Információs Rendszerek Üzemeltetése Vizsga segédlet

készítette:Bartók Tamás (2013.06) és TI

Elöljáróban: Azért készült ez a kis elméleti agytorna, mert a korábbi években nagy mérétkű volt a bukási arány vizsgákon. A tapasztalatok szerint sok helyen tévesek/pontatlanok a korábbi wikis anyagok, egy mondatos kérdésekre adott válaszok. Ez a nyalánkság ezeket próbálja meg kijavítani. Nem csak korábbi évek kérdéseit dolgozza fel, hanem saját szubjektív meglátásom szerinti értelmes, lehetséges kérdéseket is belefaragtam.
FONTOS!!! : Nem feltétlen tartalmaz ez sem 100%-os megoldásokat és az hogy minél jobb legyen a ti feladatotok is, hogy szerkesszétek ha találtok valami csiszolni valót.
Nem csak vakon a wikipédiára és a diákra támaszkodva próbáltam összeállítani(azért 85%-ban diákból), hanem több hitelesebb forrásból. Remélem segít, ha már csak pár pontot is dob a vizsgán, már megérte. Fogyasszátok egészséggel.
// A KOCKÁZATOK ÉS KELLÉKHATÁSOK TEKINTETÉBEN KÉRJÜK, OLVASSA EL A RETEKTÁJÉKOZTATÓT VAGY MÉRGEZZE MEG KEZELŐORVOSÁT, ÓVSZERÉSZÉT! //

A doksi egyes részeinek érthetőbbé tétele miatt köszönet Haraszin Péter, Somogyi Péter és Bodnár Dániel kollegáknak.

A módosításokról: Kérlek titeket, hogy ide írjátok be, hogy mikor módosítottátok utoljára, esetleg melyik részt/részeket:
Megszületése: 2013.06.

Bevezető diasor (IRU_2013_1):

1. Az információs rendszerek kialakulásának fontosabb szereplői:

- Felhasználó (körülötte forog a világ)
- Folyamattervező (inkább business mint IT)
- Rendszertervező (valahol az IT és a business között, IT beütéssel)
- Programozó
- Tesztelő
- Üzemeltető (rendszer adminisztrátor)

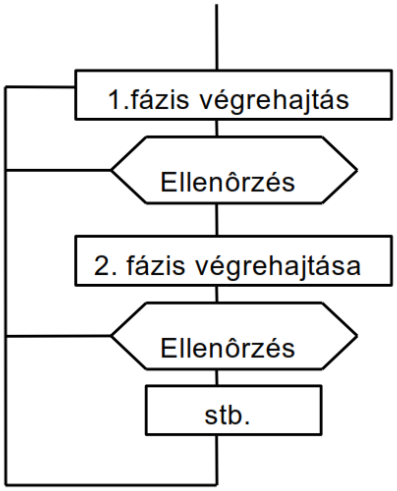
2. Mit értünk életciklus alatt?

Egy rendszer teljes élettörténete az ötlet megszületésétől a használatból való kivonásig. Hasznos, mert mások tapasztalatára építhetünk, módszeresen végiggondoljuk a feladatokat.

3.Vízesés modell fázisai (5 db):

Analízis, Tervezés, Implementáció, Teszt, Integrálás

*info: A fázisok egymásra épülnek. Az egyes fázisok végén döntési pontok(mérföldkövek) vannak, amiben értékelik, elemzik az előző fázis eredményeit.



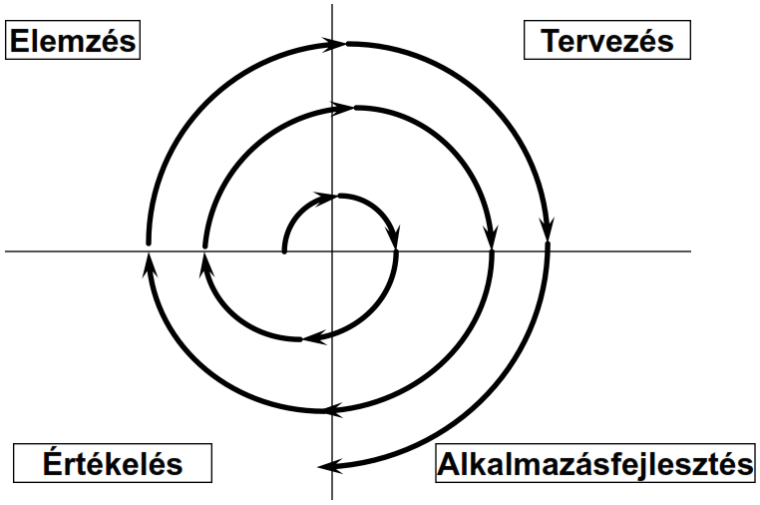
4. Inkrementális modell lényege?

A teljes program egyenként különálló és működő kisebb programokból épül fel. A

kezdeti tervezési fázisban az akkor elkészülő első kis programot teljesnek feltételezzük és utána fokozatosan fejlesztjük és adunk hozzá újabb az előzővel kompatibilis és működö programokat.

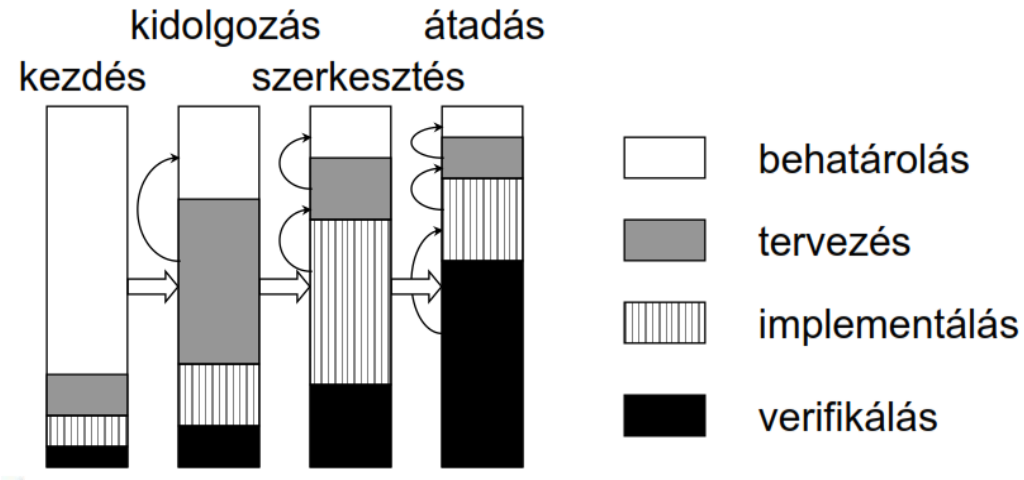
5. Spirál modell lényege?

A spirál modell iterációkból épül fel, melyek ismétlődnek a projekt során. Egy hibrid modell, mivel megtartotta a vízesés modell előnyeit és nem zárja a prototípus készítésének lehetőségét sem.



6. Érettség modell 4 fázisa?

kezdés, kidoglozás, szerkesztés, átadás



IRU_2013_Ism_Hal_Serv_deskt_1 diasor, kulcsszavak OSI/ISO, NA(P)T, DNS, szerverek, frissítés:

7. Sorolja fel az OSI 7 rétegét:

1. Fizikai réteg
2. Adatkapcsolati réteg
3. Hálózati réteg
4. Szállítási réteg
5. Viszony réteg
6. Megjelenítési réteg
7. Alkalmazási réteg

8. Mi a protokoll?

Szabályok gyűjteménye, mely vezényli a kommunikációt hálózati elemek között.

9. Hanyadik rétegbeli eszköz a hub és mi a feladata?

A hub Layer 1-es eszköz (fizikai rétegbeli), feladata hogy a bemenetére érkező jelet minden portra továbbítsa(broadcast eszköz).

10. Hanyadik rétegbeli eszköz a bridge és mi a feladata?

Layer 2-es eszköz(adatkapcsolat rétegbeli), feladata MAC cím alapú irányítás, keret analízis.

11. Hanyadik rétegbeli eszköz a switch és mi a feladata?

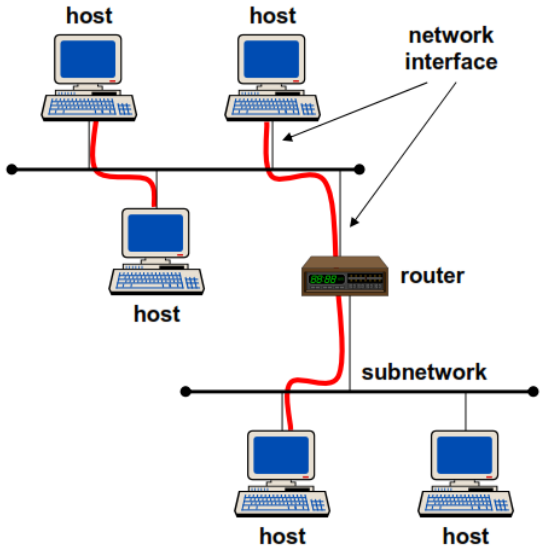
Layer 2-es eszkoz(adatkapcsolat rétegbeli), DE vannak magasabb rétegbeli switchek is (4. rétegbeli NAT switch, 7. rétegbeli). Feladata a 2. rétegbelinek MAC cím alapú irányítás, a bemenő jelet a megfelelő portra irányítja,

12. Hanyadik rétegbeli eszköz a router és mi a feladata?

Layer 3-as eszköz(hálózat rétegbeli), feladata útvonal választás/két vagy több alhálózat összekötése, irányítás IP cím alapján.

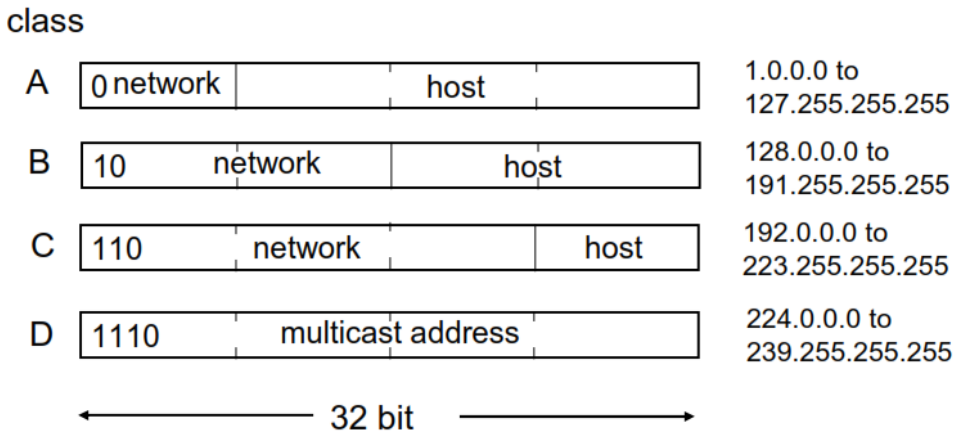
12. Sorolja fel az IP hálózat elemeit (4 db):

Host, Alhálózat(subnet), Hálózati interfész, Útvonalválasztó(router)



13. Mennyi és milyen IP címosztályok vannak, mi a hálózati cím és hogyan határozható meg?

4 címosztály van, amiket A,B,C,D-vel jelölünk, meghatározásuk pedig a következő képpen történik:



Egy IP cím két részből épül fel, egy hálózati címből(ami az IP cím első fele) és a host címből(ami az IP cím második fele).

Az, hogy melyik rész a network cím, és melyik azonosítja a host-ot a netmask határozza meg. A hálózati címet úgy határozzuk meg, hogy az alhálózati maszkot összeéseljük az IP címmel.

Alhálózati maszk:

- Ha A IP osztálybeli, akkor az első byte 255 (első 8 bit csupa 1)
- Ha B IP osztálybeli, akkor az első 2 byte 255(első 16 bit csupa 1)
- …

/**********/

SZÁMOLÓS PÉLDA(lehet kicsi szájbarágósak, de az szerintem sosem baj)

1. *Határozzuk meg a 192.168.2.1 IP cím hálózati címét.*

Az első byte binárisan 192-->1|1|0|0|0|0|0|0 → vagyis C osztálybeli, ezért az alhálózati maszk: 255.255.255.0
Bitenként összeéselve az IP címmel: **192.168.2.0, ez lesz a hálózati cím**.

2. *Változó hosszúságú alhálózati maszk esetén hány hostnak osztható ki IP cím, ha a cím 152.130.246.0 /27 ?*

A változó hosszúságot a '/' jel után jelzett szám jelenti. Jelen esetben 27 bites az alhálózati maszk, vagyis mivel 32 bites az IP cím, az utolsó 5 bit (32-27) jelzi a hostok címét.

…….....|xxxHHHHH a 'H'-val jelzettek használhatók a hostok megkülönböztetésére az adott alhálózaton belül. 2^5=32, azonban ebből 2 darab cím lejön, mivel a csupa nulla a network cím, a csupa 1 pedig a broadcast cím.

Azaz a megoldás 32-2=**30 hostnak osztható ki IP cím**

3. Mi a netmask a következő alhálózatban 192.168.1.0/5

248.0.0.0 (első 5 bit 1-es, többi 0)

/**********/

14. Mi a loopback cím?

A loopback vagy localnet címmel a saját gépünkkel tudunk kommunikálni. Bármelyik cím a 127.0.0.0 tartományon belül a saját számítógépünkkel kommunikál. például loopback cím a 127.0.0.1

15 Mi a DHCP és a feladata?

Dynamic Host Configuration Protocol, lehetővé teszi, hogy egy gép IP címet kérjen a hálózattól, hátránya, hogy minden kérésnél új IP címet kap.

16. Mi a MAC cím és a feladata?

A gép fizikai címe, a gyártók adják a kártyáknak.

17. Mi az ARP és a feladata?

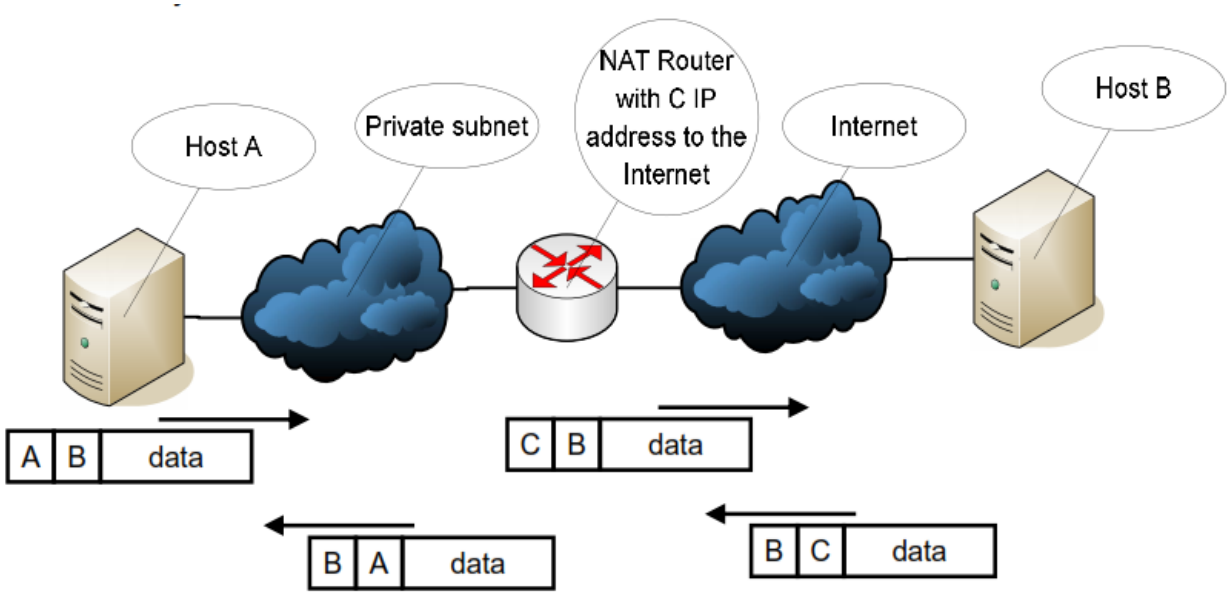
Adress Resolution Protocol. A forrásnak tudnia kell a cél hardver-címét (MAC address) mielőtt IP csomagokat küldhetne neki. Az ARP segítségével megtudhatjuk egy másik gép MAC címét, ha ismerjük az IP címét.

18. Mi a RARP és a feladata?

Reverse ARP, a feladata az ARP-val ellentétes, vagyis ismerjük a cél gépnek a MAC címét és az IP címét kapjuk meg a RARP segítségével.

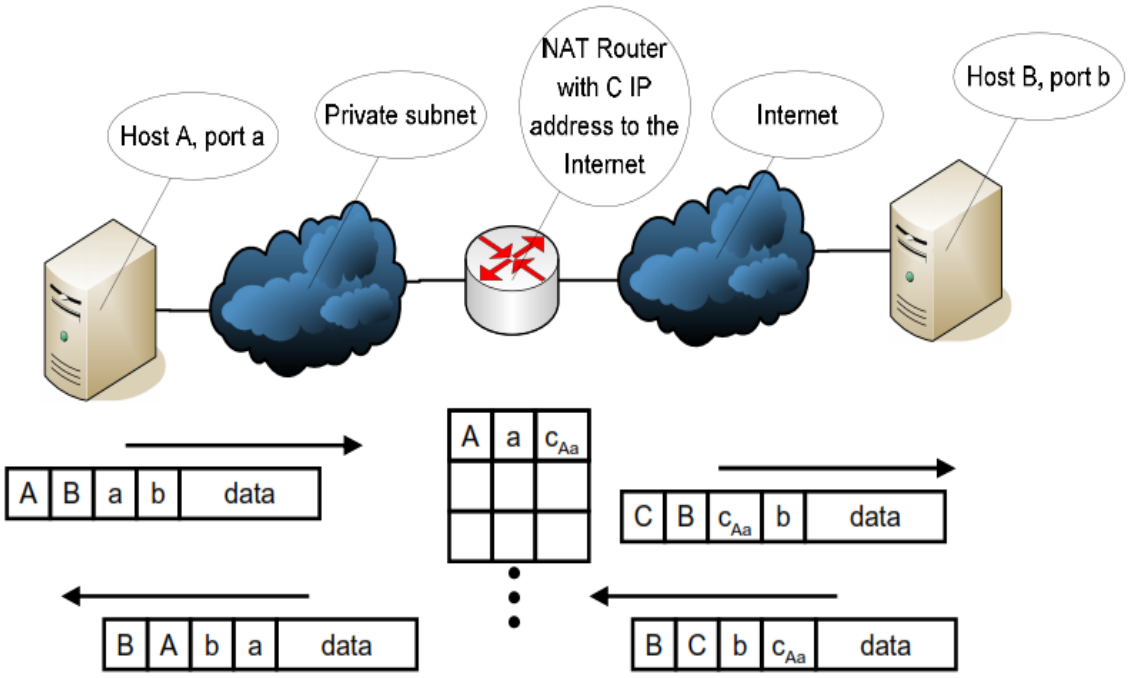
19. Mi a NAT és a feladata?

Network Adress Translation, feladata címfordítás.Egy belső hálózatra kötött gépek közvetlen kommunikációját teszi lehetővé más külső gépekkel anélkül, hogy a saját címeiket használnák(NAT-oljuk a host IP címét).



20. Mi a NAPT és mi a feladata?

NAT+port transzláció. Portot is fordít, nem csak címet.



21. Mi a DNS és mi a feladata?

Domain Name System, feladata hogy az IP címekhez valamilyen emészthetőbb megnevezést rendeljen.

22. Mi az ICMP feladata, mondjon 2 példát használatára.

Internet Control Message Protocol, hibajelzésre, illetve IP szintű kontroll üzenetek továbbítására használjuk. példák: ping, traceroute

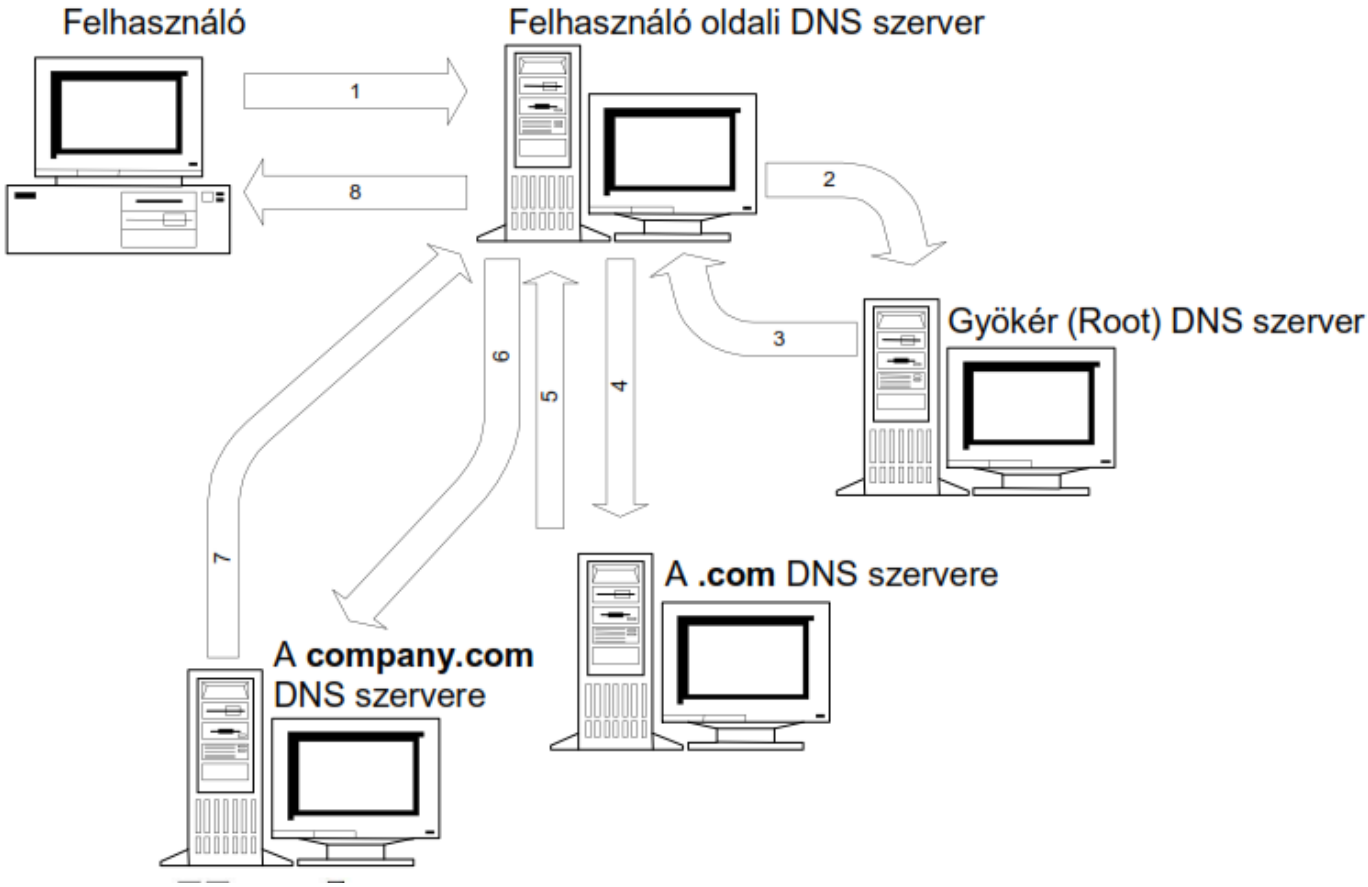
23. Mire használjuk a ping-et, melyik protokoll része?

A pinget végpontok tesztelésére használjuk, az ICMP része.

pl.:
```
Ping alpha [152.66.246.10] with 32 bytes of data:
Reply from 152.66.246.10: bytes=32 time=114ms TTL=250
Reply from 152.66.246.10: bytes=32 time=26ms TTL=250
Reply from 152.66.246.10: bytes=32 time=23ms TTL=250
Reply from 152.66.246.10: bytes=32 time=27ms TTL=250

Ping statistics for 152.66.246.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 23ms, Maximum = 114ms, Average = 47ms
```

24. Hogy működik a DNS, domain név feloldásának lépései?

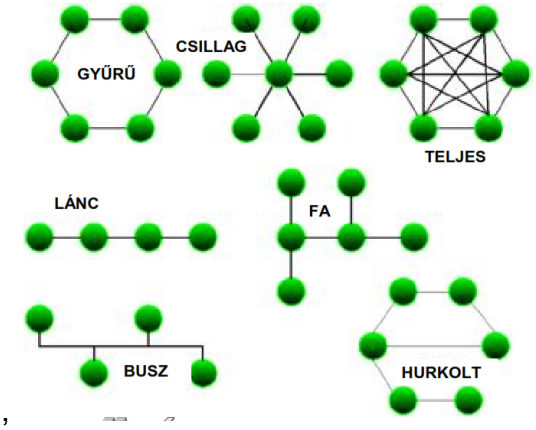


25. Mi az a 4 dolog amit kell beállítani fix IP címnél?

IP cím, gateway, netmask, DNS

26. Soroljon fel 6 hálózati topológiát, melyek decentralizáltak(D)?:

csillag, fa(D), gyűrű, teljes(D), lánc(D), busz, hurkolt(D)



27. Mit nevezünk logikai topológiának, mi a 3 típusa?

Logikai topológiának nevezzük azt a topológiát, amiben csak 3. vagy magasabb rétegbeli egységeket használunk, töntetünk fel.

Fajtái:

- Flat topology
  - csak a kijáraton 3. rétegbeli entitás (router)
- Location-based topology
  - pl. emeletenként egy-egy alháló (saját IP címtartomány)
- Functional-group based topology
  - fizikai elhelyezkedéstől függetlenül logikai csoportok szerint (eladók, mérnökök, menedzsment, marketing) flat network

28. Mit nevezünk demarkációs pontnak?

Demarkációs pont a vállalati hálózat és egy kommunális szolgáltató (telefon, hálózati szolgáltató) közötti határpont.

29. Mit nevezünk szervernek?

Szervernek nevezzük azt a számítógépet, vagy szoftvert, ami lehetővé teszi más szemítógépek számára a rajta tárolt **adatok, szolgáltatások**, illetve **erőforrások** elérését.

30. Mik a homogén szerverek előnyei?

- egyszerűbb fenntartás
- egyszerűbb oktatás
- egyszerűbb pótalkatrész raktározás (csak egy kell mindenből)
- könnyebb javítás

31. Mik a heterogén szerverek előnyei?

- nem “ragadunk be”, ha a szállítóval valami történik
- minden feladathoz a legjobb berendezést választhatjuk
- a gyártók közti versenyeztetés miatt olcsóbb beszerzési költség

32. Szerverek telepítésekor mikre kell figyelnünk, miket kell biztosítanunk?

- fizikai védelem
- elektromos zavarok elleni védelem
- UPS (Uninterruptible Power Supply) -> védett táp
- HVAC(heating, ventilating and air conditioning)-->hőmérséklet és páraszabályozás

- tűzbiztosság

33. Szerver frissítésének 11 lépését sorolja fel:

1. Feladatlista-készítés
    a. rejtett függések feltárása és dokumentálása, kevesen olvassák el általában
2. Kompatibilitási ellenőrzése
    a. a SW-t az új OS nem támogatja: olyan verzióra frissítünk, amit még/már támogat
    b. a SW-t csak az új OS támogatja: csak új OS-en lehet tesztelni-->tesztgép
    c. a SW-t az új OS semmiképpen nem támogatja:
        1. meggyőzzük a usereket, hogy nem kell a SW
        2. el kell tekinteni az OS frissítéstől
3. Ellenőrző tesztek elvégzése:
    a. automatikus tesztek(scriptek): OK, NO OK eredmények
    b. manuális tesztek
    c. regressziós tesztek: ugyanolyan kimenetet ad-e az új és a régi rendszer?
4. Visszakoz terv elkészítése: ha nem sikerülne a rendszer frissítés, akkor vissza kell állítanunk a régi állapotba
5. Karbantartási időszak:
   (Frissítési idő+ Teszt idő + Visszakoz idő+ Visszakoz-teszt idő) * [2...3]
6. Frissítések hirdetése a felhasználók körében: LÁTVÁNYOSAN, figyelem FEIkEITŐŐ módon
7. Tesztek végrehajtása
8. Frissítések elvégzése
9. Frissítés tesztelése
10. ...Ha nem volt sikeres, akkor Visszakoz
11. Karbantartási eredmények hirdetése a userek közt

34. Mit nevezünk friss installnak?

Friss install a tényleges újra telepítés, ami néha lehet előnyösebb a frissítésnél. Kis luxsu, klónozás, nagy luxus teljesen új rendszeren végezzük (új HW is)

35. Mi az a redundáns tápellátás?

Nem azt jelenti, hogy két táp van, hanem azt, hogy bármelyik meghibásodása esetén a rendszer működőképes marad, ha az egyik elromlik (n+1 redundancia).

36. Mit nevezünk meleg tartaléknak(hot swap)?

Ezzel a technológiával felruházott rendszerekben az operációs rendszer újraindítása nélkül, menet közben lehet a meghibásodott diszket kicserélni, új diszket behelyezni. n+1+1 redundanciát biztosít

Legfőbb felvetődő kérdés: Mely részek legyenek ilyenek?...

37. Sorolja fel a Desktop management szolgáltatásokat (5 db):

1. Rendszerkép készítés(system image), automatikus géptelepítés
    a. mintatelepítés az system image által
    b. Wake On LAN funkció támogatása
2. Személyre szabott SW telepítés, alkalmazás felügyelet, használat mérése
    a. felhasználói jogosultságok meghatározása, felhasználói beállítások(háttérszín, stb...)
    b. a tárolt rendszer képek általi “öngyógyítás lehetősége”
    c. használat mérése: pl hány licencelt felhasználó használja, mennyi a licence korlát és ha elértük, akkor tiltsuk le a hozzáférést mások számára
3. policy management
    a. vállalati szinten meghatározott, hogy az adott felhasználók mire jogosultak, azaz felhasználó, nem pedig gép függő!
4. Távoli felügyelet
    a. nem kell a felhasználónak érteni a hibakezeléshez-->”help request” opció--> rendszergazda távolról tudaj felügyelni és orvosolni a problémát, ha van hozzá jogosultsága
5. Teljes körű SW és HW leltár
    a. SQL-ben tárolt adatok
    b. lista a HW és SW eszközökről

38. Rendelkezésre állási idők:

Nagyságrend	A	Max. kiesési idő 1 év alatt
1 9-es	90 %	36,5 nap (1 hónap)
2 9-es	99 %	3,5 nap
3 9-es	99,9 %	9 óra
4 9-es	99,99 %	1 óra
5 9-es	99,999 %	5 perc
6 9-es	99,9999 %	32 mp
7 9-es	99,99999%	3 mp

Számítási mód: 24 óra → 1 nap, 1 év 365 nap,

24*365*X, ahol ‘X’ a kilneces rendelkezésre állásoknak megfelelően alakul, azaz 1 kilences rendelkezésre állásnál 24*365*0,1(mivel egy évben 10%os kiesés lehet, ami 0,1) = 876 óra = 36,5 nap

TMN_IRU diasor, kulcsszavak: QoS, QoE, Management, FCAPS, hibaanalízis

39. Mikor elégedett a felszhasználó egy szolgáltatással?

1. Ha kéréseit kiszolgálják
2. Ha a szolgáltatás minősége is kielégítő
3. Ha a felmerülő problémákat minél hamarabb orvosolni tudják

40. QoS 4 mércéje (paramétere) ?

1. Rendelkezésre állás
2. Throughput (áteresztőképesség)
3. Csomag késleltetés
4. Csomag késleltetési arány (Jitter)
5. Csomag vesztés

41. A csomag teljes késleltetése milyen összetevőkből áll össze?

1. feldolgozási késleltetés (processing): Csomagok feldolgozása és felkészítése az újra küldésre
2. sorban állási késletetés (queuing delay)
3. terjedési késletetés (propagation delay): A csomagok kapcsolaton való terjedési ideje
4. továbbítási késleltetés (transmission time): A csomag megérkezésének teljes ideje, az eső bit beérkezésétől az utolsóig.

teljes csomag késleltetés =
(feldolgozási idő) + sorbanállási idő +
(terjedési idő) + továbbítási idő

42. Mi az a jitter és minek a része?

A jitter a QoS (Quality of Service) egyik paramétere, csomag késleltetés ingadozását jelenti. Intenzív Audio/Video átvitelnél érdekes igazán. Nagy jitter-> börsztösebb folyamot eredményez

| | | | | | | | - csomagok közötti idő közel állandó: kis jitter

| | | ||| | | - börsztös forgalom: NAGY jitter

43. Kik közötti megállapodás az SLA (Service Level Agreement)?

Az SLA(Service Level Agreement) a hozzáférési hálózatot biztosító szolgáltató és az előfizető közötti megállapodás.

44. Mi az az SLS?

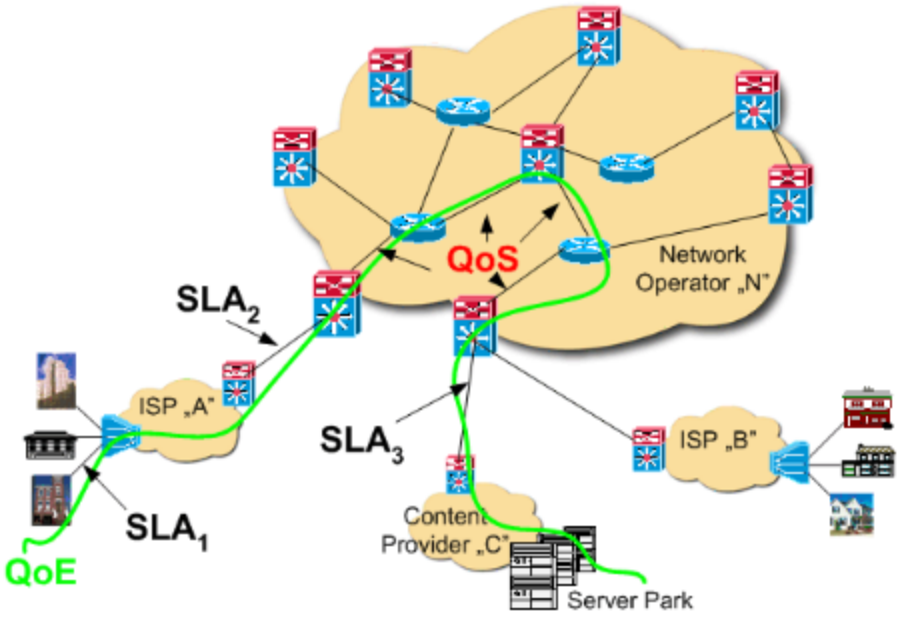
Service Level Specification, az SLA műszaki melléklete, amelyben a műszaki és nem műszaki paraméterek és azok határértékeik vannak leírva.

45. Mi az a QoE?

A Quality of Experience egy szubjektív felhasználói elégedettséget jelenti. Mércék típusai pedig a felhasználó elégedettségitípusaival egyezik meg (lásd 39.feladat), azaz rendelkezésre állás, kielégítő szolgáltatás minőség, hibák záros határidőn belüli orvoslása.

46. Hol használjuk az SLA-t, QoS-t és QoE-t?

Az alábbi remek ábra foglalja ezt össze



47. Mi az a TMN és mire használják?

Telecommunications Management Network segítségével a szolgáltatók tudják menedzselni a hálózati elemeken, operációs rendszerekben, hálózattípusokon átívelő kapcsolatot és kommunikációt.

48. Sorolja fel a TMN logikai modell elemeit:

1. Network Element
2. Element Management
    a. az egyes hálózati elemek, mint különálló funkcionális egységek kezelése, felügyelete
3. Network Management
    a. A hálózat, mint elkülöníthető funkcionális egység felügyeletére és vezérlésére vonatkozó feladatok
    b. CM → Configuration Management
4. Service Management
    a. felhasználóval való kapcsolat tartás
    b. számlázási adatok
    c. PM és FM → Performance- és Fault Management
5. Business Management
    a. Magas szintű tervezés
    b. Célok definiálása
    c. döntéshozás
    d. BLA-s → Business Level Agreements

49. Minek a rövidítése az FCAPS?

1. Fault Management
    a. Azért felelős, hogy a szolgáltatások mindig elérhetőek legyenek
    b. feladatai: hiba detektálása, jelzése az operátor felé, hibaok feltárása, hiba javítása
2. Configuration Management
    a. A hálózat elemeinek/felépítésének és egységei változásának részleteivel foglalkozik
    b. ide tratoznak: erőforrás kihasználtság, Backup and Restore, hálózatfenntartás
3. Accounting
    a. Felhasználói adatok kezelése
4. Performance Management
    a. Teljesítményre jellemző mércék gyűjtése (pl QoS) gyűjtése, elemzése, értékelése

5. Security Management
    a. Feladata a nem jogosult rendszer hozzáférések minimalizálása.
    b. AAA:
        i. Authentikáció → Kik férhetnek hozzá a rendszerhez
        ii. Authorizáció → Mihez férhetnek hozzá a rendszerben
        iii. Accounting

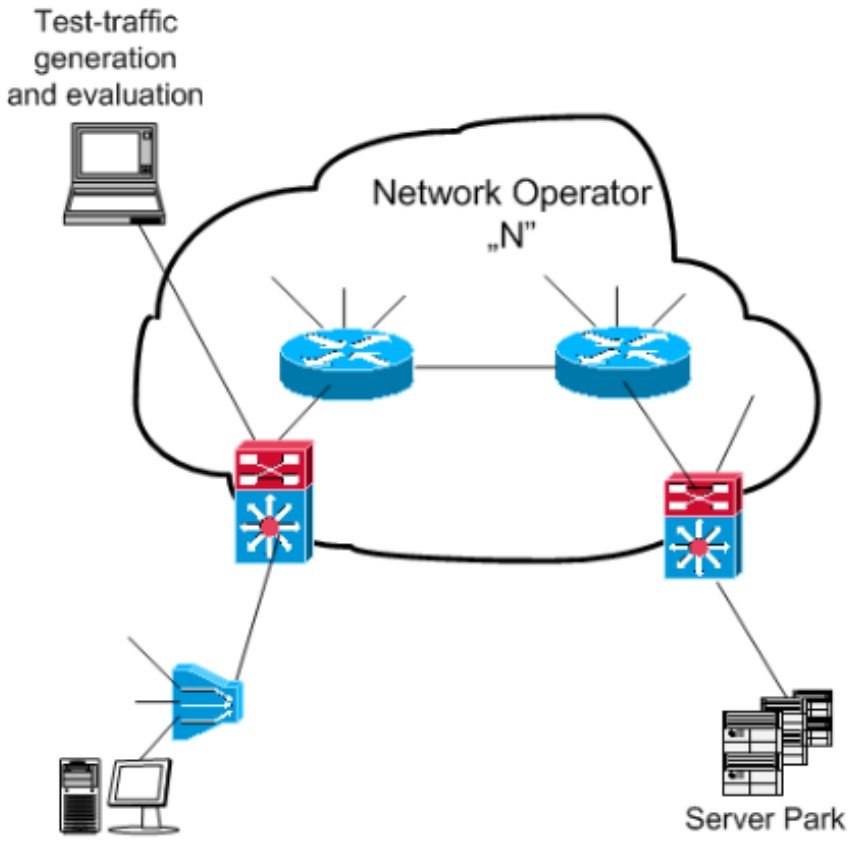
50. Mit értünk monitorozás alatt?

A monitorozó eszköz csatlakoztatását a rendszerre és segítségével adatok gyűjtése, feldolgozása, majd értékelése.

51. Milyen monitorozási módszerek vannak?

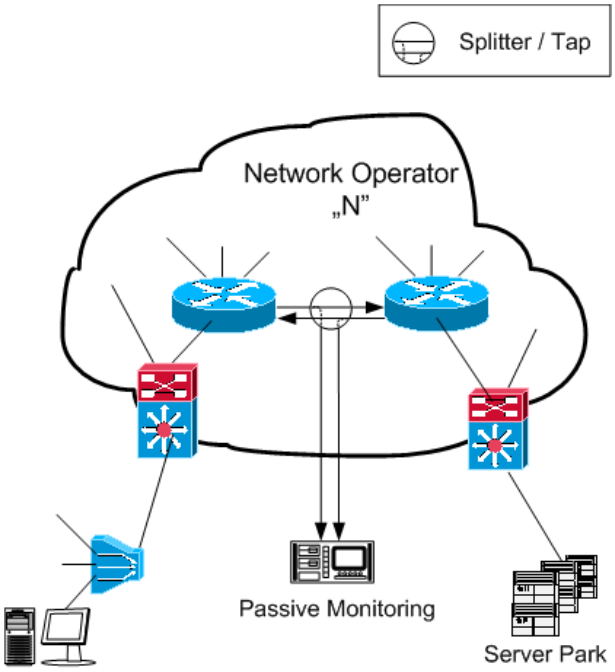
1. Aktív monitorozás:
    a. Próbaforgalom beiktatása és a “hatás” vizsgálata
    b. csak mintavételezés jelleggű eredményekkel szolgálhat
    c. a mesterséges, általunk generált forgalom torzíthatja a mérési eredményeket

Mérési összeállítás az alábbi ábrán látható



2. Passzív monitorozás:
    a. Hálózati forgalom külső szemlélőként való figyelése
    b. hibátlan eredményt ad teljes időskálán

    az alábbi ábra ismét megvilágosítja a sötét elmét



52. Milyen típusú adatokat gyűjthetünk?

- Topológiai
- naplóállományok
- nyers forgalmi szintű adatok

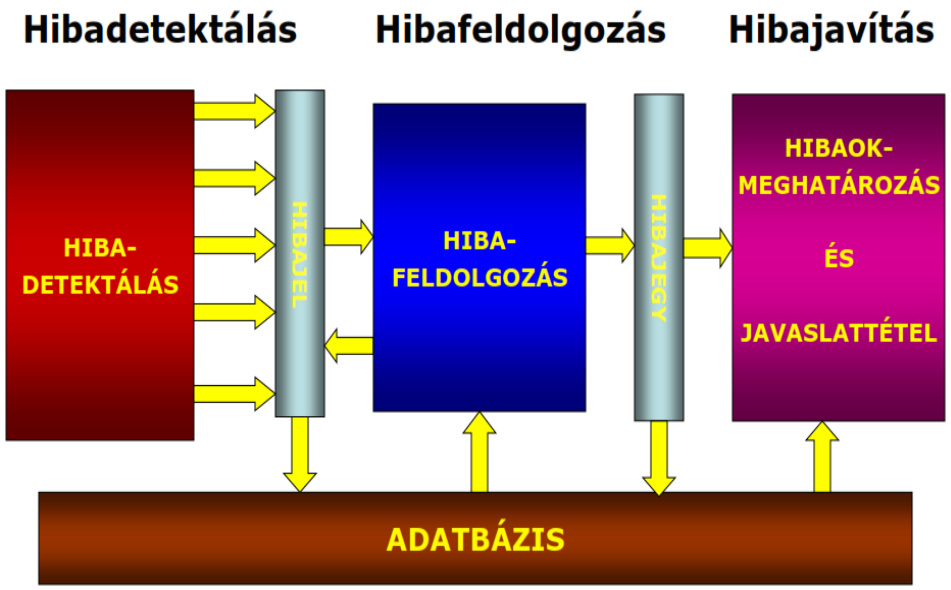
53. Tranzakció azonosításának fajtái?

5-tuple: forrás IP, cél IP, forrás port, cél port, IP protokoll
3-tuple: forrás IP, cél IP, IP protokoll
N-tuple...

54. Sorolja fel a hibamenedzselés folyamatának lépéseit és azok eredményeit:

1. Hibadetektálás, eredménye: HIBAJEL (EVENT)
   A szolgáltatást kifejezetten hátrányosan érintő események észlelése és a hibamenedzselő rendszer minél hamarabbi értesítése.
2. Hibafeldolgozás, eredménye: HIBAJEGY (ALARM)
   A detektált hibajelekből hibajegy generálása a feladata

3. Hibaok meghatározás és hibajavítás
   A keletkezett hibajegyekben megfogalmazott hibajelenségek okainak felderítése és a hiba javítása.



55. Adja meg a hibajel feldolgozás 3 típusát:

1. Szűrés: A beérkezett hibajelekre a szűrőszabályok definiálhatók, amelyekből meghatározható a hibajegy
2. Korreláció: A beérkezett hibajegyekből korrelációs szabályok segítségével új, összetettebb hibajelek generálhatóak, melyek pontosabb információt adnak a hibajegyek generálásához

56. Sorolja fel a hibaok analízis módszereit:

1. *Alarm vektor*
    a. A lényege az, hogy vannak különböző alarmok (mint pl: link nem elérhető, magas jitter, zizis a kép, stb...), ezek megfeleltethetők egy tömb egyes elemeinek. A tömbbe (nevezzük vektornak), tehát a vektornak azon celláiba írunk 1-est, ahol amelyik ALARM teljesült, a többi helyre pedig 0 kerüljön. Ekkor kapunk egy vektort és a javasolt ALARM (ez volt a diasoron de mivel hbaok analízist végzünk és már ekkor megvannak az alarmok így szerintem itt az alarm megnevezés kimenetnek nem pontos) az lesz, amelyik előre rögzített hibaok vektorokhoz képest a legkisebb lesz a Hamming távolsága. példában mutatva:

	link nem elérhető	útvonal nem elérhető	"interface down"	eszköz nem válaszol	magas vesztés	magas jitter	...	...
Link x hibás	1	1	0	1	0	0	...	...
Link x túlterhelt	0	1	0	0	1	1	...	...
"interface misconfig"	1	1	1	1	0	0	...	...
xy hardware hiba	0	1	0	1	1	0	...	...
xy irány túlterhelt	0	0	0	0	0	1	...	...
...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...

t1 és t2 időpillanatok között:

1	**1**	**1**	**0**	**0**	**0**	...	...

A t1 és t2 között beérkezett ALARMokat jelöltük a megfelelő helyen 1-el, vagyis t1 és t2 között nem volt elérhető a link, nem volt elérhető az útvonal nem válaszolt az eszköz és interface down alarmokat kaptunk. Így jött létre a 111000... vektorunk, a lehetséges hibaok vektorok közül pedig az “interface misconfig”-tól legkisebb a Hamming távolsága, így az lesz a hibaok, aminek az elhárítása azonban a **HÁLÓZATFELÜGYELETRE HÁRUL.**

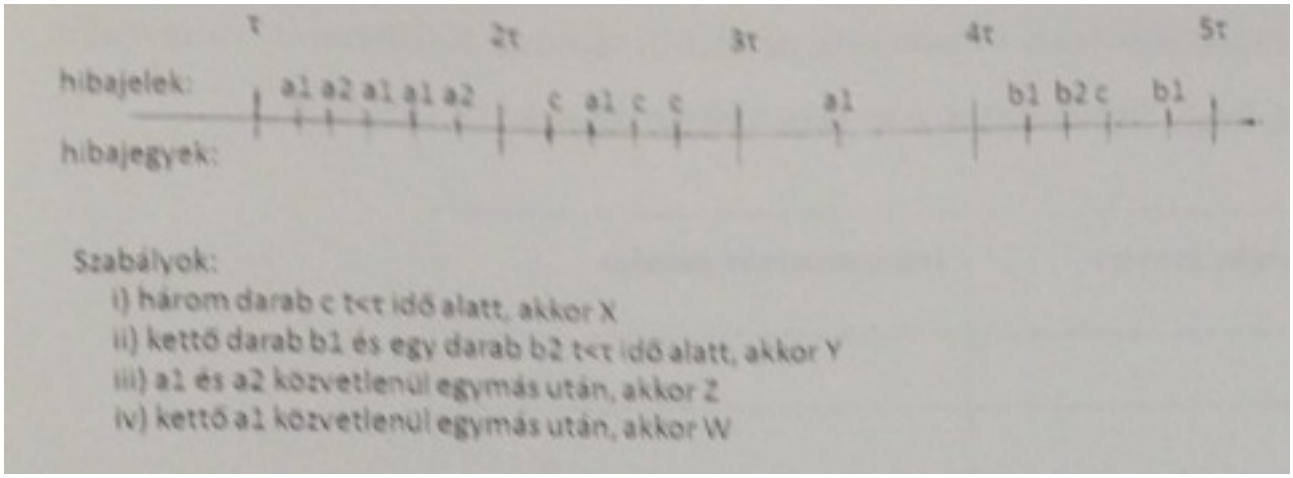
2. *Szabály alapú*

Az alapja egy tudásbázis, ami leírja, hogy milyen összetett alarmal kell helyettesíteni a bejövő elemi hibajeleket.

Alapvetően Bool algebrára jellemző relációként jelennek meg.

A 2013.05.30.-ai vizsgában szerepelt egy ilyen feladat, aminek megoldását érdemes megnézni:

Egy szabály alapú esemény-korrelációval működő hibajel-feldolgozó eljárás az alábbi ábrán feltűntetett szabályok alapján működik



a, *Hogyan bővítené a rendszert ahhoz, hogy eset alapú hibaok-analízis megoldássá alakuljon?*

- Vélt és valódi hibaokokkal és visszacsatolóval. LÁSD: eset alapú hibaok módszer ábránál

b, A visszajelzések azt mutatják, hogy csak a második és a negyedik periódusban mutatkoznak valódi rendszerhibák. Mi a legegyzerűbb, új korrelációs szabály, amit ilyenkor érdemes definiálni?

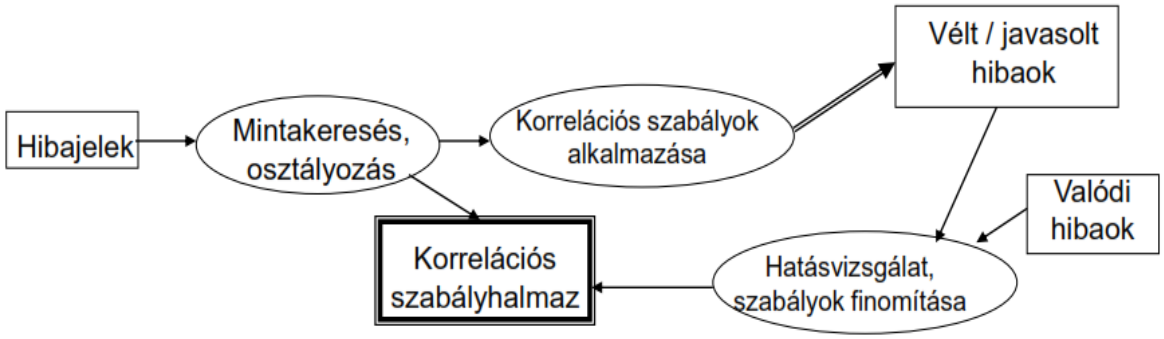
Ott generálunk hibajegyet, ahol c van, mivel c csak a második és negyedik periódusban található meg.

c, Milyen elvek mentén határozná meg a hibajeleket, eszközöket és a szabályokat egy modell alapú hibaokanalízis megoldásához?

- Hierarchikus szabályok bevezetése (, rugalmas modell létrehozása a hálózati topológiából).

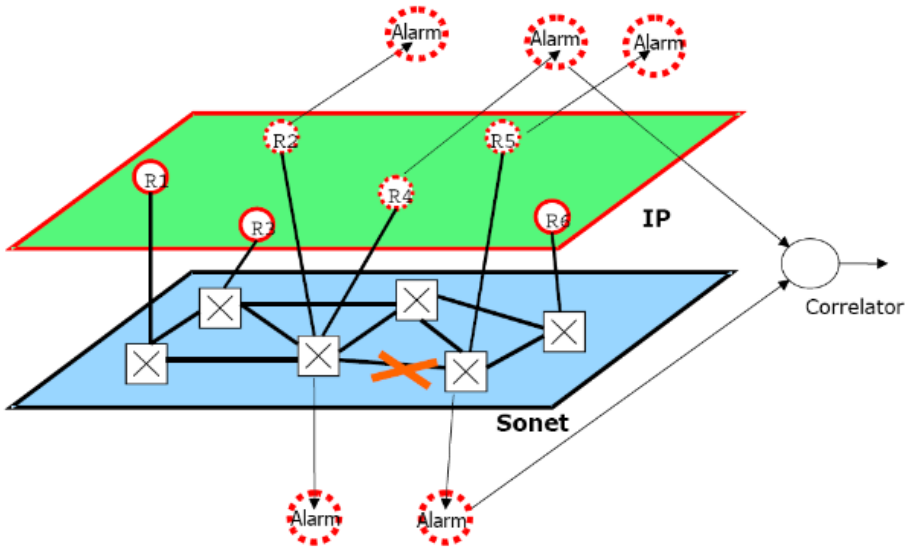
3. *Eset alapú (case-based)*

   Hasonló az előző, szabály alapú módszerhez csak ki kell még egészíteni egy vélt illtetve valós hibaokokkal és visszacsatolóval.



4. *Modell alapú*

A korrelációs szabályok hierarchikusak, a hálózati topológiát egy rugalmas modell írja le. Bonyolult, de nagyon rugalmas megoldás



5. *Fuzzy*

Erre idéznék egy kis kérdez feleleket az előadásról:

Varga Pali megkérdezte tőlünk, hogy: “nah akkor mi lehet a fuzzy módszer vajon?...” A fele csoport próbált valamit nyökögni, hogy ez a... izéé.., a másik fele meg csak himbálta a fejét, nézte a nem létező felhőket az E1B mennyezeti freskóján, mire a Tanár úr csak ennyit mondott: “Nagyon helyes! Így van! A fuzzy pont ilyen.. nem lehet biztosan megállapítani hogy pontosan az e.. olyan fuzzys”. Ezután meg elindított egy mexikói hullámot az előadóban ülő 30 ember segítségével :D

A lényeg, hogy az egyes hibaokokról való passzív hibakorrelációs döntés bizonytalan. A hálózatot és az alarmokat Fuzzy halmazokkal leírva is lehet larm-korrelációs rendszereket készíteni. Bonyolult, de gyors megoldás.

6. *Neurális hálózatok*

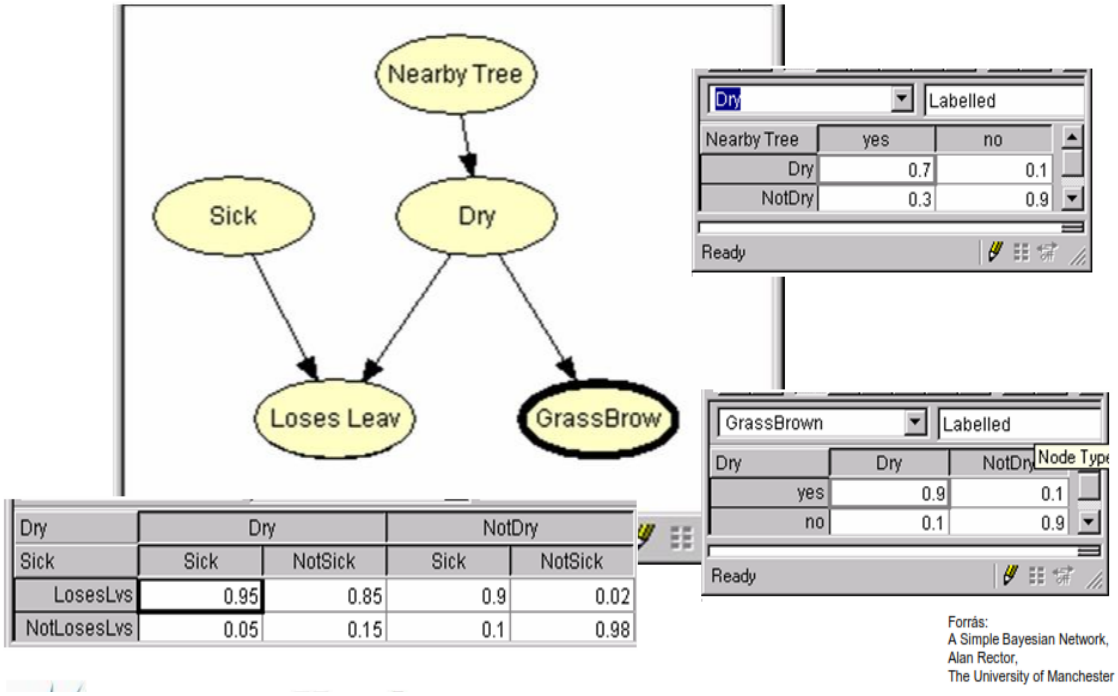
Esemény korrelációra nehezen rűhúzható folyamat, sok állapottal, bonyolult.

7. *Oksági hálózatok*

Vagy Bayes hálózat, ami ugye valószínűségekkel operál, pontosabban a bizonytalanság leírásán van a hangsúly. Az egyes hálózati csomópontokhoz rendelt állapotoktól függően különböző valószínűségekkel jutunk el a legvalószínűbb hibaokhoz.

Megfigyelés alapú. Ismét Varga Pál Tanár urat idézném példa szemléltetésére: “A legjobb példa rá a beérkező e-mailek közül a spamek kiválogatása. Amire gyakran

nyomjuk rá, hogy spam, akkor azt egyre biztosabban pakolja bele a spam boxba. Ilyen például a viagra reklámok....mindig rányomsz, hogy spam és berakja a spamek közé....aztán az idő múlásával már egyre kevesebbszer nyomsz rá, hogy spam" :D



Forrás:
A Simple Bayesian Network,
Alan Rector,
The University of Manchester

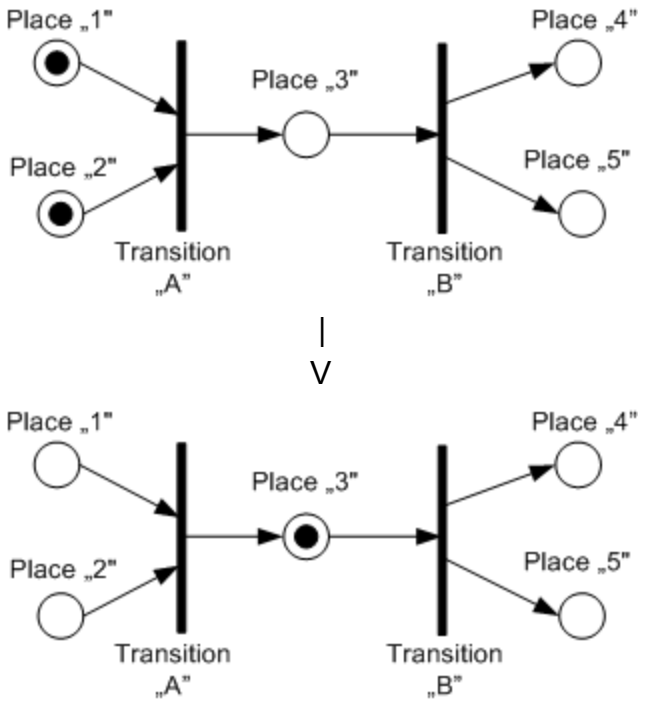
8. *Szavazás*

Központi döntés helyett elosztottan. Minden döntésképes csomópont megbecsüli, hogy a hozzá eljutott információk szerint milyen hibák korrelálhatóak, majd ezt egy dedikált csomópont kiértékeli.

9. *Adatvezérelt modell*

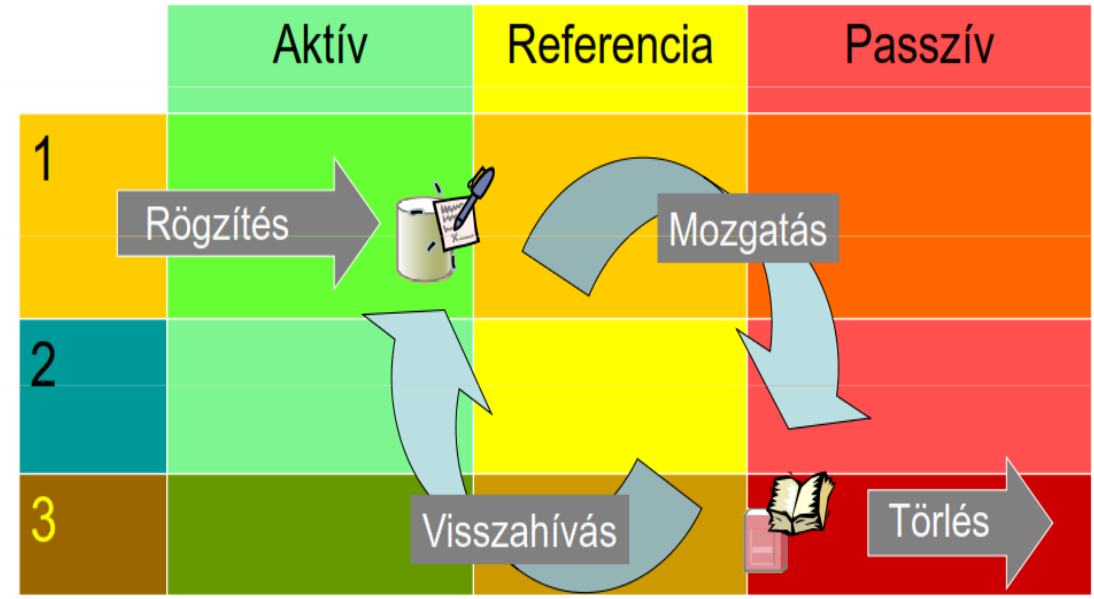
A hibajegy paramétereiből indulunk ki, és lehetséges hibaokok után kutatva aktív ellenőrzéseket kezdeményezünk. Csak abban az esetben hajtódik végre az ellenőrzés, ha a szükséges adatok rendelkezésre állnak.

Az adatvezérelt hibaok feltárási módszer legismertebb leírása a Petri háló. Vannak helyek, átmenetek és zsetonok. Az átmenet akkor tüzel (hajtódik végre egy vizsgálat) ha mind a 2 helyen van zseton(fekete pont), vagyis rendelkezésre állnak az adatok. (én legalábbis így értelmeztem, fix me)


Place „1"
Place „2"
Place „3"
Place „4"
Place „5"
Transition „A"
Transition „B"
|
V
Place „1"
Place „2"
Place „3"
Place „4"
Place „5"
Transition „A"
Transition „B"

57. Sorolja fel a HSM egyes állomásait és hogy hogyan jutunk el oda:

Először is a HSM = Hierarchical Storage Management



HSM paraméterei: adat mérete, típusa és az utolsó olvasás időpontja

58. Soroljon fel 3 adattároló típust és röviden jellemezze őket:

1. Diszk

   Azonnali adat elérést biztosít, probléma a tápellátás, 3-4éves élettartam
2. Optikai

   Másodlagos tároló, SOHO(Small Office Home office)
3. Szalag

   10-20x olcsóbb, mint a diszk, 30 éves adatmegőrzésis idő, azonban lassú, sorosan olvasható/ írható

59. RAID típusok (DIA+EGYÉB nem csak wikipediás, forrás)

Először is a **RAID NEM VÉD A LOGIKAI HIBÁK ELLEN!!! CSAK A FIZIKAI ELLEN!**

RAID0-Striping:

Nem a biztonság növelése a cél, hanem a kapacitás növelése. Párhuzamosan tudunk adatot írni/olvasni, sebesség növekedést eredményez.

RAID1-Mirroring:

Minden lemezt lemásol, így ha meghibásodik valamelyik a másik helyettesíti. Diszk duplikálással van megoldva, nagy a méret igénye (kétszeres), viszont nagy megbízhatóságot biztosít.

RAID2:

Egyes meghajtók hibajavításra vannak fenntartva, amely ECC-t (Error Correcting Code) tartalmaz és a hiba detektálására, javítására való. Ma már nem használják.

RAID3:

1 paritásdiszk van fenntartva, amely a többi diszkből XOR művelet segítségével előállítható. Ha kiesik 1 diszk, akkor nincs baj, így n+1 redundáns! Hiba detektálásra nem jó!

Csak Single User módban használható, a párhuzamos kiszolgálást nem támogatja. NAGY fájlok tárolására használják általában, kicsi a szektorok mérete!

Leggyakoribb előfordulása 2+1, 5+1, 8+1, 14+1

RAID4:

Hasonló a RAID3-hoz, azonban támogatja a multi-user módot.

A szektorok mérete nagyobb mint a RAID3 esetében, de a paritásdiszk még mindig korlátoz!! (sok a frissítés a sok párhuzamos írás/olvasás végett)

n+1 redundáns ez is

RAID5:

A RAID3 és RAID4 kombinációja. Ugyanúgy vannak paritás szektorok! szektorok, ugyanis a peritás diszk elosztva helyezkedik el a többi diszken.

n+1 redundáns, a szektorok mérete dinamikusan változtatható, ha kicsi a méretük, akkor RAID3hoz hasonló viselkedés, ha nagyok, akkor RAID4-hez hasonló.

kapacitás kiszámítása = (legkisebb kapacitású diszk) * (összes diszk - 1)

olvasási sebesség kiszámítása = (legkisebb diszk olvasási sebesség) * (összes diszk -1)

MINIMUM 3 diszk szükséges

RAID6:

A RAID5 kibővítése, kettő paritás diszk van, ezzel n+2 redundanciát biztosít

Az egyik paritás diszk sor szerint (XOR) a másik oszlop szerint (Reed Solomon kód) nyújt redundanciát

nagy hátárnya, hogy lassú!

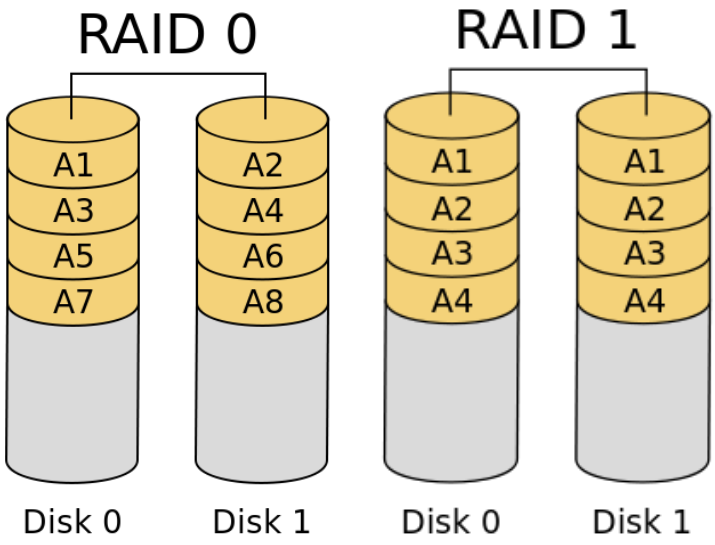
RAID01:

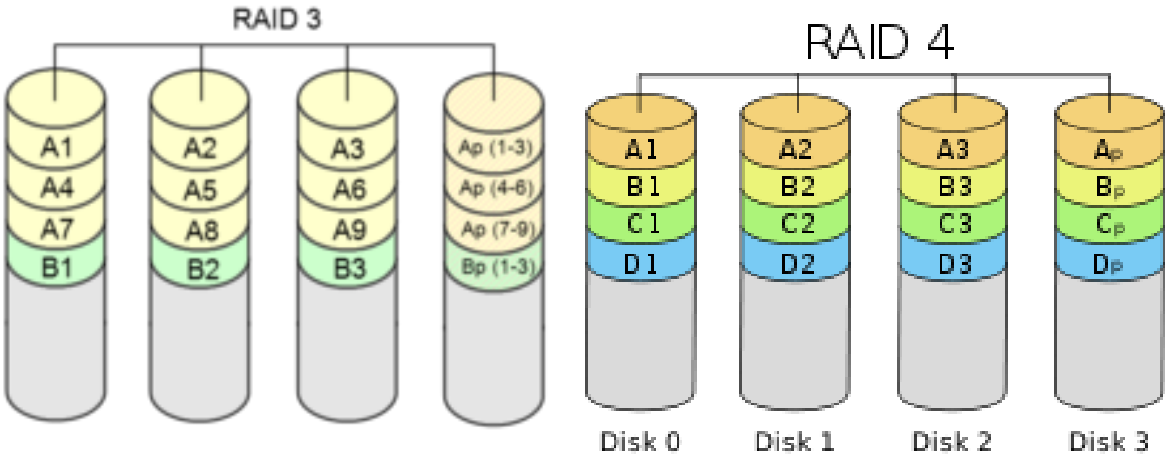
Minimum 4 diszk szükséges a használatához.

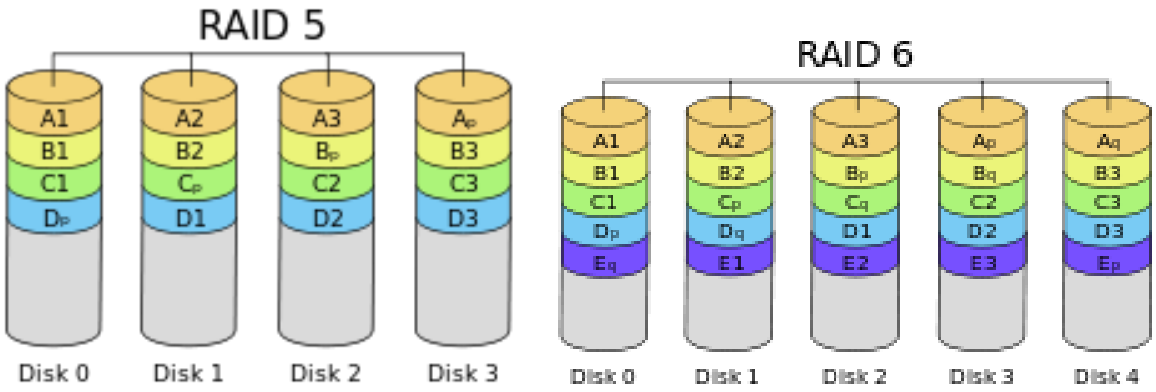
Vegyíti a RAID0 és RAID1 technikát, 2-2 diszk RAID0-val, és a két blokk RAID1-el van összefűzve. Ha meghibásodik az egyik diszk, akkor az egész blokk elszáll!

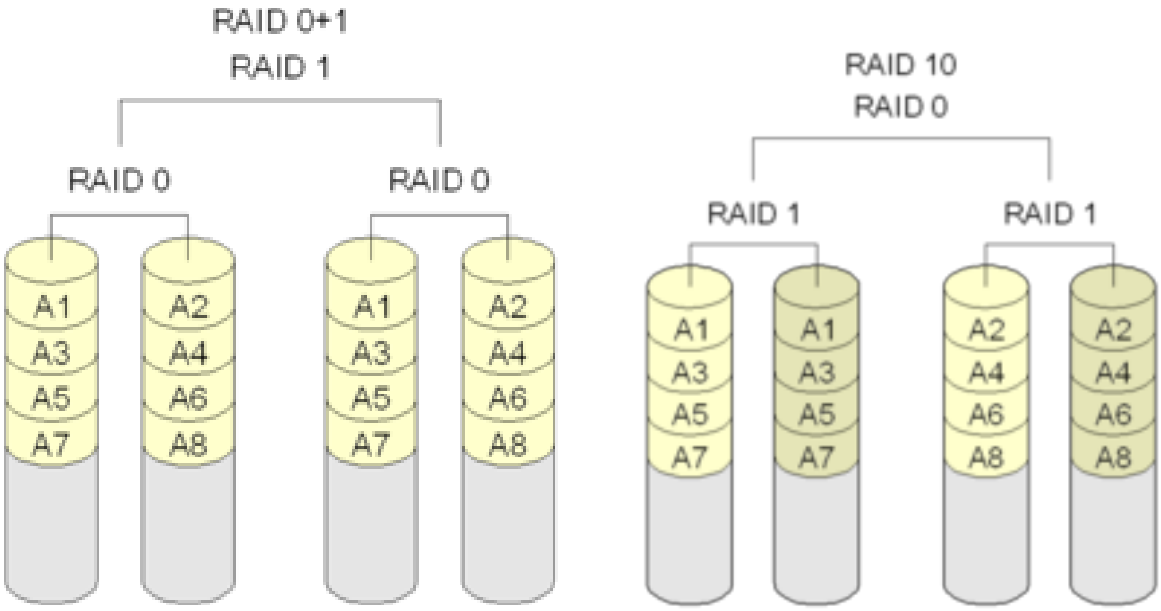
RAID10:

Itt is minimum 4 diszk szükséges, a RAID01-hez hasonló, csak itt az alsó szinten a RAID1 van, így egy diszk meghibásodása esetén nem esik ki az egész diszkblokk.









60. Jellemezze a DAS tároló rendszert:

DAS = Directly Attached Storage.

A tároló közvetlenül csatlakozik a szerverhez, kis rendszereknél használják

Blokkszintű hozzáférést biztosít!

61. Milyen típusai vannak a DAS-nak?

1. Internal DAS

   A **tároló közvetlenül csatlakozik a szerverhez**, belső soros, vagy párhuzamos buszon keresztül.

   Limitált darabszámú eszköz csatlakozhat csak

   a)PATA csatlakozó = Paralell Advanced Technology Attachment

   b)SATA csatlakozó = Serial Advanced Technology Attachment

2. External DAS

   A szerver közvetletül kapcsolódik **egy külső tárhoz**!

   Nagyobb távolságban van csatlakoztatva, általában nem (annyira) korlátozott a csatlakoztatható eszközök száma.

   SCSI csatlakoztatás = Small Computer System Interface, az összes tároló egy buszon osztozik,

   LUN = Logical Unit Number, azonban nem számot azonosít, hanem az egy SCSI csoporton belüli egységeket azonosítja

   SAS = Serial Attached SCSI, gyorsabb mint a sima SCSI full duplex átvitelre is képes

62. Sorolja fel pár előnyét és hátrányát a DAS-nak:

- Előnyök:
  - Jobb, mintha a kliens tárolná az adatokat
  - egyszerű, kis költségű
  - korlátozott redundanciát tud nyújtani
- Hátrányok:
  - korlátozott darabszámú eszköz csatlakoztatható
  - nehézkes a menedzselése
  - költséges a Backup
  - nem (jól) skálázható

63. Mi a SAN, hogy épül fel és ahol lehet, milyen típusú elérés megvalósítható?

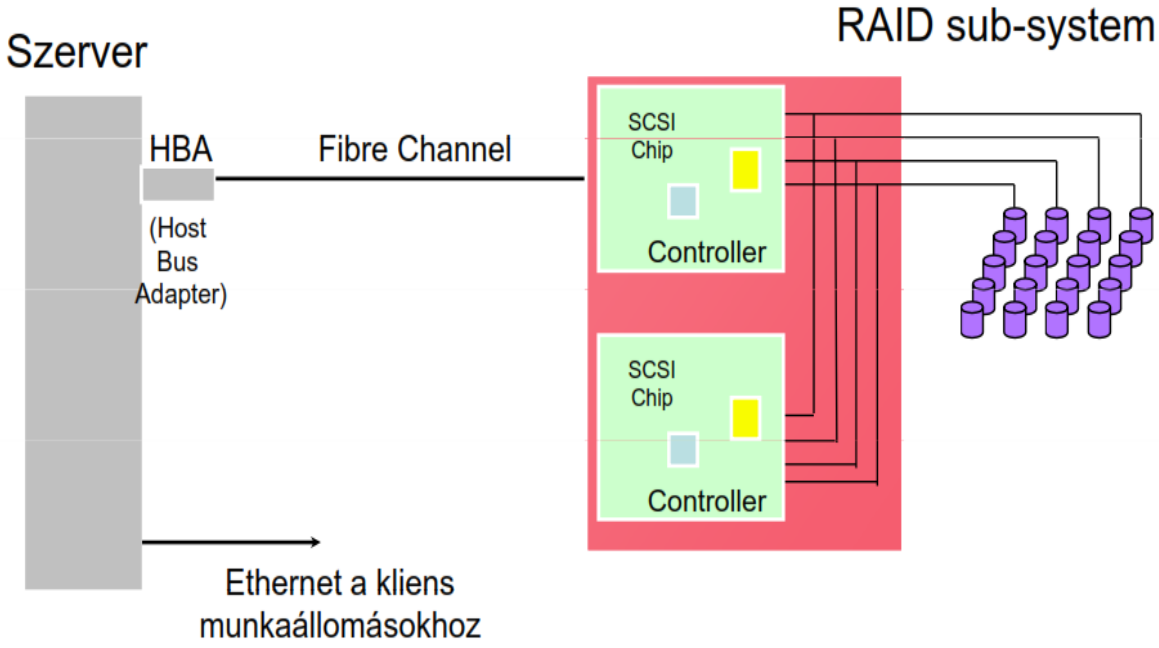
A SAN(Storage Area Network) egy központosított, nagy teljesítményű adattárolásra dedikált hálózat.

Részei: kliensek, LAN → fájlszintű elérés, szerverek, SAN → blokkszintű elérés, Storage Pool

Átviteli technológia FC (Fiber Channel), nagy szűmú eszköz nagy távolságban csatlakoztatható

64. A SAN alapkonfigurációjában hány vezérlős a RAID, hány busz van és az egyes buszhoz ház lemez csatlakoztatható?

2 vezrélős RAID, ezek közül csak az egyik dolgozza fel az I/O kéréseket, 4 SCSI busza van, mindegyiken 5 lemezzel



65. Jellemezze a NAS tároló rendszert, milyen NAS protokollok vannak?

Network-Attached Storage, hálózatra csatlakoztatott adattároló eszköz, ami támogatja az adatmegosztást kliens - szerver között.

NAS protokollok:

- NFS
  - UNIX alatt
- CIFS
  - OS független, TCP felett
- FTP

66. Milyen diszkrendszerbeli másolás fajták vannak?

1. Volume Copy

   Valódi kötet jön létre, firmware eszközökkel megvalósított másolási technológia, alkalmas backup célra!
2. Flash Copy

   Nem jön létre valódi másolat, hanem ha egy blokkot módosítunk, akkor azt nem írjuk felül, hanem máshová tesszük és ezt jelöljük a Flash Copy táblában, ami által visszaállítható lesz a rendszer bármely pillanatában (amelyiket természetesen rögzítettük (snapshotoltuk) a Flash Copyban)

Flash Copy Vizsga feladat megoldás levlistről:

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
Írás t3	B1	B1	**B1>B10**	B1	B1	**B10**
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10	11	8	8	8
Delta (flashcopy inkrementum)	0	2	3	Látszólagos Volume A	B	C

A lényeg:

T2 időpillanatban a B0 és B2 blokkokat akarod írni, T3 időpillanatban pedig B1-et. Annak érdekében, hogy a fájl tetszőleges időpillanatbeli állapota visszaállítható legyen, nem írsz felül semmit, hanem a B0, B2, B1 blokkok helyett a B8, B9, B10 (eddig üres) blokkokba írod a tartalmakat. A flashcopy táblába pedig feljegyzed az F2 oszlopba, hogy a B0 blokk tartalma az T2 időpillanatban valójában a B8 blokkban van. (Hasonlóan a B9-et és B10-et is feljegyzed a táblába). Ezek után, ha valakit a fájl T1,T2,T3 időpillanatbeli állapota érdekli, azt össze tudja halászni a flashcopy tábla F1,F2,F3 oszlopai segítségével.

67. Sorolja fel a NAS előnyeit:

- skálázható, bővíthető, de a LAN miatt a sávszélesség korlátozott
- könnyen telepíthető, üzemeltethető eszköz

68. Sorolja fel a SAN előnyeit:

- Skálázható, bővíthető, nagy adatátviteli sebesség

69. Mit jelent a tárterület virtualizáció?

A virtualizáció olyan technológia, amely lehetővé teszi hogy bizonyos erőforrások másteszi, hogy bizonyos erőforrások más erőforrásoknak tűnjenek, lehetőleg kedvezőbb tulajdonságokkal.

70. Vitrualizációs motor működése:

Szerver: LUN=1, LBA=32 LBA Logical Block Address

VM: táblázatból, ez megfelel a fizikai LUN=4, LBA=0 címnek

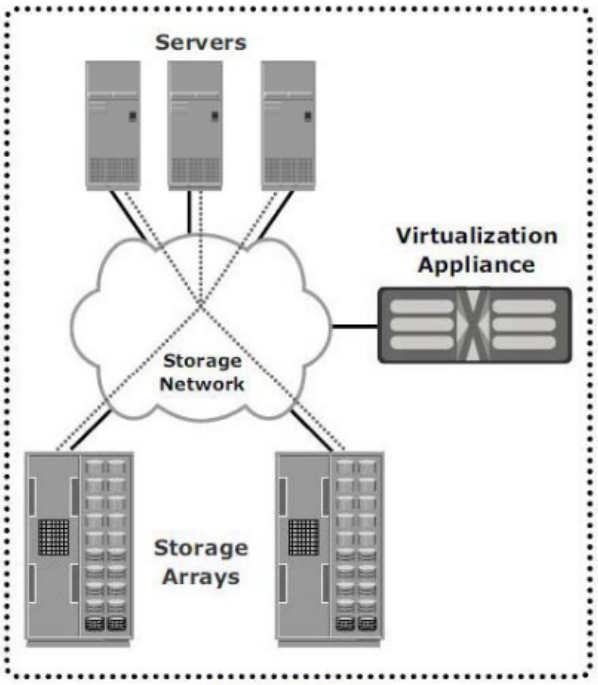
Elkéri az adatot a fizikai diszktől

A megkapott adatot úgy továbbítja a szervernek, mintha az a LUN=1mintha az a LUN=1, LBA=32 címről érkezett volna.

71. Milyen virtualizációs konfigurációk vannak?

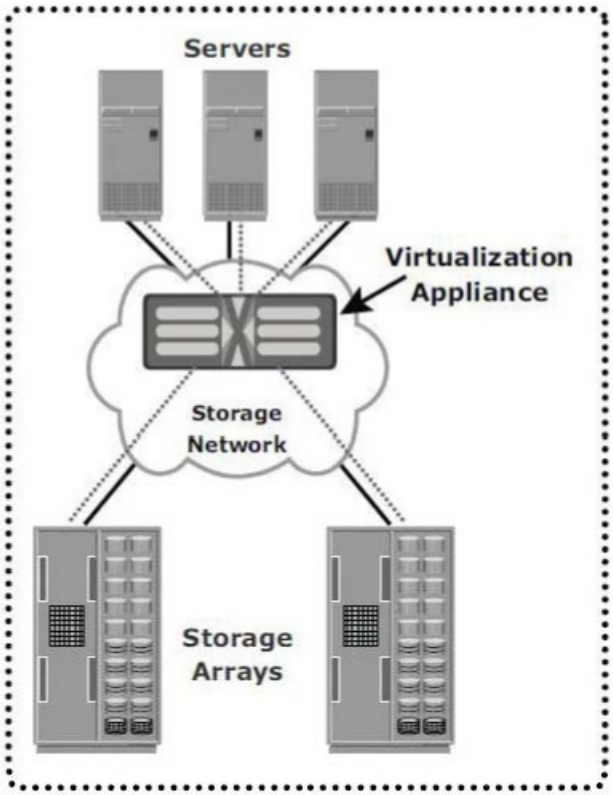
1. out-of-band

A vezérlés és az adatút elválik, a szerveren külön kell SW, mert először ez elkéri a VM-től az adat fizikai helyét/címét , majd közvetlenül eléri az adatot.



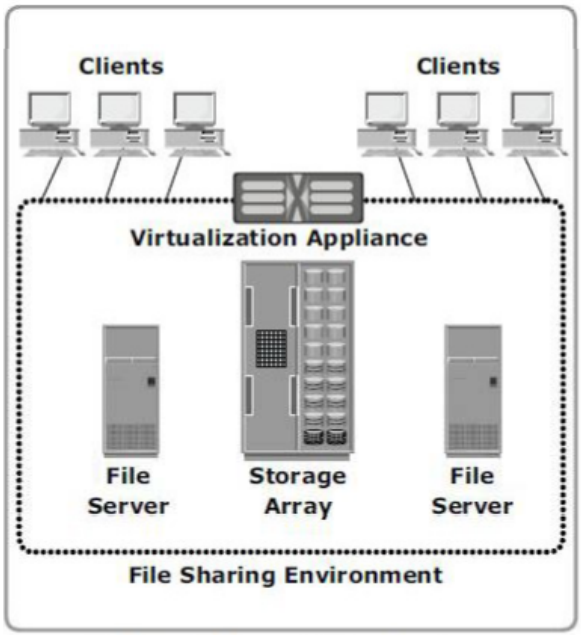
2. in-band

A virtualizációs motor az algútban van, lassabb, mivel egy VM-en megy át az adat



72. Mi a legnagyobb előnye a fájl szintű virtualizációnak a blokkszintűvel szemben?

A fájl szintű virtualizációnál nem kell tudunk, hogy hol található fizikailag a fájl, eygszerűbb fájlmozgatást, terhelés megosztást tesz lehetővé.



73. Mik az erőforrás menedzsment főbb lépései (4 db)?

1. Azonosítás

   Eszközleltár, allokált de nem lefoglalt területek, illetve lefoglalt területek kigyűjtése
2. Értékelés

   Fájl, könyvtár szintű analízis, a feleslegesen foglalt tárterületek azonosítása, duplikált, régóta nem használt adatterületek azonosítása
3. Vezérlés

   Központi riasztási rendszer, kvótakezelés, automatikus válaszakciók indítása
4. Előrejelzés:

   Trendek azonosítása és előrejelzés, kockázat elemzés

74. Mi a mentés/archiválás célja?

A mentés / archiválás célja: a helyreállíthatóság biztosítása adatvesztések elkerülésebiztosítása, adatvesztések elkerülése (minimalizálása) másolati adatpéldányok készítésévelkészítésév.

75. Mi az archiválás célja?

Referencia időpontnak megfelelő adattartalom megőrzéseadattartalom megőrzése.

76. Mi a helyreállíthatóság szükségességének 3 fő oka?

Archiválás, Véletlen adat törlés, Diszk meghibásodás

77. Sorolja fel a 4 mentési módszert:

1. Teljes mentés

   Minden nap a teljes diszktartalmat mentjük, nem jó a szalag kihasználtásg szempontjából, lassú viszont egy szalagról helyre állítható

2. Inkrementális mentés

   A ciklus első napján teljes mentés, utána minden nap az előző mentés óta történt változásokat menjtük le.

3. Differenciális mentés

   A ciklus első napján teljes mentés, utána minden nap a teljes mentés óta történt változtatásokat menjtük le

   Nagyobb egyre növekvő napi adatmennyiség, de rövidebb a visszaállítási idő és több szalag

4. Progresszív mentés

A ciklus első napján teljes mentés, utána minden nap az előző nap óta történt változást mentjük, viszont az adott napi fájlstruktúrát is elmentjük!!!

Inkrementális / Differenciális mentés problémája

Day 1	Day 2	Day 3	Day 4	Day 5
File A	File A renamed to File F	File F	File F	File F deleted
File B	File B deleted			
File C	File C renamed to File G	File G	File G	File G
File D	File D moved to new location	File D (new location)	File D deleted	
File E	File E	File E	File E	File E

Files from Day 1 FULL backup		Files from Day 3 INCREMENTAL / DIFFERENTIAL backup		Hard Drive after a restore to Day 3
File A		File F		File A **– wrong** File F
File B	+		=	File B **– wrong**
File C		File G		File C **– wrong** File G
File D		File D (new location)		File D **– wrong** File D (new location)
File E				File E

Progresszív mentés előnye

Day 1	Day 2	Day 3	Day 4	Day 5
File A	File A renamed to File F	File F	File F	File F deleted
File B	File B deleted			
File C	File C renamed to File G	File G	File G	File G
File D	File D moved to new location	File D (new location)	File D deleted	
File E	File E	File E	File E	File E

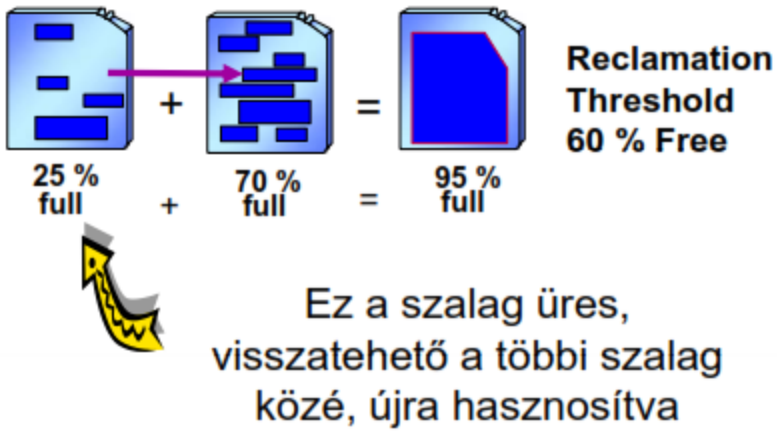
Required files from Day 1 FULL backup		Required files from Day 2 & Day 3 INCREMENTAL backups		Hard Drive after a restore to Day 3
	+	File F	=	File F
		File G		File G
		File D (new location)		File D (new location)
File E				File E

78. Mit nevezünk kollakációnak?

Az egy klienshez vagy klienscsoporthoz tartozó adatokat egy szalagra vagy tartozó adatokat egy szalagra vagy szalagcsoportra másolja. Csökkenti az adott visszaállítás során a szalagbefűzéseket és rövidebb visszaállítási idő biztosítható visszaállítási idő biztosítható.

79 Mit nevezünk szalagvisszanyerésnek?

A felhasználó által definiálható küszöbérték elérésekor az adatokat egy új szalagra másoljuk át. Ez a másolás időzíthető, kontrollálható.



80. Mi a LAN-free, mire jó ez?

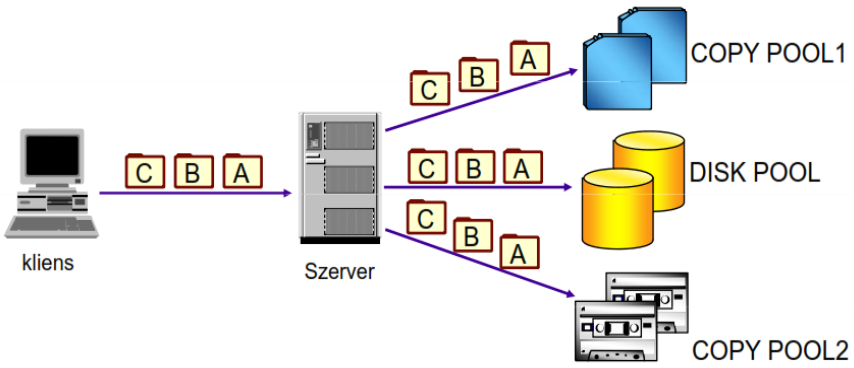
A kliens végzi a tényleges mentést, ő mozgatja az adatokat diszkről azalagra vagy SAN-on lévő diszkre, a szerver csak menedzseli a belső tárterületet, illetve ezt a folyamatot.

Előnye, hogy a LAN hálózaton alapvetően csak a metaadatok mozognak , így nem terheli azt, valamint megnöveli a tároló eszközök kihasználtságát.

81. Mi a párhuzamos mentés lényege, mikor hasznos?

A párhuzamos mentés lényege az, hogy a cél storage pool-on kívül akár több másik copy storage pool definiálható és ezekre szimultán(együttesen) történik az írás.

A cél storage poolok különbözőek lehetnek (diszk, merevlemez).



82. Mit jelent a Zero down-time mentés és mi az előnye?

A tükrözött kötet, vagy snapshot tartalmazza az adott pillanatbeli másolatot, a mentés pedig az így készült másolatról készül.

Előnye, hogy nincs szükség az alkalmazás jelentősebb leállítására.

83. Mi az a Disaster Recovery Manager, mi a feladata?

Feladata a rendszer által támogatott katasztrófa tervezés és visszaállítás. Pontos útmutatók készítése vészhelyzet esetére, visszaállítási scriptek.

84. Soroljon fel 3 speciális archiválási követelményt.

1. Előre definiált megőrzési idő
   Szerződés kötés kötés pl 4 évre szólóan, addig megőrzés
2. Esemény alapú megőrzés
   Például életbiztosításnál, a biztosított halála után 70 évig
3. Törlés tiltás, engedélyezés
   Bizonyos esetekben pl bírósági eljárásban a végéig törlés tiltás

85. Sorolja fel a mentés tervezési menetének 4 lépését.

1. Vállalati stratégia

   Ez az egész szervezetre vonatkozik, nagyvonalakban határozza meg a mentési tevet. Jogi minimumokat, mentési célokat határoz meg, a mentés megvalósításának részleteivel nem foglalkozik.

2. Szolgáltatási szint meghatározása (SLA)

   Az adott telep helyen mik az elvárt és a biztosítandó szolgáltatási szintek.

   Tipikusan használók egyeztetésével történik, pl megntések típusa, adatok megőrzésének ideje, elvárt helyreállítási idők az egyes típusokra

   Konkrét példa: A használók az utolsó 6 hónap – 3 év bármelyik fájljának 1 hónapos pontossággal való visszaállítását kérhetik.

3. Mentési politika

   A mentési politika az a politika, amely az SLA-ban leírt követelményeket teljesít

4. Mentési ütemterv

   Ez konkrétan leírja, hogy melyik host melyik partícióját kell menteni, gyakran csak a mentő szoftver konfigurációjában van leírva.

   Az SLA és a mentési politika ritkán változik

86. Mit nevezünk 80/20-as szabálynak?

A hozzáférések 80%-a az adatok 20%-nak ismételt elérésére irányul.

/*/**

SZÁMOLÓS PÉLDA (ezeket kimásoltam a diákból, mert érthetőek úgy, ahogy vannak)

Egy szerverkörnyezetben 2TB adatmennyiséget kell menteni.
• Inkrementális mentést használunk.
• A változás mértéke kb. 10%/nap.

– a. Határozza meg, hogy hetes mentési ciklus, és napi mentések esetén mekkora adatmennyiséget kell menteni az első 4 hétben.

1. nap teljes mentés → 2TB
Inkermentum → 2TB*0,1=0,2TB naponta

1 hét → 2TB + 6*0,2TB = 3,2 TB
4 hét → 3,2 * 4 =12,8 TB

b. Mekkora lesz a szükséges mentési időablak az egyes napokon, ha egy mentőeszköz effektív írási teljesítménye 100 GB/h?

vasárnap (full backup) → 2TB / 100GB = 20 óra
többi napon → 2 óra

c. Hány mentőeszköz szükséges, hogy a mentési ablak 8 óránál ne legyen több?

Legrosszabb vasárnap 20 óra, így 3 mentőeszköz kell

d. Hány média szükséges a mentéshez, ha feltételezzük hogy minden mentés új médiára kerül, és egy média maximális kapacitása 500 GB?

Vasárnap: 2 TB / 500GB = 4 média
Hétköznap: 0,2 TB (= 200GB) = 1 média
Összesen: 4+ 6*1 = 10 média / hét
40 média / 4 hét

e. Egy adott időpont visszaállításához maximum hány média visszatöltésére van szükség?

Legrosszabb: szombat
Visszaállítás: 1 full + 6 inkrementum
4+6*1 = 10 média kell
/*******/***

87. Miért előnyös a centralizáció?

1. Csökkenteni tudjuk a berednezések költségét
2. Csökkenteni tudjuk a szalagcserék költségét

88. Soroljon fel 6 okot, amiért sikertelen lehet a mentés

1- Nem megfelelő mentő rendszer tervezési probléma
2- Nem megfelelő menedzsment , emberi tévedések
3- Nem elegendő kapacitás mentési idő
4- Hardver hibák
5- Média hibák

6- Hálózati hibák

89. Soroljon fel 6 okot a visszaállítás sikertelenségére

1. Tervezés, tesztelés gyakorlati hiánya
2. Olvasatlan vagy üres szalagok
3. Korrupt adatok
4. Nem teljes szalagállomány
5. Szoftver vagy eszköz hibák
6. Kapacitás problémák

IRU_2013_felho, kulcsszavak: virtualizáció, felhő IT, SaaS, PaaS, IaaS, UCI, OCCI

90. Mit nevezünk virtualizációnak?

Virtualizáció: az a képesség, hogy egy fizikai rendszeren több(féle) operációs rendszer futtatható (és megosztják a rendelkezésre álló erőforrásokat).

91. Mi a felhő IT?

Szolgáltatások kívánságok szerint az erőforrások le/felskálázásával

92. Vázolja fel szavakkal a virtuális szerver koncepciót:

Logikailag elválasztja a szerver szoftvert a hardvertől. Egy virtuális szervert egy vagy több host is megvalósíthat és fordítva: egy host több virtuális szervert is magába foglalhat. A virtuális kiszolgálókat (is) funkció szerint szokás hivatkozni (levelező, adatbázis, fájl szerver , stb.).

93. Mik a virtuális szerver koncepció előnyei és mik a hátrányai?

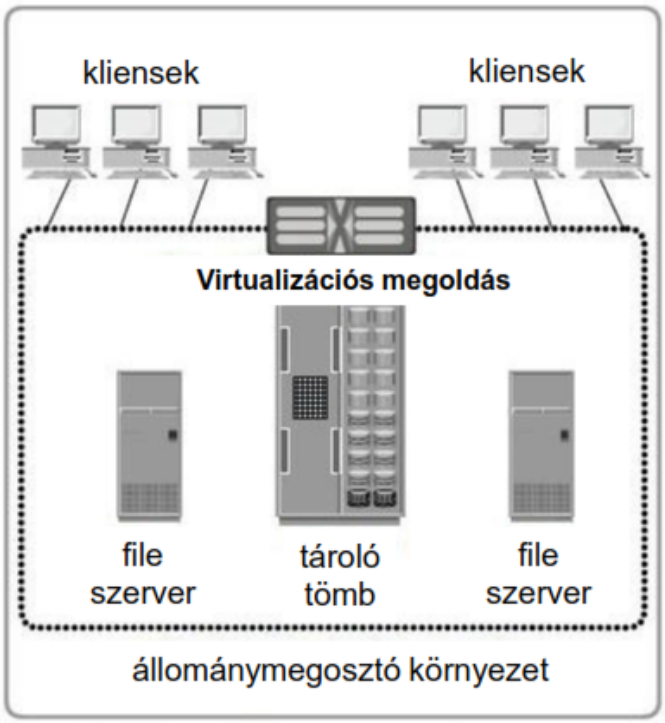
- Előnyök:
  - redundancia
  - közös erőforrás gazdálkodás
  - fizikai erőforrások
  - új szerver gyors telepítése
  - magas rendelkezésre álás
  - leállás nélkül konfigurálható!!!
- Hátrányok:
  - bonyolultabb tervezés
  - drágább konfiguráció, mint a hagyományos

94. Mik a Cloud IT főbb tulajdonságai:

Felhasználás alapján fizetett IT erőforrás(pay per use) igénybe vételi modell. Hálózati hozzáférés egy megosztott IT erőforrás készlethez (pl., szerverek, tárolók, alkalmazások, szolgáltatások), amit (a szükséges verzióban) gyorsan lehet biztosítani, kevés szolgáltatói interakcióval.

94. Mi a fájlszintű virtualizáció előnye a virtualizásió nélkülivel szemben?

Nem kell tudnia a kliensnek/klienseknek, hogy hol van a keresett fájl fizikailag a szerveren.



95. Mi a Saas, Paas, Iaas?

1. SaaS (Software as a Service): Szoftver szolgáltatási modell, amiben a felhasználó alkalmazás licencet kap, igény-szerinti(on demand) szolgáltatásként.

2. PaaS (Platform as a service): IT platform & megoldási csomag szolgáltatásként.

3. IaaS (Infrastructure as a Service):IT infrastruktúra, mint szolgáltatás (tipikusan platform virtualizációs környezet).

96. Mi az a pay-per-use modell?

Létező, kényelmes és igény-szerinti hálózati hozzáférés engedélyezésére konfigurálható IT erőforrások (hálózatok, szerverek, tárolók, alkalmazások és szolgáltatások) megosztott készletéhez, amelyek könnyen létesíthetők és változtathatók minimális menedzsment erőfeszítéssel vagy szolgáltatói interakcióval.

97. A felhő IT 3 fajtája?

1. Privát felhő

Dedikált IT infrastruktúra egy bizonyos szervezet számára, nem osztozik mással. Drágább, biztonságosabb, mint a nyilvános felhő IT. Az adott szervezet telephelyén, vagy egy felhőből dedikálva.

2. Publikus felhő

Az IT infrastruktúrát egy szolgáltató a saját telephelyein működteti. Az ügyfél nem tudja, nem befolyásolja, hogy hol. Az infrastruktúrán tetszőleges ügyfelek osztoznak.

3. Hibrid felhő

Az előző két modell legoptimálisabb kombinációjaként, a hibrid felhő a privát felhő nyilvános elemekkel történő kiegészítése, kiterjesztése. Pl. egy vállalat alapvetően arra használja a privát felhőt, hogy megossza a fizikai és virtuális erőforrásait a hálózatán keresztül, de a public cloud igénybevételével akár ki is terjeszthet i ezeket az erőforrásokat, amikor éppen arra szüksége van. Továbbá a vállalat eldönthet i, hogy a sokszor több ezer alkalmazás közül, melyeket szeretnék a privát és melyeket a nyilvános felhőn keresztül igénybe venni. Pl. a pénzügyi szoftvereinket a saját tűzfalunkon belül tarthatjuk, míg a kollaborációs szoftvereket a nyilvános felhőből lehet igénybe venni.

98. Soroljon fel 2 Cloud IT szabványosítási törekvést.

UCI, OCCI

99. Mi az OCCI?

Open Cloud Computing Interface, lényegében egy API a különböző felhő IT menedzsment feladatokhoz.

IRU_informaciobiztonsag, kulcsszavak: biztonság, szabályozás, incidens, CSIRT

100. Mit értünk Információvédelem alatt?

Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása. Az információvédelem nem más, mint az információval kapcsolatos biztonsági kockázatok folyamatos menedzselése.

101. Mi a bizalmasság?

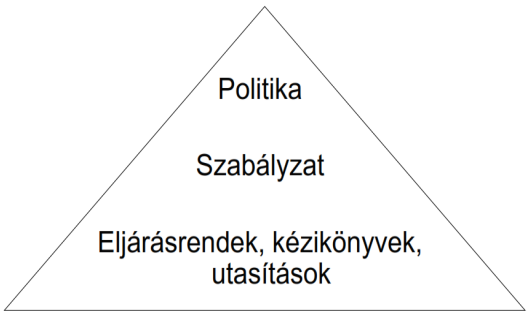
Annak biztosítása, hogy az információ csak az arra felhatalmazottak számára elérhető.

102. Mi a sértetlenség?

Az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése.

103. Mi a 'szabályozás piramis' 3 eleme?

1. Politika
    - Hosszú távra szól
    - általános irányelvek, felelősségi körök
    - Legfelső szintű vezetői jóváhagyást igányel



2. Szabályzat
    - Középtávra
    - Legfelső szintű jóváhagyást igányel
3. Eljárások, kézikönyvek, utasítások
    - Rövid távra készülnek
    - technológiai irányultságú intézkedések
    - Informatikai jóváhagyást igényel

104. Milyen információ biztonsági szerepek vannak?

1. Információgazda
    - adat-, hálózat-, rendszergazda
    - általában üzletági vezetők
    - Teljes felelősséggel tartoznak az adatért, hálózatért, rendszerért

2. Információkezelő
    - Neki delegálja az információgazda a napi teendőket

3. Információhasználó
    - bárki, aki az adatokat használja
    - cégen belül, vagy külső ügyfél

105. Sorolja fel az üzemeltetés biztonsági feladatokat.

1. Védelem rosszindulatú kódok ellen
    - spam, mobil kódok elleni védelem
    - vírusvédelmi szoftver:
        - vírus megelőzés
        - vírusmentesítés
    - központilag vezérelt
    - felhasználók ne tudják semlegesíteni

2. Adatmentés és -megőrzés
    - Adatoknak a kritikussági szintnek megfelelő mentése
    - Adatgazda feladata
    - megőrzési idő után az adatok szakszerű megsemmisítése
    - fajtái:
        - teljes mentés
        - inkrementális mentés
        - differenciális mentés

3. Naplózás
    - Olyan attribútumokat naplózunk, amely biztonsági események észlelésénél keletkeznek, pl esemény, dátum stb...
    - NEM jelszót és hasonlókat!!!!!
    - Monitorozás, riasztáshoz szükségesek

4. Biztonsági frissítések
    - védelmi rések betömése
    - lehet manuális vagy automatizált
    - kritikus a gyorsaság → zero day attack (levilistáról)
    - Erre muszáj reagálnom. Bemásolom:

19. Mit nevezünk "zero day attack"-nak?

"A nulladik napi támadás (zero-day vagy zero-hour támadás) egy biztonsági fenyegetés, ami valamely

számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás." - Wikipedia
Na ezt nekem nem fogadták el, ugyanis elvileg a fejlesztő már tud róla, csak még nem került publikálásra (ezért 0-day, 0 napja lett volna a fejlesztőnek a javítást közzétenni a támadás előtt), tehát majdnem jó a wikis megfogalmazás, csak pontot éppen nem ér.

5. Adathordozók kezelése
    - biztonságos szállítás, tárolás (HVAC, UPS)
    - ne szivárogjon adat, pl.:USBről stb..
    - biztonságos megsemmisítés

6. Logikai hozzáférések kezelése
    a. Authorizáció → mihez van jogosultsága az adott usernek
    b. Authentikáció → user azonosítása
    - alapelvek:
        - Need-to-know → csak annyit tudjon a user, amennyi szükséges a feladata elvégzéséhez
        - csak ahhoz férjen hozzá a user, amihez jogosultsága van → minimális jogosultság
        - feladatok elhatárolása

7. Kriptográfiai megoldások
    - Bizalmassági szempontok
    - Integritásvédelmi szempontok

106. email bizonság hogyan oldható meg?

Spam szűrés, smtp, pop protokoll, nem volt szempont régen az email biztonság.

107. Hálózatbiztonsági megoldások?

Tűzfalak, behatolás észlelő és megakadályozó rendszerek (IDS/IPS).

Honeypot → védtelen eszköznek mutatja magát, megtámadják a vírusok és rosszindulatú SW-ek, mi pedig megismerhetjük a viselkedését, patternjét, így védekezhetünk a valódi eszközökben.

108. Szerverek biztonsági megoldások?

- dedikált szerverek
- távoli adminisztráció csak titkosított kapcsolaton keresztül
- naplógyűjtés, riasztás
- Patch menedzselés
- fizikai elhelyezés

109. Definiálja az incidens fogalmát.

Minden olyan esemény, ami negatívan befolyásolja az információs rendszerek biztonságát.

110. Mit jelent a CSIRT?

Információbiztonsági Incidens Elhárító Csapat , feladatuk az incidens feltárása, hibaanalízis, a nem sérült kritkus rendszerek működésének megóvása, adatok gyors visszatöltése+NEGATÍV visszhang elkerülése → a rossz kommunikáció nagyobb bajokat képes okozni, mint maga az incidens!

Csapat összetétele:

- CSIRT vezető
- ügyfélszolgálati munkatárs
- jogi osztály munkatárs
- Felső vezető
- Rendszer és hálózati adminisztrátor
- PR munkatárs
- HR munkatárs
- Épületbiztonsági munkatárs

111. Definiálja az eszkaláció fogalmát.

Ha az incidens nem oldható meg egy előre rögzített időtartományon belül, akkor több szakértelem, vagy hatáskör bevonása szükséges. Fajtái:

1. Funkcionális eszkaláció → képzettebb szakember bevonása
2. Hierarchikus eszkaláció → Felsőbb rétegek bevonása

112. Milyen részekből épül fel a bizonyíték gyújtés és -kezelés?

1. Részletes napló vezetése
   - időbélyegek
   - bizonyítékok azonosítása (IP cím, MAC cím, stb..)
   - helyszín, ahol a bizonyítékot tárolták

2. Bizonyítékgyűjtés
   - teljes disk image készítése
   - kettesével dolgozni(tanú, tévedés mérséklése)
   - Minden bizonyítékot aláírni és dátummal ellátni

3. Bizonyítékkezelés
   - Bizonyíték megőrzése a tárgyalás lezárásáig, hozzáférés szigorú

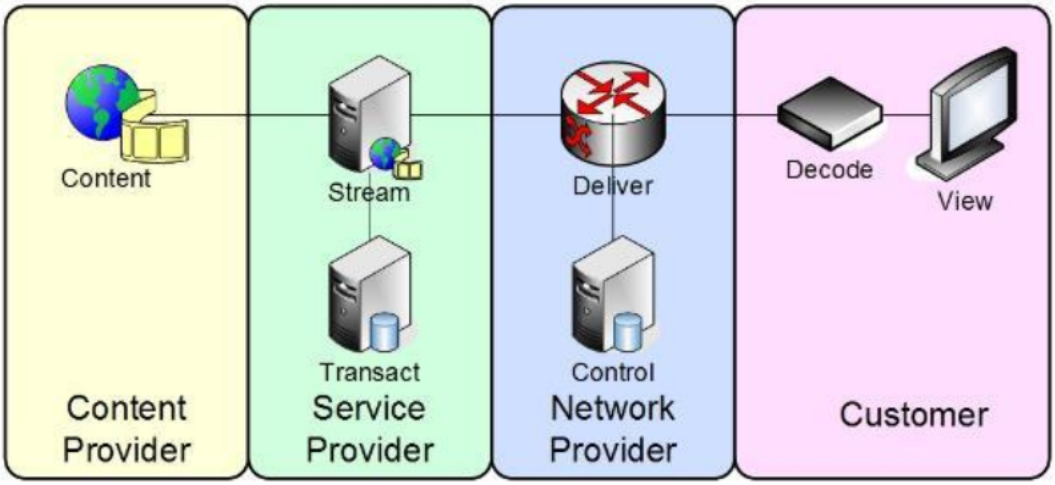
kontrollálása

113. Milyen információ-szétosztási közegek vannak?

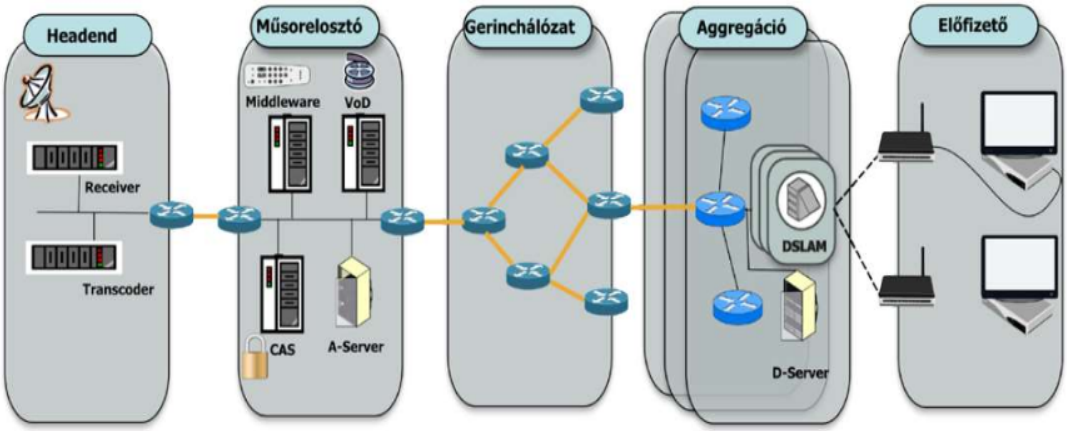
1. Vezeték nélküli műsorszórás
2. Vezetékes műsorszórás
3. Internet

114. Milyen szereplői vannak az IPTV-nek?

1. Content Provider
2. Service Provider
3. Network Provider
4. Customer



szakirányos médiatechnológia tárgyban részletesebb ábra:

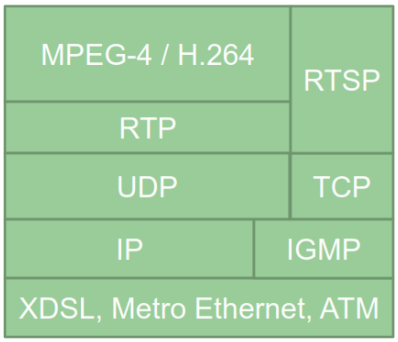


115. Milyen QoE szempontok vannak IPTV esetén?

1. Rendelkezésre állás
2. Késleltetés
3. “kockásodás”
4. Csatorna váltási sebesség

116. Soroljon fel legalább 3 IPTV protokollt.

1. UDP
2. RTP
3. TCP
4. RTSP
5. IP
6. IGMP
7. MPEG-4

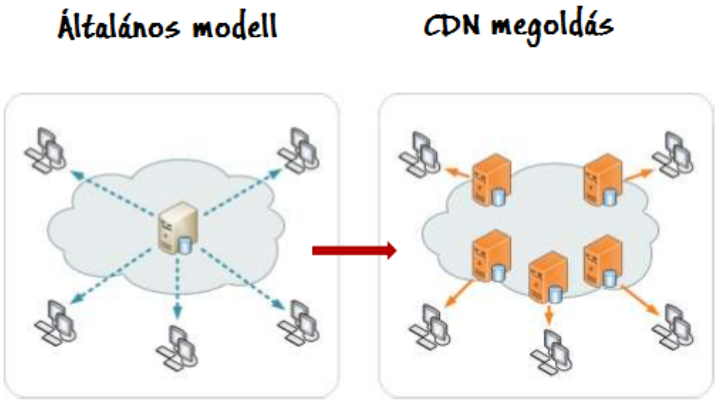


117. Milyen üzenettekl történik az IPTV csatornaváltás, melyik protokoll érte a felelős?

Az IGMP protokoll érte a felelős. Minden csatorna külön multicast csoport (nem kell minden csoportbelinek egyenként elküldeni a csomagot, nem úgy mint az unicastnál), a JOIN üzenettel (IGMP beli) tudunk feliratkozni a multicast csoportra és a LEAVE üzenettel leiratkozni. Csatorna váltáskor az éppen nézett csatorna multicast csoportjának küldünk egy LEAVE üzenetet, az újnak pedig egy JOIN-t.

118. Mit jelent a CDN?

Content Delivery Network,elsődleges célja gyorsítani a felhasználói forgalmat és csökkenteni a hálózati forgalmat. Megvalósítása történhet szerver farmmal, ami azt jelenti, hogy ugyanazt a tartalmat több szerveren is tároljuk, hogy kéréskor melyikről szolgálunk ki az terhelés és teljesítmény alapú.

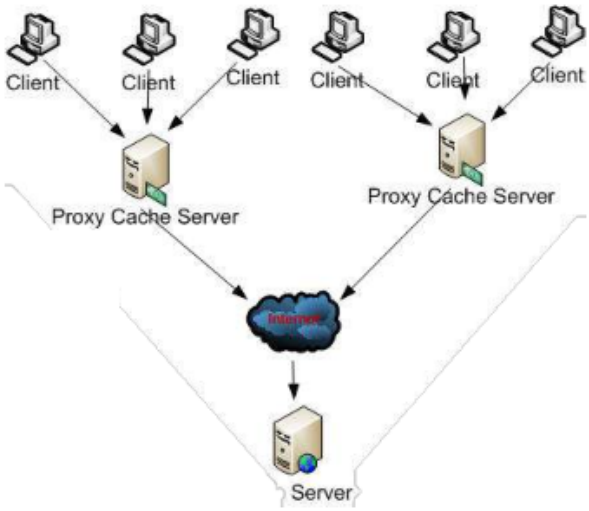


119. Minek a rövidítése az ISP?

Internet Service Provider

120. Mi az a Caching proxy és mire használják?

A caching proxy elsősorban az ISP-k internetes sávszélesség-igényének csökkentésére szolgál, vagyis elsődlegesen az ISP előfizetők kiszolgálási késleltetését hivatott csökkenteni. A lényege, hogy vannak Proxy Cache szerverek, amik különböző technológiai megoldásokkal (csúszóablakos stratégia, prefix caching...) eltárolják a nemrég lekért csomagokat, vagy részeiket és így gyorsítják a kiszolgálást újboli elérés által,



121. Mi az az OTT?

Over the Top TV, egy nemlineáris tartalom elérés biztosítása a cél, az OTT elnevezés a szolgáltatási modellre is utal egyben.

(Nemlineáris médiafogyasztás: Azt érjük el, töltjük le, nézzük/hallgatjuk, amit kiválasztunk, akkor amikor akarjuk)

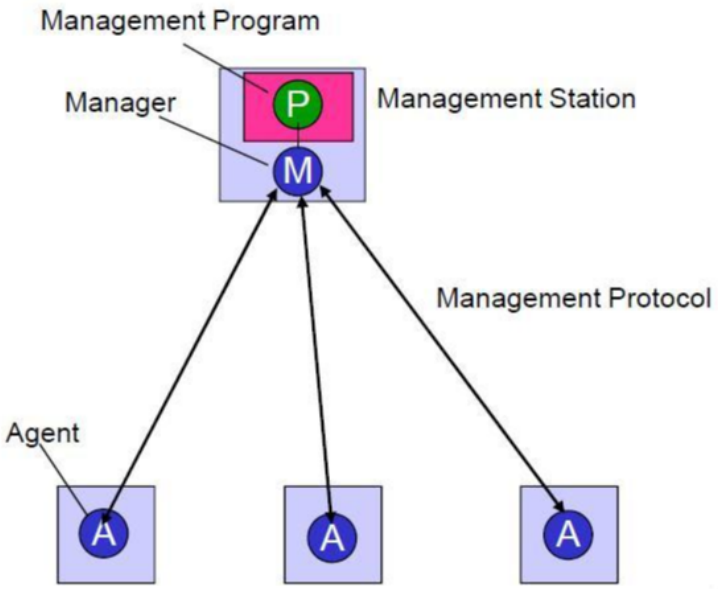
IRU_SNMP diasor, kulcsszavak: SNMP, MIB, ASN

122. Mi az az SNMP , mik a keretrendszer elemi?

SNMP= Simple Network Management Protocol

Elemei:

- Management Station:
  - Management Program
  - Manager
- Management Protocol
- Agent



123. Sorolja fel az SNMP eljárásokat és üzenetszekvenciáit.

1. Get-Request

   Egy vagy több értéket kér a Manager a Management Agent MIB-től

2. Get-Next-Request

   A lexicografikus leírásban a következő Object Identifiert kéri el a MIB fán, úgy hogy megadja a jelenlegi Object Identifiert

3. Get-Response

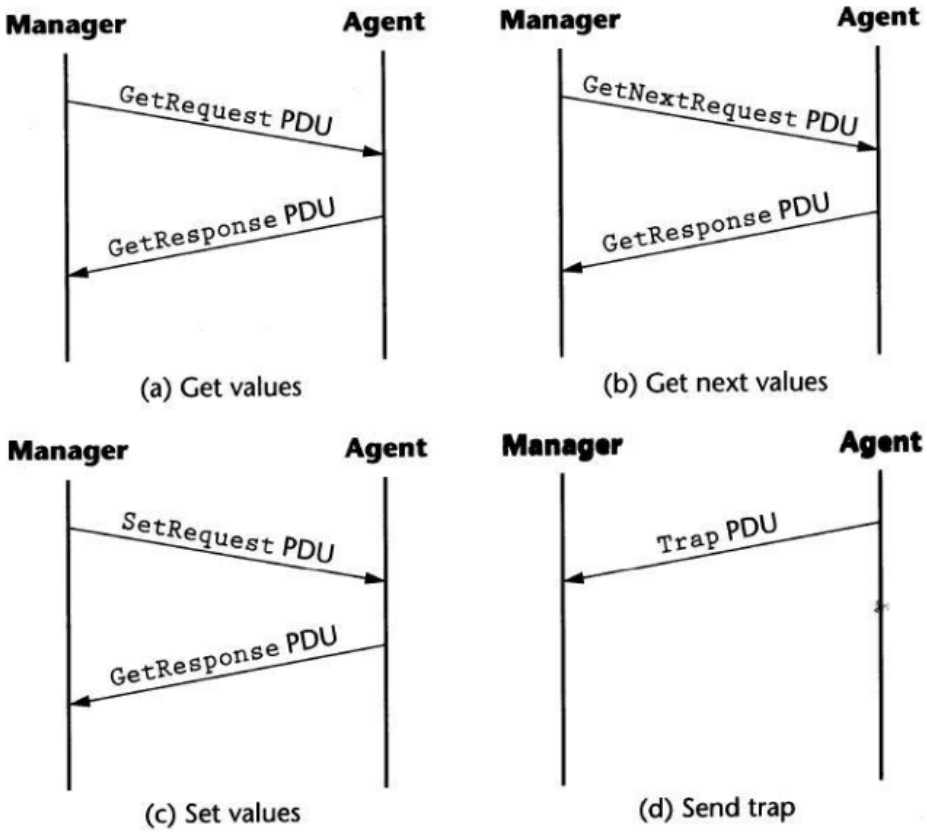
   Válasz az érték kérésre

4. Set-Request

   Beállítja az adott értéket (vagy feladatot) a menedzselt eszköz MIB-jében

5. Trap

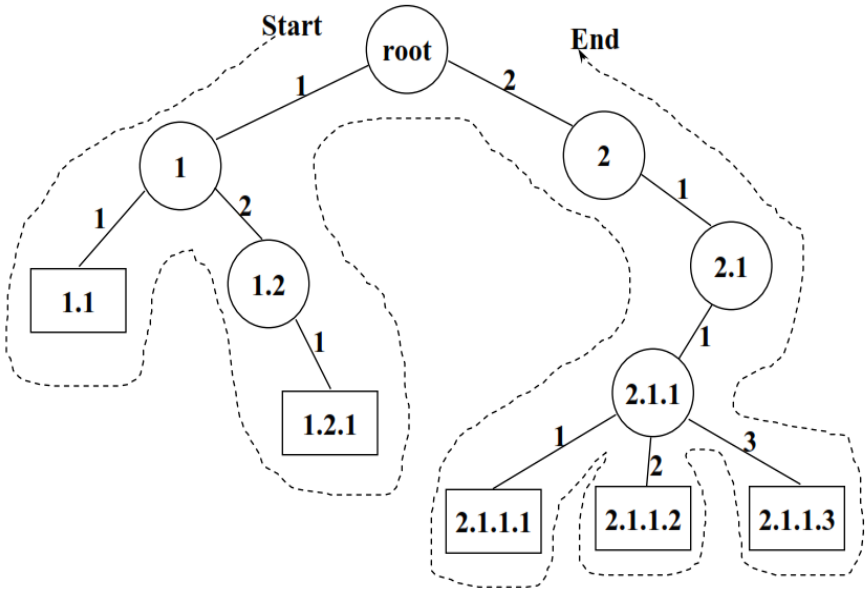
   Egy kéretlen üzenet a menedzselt eszköztől, amit egy ott beállított esemény triggerelt.



124. Mikor van egy MIB fa lexicografikusan rendezve, más néven hogy nevezhetjük?

Ha adott a MIB fa-struktúrája, az objektum-azonosító (OID, ObjectID) meghatározható a gyökértől az objektumig haladó úton.

Más néven preorder traversal, vagy depth-first search.



125. Mi a MIB?

Management Information Bases, objektumok gyűjteménye, adott menedzselt cél érdekében csoportosítva.

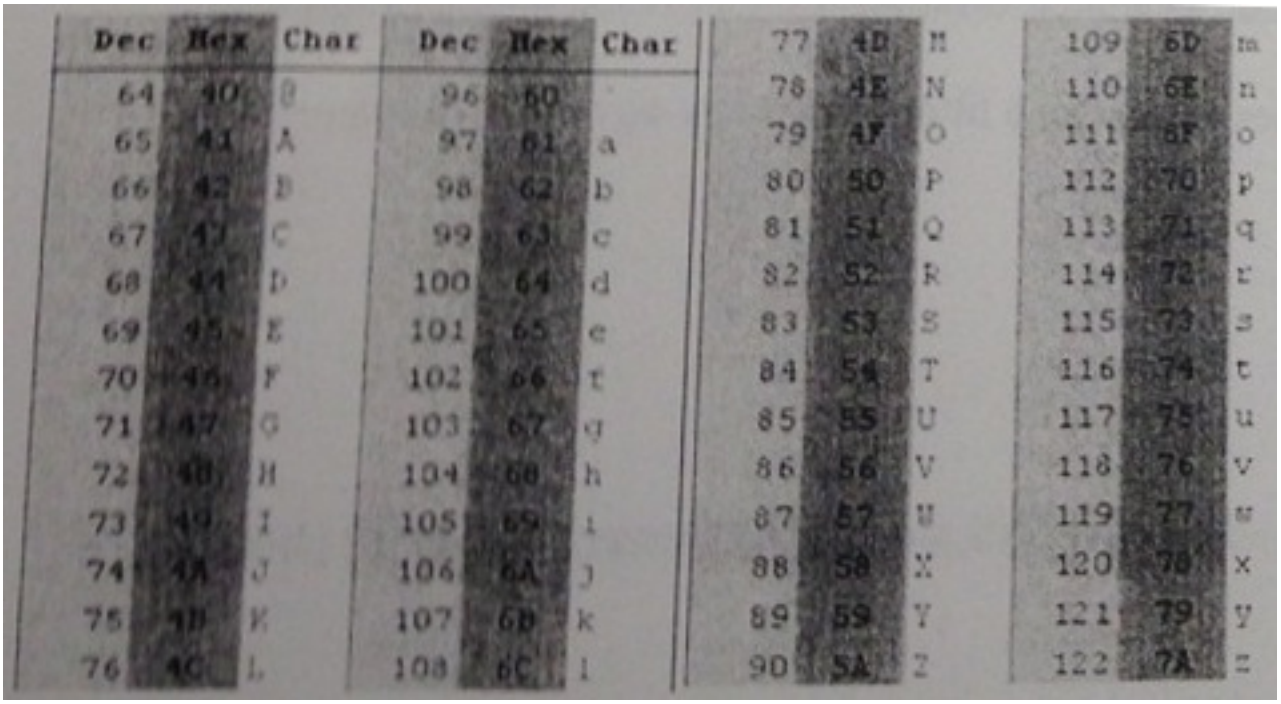
Semmilyen explicit parancs nem adható ki az objektummal kapcsolatban, csak a levél-elemeihez van hozzáférés

126. Mi az az SMI és miben íródnak?

SMI = SNMP Management Information modell iránymutatásokat ad, hogyan lehet MIB-eket, objektum-típusokat és objektum-azonosítókat definiálni. Ezek ASN1-ben íródnak

FELADAT

Kódolja ezt a szöveget "Think Good Talk Good Act Good" ASN.1-el (Basic Encoding Rules) mint 6 darab sorozat sorozata ("sequence of 6 sequences")(Tag code: H'10, Universal: 00, Constructed: 1). Minden szó egy oktett-sztring sorozatként legyen reprezentálva (Tag code: 04, Universal: 00, Primitive: 0), a szóközt nem kell kódolni.



Dec	Hex	Char	Dec	Hex	Char	77	4D	M	109	6D	m
64	40	@	96	60	`	78	4E	N	110	6E	n
65	41	A	97	61	a	79	4F	O	111	6F	o
66	42	B	98	62	b	80	50	P	112	70	p
67	43	C	99	63	c	81	51	Q	113	71	q
68	44	D	100	64	d	82	52	R	114	72	r
69	45	E	101	65	e	83	53	S	115	73	s
70	46	F	102	66	f	84	54	T	116	74	t
71	47	G	103	67	g	85	55	U	117	75	u
72	48	H	104	68	h	86	56	V	118	76	v
73	49	I	105	69	i	87	57	W	119	77	w
74	4A	J	106	6A	j	88	58	X	120	78	x
75	4B	K	107	6B	k	89	59	Y	121	79	y
76	4C	L	108	6C	l	90	5A	Z	122	7A	z

Nem olyan nagy ördöngősség ez az ASN.1 kódolás, annyi az egész, hogy mindig raksz egy TAG és egy LENGTH elemet (hexa) a tényleges adat elé. A TAG jelzi az adat típusát, a LENGTH meg nyilván a hosszát. A TAG-ekre vannak kódok, pl. 30->Sequence, 04->Octett String, 02->Integer, 01->Boolean, stb

04 a TAG kód, az oktett sztringnek, minden szó elé kel írnunk és utána azt a számot, ahány betűből áll

30 a sequence, mert 00-universal, 1 constructed és 16decimálban a sequence ami binárisan egymás mellett 00|1|10000 ami decimálban 48 hexában pedig 30

A feladatban kellett egy sequence ami octett stringeket (6db-ot) tartalmazott. Az octett stringek belsejében az ASCII kódokat kellett használni, ez alapján a megoldás (Think good Feel good Act good):

30 24 (Sequence, 36 hosszú-> ezt legkönnyebb utólag megszámolni)

04 05 54 68 69 6E 6B (Octett string, 5 hosszú, "T", "h", "i", "n", "k")

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

04 04 46 65 65 6C (Octett string, 4 hosszú, "F", "e", "e", "l")

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

04 03 41 63 74 (Octett string, 3 hosszú, "A", "c", "t")

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

A vizsgán nem biztos hogy ez a szöveg volt, de a lényeg az hogy alapvetően így kell megoldani. Remélem így érthető. :)

De akkor már az egyik barátom megoldását is beraknám ide, aki a szakirányán ilyennel már találkozott:

30 24 (Sequence, 24(hex) hosszú-> mert az "al-sequencek" méreteit kell összeadni 07+06+06+06+05+06=36(dec)=24(hex))

30 07 ('Think' szóhoz a sequence)

04 05 54 68 69 6E 6B (Octett string, 5 hosszú, "T", "h", "i", "n", "k")

30 06 ('good' szóhoz a sequence)

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

30 06 ('Feel' szóhoz a sequence)

04 04 46 65 65 6C (Octett string, 4 hosszú, "F", "e", "e", "l")

30 06 ('good' szóhoz a sequence)

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

30 05 ('Act' szóhoz a sequence)

04 03 41 63 74 (Octett string, 3 hosszú, "A", "c", "t")

30 06 ('good' szóhoz a sequence)

04 04 47 6F 6F 64 (Octett string, 4 hosszú, "g", "o", "o", "d")

A fenti számpárosok mind 8biten kódolt hexadecimális számokat jelölnek!!!

A következő oldalon látható hozzá az ábra!!!!

127. Sorolja fel az SNMP 3 biztonsági szolgáltatását.

1. Authentication

   Az Agent limitálni szeretné a MIB hozzáférést authentikálatlan menedzsereknek.

2. Access

   Az Agent különféle privilégiumokat akar kiosztani különböző menedzsereknek.

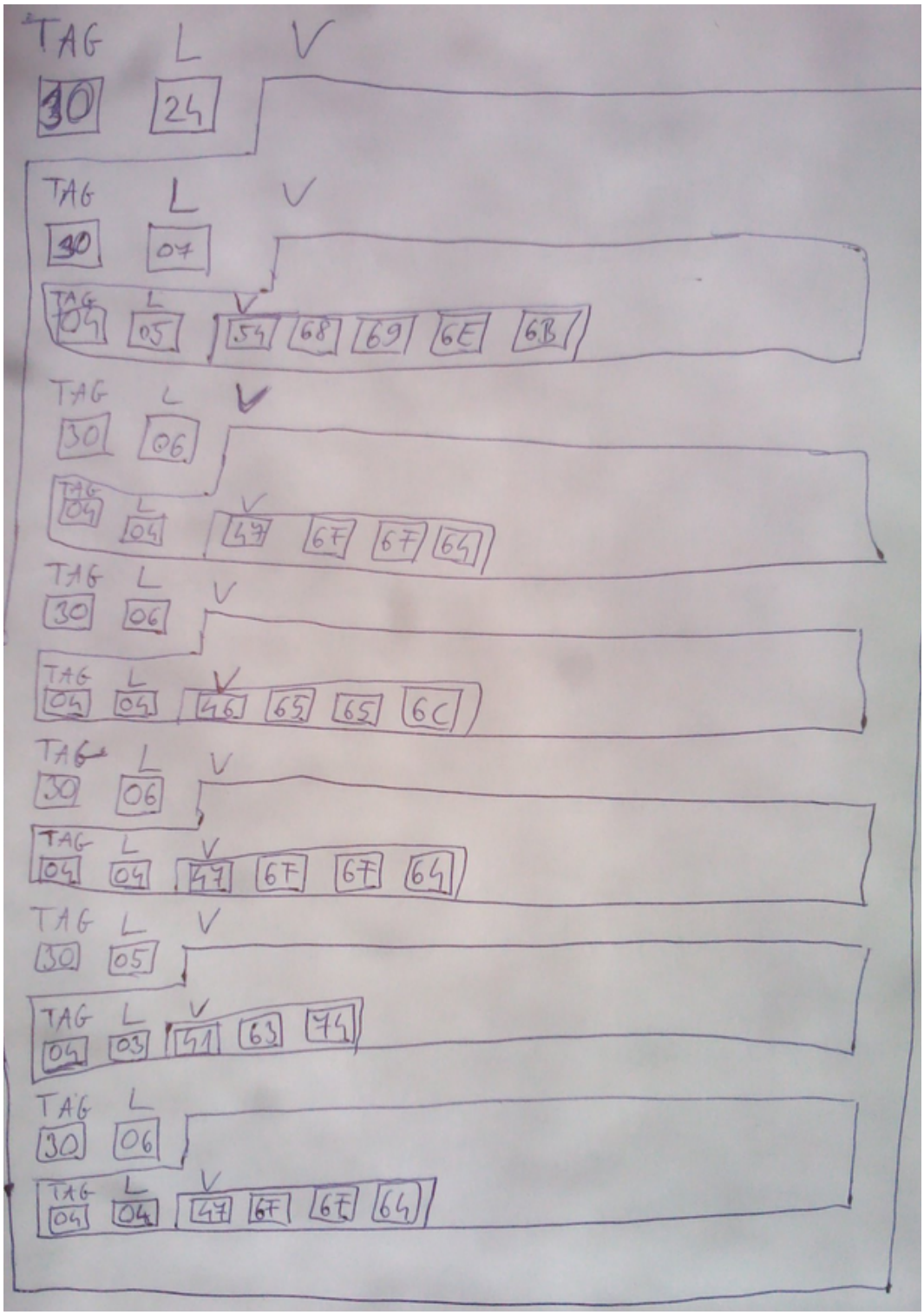
3. Proxy szolgáltatás

   Special Access + Authentication

128. Mi az SNMP community és milyen fajtái vannak?

Ez egy kapcsolat egy „agent” és egy csoport manager között – itt az authentikáció, hozzáférés és proxy lehetőségek is definiáltak közöttük.

ÁBRA a 126-os feladat ASN-es megoldásához



129. Milyen hozzáférési kategóriái vannak (Access Policy) az SNMP communitynek?

1. SNMP MIB View
    - objektumok részhalmaza a MIB-en belül
    - különféle MIB nézetek lehetnek definiálva a communityk számára
2. SNMP Access Mode
    - Egy hozzáférési mód {READ-ONLY, READ-WRITE} definiálható a community-nek

MIB ACCESS Category	SNMP Access Mode	
	READ-ONLY	READ-WRITE
read-only	get és trap eljárásokhoz	
read-write	get és trap eljárásokhoz	get, set és trap eljárásokhoz
write-only	get és trap eljárásokhoz – de az érték implenetációfüggő	get, set és trap eljárásokhoz – de az érték implenetációfüggő get és trap esetben
not accessible	nem használható	

3. SNMP Community Profile
    - MIB view és egy access mode kombinációja

IRU_IT_Szolgaltatasok_13 diasor, kulcsszavak: e-mail, MIME, POP, IMAP, SMTP, RAS, RAW, PCL

130. Mitől szolgáltatás egy szolgáltatás?

- Megtervezés
- Beüzemelés
- Fejlesztés
- Monitorozás
- Karbantartás
- /Támogatás/

131. Soroljon fel alapszolgáltatásokat.

- Email
- Authentikáció
- Távoli elérés
- Nyomtatás
- DNS

132. Mik az jól karbantartható szolgáltatás jellemzői?

- Egyszerű
- Kevés függőséget tartalmaz
- redundáns HW
- Szabványos SW és HW

133. Mi a különbség a vastag és vékony kliens szolgáltatások között?

- Vastag kliens szolgáltatás:
  - Nagyrészt a gazda gépén fut
- Vékony kliens szolgáltatás
  - Nagyrészt a szerver gépen fut

134. Mit jelent az SPF és mi okozhatja?

SPF = Single Point of Failure, például protokoll gateway-ek használata idézheti elő.

135. Sorolja fel az e-mail küldés lépéseit.

1. Üzenettovábbítás → ahogyan az e-mail szerverről szerverre jut
2. Kézbesítés → amikor az e-mail a fogadó mailbox-ába kerül
3. Üzenet-listák feloldása → Amikor a listacímre küldött levél megsokszorozódik és így kerül továbbításra

136. Milyen részekből épül fel egy e-mail?

1. Fejléc → Címzés, tárgy megjelőlés
2. Törzs

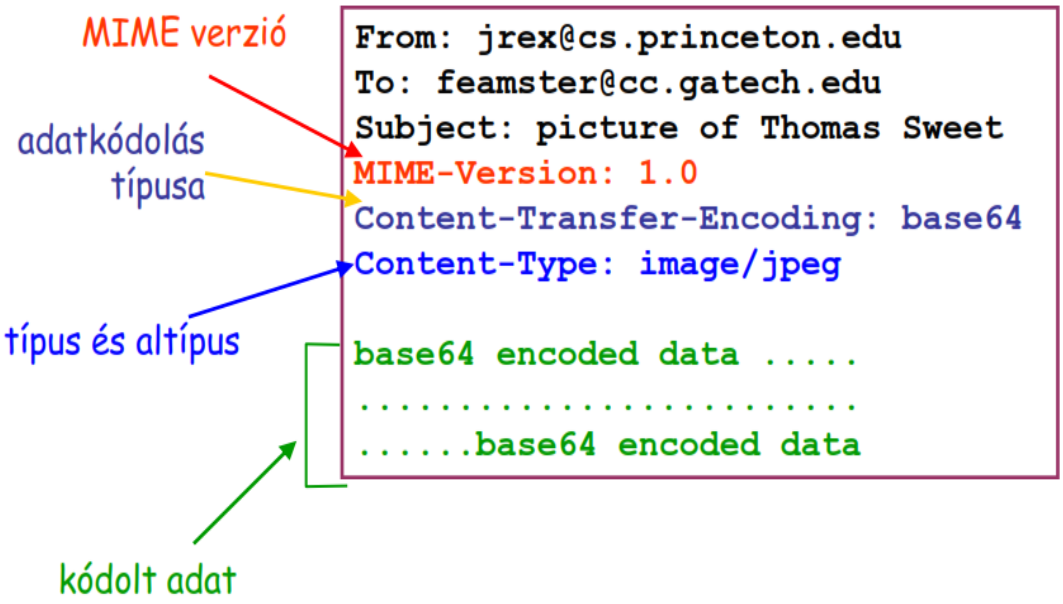
137. Milyen megszorítások adódnak e-mail küldésekor és mi rájuk a megoldás?

1. Nem szöveges adat küldése → MEGOLDÁS: konvertálás Base64-es kódolással. nem ASCII-ból ASCII konvertálás
2. Több adategység küldése → MEGOLDÁS: több emailt egy üzenetbe csomagolunk, elválasztásuk pl stringel

138. Mi a MIME és mikből áll?

MIME = Multipurpose Internet Mail Extension, hozzáadott fejlécek a törzs leírásához
Részei:

- MIME version
- content type
- content-transfer-encoding



139. Mik az e-mail címek részei?

Helyi mailbox és domain név. Pl. Tibiatya@humbakfalva.com, itt Tibiatya mailbox és humbakfalva.com a domain

140. Mi az az SMTP és mi a feladata?

SMTP = Simple Mail Transfer Protocol. A mail üzeneteket szerverek sorozata szállítja, a szerverek a bejövő üzeneteket üzenet sorba állítja, hop by hop módszer.

Minden “hop” beírja az azonosítót a fejlécbe.

Az SMTP egy kliens szerver protokoll, kliens a küldő szerver, szerver a fogadó szerver. (küldés kezdésekor a kliens a tényleges kliens aki a mailt küldi, a szerver az első fogadó mail szerver).

Megbízható adattovábbítás TCP protokoll (on port 25) felett.

Az SMTP egy “PUSH” protokoll, ugyanis csak benyomja a következő szerver mailboxája amint megkapta a “response” választ a “command” üzenetre.

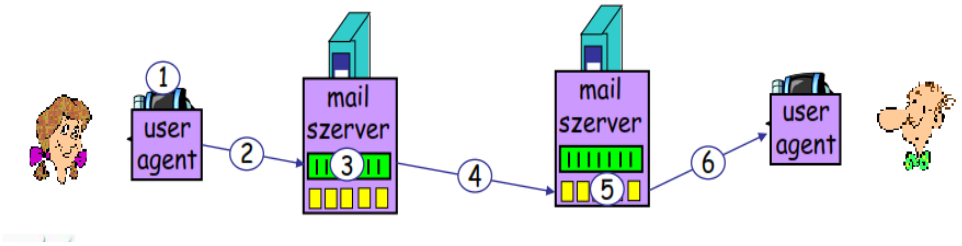
Továbbítás 3 fázisa:

- Handshaking (kézrázás)
- Üzenettovábbítás
- Lezárás

Eset:

Anna üzenetet küld Bélának

1) Anna az UA-t használja, hogy üzenetet írjon ide: beela@nagyceg.com
2) Anna UA-je üzenetet küld a mail szerverének; az üzenet bekerül egy sorba
3) A kliens oldali SMTP egy TCP kapcsolatot nyit Béla mail szerverével
4) Az SMTP kliens átküldi Anna üzenetét a TCP kapcsolaton
5) Béla mail szervere berakja az üzenetet Béla postaládájába (mailbox)
6) Béla aktiválja az UA-ját az üzenet elolvasásához



141. Mi a POP, mik a korlátai?

POP = Post Office Protocol. Célja, hogy időszakosan is el tudjuk érni a mailjeinket, letölthessük és tetszés szerint manipulálhassuk őket, ha nincs csatlakozva.

Tipikus user-agent interakció POP szerverrel:

- Kapcsolódás a szerverhez
- e-mailek leszedése
- Az üzenetek "új"-ként való tárolása a PC-n
- kapcsolat lezárása a szerverrel

POP korlátai:

- Nem könnyen kezel többszörös mailboxokat
- nem az üzenetek szerveren való tárolására tervezték
- a mailboxhoz a többszörös kliens-hozzáférés nehéz
- nagy hálózati sávszélességet igényel

142. Mi az IMAP?

IMAP = Interactive Mail Adress Protocol.

- Connected" és „Disconnected" módok támogatása
- Egyszerre több kliens is csatlakozhat a mailboxra
  - Detektálja a más kliensek által a mailbox-on történt változtatásokat
- Hozzáférés az üzenetek MIME részeihez & részleges letöltés
- A kliens tud létrehozni, átnevezni, és törölni mailboxot
- A kliens tud egyik folderből másikba áthelyezni üzenetet
- Az üzenet letöltése előtt a szerveren lehet keresést indítani rá

143. Jellemezze a webes mailt.

- User agent: hagyományos Web browser
- A felhasználó HTTP-n kommunikál a szerverrel
- A Weboldalak a folderek tartalmát jelenítik meg
- A szöveget egy „form"-ba írjuk, majd „submit" a szervernek
- "POST" kérés és adatfeltöltés a szerverhez
- A Szerver SMTP-vel küldi az üzenetet más szerverhez
- Könnyű az anonymous e-mail (pl. spam) küldése

144. Vállalati e-mail fontos jellemzői

- Privacy Policy:
  - A hely e-mail policy-jével mindenki legyen tisztában (...és fogadja el...)
  - A vezetőség dönthet úgy, hogy privát levelek küldését céges címről nem támogatja.
- Namespace-ek
  - Az e-mail cím a vállalat namespace-ének egyik legláthatóbb része

        - Ugyanaz legyen a belső és a külső e-mail cím
        - Legyen standard címformátum –például → first.last
    - Megbízhatóság
        - Az e-mail alapeszköz. Mindig Jól Működjön
        - Melegtartalék az egész rendszerről
        - Ha nem lehetséges a hot swap (mivel eléggé költséges) → készenléti terv, begyakorolt lépések a hibából való helyreállásra
    - Egyszerűség
        - Korlátozzuk a szükséges gépek számát
        - Kerüljük a protokoll- vagy formátum-gateway-ek használatát → mert ezek SPF
    - Automatizáltság
        - Az e-mail account létrehozása legyen az általános account-készítési folyamat része
        - A búcsúzó kollegák e-mailjeit nem forwardoljuk; listákról töröljük
        - Accountok másolása szerverek között
    - Monitorozás
        - Hálózat: ping (ICMP echo üzenetet küld)
        - TCP 25-ös port elérhető?
        - Visszapattanó üzenetek – diagnosztikai info
        - Naplóállományok (pl. üzenet-mennyiségek, előrejelzéshez)
    - Skálázhatóság
        - Növekvő felhasználói bázisnak
        - Forgalmi börsztök kezelése
        - Óriási, akkumulálódó adattömeg tárolása
        - Mail spool használata segít
        - Üzenetméret korlátozás is segít (időszakosan)
    - Security
        - Ellenőrzés a szervereken ÉS a felhasználói gépeken is
        - A tűzfallal együtt: vállalati biztonsági stratégia

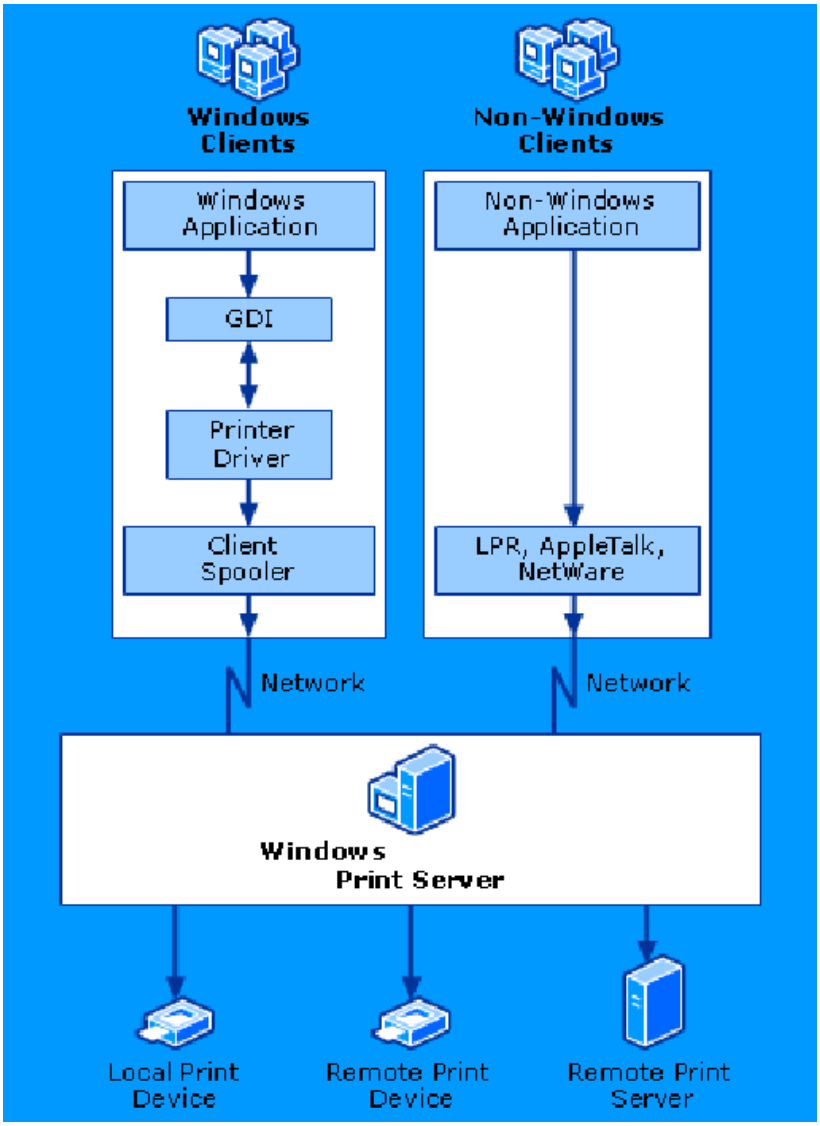
145 Mi a RAS, mondjon példákat rá.

RAS = Remote Access Controll. A külső alkalmazások eléréshez tűzfal lyukasztás → a tűzfalat az alkalmazás protokolljához rendelt porton átjárhatóvá kell tenni

Hozzáférésre jogosultak léphetnek be a vállalati hálózatba, alapos tervezést igényel

Példák: Remote Destkop(win alapú), VNC (bármilyen OS alatti gépre), TeamViewer, Join.Me, Mikogo

146. Nyomtatás windows szerveren.



147. Soroljon fel hálózati nyomtatási protokollokat.

- klienstől a szerverig:
  - SMB – Server Message Block
  - LPR (LPD) - Line Printer Remote
  - IPP – Internetwork Printing Protocol
- szervertől a nyomtatóig:
  - LPR
  - IPP

148. Mit nevezünk RAW-nak?

„Nyers”, a nyomtató által emészthető formátum, PCL (Printer Command Language) és PostScriptben írva

IRU_2013_szabvanyok_policy diasor, kulcsszavak: IPMI, CIM, DMI, WBEM, névtér

149. Mi az IPMI?

IPMI = Intelligent Platform Management Interface

A számítógépek hardver és firmware eszközei számára határoz meg közös interfészeket, amelyekkel a rendszer-adminisztrátor a rendszerek állapotát ellenőrzés alatt tarthatja és menedzselheti.

The Intelligent Platform Management Interface (IPMI) is a standardized computer system interface used by system administrators for out-of-band management of computer systems and monitoring of their operation.

150. Mik az IPMI jellemzői?

OS független, sőt OS hiányában is képes a rendszer adminisztrátor a szükséges adatokat lekérdezni külön soros vonalon, vagy serial over LAN-on keresztül.

A szabvány előírja a riasztási mechanizmust is. SNMP protkollon keresztül!

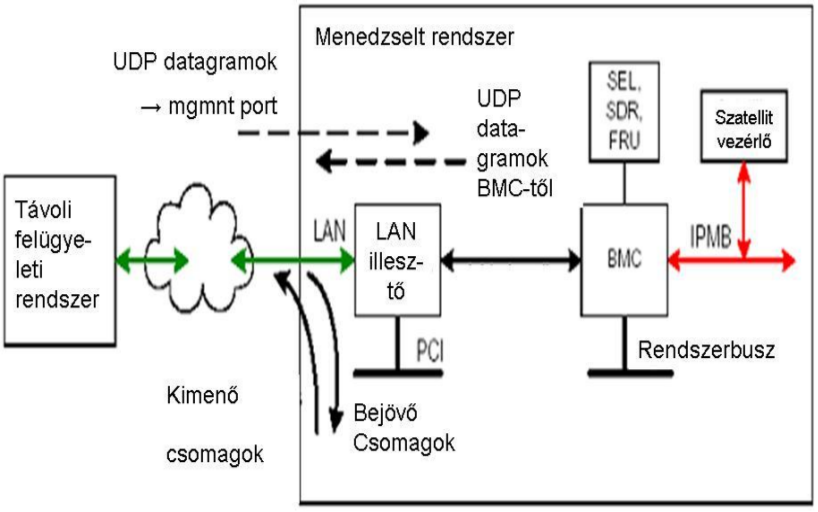
Az IPMI (az állapot adatok közel valós idejű figyelése révén) problémák megelőzésére is alkalmas. Javítja a rendszerek biztonságát is

151. Mikből épül fel az IPMI?

Egy fő és több mellékvezérlőből állhat. Fővezérlő: BMC (Baseboard Management Controller) és a mellékvezérlők = szatellitek

Nagyobb rendszerben a mellékvezérlők az IPMB (Intelligent Platform Management Board/Bus) interfésszel kapcsolódnak a BMC-hez. A BMC a mellékvezérlőket képes más BMC-khez csatolni az IPMC (Intelligent Platfrom Management Chassis) segítségével.

Az egészet a RMCP(Remote Management Control Protocol) felügyeli, amit az IPMI definiál.



152. Mit jelent az, hogy az IPMI nem ügynök-alapú megoldás?

A nem ügynök-alapú megoldás azt jelenti, hogy szoftver ügynökökön alapul a megoldás, hanem vezérlőkön.

153. Milyen tárolói vannak az IPMI-nek?

FRU (Field Replacable Unit), ami tárolja a cserélhető eszközök leltárát, valamint az SDR (Sensor Data Records) tárolóban találhatóak az eszközben működő érzékelők adatai.

154. Mi az a CIM és "ki" hozta létre?

CIM = Common Information Modell

Hierarchikus, objektum-orientált menedzsment információs modell.

Definiálja egy információtechnológiai környezetben üzemeltetett eszközök objektum-alapú reprezentációját.

CMI is an interface between content providers and service providers, which does not directly involve the end user. The scope of the standard covers the entire off-deck content management lifecycle but does not include implementation or behavior beyond the API. Therefore it can accommodate a broad range of services and service policies.

A DMTF (Distribute Management Task Force) fejlesztette ki, úgy ahogy a DMI-t is.

155. Mik a CIM jellemzői?

Lehetővé teszi a különböző gyártók által gyártótól száramzó berendezések üzemeltetési adatainak kicserélését, az aktív vezérlést, beavatkozást.

Objektum orientált menedzsment modell, UML nyelven van leírva. Ebben a leírásban a modell a menedzselt elemeket (HW eszközök, SW-ek) külön CIM osztályokként definiálja, a köztük lévő kapcsolatokat pedig CIM kapcsolatokként.

A menedzsment adatok számára szbványos keretet biztosít.

A CIM a rendszerelemek állapotának nem csak a lekérdezését, hanem a menedzselt
elemek manipulálását is lehetővé teszi.

156. Sorolja fel a CIM infrastruktúra elemeit.

- metaséma
- szintakszis
- szabályok
- formátum (MOF - Management Object Format)

157. Egy CIM profilt mi azonosít?

A neve, a felhasználó szervezet neve és verziószáma.

158. Miből áll a CIM szabvány?

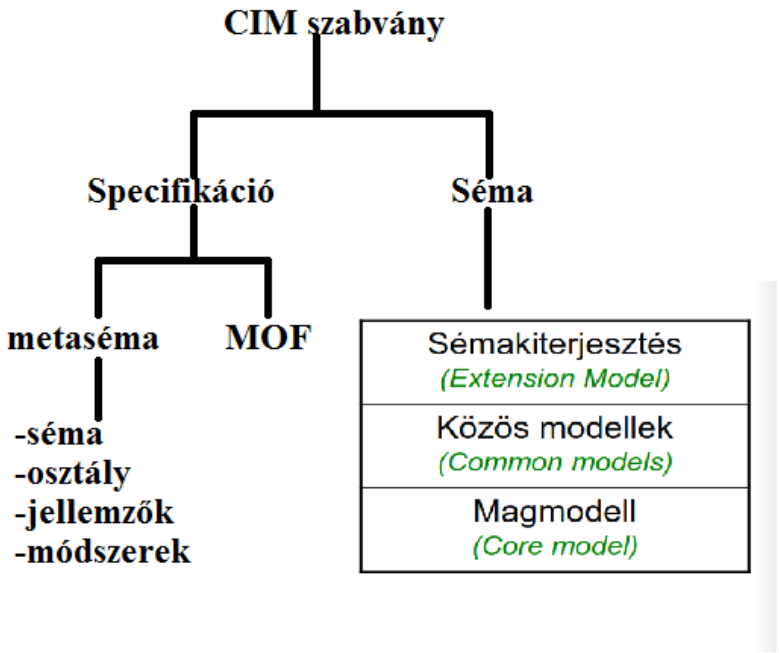
1. Specifikáció

   Definiálja a más menedzsment modellekkel való integráció részleteit.

2. Séma

   Az aktuális modell leírását tartalmazza.

Előzetesen is összefoglalva



159. Jellemezze a CIM specifikációt.

Metasémákat, a metaséma elemeit és minden egyes elemhez a szabályokat tartalmazza.

A metaséma a modell formális leírása, tartalmazza: modell kifejezését, modell haználati folyamatát, modell szemantikáját

Definiálja továbbbá a MOF-ot, amely definiálja az osztályokat és az eseteket.

160. Sorolja fel a CIM metaséma elemeit:

1. Sémák (Schemas)

   A séma osztályok csoportja ugyanazon csoporttulajdonossal.

   A sémát adminisztrációs céllal használjuk

2. Osztályok (Classes)

   Az osztály egy menedzselt objektum jellemzőit fogja össze

3. Jellemzők (Properties)

   Az osztály jellegének kifejezésére szolgáló érték, egyedinek kell lennie az osztályon belül.

4. Módszerek (Methods)

   A módszer egy meghívható művelet, az osztályára értelmezett és azon belül egyedinek kell lennie. Egy osztályban nulla, vagy több módszer lehet.

161. Mi a CIM MOF?

MOF = Managed Object Format, szöveges leírása az osztályoknak, a kapcsolatoknak, jellemzőknek, referenciáknak, módszereknek és esetdeklarációknak, a hozzájuk rendelt minősítőkkel együtt. Megjegyzések is lehetnek benne.

Unicode vagy UTF-8 kódolású lehet.

162. Jellemezze a CIM sémát.

A menedzsment sémák az építő elemei a platformok és alkalmazások menedzselésének: például az eszköz konfigurálásának, a teljesítmény hangolásának, a változáskövetésnek.

163. Milyen modellekből épül fel a CIM séma?

1. Sémakiterjesztés (Extension Model)

   A sémakiterjesztés azért szükséges, mert a rendszerelemek jellemzően termék- illetve gyártó-specifikusak. A sémakiterjesztéssel tetszőleges tulajdonságok és viselkedések leírhatóak.

   Új tulajdonság vagy metódus hozzáadása létező séma létező osztályához.

2. Közös modell (Common Model)

   Egy közös modell egy adott technológia vagy implementáció esetére vonatkozik. Például: a hálózati eszközökre, a rendszeren futtatott operációs rendszerekre, stb.

- Applications Alkalmazások
- Event Eseménykezelés
- Network Hálózatok menedzselése
- Support Terméktámogatás
- Database Adatbáziskezelés.
- Interop A webalapú vállalati menedzsment (WBEM)
- Physical A fizikai eszközkészlet kezelése
  - Pl. a különböző bővítőkártyák és kábelezések leírásai

3. Magmodell (Core Model)

A magmodell osztályok, a kapcsolatok, jellemzők és módszerek készlete, azoké, amelyek a menedzselés valamennyi területére vonatkoznak.

A magmodell definiálja a menedzselt környezet alapvető osztályait és asszociációit.

Minden osztály a CIM_ManagedElement osztály leszármazottja.

A mag modell a menedzselt rendszer „alapszótára”.

164. Mi a DMI?

DMI = Desktop Management Interface, felhasználói végberendezések és szerverek alkatrészeinek kezeléséhez (menedzsmentjéhez) nyújt szabványos keretet.

A DMI a Rendszer Menedzsment BIOS (SMBIOS) része, ez teszi szabványossá a számítógépkonfigurációról szóló adatok hozzáférését a felhasználók vagy erre feljogosított alkalmazások számára.

A DMI tehát szabványos módon kérheti le a BIOS-ból a számítógép alkatrészeiről, felépítéséről az adatokat.

165. Mi a WBEM?

WBEM = Web Based Enterprise Management, A WBEM rendszermenedzsment technológiák olyan készlete, ami az elosztott IT környezet menedzselésének egységesítésére szolgál.

Alapjai: CIM standardok és Internet technológiák (CIM infrastruktúra és séma, CIM-XML, CIM over HTTP, WS-Management, SNMP)

A WBEM a CIM web-alapú implementációja, beleértve a protokollokat, amelyekkel detektálhatók és elérhetők más CIM implementációk.

Tartalma:

- protokol(lok)
- lekérdezési eljárások
- felismerési mechanizmusok
- leképezések

166. Sorolja fel a WBEM technológia kulcselemeit.

- alkalmazások távmendzsmentje
- egy alkalmazás több esetének egyetlen egységként való menedzselése
- standard interfész különböző alkalmazások távmenedzseléséhez
- az alkalmazás menedzsment leválasztása a kliensről

167. Foglalja össze a WBEM architektúrát röviden.

Az operátor felhasználói felületen éri el a menedzsment rendszert, azt, hogy milyen a felhasználói felület a WBEM nem köti meg. → következésképpen a a felhasználói felületet változathatjuk anélkül, hogy a többi elemet módosítanánk.

A WBEM kliens, hogy megtalálja a WBEM szervert, a menedszelni kívánt eszköz számára létrehozza a kérést tartalmazó XML üzenetet, amit HTTP vagy HTTPS protkollon továbbít.

A kliens kizárólag a modellel kommunikál, a modell pedig a valóságos HW-el vagy SW-el!!! Akommunikációt a szolgáltatók kezelik le.

168. Mit szükséges egy eszközfejlesztőnek (vagy szolgáltatónak) elkészítenie ahhoz, hogy eszköze vagy szolgáltatása szabványosan menedzselhető legyen?

- A modellt
- a “szolgáltatókat”

169. Soroljon fel 3 ismert WBEM impelentációt.

Solaris WBEM Services, IBM TIvoli Monitoring, Open Pegasus, Purgos, SMI-S

170. Sorolja fel az üzemeltetési politika 5 elemét.

1. Rendszerüzemeltetési etika

Egy szervezetben az etikai elvárásokat feladatkörökhöz illeszkedően a napi teendők tükrében érthető módon célszerű megfogalmazni. pl.: szakmai vicelkedési kódex, felhasználói viselkedési kódex

2. Névtér-politika

A névtér (namespace) bizonyos típusú elemek (pl. személynevek, földrajzi nevek, műszaki kifejezések, stb.) felsorolása és összefüggéseinek megadása egy rögzített szabályokon alapuló tároló elrendezésben

A névtér-elemek vonatkozhatnak valóságos tárgyakra, élőlényekre és elvont fogalmakra is.

A névterekre vonatkozóan határozott, rögzített, írot egyértelmű politika kell.

3. A rendkívüli helyzetek teendői
4. Változáskezelés
5. IT biztonsági politika

171. Sorolja fel milyen névterek vannak? (ez elég pongyola)

- absztrakt névtér
- konkrét névtér
- egyszerű névtér

  A névtér elemeinek egy és csak egy értelmezése lehet.
- hierarchikus névtér

  Konténereket is tartalmaz valamilyen elrendezésben.

172. Sorolja fel a névtér politika kiterjedéseit. (ez is bullshit megfogalmazás, sorry eddig tartott az energiám :D)

- Elnevezési politika
- Élettartam p.
- Látahtósági p.
- Konzisztencia p.
- Újrahasználati p.
- Védelmi p.

173. Sorolja fel anévválasztás főbb módszereit.

- Formális

  Kötött, szigorú szabályok szerint adunk neveket, pl.: gépnév: pc + 4 számjegy, login név: vezeték első hat jegye + keresztnév kezdőbetűje + n jegyű azonosítószám

- Téma szerinti

  A különböző típusú nevek különböző téma köré csoportosulnak, pl. szerverek csillagok, printerek bolygók stb.

- Funkcionális

  Felhasználói szerepek (admin, titkár, vendég)

  A gép által betöltött szerep (dns, cpuserver12, web001)

- “Nincs szabály” módszer

  Mindenki úgy nevez el valamit, ahogy ő gondolja, az ütközések feloldása elsőbbségi alapon történik.

174. Mi a névtér séma?

Egy séma típus megadása, kizárólag neveket és definíciókat tartalmaz.

175. Mi az névtér alkalmazás profil?

Egy séma típus leírása, az alkalmazási környezetben használt nevek leírása. Szemantikus definíciót is tartalmazhat.

Alapvető műveletek:

- cd :könyvtárak közötti navigációhoz
- mkdir :könyvtár létrehozása
- rmdir :könyvtár törlése
- ls :könyvtár tartalma
- echo $PATH :végrehajtható parancsok helyei → könyvtárai!!! legalábbis megtekintésen így fogadták el, mind1, h a diában is ez van szó szerint

  pl.: /usr/local/bin/:/usr/bin:/bin/
- export :környezet i változó beállítása pl. PATH=$PATH:/new/directory/path
- man :help a parancsok használatához
- history :eddig használt parancsok listája
- & :parancs után írva: fusson a háttérben ls & -> [1] 23142
- fg :futó job visszahozása előtérbe fg 23142

Szövegszerkesztés:

- cat :teljes file szövegének összeállítása (kiírás)
- tac :utolsó sor legelöl (hasznos pl. log file esetén)
- head :a file kezdő sorai (default:10)
- tail :a file záró sorai (default:10)
- more :szöveg kiírása oldalanként a terminálra
- less :szöveg kiírása: a felhasználó mászkálhat benne
- grep :szövegben keresés szabályok szerint regxp – regular expressions
- (g)awk :szövegben keresés/manipuláció
- sed :szöveg egyszeri futás alatti szerkesztése
- vi :klasszik szövegszerkesztő
- emacs :legendás szövegszerkesztő

Account:

– felhasználónév azonosít ja,

– jelszó védi

Password file: username:password:uid:gid:gecos:homedir:shell

• Két féle account:

- Root
- User

– Parancsok:

• su :root átvált az adott userre/ré

• adduser :felhasználó hozzáadása

• passwd :jelszó megváltoztatása

• userdel :felhasználó törlése

• /etc/passwd :elem törlése

Hozzáférés:

– Mult i-user környezet!

– Felhasználók nem férnek hozzá egymás file-jaihoz

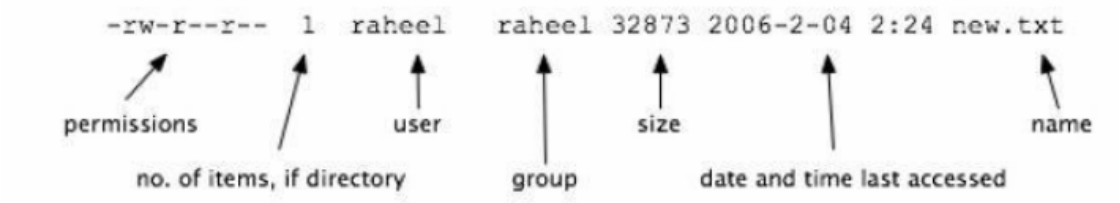
– Speciális file-okhoz csak a root fér hozzá

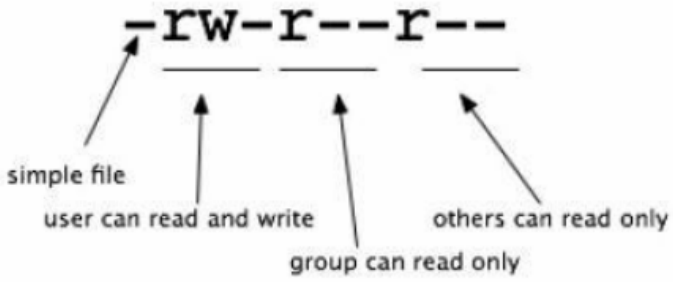
• Csoportok – groups

– a felhasználók több csoporthoz tartozhatnak

– könnyebb/rugalmasabb hozzáférés-kezelés

• Hozzáférés: felhasználók / csoportok / egyéb





Ownership változtatás:

- Ownership (birtoklás) változtatás: chown pl.: chown username file_or_dir
- Csoport-birtoklás változtatás: chgrp pl.: chgrp groupname file_or_dir
- Kombinált csoport és felhasználónév: chgrp name.name file_or_dir

Hozzáférés változtatás:

- chmod parancs
- r, w, x :read, write, execute
- Root :megváltoztathatja bármely file/directory hozzáférés-szabályait
- A root mellett csak a birtokos (user) tudja változtatni