Backup Strategies for the Data Paranoid v2   by K8UT

Very few hams are still using paper logs – the computer has become an essential peripheral in the ham shack. I abandoned paper logs 13 years ago and since then have captured 40,000+ QSOs on a PC's hard drive. As you might expect, during those years I've replaced the computer a few times and suffered a few hard drive crashes. Fortunately {knock on wood} I've never lost any data nor had to manually rebuild a log file. But, I've been lucky and I know it. I needed a better backup mechanism that works automatically and stores essential files in more than one location.

My goal in designing a backup system covers worst-case scenarios that span a range of misfortunes. What if my: hard disk crashes; the lights blink; the basement floods; the house burns down?

The resulting backup solution involves a combination of hardware and software. On the hardware side, I equipped each PC in my house with a secondary hard disk and a USB thumb drive. Each PC connects to a router and through it to a Linux Ubuntu computer that functions as a web host and file server. All of those computers are networked together with a router that provides upstream Internet connectivity. On the software side, the computers are running four programs that provide varying degrees of backup capability: Microsoft *Windows*, Acronis *True Image Home*, 2BrightGuys *SyncBack*, and a utility program I wrote called *TRNmirror*.

Backup Within each Computer – Each computer performs a local backup from its primary to its secondary disk. The built-in *Windows* backup utility runs monthly to create a full image of the primary disk on the secondary disk, while *True Image Home* runs twice a week to create incremental backups of the hard disk. Aside from whole-disk copies, scheduled *SyncBack* profiles run nightly snapshots of essential files - like My Documents, all ham radio programs, and all logs files – from the primary to the secondary disk and to the USB thumb drive. These operations happen automatically without any human intervention.

Backup to the File Server – Included in each computer's Syncback schedules are profiles that run nightly and transfer files between the computers' secondary hard disks and the Ubuntu server. For added data insurance, Syncback's profiles are configured with *VERSIONING = ON*, which examines files for changes and renames an existing backup file with a version number (myfile(001), myfile(002), myfile(003)…) before copying the current file from the PC. This technique creates generations of backup files in the event that I need to restore a version from the distant past. These operations are also automatic and require no intervention from me.

Backup to an Internet Service – My "Beginner Web Hosting Account" at www.1and1.com includes 250 GB of storage space, which serves as an off-site repository for my "if the house burns down" scenario. Nightly Syncback profiles connect from the PCs to 1and1.com and use the FTP protocol to copy files up into the cloud. In addition to ham radio files, I also copy other files – things like the family photo album, legal and accounting documents and important correspondence. Like the previous backups, this one is also automatic.

Real-Time File Copying – In addition to the previous traditional instances of static backups, there are also special times – like when I am running a contest – that I want the added security of instantaneous file backups. The elegant solution to this problem would be an expensive RAID disk array; my inelegant solution is a utility program that I wrote myself. *TRNmirror.exe* monitors a given disk directory and detects when a file's size or date-stamp changes, at which time it makes a copy (with versioning) of the log in a second location. If my logging software were to fail, the logfile were to become corrupted, the hard disk were to crash, or the PC's power supply were to go up in smoke, I would still have a copy of that 1000 QSO contest log file in another location. If you're interested, that log-copying utility is available from my website.

Alternatives – The architecture and techniques described in this article work fine for me, but may not fit in your environment. Feel free to make substitutions. Maybe your version of Windows lacks a backup/restore program? Perhaps you only have one computer in the house, you don't have an Ubuntu server, or your computers are not networked together? No secondary hard drives? Thumb drives are cheap! Or burn the files to a DVD! No Internet connection? Snail mail a CD/DVD to a local ham for safe-keeping. The important thing is that your long-term investments in this hobby are safeguarded.

K8UT, Larry Gauthier 2013-02/08

References

Monthly full image backup – Microsoft Windows 7
Incremental backups – Acronis True Image Home, www.acronis.com
Nightly snapshots – 2BrightSparks SyncBackSE, www.2brightsparks.com
Off-site backup – 1and1, www.1and1.com
Real-time copy – K8UT TRNmirror.exe, www.k8ut.com