INSTITUTE OF
TECHNOLOGY
DEVELOPMENT
OF CANADA

Introduction to Computers

ICR100

Fall Semester 2020

Backups and RAID

Backups

What is a backup?

- With the term **backup** we mean the procedure to create one or more copies of our files in a secondary location

- The purpose is the *preservation* in case of hardware failure, data loss, data corruption, malicious attacks and lots of other reasons.

- Basically, the backup give us security for our information thanks to the **redundancy** of the data.

What is a backup?

- Plus, the backup give us the chance to recover data from an earlier time.

- The backup is a simple form of **disaster recovery**.

- The only flaw is that backups might be huge, which means data storage requirements can be significant.

How many backups should I have?

- If you think 1 backup is enough, **think again**.

- Not 1, not 2, but at least **3 backups** are necessary to be considered safe and secure.

- The more *redundant* your data is, the safer you are.

How many backups should I have?

THE 3-2-1 BACKUP RULE

- **3 copies of anything you care about**: 2 are not enough if these files are important.

- **2 different formats**: for example, Dropbox+DVDs, HDD+Memory Stick, etc.

- **1 off-site backup**: a backup that physically NOT resides where you are. If the house burns down, how will you get your memories back?

Still not convinced? Read this.

WANNACRY

- In May 2017, a *ransomware* called **WannaCry** (Or *WanaCrypt0r 2.0*) has been the responsible for a large scale epidemic on computers running Microsoft Windows.

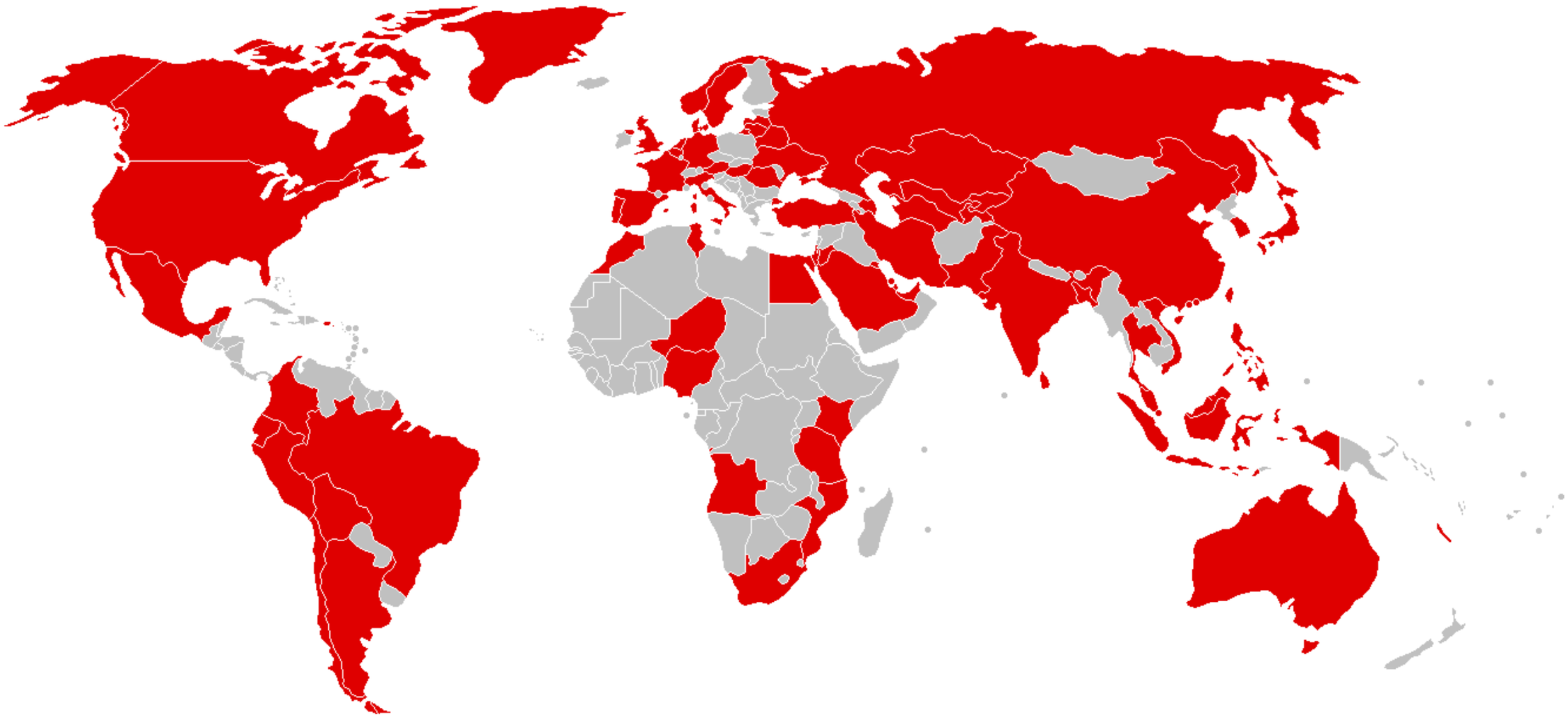
- Once executed it encrypts all the files on your computer demanding for a ransom payment in BitCoin in order to get your files back. Plus, if you connect your backup device to the computer, the backup as well gets encrypted.

- WannaCry is today known as one of the biggest computer infection of the history, infecting more than 200,000 computers over 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

WANNACRY


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

WANNACRY



COUNTRIES INFECTED BY THE VIRUS

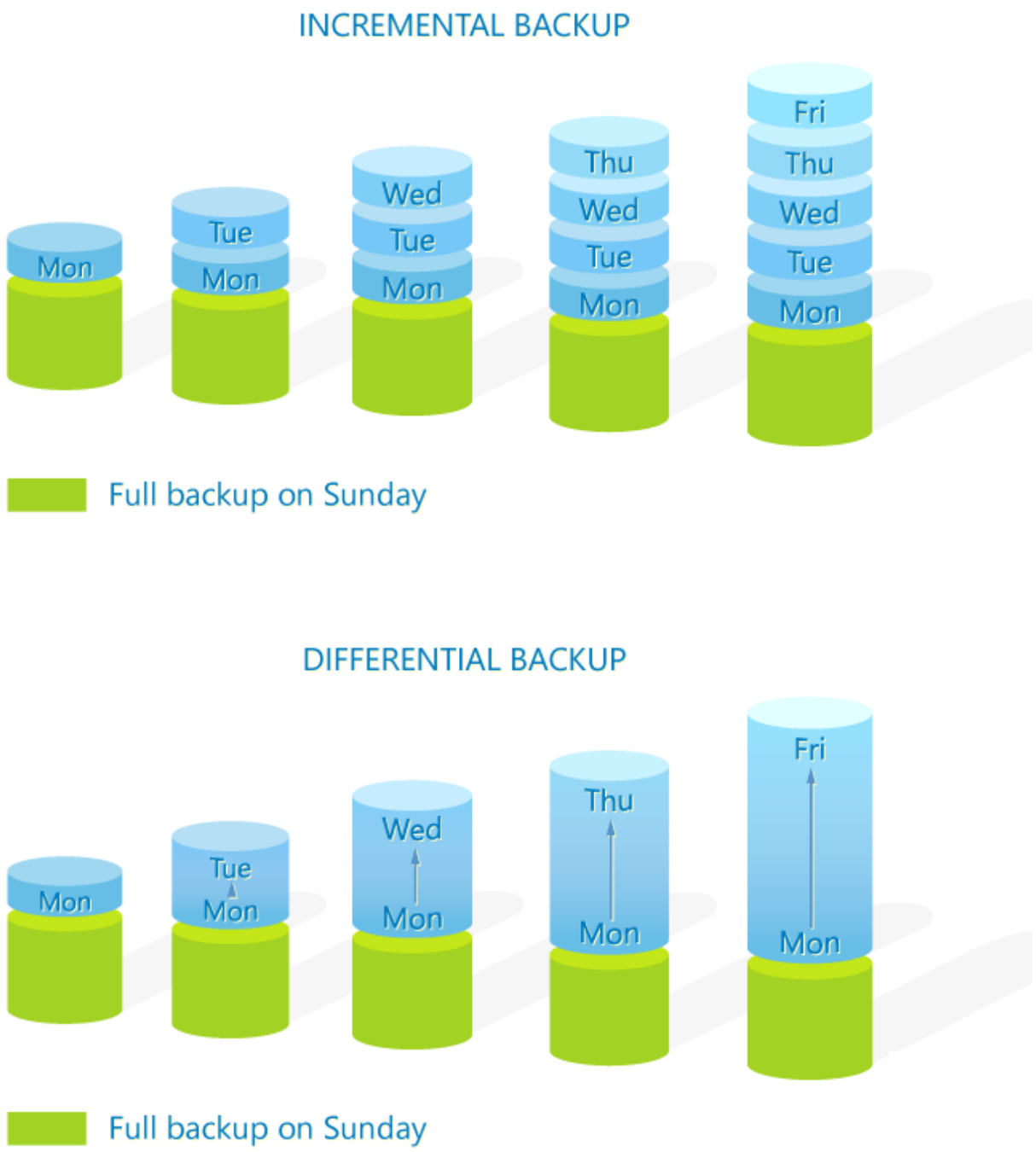
TYPES OF BACKUP

- **FULL BACKUP**: The entire copy of all your files. Necessary at least once.

- **INCREMENTAL BACKUP**: The backup of all the changes made since the **last backup**, whether it was full or incremental.

- **DIFFERENTIAL BACKUP**: The backup of all the changes made since the **last full backup**.

TYPES OF BACKUP



RAID

What is a RAID?

- **RAID** stands for **R**edundant **A**rray of **I**ndependent **D**isks.

- The RAID is **not** a backup type.

- The RAID indicates the procedure of installing multiple hard disk drives on the computer - or linking them to it - that looks like a unique storage device.

- Therefore, in order to make a RAID, more than one disk is required - even though they act as a single one.

What is a RAID?

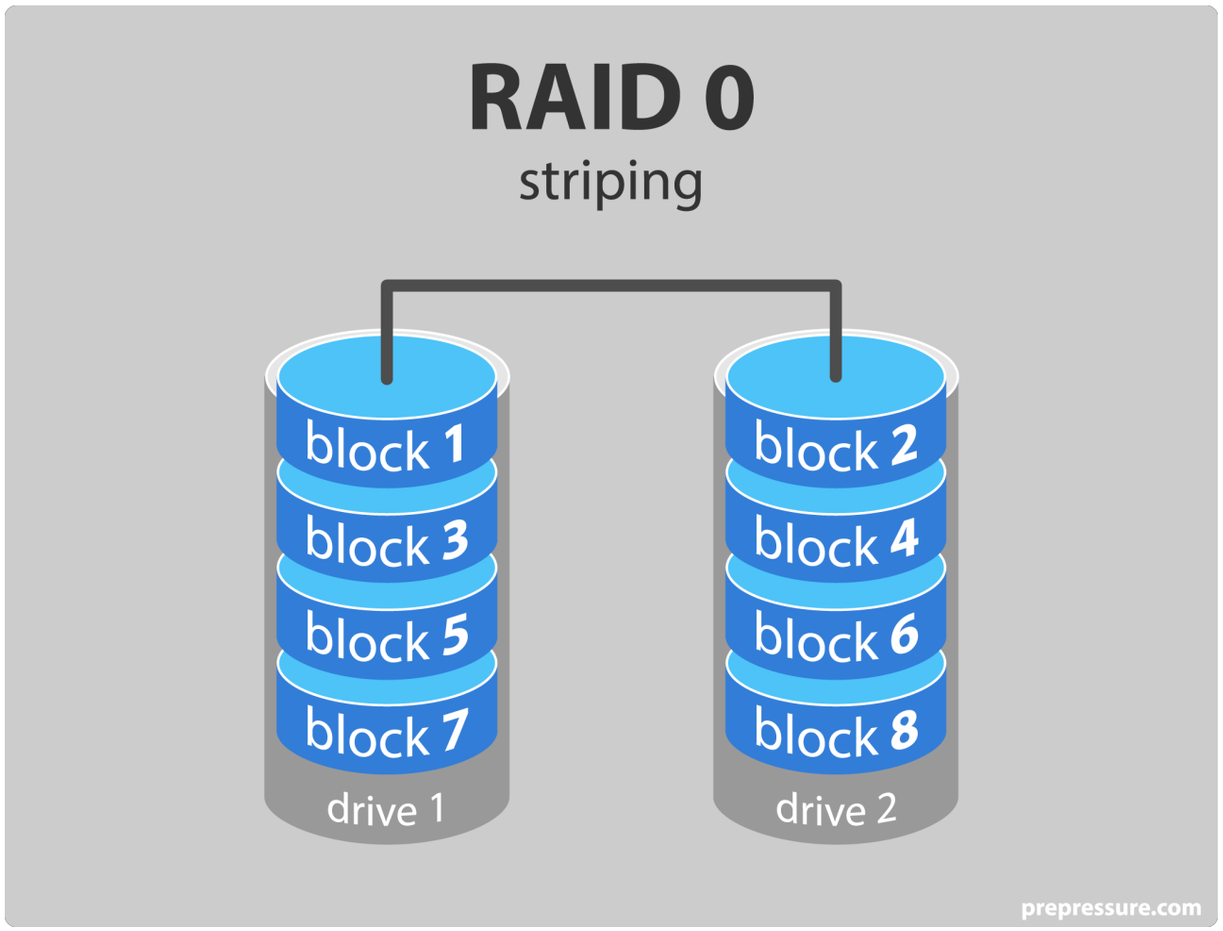
- There are different types of RAID such as RAID 0, RAID 1, RAID 10.

- RAID gives you **protection** in case of data loss or failure. If one hard disk fails, there are others which substitute it.

- Plus, the RAID improve the computer **performance**.

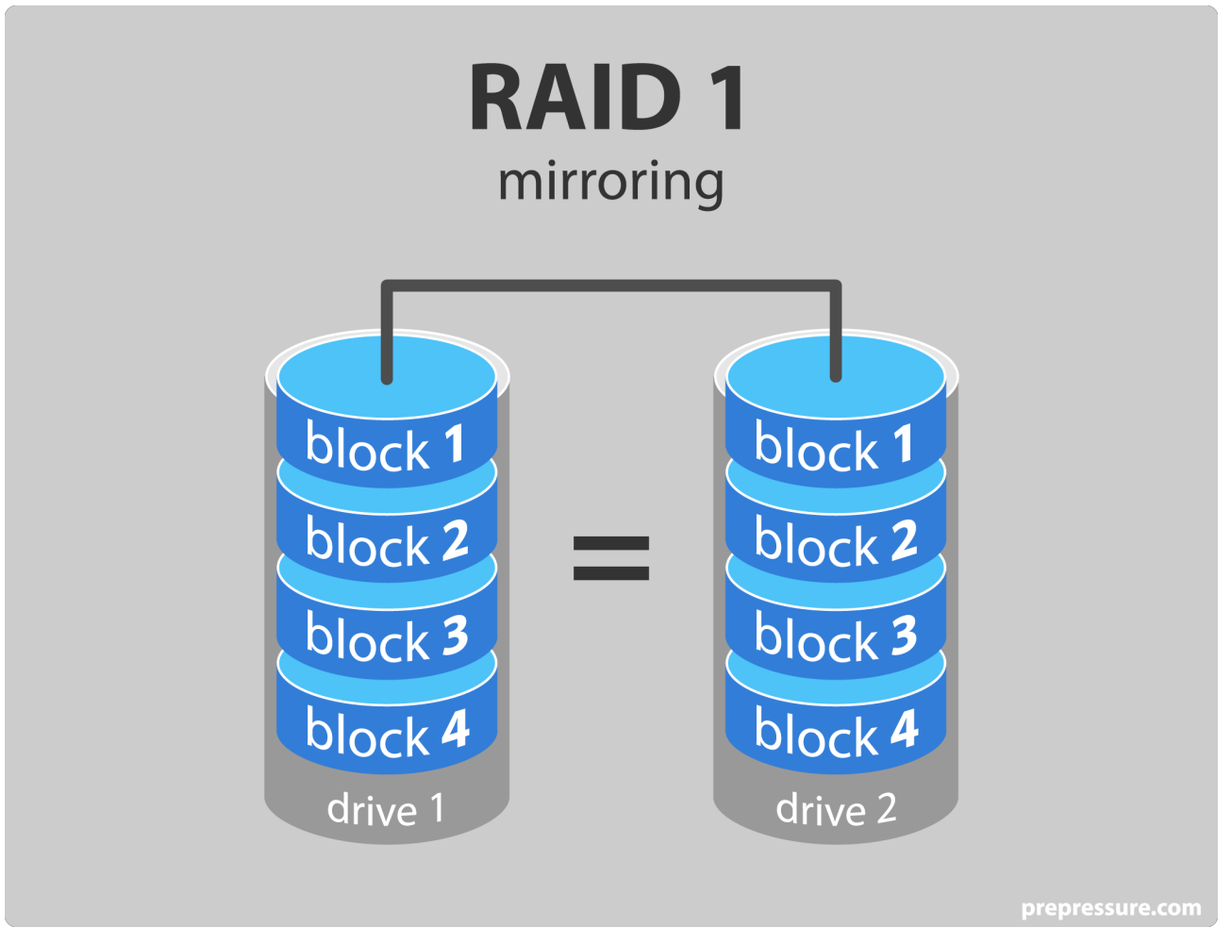
RAID 0 - STRIPING

- 2 disks which divide the data **50-50**.
- RAID controller split the data.
- **No redundancy** - just benefits of performance.



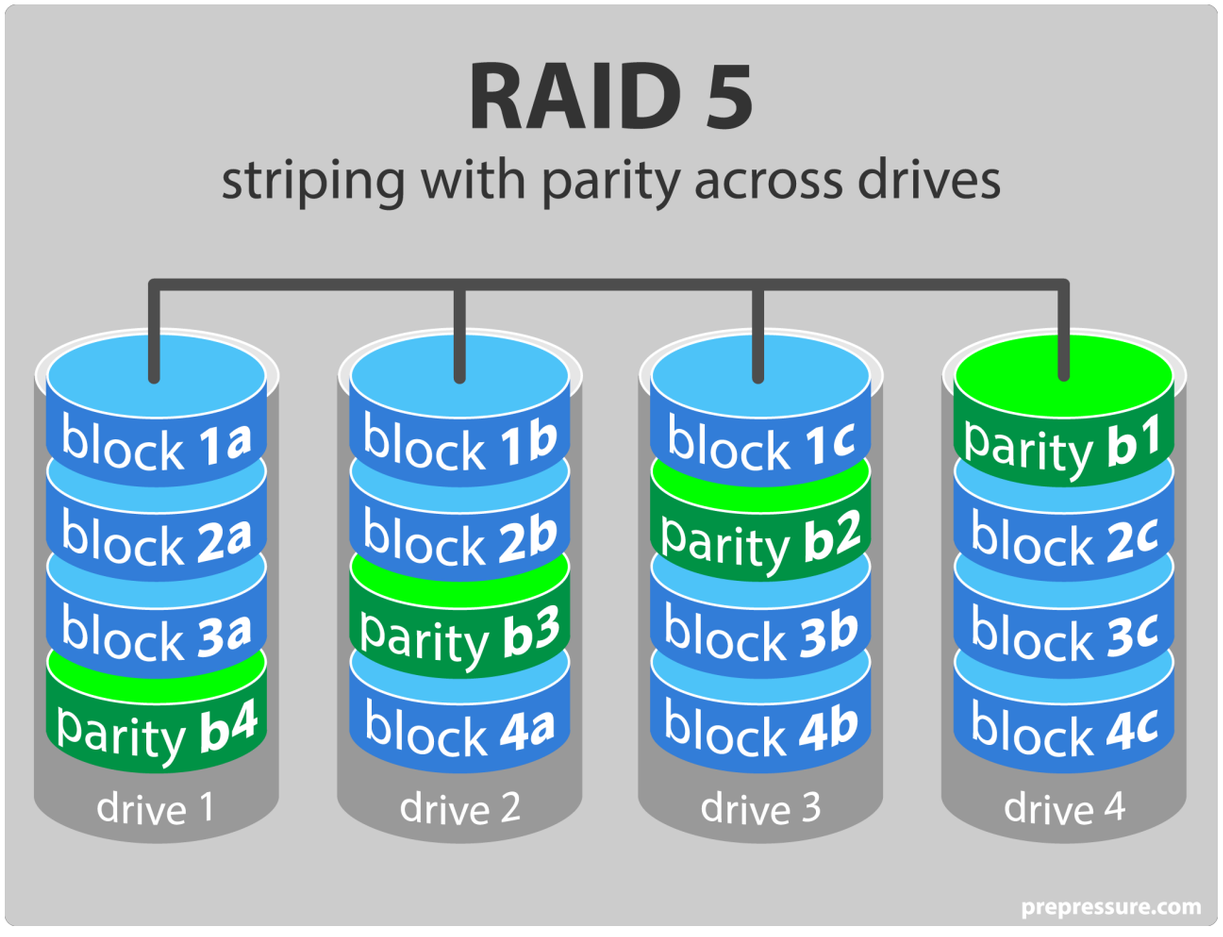
RAID 1 - MIRRORING

- 2 disks identical to one each other.
- It gives redundancy which means **file protection**.
- Performance remains pretty much the same of a single disk.



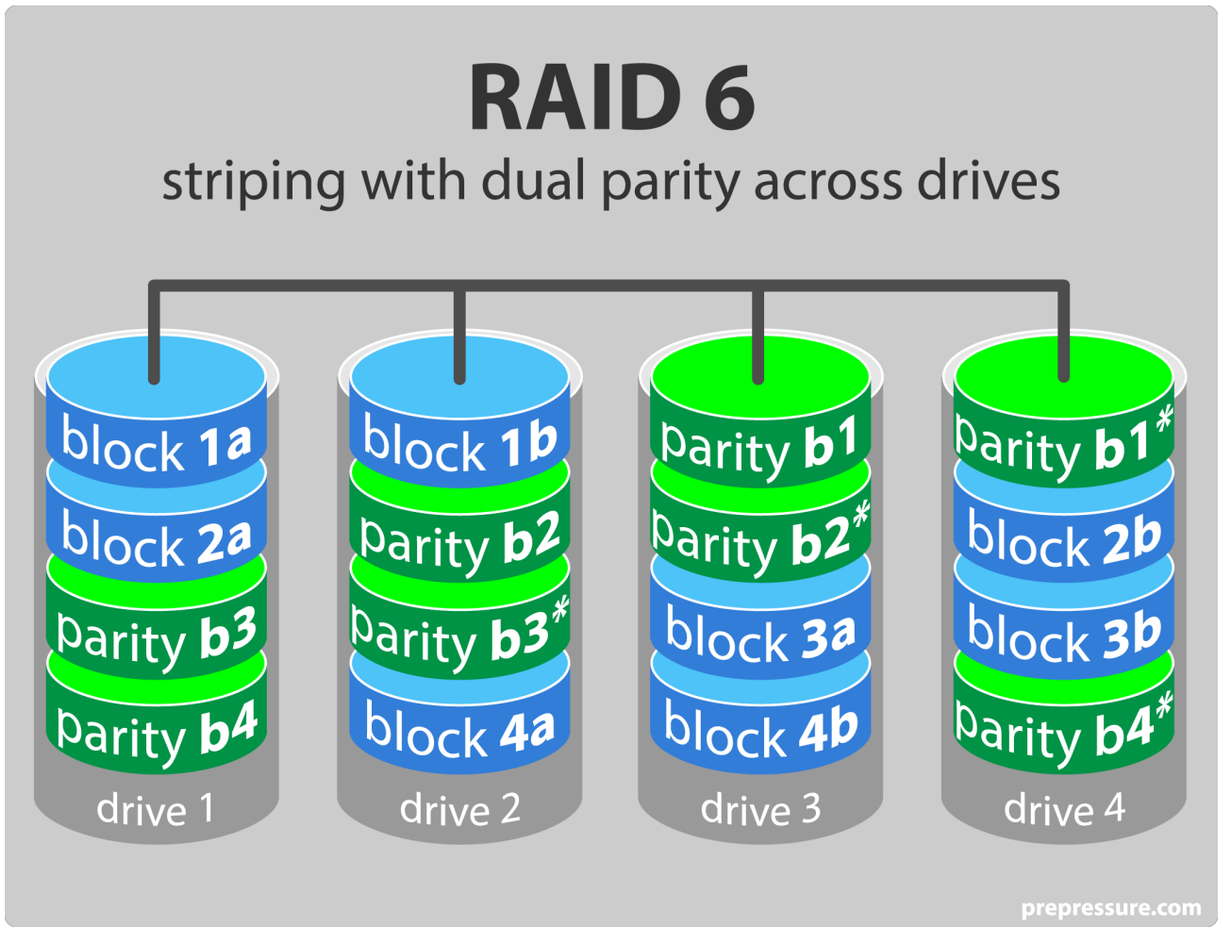
RAID 5 - STRIPING WITH PARITY

- Minimum of 3 disks.
- Can sustain **1 failure**, one hard disk is dedicated for data recovery thanks to **parity data**.
- The parity blocks inside each hard disk basically tell you which data is stored on that row (in all hard disks). In this way, if one hard disk fails it can rebuilt the data using these parity information.



RAID 6 - STRIPING WITH DOUBLE PARITY

- Minimum of 4 disks.
- Can sustain **2 failures**.
- It contains 2 parity schemes (RAID 5 contains 1).

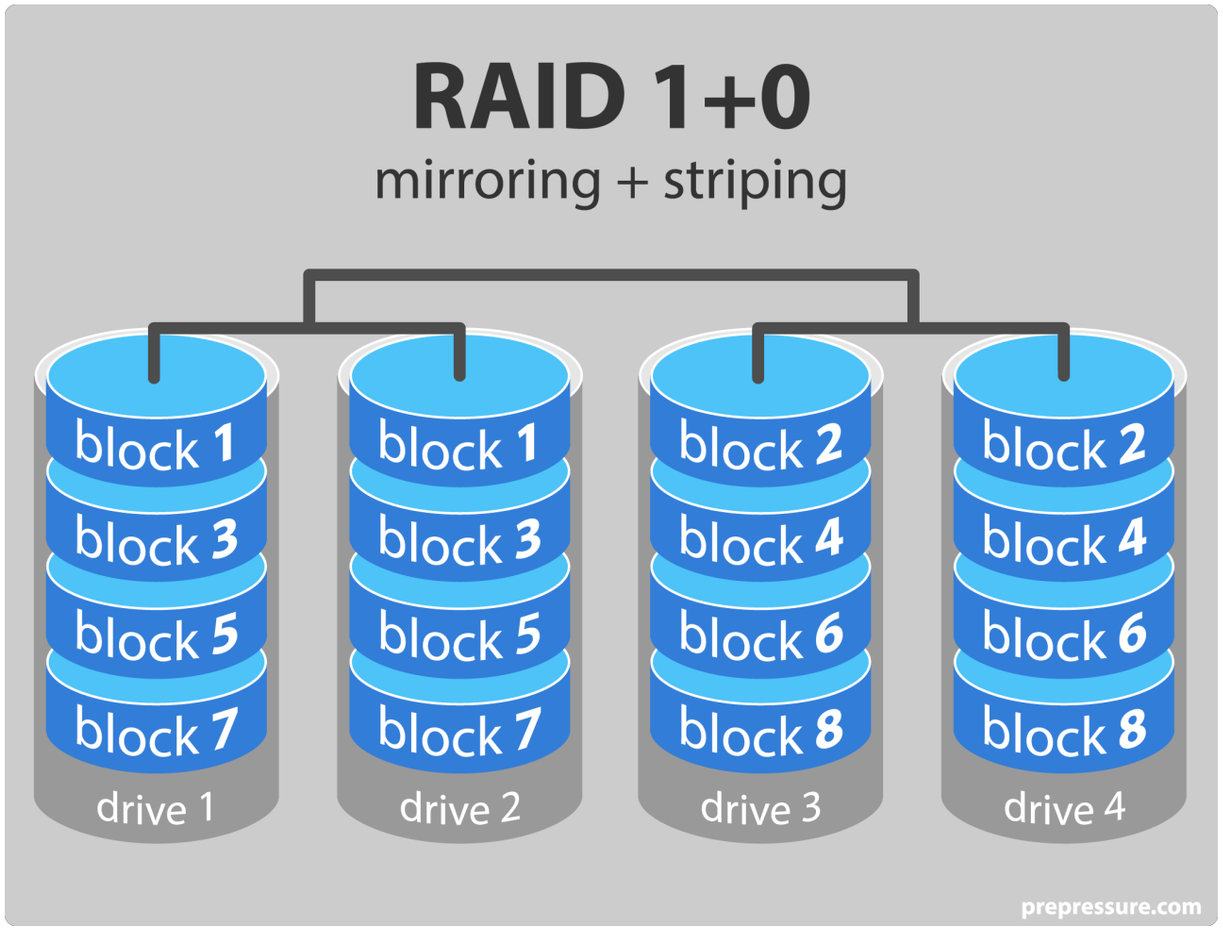


RAID 10 - STRIPING + MIRRORING

- Combination of RAID 1 and RAID 0.

- With RAID 10, both mirroring and striping are used.

- Really good because it takes the advantages of both, but expensive.



What are different RAIDs for?

- **RAID 0** and **RAID 1** are better solutions for private users.

- **RAID 5** and **RAID 6** are better for professionals, since they are really complex solutions. They are generally used for servers.

- **RAID 10** is used for servers too.

Thank You!