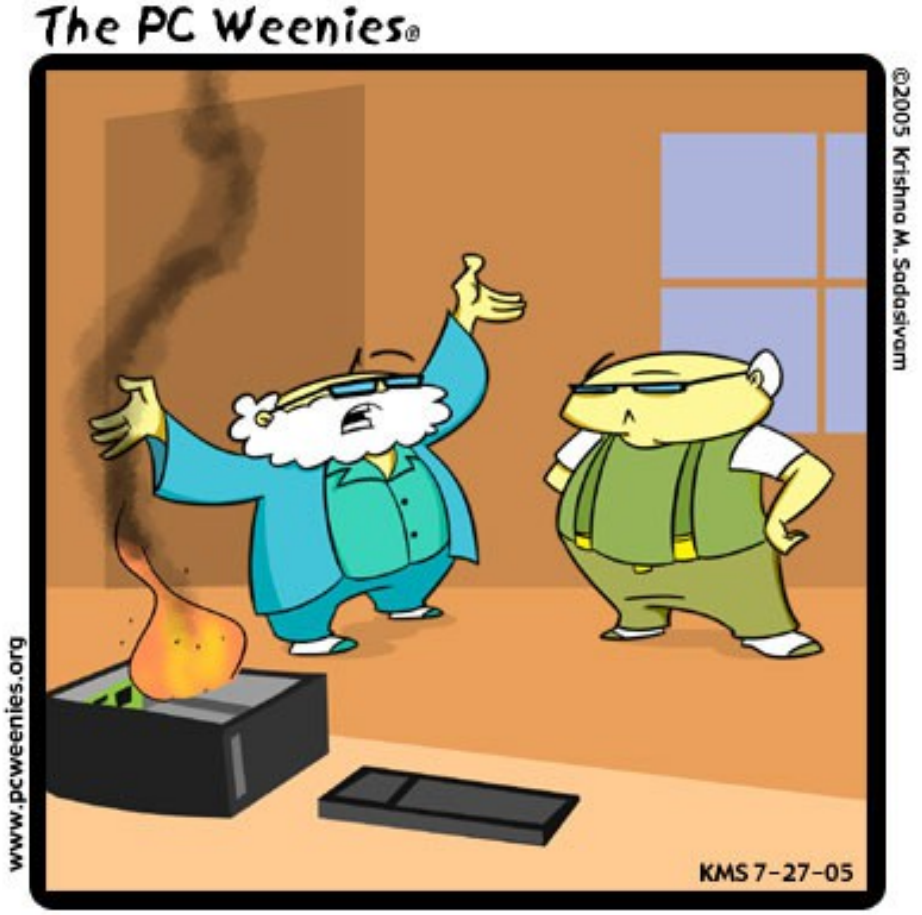
CSE 265: System and Network Administration

- Backup and Restore
  - Why do you need backups?
  - What are backups?
  - Backup and restore policies
  - Backup schedule
  - Capacity and consumables planning
  - Backup media
  - Dump, tar, and AMANDA



"I WOULD HAVE MADE BACKUPS, BUT I COULDN'T FIGURE OUT HOW TO PUT MY PC IN 'REVERSE'."

Backup and restore

- Why do we need backups?

Backup and restore

- Why do we need to restore from backups?
  - Data gets lost.
  - Equipment fails.
  - Humans delete data by mistake and on purpose.
  - Judges impound all documents related to a lawsuit that were stored on your computers on a certain date.
  - Data gets corrupted, either by mistake, on purpose, or by gamma rays from space.
- You **need** reliable backups.

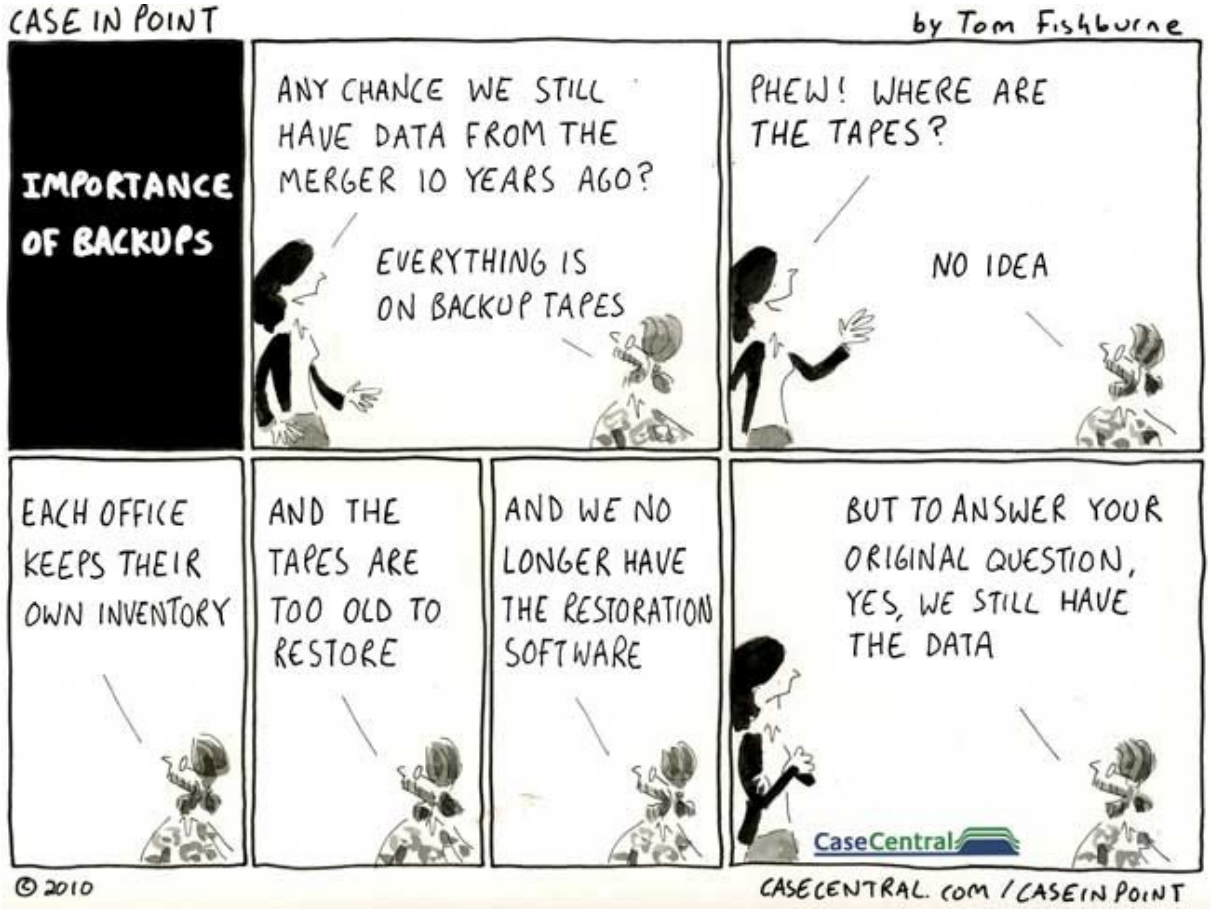
Three reasons to need restores

Three reasons to need restores

- Accidental file deletion
  - Most common case
  - Users want immediate restoration, but 3-5 hours is typical, from a day-old backup
    - As a result, some users will re-generate (losing productivity) rather than restore
  - Newer systems offer self-service restores (typically from a system that takes regular snapshots)
    - Currently true for CSE/ECE home directories
- Disk (or drive controller) failure
  - Implies both loss of service and loss of data
  - RAID should be used to minimize loss

Three reasons to need restores

- Archival
  - Need to record snapshot for business or legal reasons or for disaster recovery
  - Work is similar to a full disk restore
  - Archives are typically stored off-site



Data integrity

- Data can be corrupted
  - Maliciously by viruses or individuals
  - Inadvertently by individuals, bugs, and hardware failures
- Ensuring integrity can be a day-to-day operation
  - Compare static files against a checksum
    - ZFS does this automatically, both during writes and scrubbing
  - Keep virus-checking software up-to-date
  - Look for anomalies (e.g., large changes to static data)
- Need long-term backups to handle unnoticed problems

What are backups?

- A full backup (level 0) is a complete copy of the files on a partition (at a particular time)
- An incremental backup is the storage of the changed files since the last full backup (a.k.a. a level 1 backup)
  - The size of incremental backups grows over time
- Some systems allow incremental backups (e.g., level 2) of changes since the last incremental backup (level 1)
  - Thus, there can be level 3, level 4, level 5 backups, etc.

Example

- Usage
  - Sat: A1 B1 C1 D1
  - Mon: A2 B1 C2 D1
  - Tue: A3 B1 C2 D2
  - Wed: A4 B2 C3 D3
  - Thu: A5 B2 C4 D3
  - Fri: A5 B3 C5 D3

Example

- Usage
  - Sat: A1 B1 C1 D1
  - Mon: A2 B1 C2 D1
  - Tue: A3 B1 C2 D2
  - Wed: A4 B2 C3 D3
  - Thu: A5 B2 C4 D3
  - Fri: A5 B3 C5 D3
- Backups
  - Sat: L0-A1 B1 C1 D1
  - Mon: L1-A2 C2
  - Tue: L1-A3 C2 D2
  - Wed: L1-A4 B2 C3 D3
  - Thu: L2-A5 C4
  - Fri: L2-A5 B3 C5

Different customers

- The three types of restores serve different kinds of customers
  - Individual user requests file restoration
  - Legal and financial departments require archival backups
    - Although sometimes the requirement is to **not** back up data, or keep for relatively short periods so that it cannot be the target of a subpoena
  - Complete disk restores are needed for sysadmins who are maintaining some SLA

Backup policies

- Need an organization-wide document that dictates requirements for backup systems
  - Explain why backups are needed
  - What constitutes a backup
  - What data should be backed up
  - Define legal requirements
  - Define when backups should be performed

Data recovery SLA

- Consider the three types of restores needed
  - negotiate the desired time to restoration
  - determine the granularity and retention period
  - time window in which backups are performed

Sample (aggressive) service level agreement on next slide.

Example SLA

Customers should be able to get back any file with a granularity of one business day for the last six months and with a granularity of one month for the last three years.

Disk failures should be restored in four hours, with no more than two business days of lost data.

Archives should be full backups on separate tapes generated quarterly and kept forever.

Critical data will be stored on a system that retains user-accessible snapshots made every hour.

Backup schedule

- Given an SLA and policy, we need to schedule the backups
  - list the details of which partitions are backed up and when
  - modern backup software will (mostly) schedule for us automatically
    - Need to specify how often full backups are run
  - the schedule determines the amount of backup media required

Example #1

- Partition of 4GB
  - Scheduled full backup every 28 days
  - Incremental other days
- Assume incremental size grows 5% per day
- Tape capacity needed:
  - First day, 4GB (full backup)
  - 2nd day, 200MB, 3rd day 400MB, etc.
  - 11th day, 2GB, 21st day 4GB, etc.

Example #1, continued

- At some point, it is better to generate level 0 backups more often
  - The best case for this example is a 7-day level 0 cycle (49.2GB)
  - Longer cycles write too much duplicate content
  - Smallest cycle (full dumps each day) worst case at 168GB dumped!
- Amount of data dumped determines amount of media required ($$)

Example #2

- Previous example somewhat simplistic
- Assume customers modify 10% of files per day, but overlaps with previous day's changes.
- Thus, first incremental is 10%, but subsequent ones grow only by 1%
- The best case for this example is a 14-day level 0 cycle (37GB); worst case of daily level 0 (168GB)

Scheduling

- More complex scheduling (e.g., incorporating level 2 backups, etc.) can minimize tape usage
- Drawbacks
  - More complex to track (not really a problem)
  - Restores are slower, more difficult and error prone

Time and capacity planning

- Backups and restores are constrained by time
  - Backups must be performed during certain time windows
  - Restores must occur within an SLA
- Backup performance is affected by
  - read performance of disk
  - write performance of backup medium
  - bandwidth and latency of network between
- Restore performance is affected by reverse
  - Often much (5-15 times) longer!
- Need to do real test to verify time and capacity!

Consumables planning

- Policy and schedule determine consumables usage (tapes, cleaners, etc.)
- Using sample policy, incrementals can be recycled after six months storage, and full backups after three years
- For first six months, need new tapes for everything
  - If we need 8 tapes per day, six days a week, for six months (1248 tapes), at $40 ea, or $49,920

Consumables planning (2)

- In 2nd six months, we (mostly) just need to buy tapes for full backups
  - Assume 9 tapes per week, plus one tape for growing incrementals
  - 260 tapes, at $9,100 (assuming $35/ea)
- 2nd and 3rd year are similar
- 4th year is cheaper (can recycle archives) but capacity will likely soon be insufficient
- Need to determine backup policy that balances cost with required capabilities

The restore process

- Need to set customer expectations
  - Even a simple explanation is helpful
- Consider security implications
  - Who can request file restoration?
  - Where will the restored file be placed?
- **Multiple people need to know how to restore data**

Backup automation/centralization

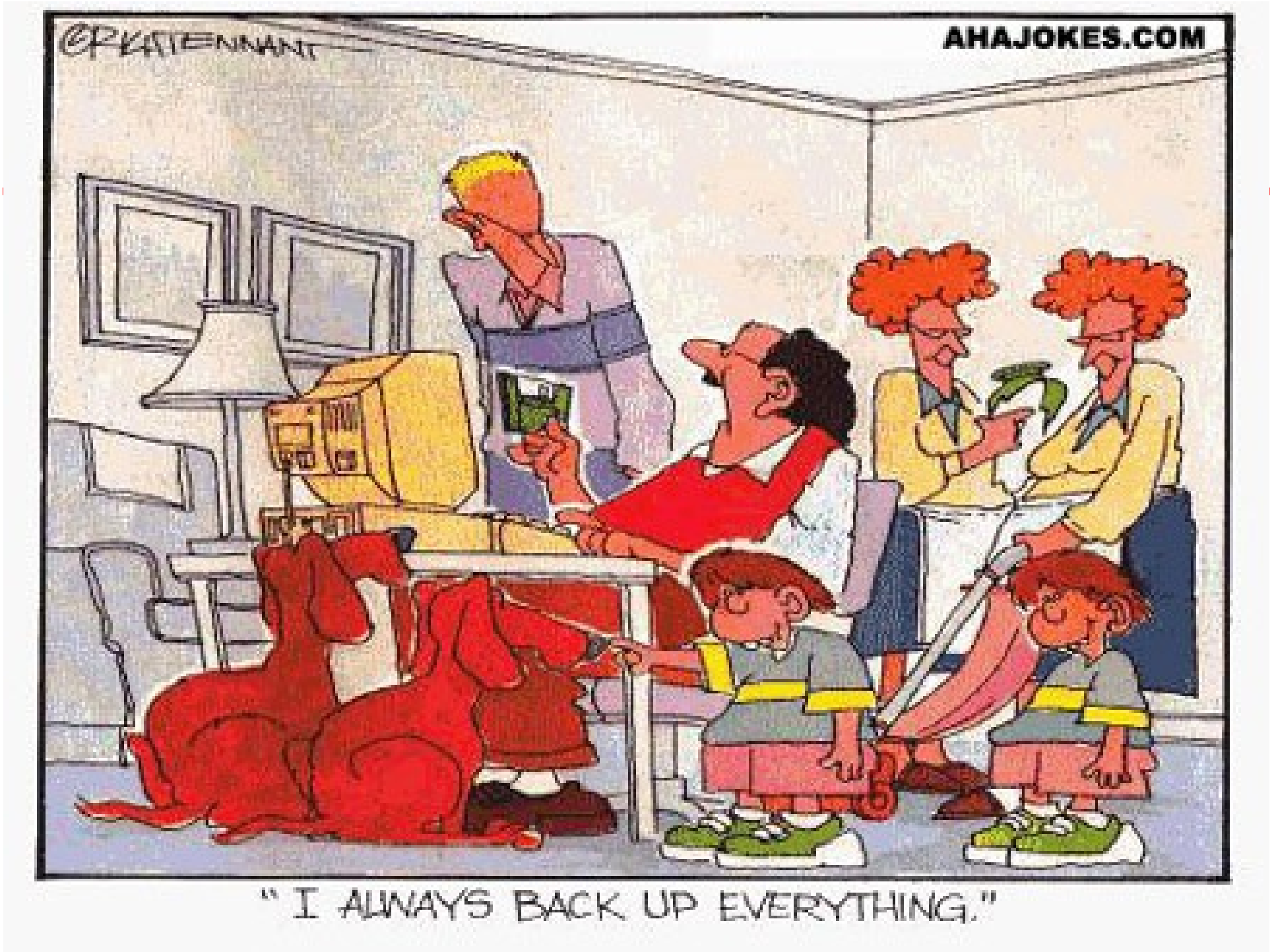
- Backups must be automated
  - boring – automation is only way for reliability
  - tape handling can be provided by clerks
- Backups should be centralized
  - they are expensive and important!
  - distributed tape drives are expensive and manually intensive (to change tapes)
  - tape jukeboxes are expensive, but worth it

Other concerns

- Fire drills
  - Only way to fully test system
  - Good way to burn in new hardware
- Off-site storage
  - Backups should not be affected by disaster that affects systems backed-up
  - Media off-site is a security risk
  - Can be informal (home with company officers)
  - Can be formal (storage service)
- Tape capacity vs. disk capacity – ratio varies over time

Helpful hints

- Perform all dumps from one machine
  - Ease of operation, backup to a single device
- Label your tapes
  - Unlabeled tape == blank tape
  - Label with info needed to restore root and /usr
- Pick reasonable backup interval
  - How much data are your users willing to lose?
- Limit activity during dumps
- Choose filesystems carefully
  - Some rarely change
- Make filesystems smaller than your dump device
- Keep tapes off-site
- Protect your backups
  - Copies of everything!
- Check your tapes
- Develop a tape life cycle
- Design your data for backups
- Prepare for the worst



Backups and magnetic media

- Companies exist to backup over the Internet
- Most backups still performed locally
- Should be to removable media (to prevent failure/disaster from affecting all copies)
- Care of magnetic media – avoid magnetic fields, such as
  - audio speakers, transformers and power supplies, unshielded tape and hard drives, fans, monitors, and earth's background radiation

Backup media

- CD-R/RW, DVD+-R/RW, DVD-RAM, Blu-Ray
  - Photochemical process initiated by laser
  - Much longer shelf life believed than magnetic media
  - 650MB CD-ROM; 4.7GB or 8.5GB DVD; 25-100GB Blu-Ray
  - many competing DVD formats
- Removable hard disks
  - USB, FireWire
  - Small (e.g., 128GB) flash memory drives

Tapes

- Many formats
  - 8mm cartridge tapes
  - DDS/DAT (4mm) cartridges
  - DLT/S-DLT
  - AIT and SAIT
  - VXA/VXA-X
  - LTO-4, LTO-5, LTO-6
- Variety of capacities and speeds

Tape jukeboxes/stackers/libraries

- Many times you need multiple tapes for a full backup
- Stacker
  - Simple tape changer for use with a standard tape drive

- Jukebox
  - automatically change removable media among a set of drives
- Tape library
  - large mechanisms, multiple drives, robotic arm for retrieval

Incremental backups with dump

- dump and restore are basic commands
  - often the building blocks used by commercial systems
- dump
  - builds a list of files that have been modified since a previous dump
  - packs them into a single file to archive on an external device

Dump: pros and cons

- Advantages
  - Can span multiple tapes
  - Files of any type (including devices) can be backed up
  - Permissions, ownerships, and modification times are preserved
  - Files with holes are handled correctly
  - Backups can be performed incrementally
  - Understands filesystem internals (reads inode tables via device entry)
  - Can handle arbitrarily long filenames/paths
- Limitations
  - Every filesystem (partition) must be dumped independently
  - Only local (not NFS-mounted) filesystems can be dumped
  - Incremental dumps may require restoring files from several sets of tapes

rdump

- Can dump a local filesystem to a remote tape drive with rdump
- dump takes parameters
  - the backup level (0-9)
    - A level N backup is incremental from the last dump < N
  - the device to store on (or stdout)
  - the filesystem to back up
- **# rdump -2u -f anchor:/dev/nst0 /spare**
- Modern versions of dump can also dump remotely

Restoring from dumps

- Create and **cd** to a temporary directory
- Interactive restore with **restore -i**
  - reads the table of contents, lets you navigate a normal directory tree (ls, cd, pwd)
  - select files to restore with add command
  - extract starts retrieving files
- Ex:
  - **mkdir /var/restore; cd /var/restore**
  - **rsh tapehost mt -f /dev/nst0 fsf 3**
  - **rrestore -x -f tapehost:/dev/nst0 ./janet/iamlost**

Restoring entire filesystems

- First need to create and mount target filesystem
- Start with first tape of most recent level 0 dump
  - type **restore -r**
  - mount and restore incremental dumps in order of creation

Example dump sequences

- 0 0 0 0 0 0

Which dump(s) do you use for restores?

Example dump sequences

- 0 0 0 0 0 **0**
- 0 5 5 5 5

Which dump(s) do you use for restores?

Example dump sequences

- 0 0 0 0 0 **0**
- **0** 5 5 5 **5**
- 0 3 2 5 4 5

Which dump(s) do you use for restores?

Example dump sequences

- 0 0 0 0 0 **0**
- **0** 5 5 5 **5**
- **0** 3 **2** 5 **4** **5**
- 0 9 9 5 9 9 3 9 9 5 9 9

Which dump(s) do you use for restores?

Example dump sequences

- 0 0 0 0 0 **0**
- **0** 5 5 5 **5**
- **0** 3 **2** 5 **4** **5**
- **0** 9 9 5 9 9 **3** 9 9 **5** 9 **9**
- 0 3 5 9 3 5 9

Which dump(s) do you use for restores?

Example dump sequences

- 0 0 0 0 0 **0**
- **0** 5 5 5 **5**
- **0** 3 **2** 5 **4** **5**
- **0** 9 9 5 9 9 **3** 9 9 **5** 9 **9**
- **0** 3 5 9 **3** **5** **9**

- Tapes required for restoration are in bold

Dumping & restoring for upgrades

- Dump before upgrading
  - as insurance for problems (can drop back to previous version)
  - to be able to change partitioning
  - to handle different filesystem formats
- Need to include system-specific files
  - in / or /usr, such as /etc/passwd, /usr/local

Other archiving programs

- tar
  - also useful for moving directory trees
    - **tar -cf – fromdir | (cd todir ; tar -xfp -)**
  - GNU version of tar can do most of what dump can do
- dd
  - file copying and conversion program

AMANDA

- Advanced Maryland Automatic Network Disk Archiver
  - Sophisticated, popular, free, network backup system, but getting old
  - Wrapper around **dump** and **restore**
  - Tape management – writes a header so it never overwrites wrong tape
  - Manages dump levels based on configuration and fullness of tapes
- Amanda does not rigidly schedule dumps
  - You specify amount of redundancy to retain
  - Amanda spreads out workload across dump cycle
    - Using tapes/network more efficiently
  - Will automatically move to higher dump level when dump size is large enough

Additional alternatives

- Open source choices
  - BackupPC, Bacula (covered in text), etc.
- Commercial backup software/systems
  - IBM Tivoli, Veritas, EMC
- Near-continuous backup file systems
  - EMC, NetApp, Microsoft
- Online services
  - Amazon Glacier, Backblaze, many others
- and many more
  - See http://www.backupcentral.com/

