INFORMATIKAI BIZTONSÁG ALAPJAI

5. előadás

Göcs László
főiskolai tanársegéd
Neumann János Egyetem GAMF Műszaki és Informatikai Kar
Informatika Tanszék

2018-19. 1. félév

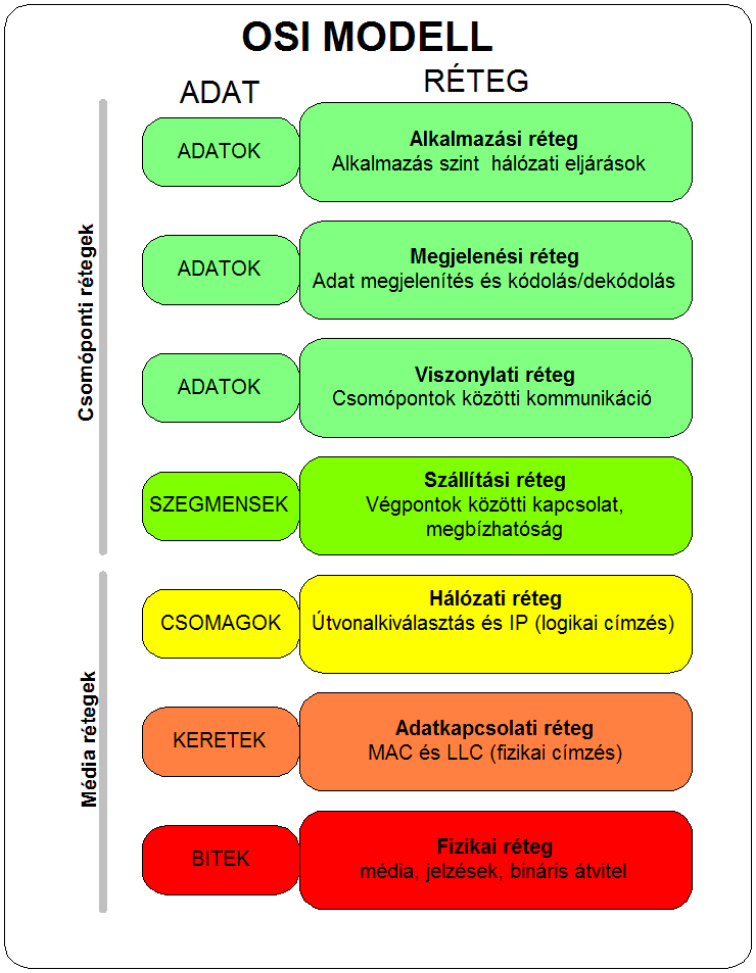
Vállalati biztonság

Előkészítés

- Az információbiztonsági osztály meghatározása (A,F,K)
- Rendelkezésre állás kalibrálása

OSI réteg védelme

- Minden egyes rétegnek megvan a meghatározott védelme.
- Maximális védelem kialakítása minden rétegben.



Fizikai réteg védelme

- Itt történik a jeltovábbítás (Kábelezés, csatlakozás).

- A kábeleken lévő jeleket, biteket (1 0 0 1 1 0 1) kódolási eljárással és órajel segítségével továbbítják.

Fizikai réteg védelme

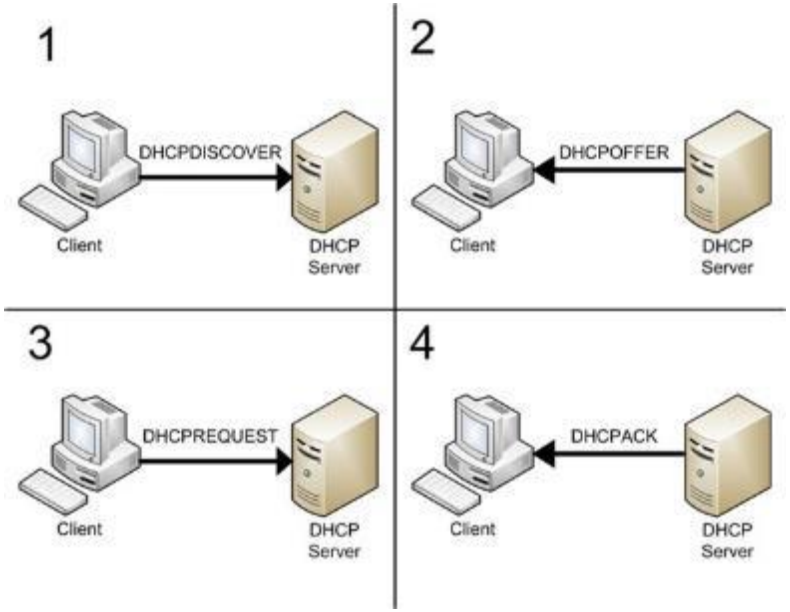
- A fizikai réteg védelme a helységek, berendezések biztonsága, hozzáférhetősége.
  - Tápellátás megszüntetése (szerver leállás)
  - Kábel megsértése (bejövő internet, helyi hálózat megszakítása)

Beléptetés, biztonságtechnikai felügyelet.

IP címek védelme

- **DHCP** *(Dynamic Host Configuration Protocol).*

Dinamikus IP cím kiosztás a hálózaton.



IP címek védelme

- Alhálózatok kialakítása (Maszkolási technika)

Jelöl	Címek	Alhálózati maszk	Alhálózati maszk binárisan
/22	4x256	255.255.252.0	11111111.11111111.11111100.00000000
/23	2x256	255.255.254.0	11111111.11111111.11111110.00000000
/24	1x256	255.255.255.0	11111111.11111111.11111111.00000000
/25	128x1	255.255.255.128	11111111.11111111.11111111.10000000
/26	64x1	255.255.255.192	11111111.11111111.11111111.11000000
/27	32x1	255.255.255.224	11111111.11111111.11111111.11100000
/28	16x1	255.255.255.240	11111111.11111111.11111111.11110000
/29	8x1	255.255.255.248	11111111.11111111.11111111.11111000
/30	4x1	255.255.255.252	11111111.11111111.11111111.11111100
/31	2x1	255.255.255.254	11111111.11111111.11111111.11111110
/32	1x1	255.255.255.255	11111111.11111111.11111111.11111111

IP címek védelme

- **MAC-cím** *(Media Access Control)* cím alapján történő IP cím kiosztás.

Egy **hexadecimális** számsorozat, amellyel még a **gyártás során** látják el a hálózati kártyákat.

A hálózati kártyák újlenyomata.

(parancssori utasítással: getmac)

A9-AF-23-C8-F2-2B -> 192.168.1.25

Menedzselhető switchek

- A switch portjait külön menedzselhetjük
  - VLAN-ok létrehozása
  - Port tiltások (80-as http port)
  - Port Sec

Vezeték nélküli kommunikáció (WiFi)

- **SSID**

Maga az azonosító szöveges és alfa numerikus karakterekből állhat és **maximum 32 karakter** hosszú lehet. Az egy hálózathoz tartozó eszközöknek ugyanazt az SSID-t kell használniuk.

- Fontos a jó elnevezés, mert a „default” beállításokból megfejthető a Router konfigurációs elérése.
- Az SSID elrejtése

TP_link_0234war -> 192.168.1.x -> admin

Vezeték nélküli titkosítás

A **Wired Equivalent Privacy (WEP)** = Vezetékessel Egyenértékű (Biztonságú) Hálózat mára már egy korszerűtlen algoritmus az IEEE 802.11-ben megfogalmazott vezeték nélküli hálózatok titkosítására.

Nem biztonságos, könnyen feltörhető.
Régi eszközök miatt még néhol használatos.

Vezeték nélküli titkosítás

A **Wi-Fi Protected Access** (**WPA** és **WPA2**) a vezeték nélküli rendszereknek egy a **WEP**-nél biztonságosabb protokollja.

A WPA tartalmazza az **IEEE 802.11i** szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

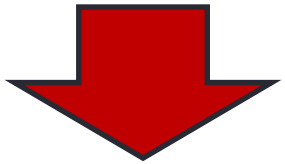
A **WPA2** a teljes szabványt tartalmazza, de emiatt nem működik néhány régebbi hálózat kártyával sem. Mindkét megoldás megfelelő biztonságot nyújt, két jelentős problémával:

Vezeték nélküli titkosítás

- Vagy a WPA-nak, vagy WPA2-nek engedélyezettnek kell lennie a WEP-en kívül. De a telepítések és beállítások során inkább a WEP van bekapcsolva alapértelmezettként, mint az elsődleges biztonsági protokoll.
- A „Personal” (WPA-PSK) módban, amit valószínűleg a legtöbben választanak otthon és kishivatali környezetben, a megadandó **jelszónak hosszabbnak** kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.

MUNKACSOPORT / TARTOMÁNY

- 4-7 kliens gép → Munkacsoport
- 7-10 gépnél több állomás → Tartomány

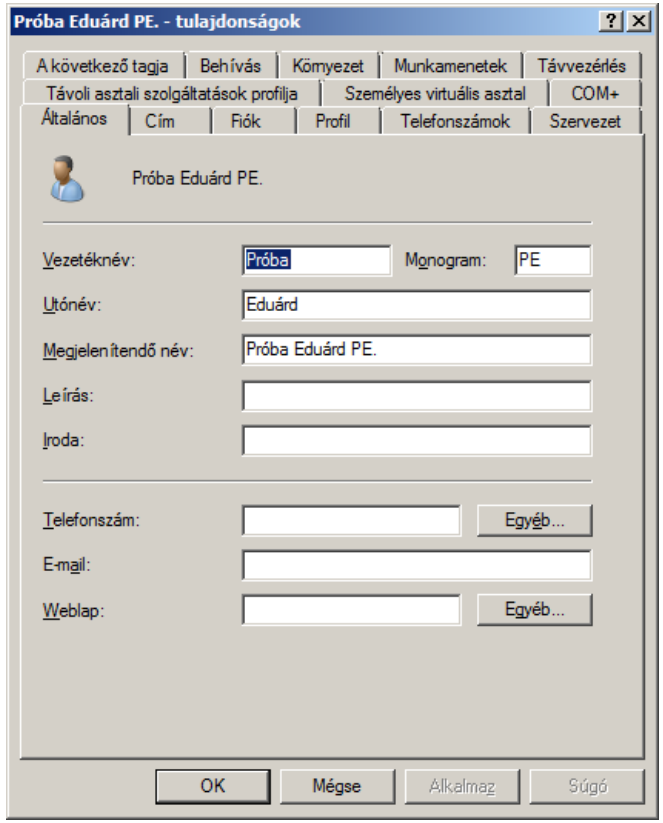


KÖZPONTOSÍTOTT FELÜGYELET

Központosított menedzsment

Központi beléptetés a kliens gépekre

- A Kliens gépeket Tartományba „fűzni”
- Az Active Directory –ban a felhasználók kezelése
- Központilag, 1 szerveren történik a menedzsment

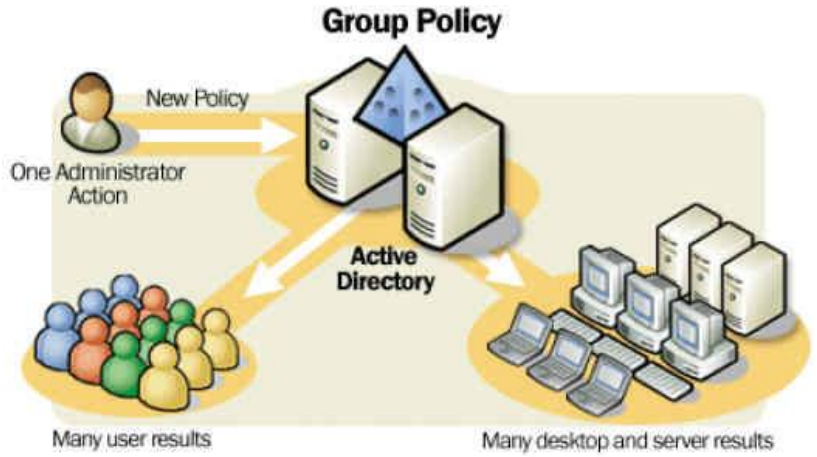


Egy nagy ADATBÁZIS a vállalatról

Központosított menedzsment

Központilag kezelt házirend (Group Policy)

- Felhasználóra vagy Kliens gépre történő beállítások
- Tiltások, engedélyezések



Központosított menedzsment

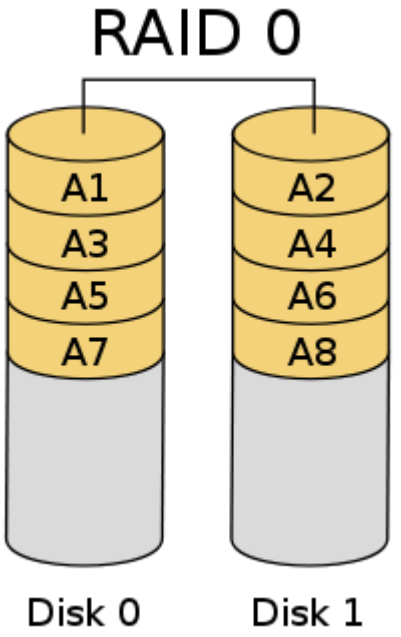
Adat Biztonság, adatvédelem

- RAID technológia
- Időzített biztonsági mentés (Backup)
- Replikáció
- Tükrözés

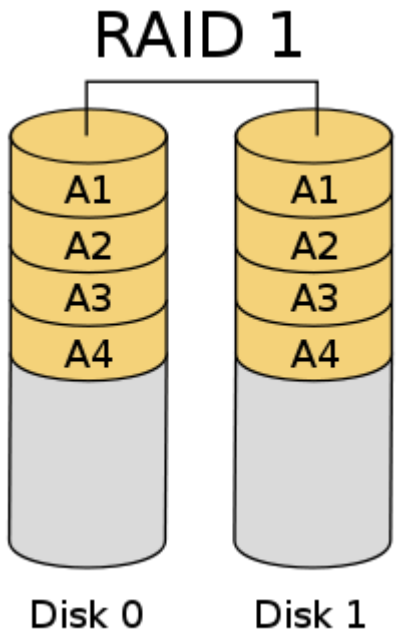
RAID

- A RAID technológia alapja az **adatok elosztása vagy replikálása több fizikailag független merevlemezen**, egy logikai lemezt hozva létre.
- Minden RAID szint alapjában véve vagy az adatbiztonság növelését vagy az adatátviteli sebesség növelését szolgálja.
- A RAID-ben eredetileg 5 szintet definiáltak (RAID 1-től RAID 5-ig). Az egyes szintek nem a fejlődési, illetve minőségi sorrendet tükrözik, hanem egyszerűen a különböző megoldásokat.

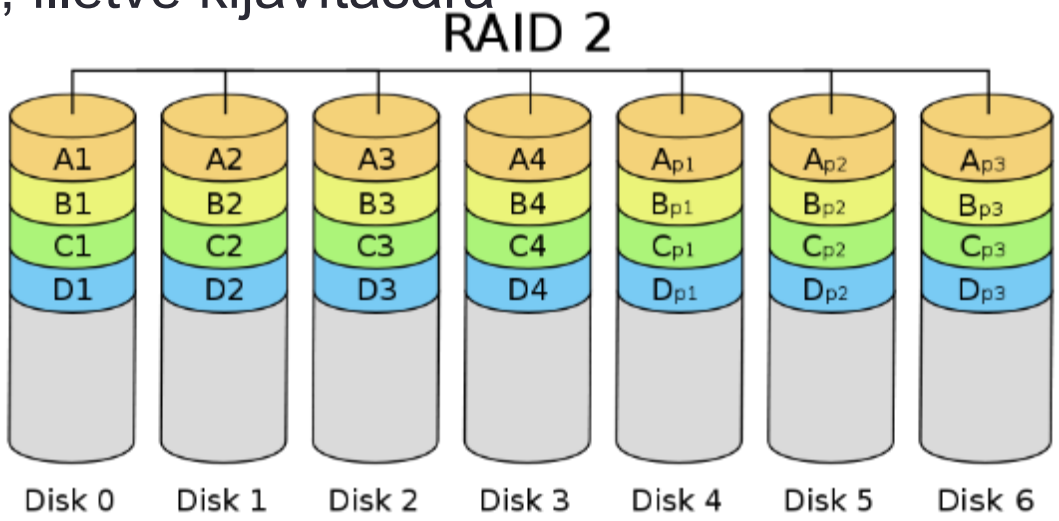
- A **RAID 0** az egyes lemezek egyszerű összefűzését jelenti, viszont semmilyen redundanciát nem ad, így nem biztosít hibatűrést, azaz **egyetlen meghajtó meghibásodása az egész tömb hibáját okozza.**
- A megoldás lehetővé teszi különböző kapacitású lemezek összekapcsolását is, viszont a nagyobb kapacitású lemezeken is csak a **tömb legkisebb kapacitású lemezének méretét** lehet használni (tehát egy 120 GB és egy 100 GB méretű lemez összefűzésekor mindössze egy 200 GB-os logikai meghajtót fogunk kapni, a 120 GB-os lemezen 20 GB szabad terület marad, amit más célokra természetesen felhasználhatunk).



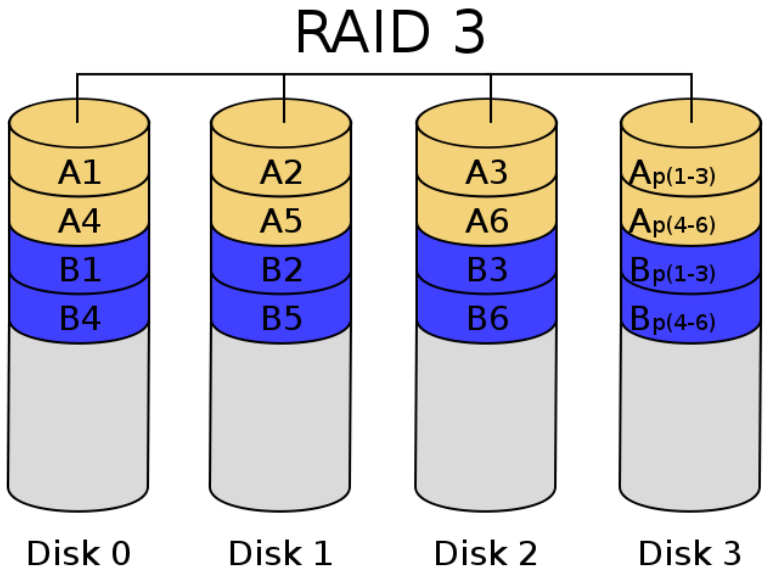
- A **RAID 1** eljárás alapja az adatok tükrözése (disk mirroring), azaz az információk **egyidejű tárolása** a tömb minden elemén.
- A kapott logikai lemez a tömb legkisebb elemével lesz egyenlő méretű. Az adatok **olvasása párhuzamosan történik** a diszkekről, felgyorsítván az olvasás sebességét; az **írás normál sebességgel**, párhuzamosan történik a meghajtókon.
- Az eljárás igen jó hibavédelmet biztosít, bármely meghajtó meghibásodása esetén folytatódhat a működés. A RAID 1 önmagában nem használja a csíkokra bontás módszerét.



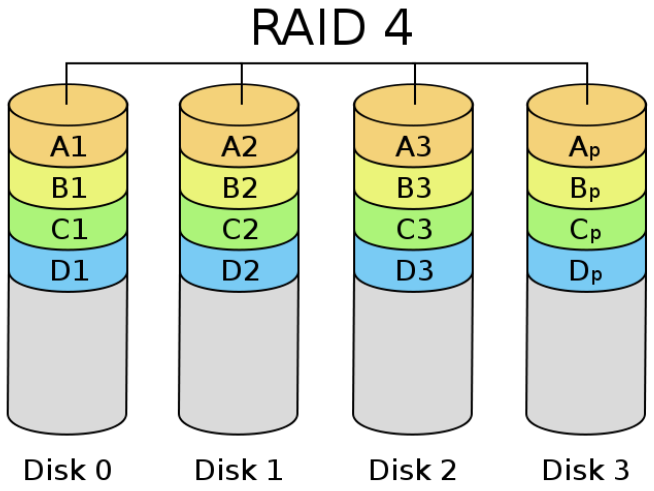
- A **RAID 2** használja a csíkokra bontás módszerét, emellett egyes meghajtókat **hibajavító kód** (ECC: Error Correcting Code) tárolására tartanak fenn. A hibajavító kód lényege, hogy az adatbitekből valamilyen matematikai művelet segítségével redundáns biteket képeznek.
- Ezen meghajtók egy-egy csíkjában a különböző lemezeken azonos pozícióban elhelyezkedő csíkokból képzett hibajavító kódot tárolnak. A módszer esetleges lemezhiba esetén képes annak detektálására, illetve kijavítására



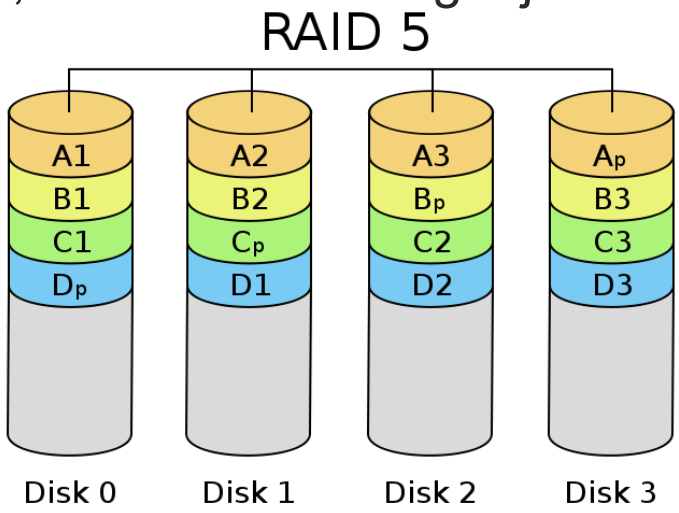
- A RAID 3 felépítése hasonlít a RAID 2-re, viszont nem a teljes hibajavító kód, hanem csak egy lemeznyi paritásinformáció tárolódik. Egy adott paritáscsík a különböző lemezeken azonos pozícióban elhelyezkedő csíkokból XOR művelet segítségével kapható meg.
- A rendszerben egy meghajtó kiesése nem okoz problémát, mivel a rajta lévő információ a többi meghajtó (a paritást tároló meghajtót is beleértve) XOR-aként megkapható.



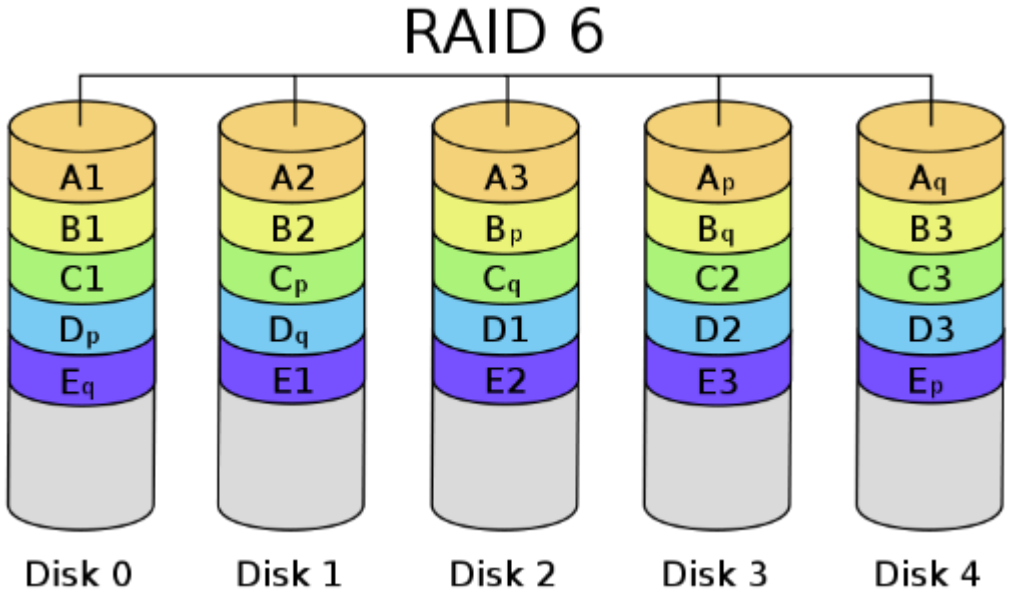
- A **RAID 4** felépítése a RAID 3-mal megegyezik. Az egyetlen különbség, hogy itt **nagyméretű csíkokat definiálnak**, így egy rekord egy meghajtón helyezkedik el, lehetővé téve egyszerre több (különböző meghajtókon elhelyezkedő) rekord párhuzamos írását, illetve olvasását (multi-user mode).
- Problémát okoz viszont, hogy a paritás-meghajtó adott csíkját **minden egyes íráskor frissíteni kell** (plusz egy olvasás és írás), aminek következtében párhuzamos íráskor a paritásmeghajtó a rendszer szűk keresztmetszetévé válik. Ezenkívül valamely meghajtó kiesése esetén a rendszer olvasási teljesítménye is lecsökken, a paritás-meghajtó jelentette szűk keresztmetszet miatt.



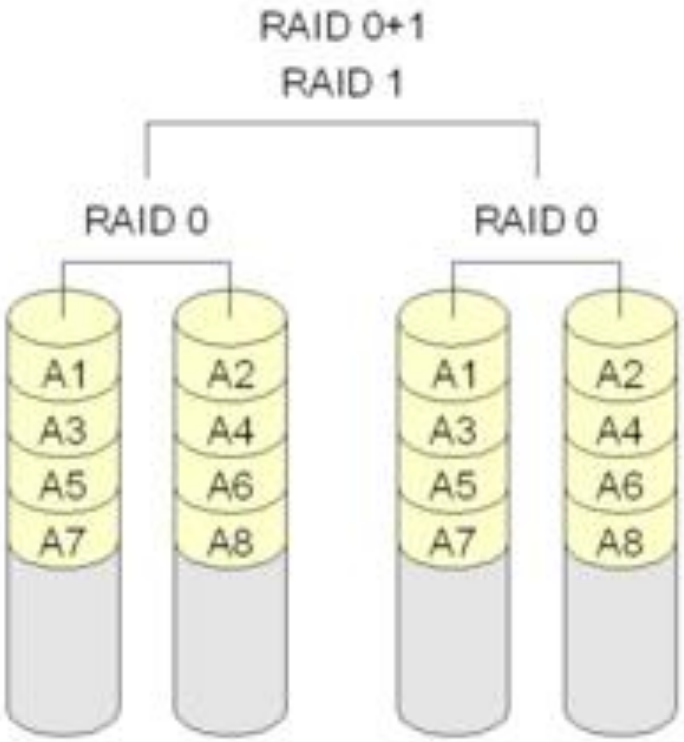
- A **RAID 5** a paritás információt nem egy kitüntetett meghajtón, hanem „**körbeforgó paritás**” (rotating parity) használatával, egyenletesen az összes meghajtón elosztva tárolja, kiküszöbölvén a paritás-meghajtó jelentette szűk keresztmetszetet. Minimális meghajtószám: 3. Mind az írási, mind az olvasási műveletek párhuzamosan végezhetőek.
- Egy meghajtó meghibásodása esetén az adatok sértetlenül visszaolvashatóak, a hibás meghajtó adatait a vezérlő a többi meghajtóról ki tudja számolni. A csíkméret változtatható; kis méretű csíkok esetén a RAID 3-hoz hasonló működést, míg nagy méretű csíkok alkalmazása esetén a RAID 4-hez hasonló működést kapunk. A hibás meghajtót ajánlott azonnal cserélni, mert két meghajtó meghibásodása esetén az adatok elvesznek!



- A **RAID 6** tekinthető a RAID 5 kibővítésének.
- Itt nemcsak soronként, hanem oszloponként is kiszámítják a paritást. A módszer segítségével **kétszeres meghajtó meghibásodás** is kiküszöbölhetővé válik. A paritáscsíkokat itt is az egyes meghajtók között, egyenletesen elosztva tárolják, de ezek természetesen kétszer annyi helyet foglalnak el, mint a RAID 5 esetében.

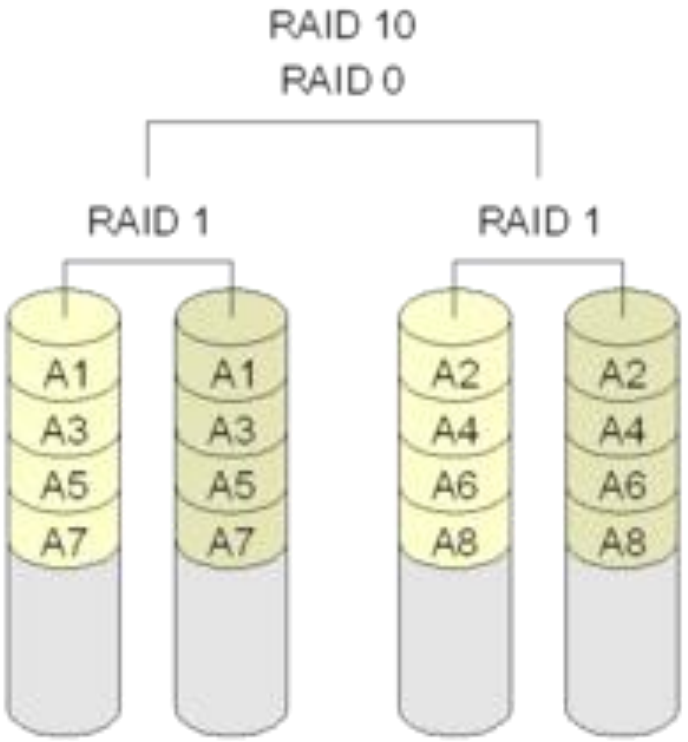


- Ez egy olyan hibrid megoldás, amelyben a RAID 0 által hordozott sebességet a RAID 1-et jellemző biztonsággal ötvözhetjük.
- Hátránya, hogy **minimálisan 4 eszközre** van szükségünk, melyekből 1-1-et összefűzve, majd páronként tükrözve építhetjük fel a tömbünket, ezért a teljes kinyerhető kapacitásnak mindössze a felét tudjuk használni.
- Mivel a tükrözés (RAID 1) a két összefűzött (RAID 0) tömbre épül, ezért egy lemez meghibásodása esetén az egyik összefűzött tömb mindenképp kiesik, így a tükrözés is megszűnik.



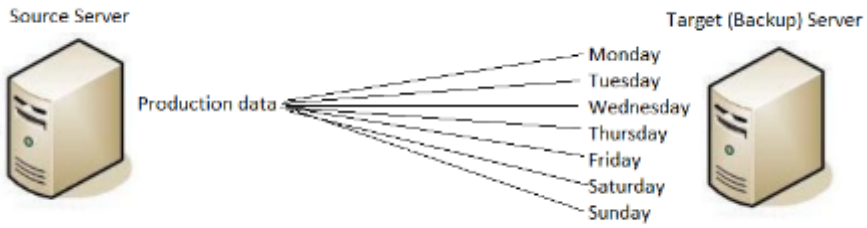
- Hasonlít a RAID 01 megoldáshoz, annyi különbséggel, hogy itt a lemezeket **először tükrözzük**, majd a kapott tömböket fűzzük össze.

- Ez biztonság szempontjából jobb megoldás, mint a RAID 01, mivel egy diszk kiesése csak az adott tükrözött tömböt érinti, a rá épült RAID 0-t nem; sebességben pedig megegyezik vele.



Biztonsági mentés

- A szerver beállításairól, megosztott mappákról időzített mentés.



Biztonsági mentés típusok

- **Normál:** minden kiválasztott állományról az A attr.-tól függetlenül. Az A attr. törlődik.
- **Másolat:** minden kiválasztott állományról az A attr.-tól függetlenül. Az A attr. *nem* törlődik.
- **Különbségi:** a kiválasztottak közül csak az A attr.-al rendelkezőket. Az A attr. *nem* törlődik.
- **Növekményes:** a kiválasztottak közül csak az A attr.-al rendelkezőket. Az A attr. törlődik.
- **Napi:** a kiválasztottak közül csak azokat, amelyek módosultak a mentés napján. Az A attr. *nem* törlődik.

Biztonsági mentési terv példa

Mikor?	Milyen?	Mit ment?
Hétfő	Növekményes	Vasárnap óta változottakat
Kedd	Növekményes	Hétfő óta változottakat
Szerda	Növekményes	Kedd óta változottakat
Csütörtök	Növekményes	Szerda óta változottakat
Péntek	Növekményes	Csütörtök óta változottakat
Szombat	Növekményes	Péntek óta változottakat
Vasárnap	Normál	Mindent

SZERVERSZOBA KIALAKÍTÁSA

SZERVERSZOBA

- Biztonságtechnikai-, beléptető-, vagyonvédelmi rendszerek

SZERVERSZOBA

- Szünetmentes tápellátó berendezések (rendelkezésre állás)

SZERVERSZOBA

- Túlfeszültség-, és zavarvédelmi megoldások

SZERVERSZOBA

- Érintésvédelem

Az érintésvédelem üzemszerűen feszültség alatt nem álló, de meghibásodás esetén feszültség alá kerülő vezető részek érintéséből származó balesetek elkerülésére szolgáló műszaki intézkedések összessége.

SZERVERSZOBA

- Füstérzékelők, tűzérzékelő- és oltóközpontok, Tűzoltórendszerek

- **Szén-dioxid**

Oltóanyaga élelmiszeripari tisztaságú szén-dioxid, elsődlegesen éghető folyadékok és gázok tüzeinel oltására alkalmas. De alkalmas **feszültség alatti** berendezések oltására is. A Széndioxid térfogat-kit megállítja az égést, azaz lecsökkenti az égéshez szükséges Oxigén mennyiséget.

SZERVERSZOBA

- Páratartalom, hőmérséklet