This paper is in development

Redundancy Requirements for Computer Networks

John P. Abraham
Professor, University of Texas Pan American
jabraham@utpa.edu

ABSTRACT

Consumers have become so dependent on computer systems that it is very difficult for any organization to function without making proper arrangements for reliability, availability and serviceability (RAS) of computer networks. This paper, based on my experience as an IT consultant, examines the redundancy requirements and alternatives for practical implementations of redundancy at every stage of a computer system beginning with the power source and ending with data availability.

Maximizing RAS should be the goal of every IT department. Many are under the false assumption that having tape backup provides for redundancy. If any part of the hardware becomes defective the entire system is made ineffective. Power failures and power supply malfunction are common causes of inoperative servers. Servers should be equipped with redundant power supply and dual power sources. Broadband connection is another source of malfunction. More and more organizations are becoming dependent on cloud computing either as providers or consumers. Broadband unavailability can cripple such organizations. For maximum uptime dual broadband sources should be available along with routers capable of failover or load-balancing. To assure redundancy of Ethernet switches, at the minimum, spare switches should be on hand. Routers and switches should be connected to two power sources through a power transfer switch. In order to assure authentication services are always available, it is essential to create multiple domain controllers that replicate active directory and DNS.

Thus far the redundancy requirements of all physical inputs and outputs of a computer system were summarized. And now the redundancy requirements for data storage needs to examined. Data redundancy is a well discussed topic in Information Technology. Cloud backup services have made the topic even more popular. Data backups do not provide for high level of data availability. Defective hardware needs to be ordered, replaced and then only data can be restored. Depending on the quantity of data, it could consume a substantial amount of time for restoration. Online backups can even take longer. Data can be stored across several hard drives using RAID technology. Error correcting algorithms can calculate missing bits from defective drives. Hot swapping defective hard drive will rebuild the data, all the while making the data available to users. Though rare, hard drive controllers can fail, and dual controllers should be installed. This is referred to as duplexing. This paper will discuss most appropriate raid level and duplexing options. In order to assure data availability in time critical operations, failover clustering should be implemented. In failover clustering mirror servers are located in different geographical locations to protect against natural disasters. Small organizations can

implement failover clustering in virtual machines. This paper also examines backup options including cloud backup services.

1. INTRODUCTION

We are so dependent on computers today that most organizations cannot function when their network is down. Most, if not all, IT professionals are aware of the importance of backup. But, anything that might cause a hardware failure or software corruption can render the computer system unusable for a prolonged period of time. Every precaution must be taken to prevent computer downtime thereby maximizing computer availability. Computer availability can be measured dividing uptime by total time. Computer availability can be maximized by detecting points of failures and transferring services (failover) to redundant components. I have been providing IT related consulting for over thirty years and have been called in to solve total failures due to poor planning for redundancy. South Texas is prone to hurricanes and power failures. Many of the Maquiladora companies (plant in Mexico and offices in USA) are also located here. Power supply in Mexico is not very reliable and I take majority of this paper to explain power redundancy for that reason.

2. POWER REDUNDANCY

Two different power sources should be provided to redundant power supplies in mission critical hardware. Many servers, routers, and switches come with two power supplies installed that provides for power failover. I have observed in some installations both redundant power supplies connected to the same uninterruptable power supply (UPS). In this case, a single source of failure, the UPS, can bring the system down. Obviously the first source of power should be the AC provided by the power grid. The electric line providing current to a server should be isolated with its own breaker and surge protector at the AC panel. Such plugs should be marked with orange outlets. The ground wire to such outlets is also isolated, not connected to the common ground. A red outlet indicates backup power provided in case of outage.

Uninterruptable Power Supplies (UPS) can provide short term (just minutes to few hours) power backup. All critical components should be connected to UPSs. For longer term power, gas or solar generators are required. Gasoline, Diesel or Butane generators should be started and run frequently to maintain them in good working condition. If it has an autostart verify that it is working. Generated power should be connected to an automatic transfer switch which will change power source from grid AC to backup power when outage is detected. The transfer switch is connected to a predetermined number of circuit breakers. Standalone automatic transfer switches are also available for limited amperage.

My preferred source of power is Solar. For about the same amount of money one invests in a gas generator, a solar power generator can be setup. Here is what I have done. I purchased enough solar panels to yield 4 megawatt of power. You need to make that decision based on amount of power required. I connected them in serial to increase voltage so that I do not have to run thick wires. I connect these wires to a charge controller, with a cutoff switch between them.

I chose Outback Flexmax for this purpose. Charge controllers protect batteries from overcharging. I have several banks of 6 volt golf cart batteries serially connected to give 24 volts each. These 24 volt battery banks are parallel connected to increase the amperage. These batteries are then connected to an Outback inverter to produce either 110 or 220 Volts alternating current desired. The Outback inverter is also connected to the power from the grid which serves two purposes: (1) if the batteries are fully charged put the generated power back on to the grid and (2) if there is no sunlight, keep the batteries charged. Number of batteries you need depends on the duration of power needed in the absence of sunlight. In this installation power generated by the inverter in one of the two inputs to a standalone rack mount automatic transfer switch from APC. I installed cutoff switches and breakers to protect equipment and users. Though I have a gas generator, I have not had to use it since the solar was installed two years ago.

3. Broadband and Switch redundancy

Normally broadband service should work seamlessly. However we do encounter problems such as low speed, intermittent connectivity or no connectivity. Many organizations are subscribing to cloud based services that connectivity problems can cripple their business. The solution is to subscribe to two broadband services (from two different ISPs such as AT&T and Cable Company) and implement either failover or load balancing. Routers capable of load balancing are equipped with two or more Ethernet WAN ports. In order to give inputs into these Ethernet ports each provider must provide one or more useable IP addresses. In case of low cost broadband services only one IP address may be provided which will be assigned to the WAN side of their equipment. In such cases that IP address would be bridged.

A load balancing device may be a router, firewall, or a computer with multiple Ethernet ports. When configuring such a device, it may be setup to handle failover or load balancing. Failover setup is usually done if the secondary service is much slower than the primary. In case of the primary service failure it will automatically switch over to the slower secondary service. Secondary service is not used most of the time in case of the failover setup. In case of the load balancing configuration, both services are used and the traffic would be balanced between them. Caution should be used when configuring load balancing for secure sites or other sites that authenticate users. Switching between two routers will cause authentication errors. To solve this problem, rules can be set up to use primary or secondary port in special cases.

4. Data redundancy

In 2001, Information Week reported that 57% of all small businesses do not have a disaster recovery plan[]. Tandberg Data [] cites a 1994 survey by the University of Texas, Center for Research on Information Systems, where they reported 30% of small businesses lack formal data backup. The author has consulted many small businesses after they lost their data due to no backups or faulty backups. Most of them blindly trust the automated backups and do not review error logs. Others just use one or two tapes for backups. When data become corrupt the backup also has corrupt data. Incremental or differential tape backups using a seven tape rotation is still a viable option. In addition I recommend weekend and month-end full backups to be stored in a remote location.

Backups can be made on removable hard drives. A simple solution is to use inexpensive hard drive toasters and USB hard drives. The same software used for tape can be used with these hard drives. Hard drive backups are much faster.

Errors caused by hard drive failures can be minimized by setting up RAIDs. I set up boot drives on RAID 1 and Data drives on RAID 5. RAID 5 provides for parity and data distributed across all drives (minimum three drives required). If one drive becomes defective the missing data can be calculated using such techniques as Hamming. When the defective hard drive is replaced the data and parity information is rebuilt. RAID 10 provides for mirroring on sets of RAID 0. There are many other RAID levels such as RAID 6, 50 and 60. Regardless of the level used, installed hardware should allow for hot swap of hard drives in a mission critical server.

Cloud based backup has become very popular in recent years. The main advantage of cloud backup is the remote storage of the data in case of a local disaster. Most firms that provide cloud backup install an application on the local computer that looks for changes in existing files and for new files and upload only those files to the remote location. The initial full backup may take days to weeks depending on the amount of storage. Similarly a restore operation may take very long time. In a mission critical installation this is not acceptable. Many of these firms provide overnight shipping of data transferred to hard drives. Only some of these services provide version backups. If previous versions are available corrupted local data would also corrupt remote backups. There is a hefty monthly service fee for backup of servers, usually charged per gigabyte.

4. Server redundancy

In mission critical installations where downtime is unacceptable, Maximum Availability Architecture (MAA) must be installed. Redundant servers should be located in geographically different locations. In case one server goes down for any reason one of the other servers will take over without interrupting the service. Redundant servers can be set up either as failover or load balancing. In case of Linux servers, one may use Distributed Replicated Block Device (DRBD), which is like a RAID-1 between two servers. Microsoft Windows provides Clustering services that provide for failover.