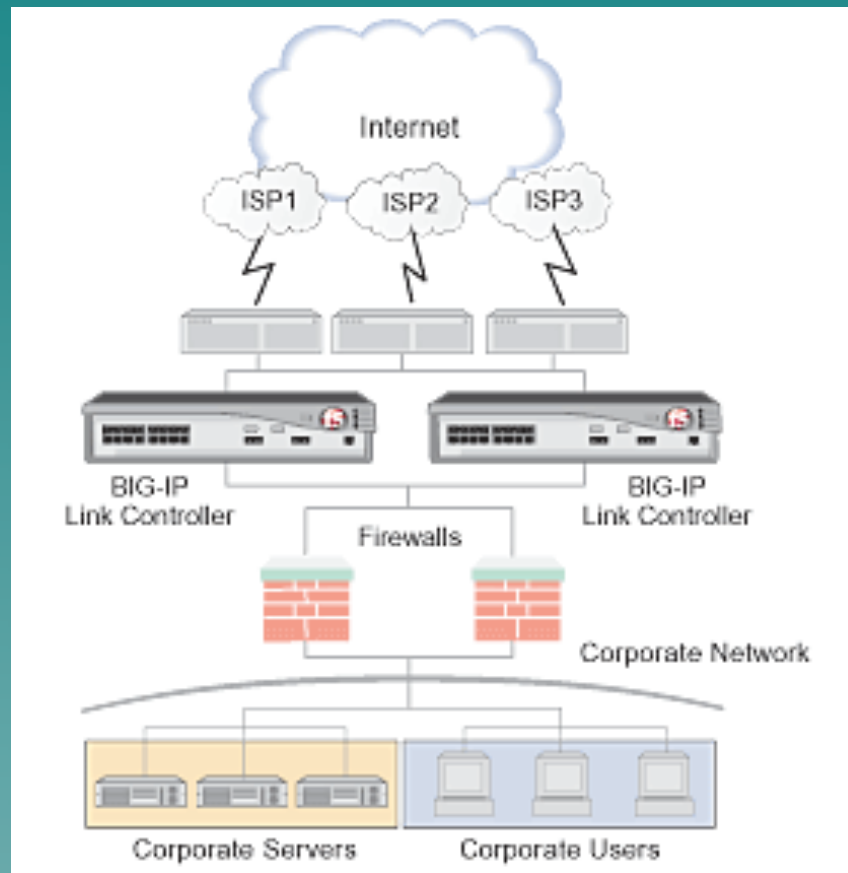
PROVEN SOLUTIONS

◆ SAN



PROVEN SOLUTIONS

- ◆ F5 Link Controller, Multiple Links



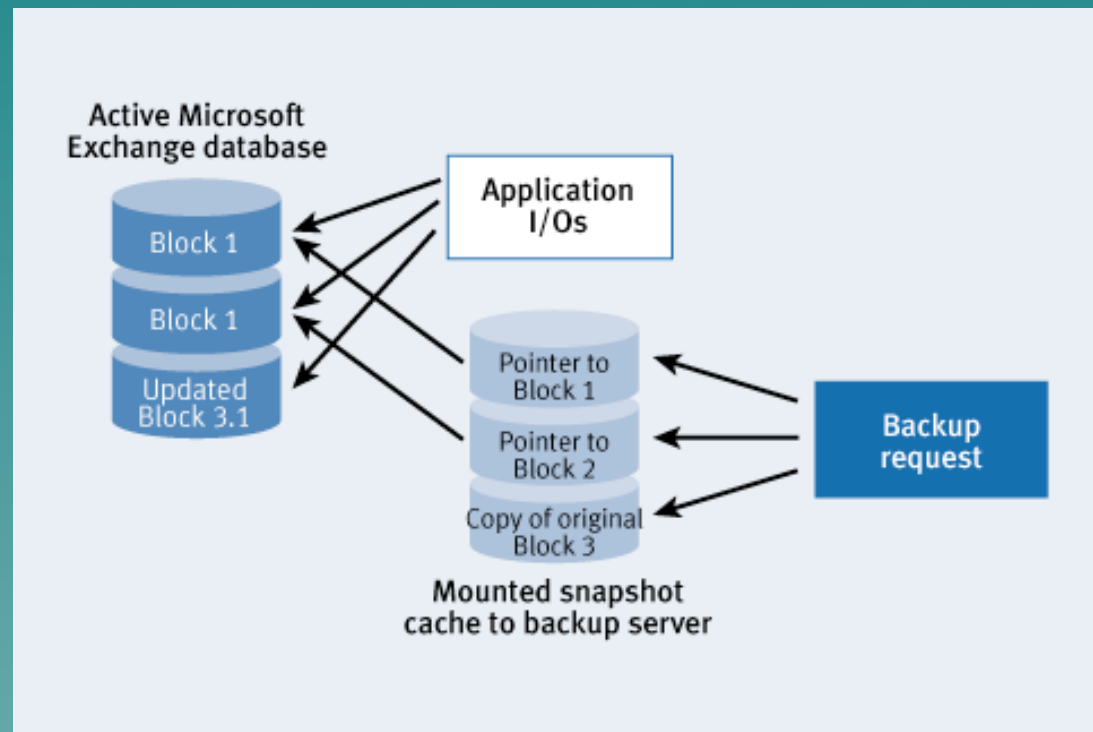
PROVEN SOLUTIONS

- ◆ Backup Device / Procedure



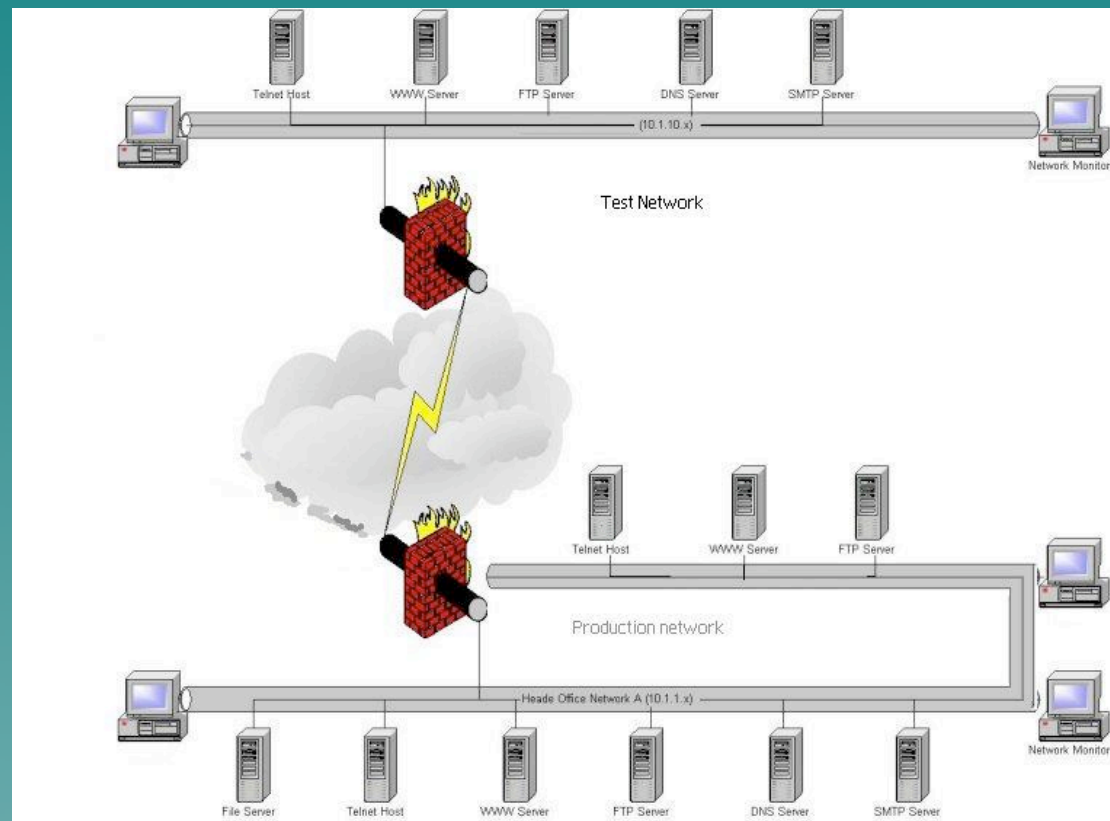
PROVEN SOLUTIONS

◆ Snapshot Server



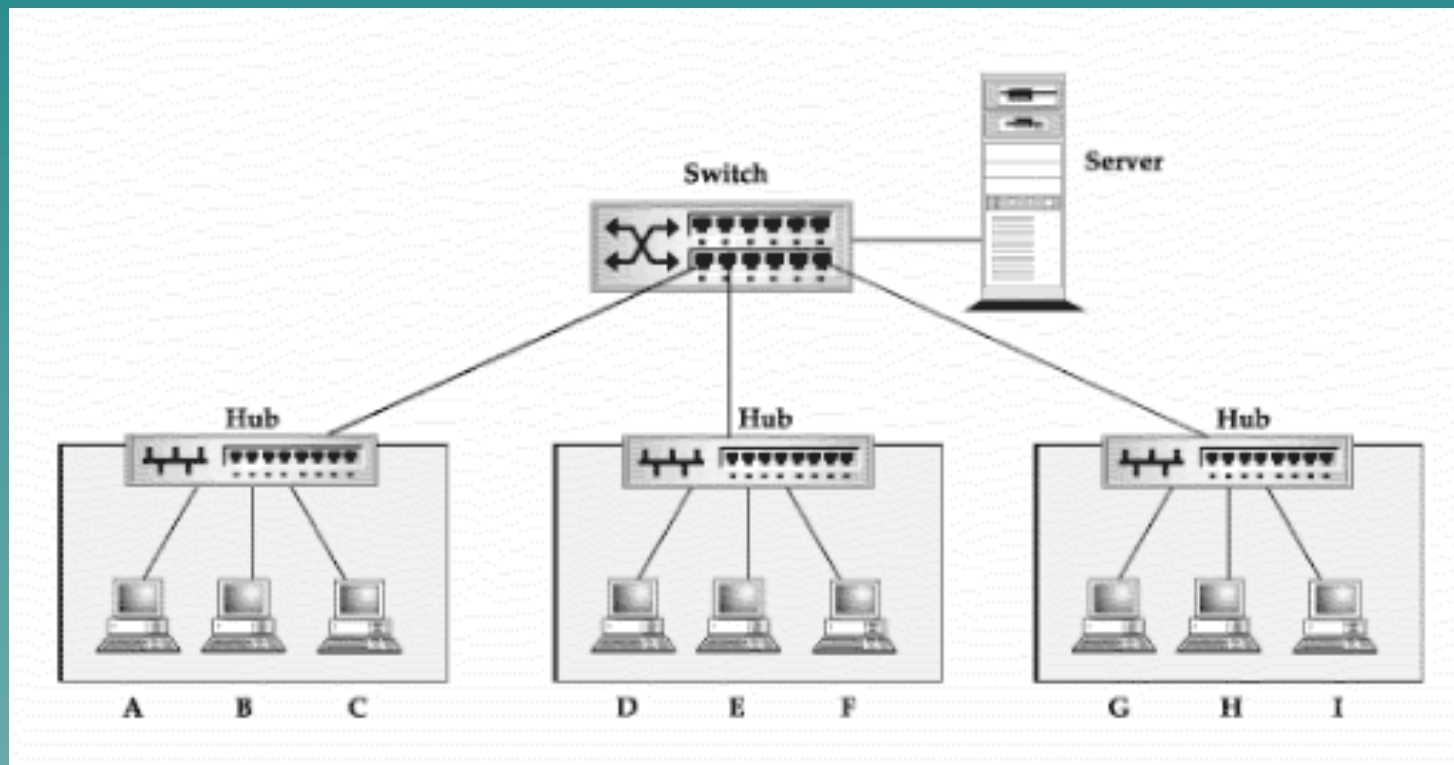
PROVEN SOLUTIONS

- ◆ Offline Testing Environment



PROVEN SOLUTIONS

- ◆ Segmented Network



PROVEN SOLUTIONS

- ◆ Monthly Maintenance



PROVEN SOLUTIONS

- ◆ Secure Server Room



PROVEN SOLUTIONS

- ◆ Vulnerability Scan / Security Audit



PROVEN SOLUTIONS

◆ Password Policy

"The red condor flies at midnight" is not a valid password. Please choose another.



PROVEN SOLUTIONS

- ◆ Lockdown



PROVEN SOLUTIONS



Acendex

**Emergency
Network
Services**

24 hours a day, 7 days a week

216.292.4878

M-F 8:00 am to 5:00 pm – dial “8”

After hours - extension 3099