NIS
LDAP
Kerberos
SMB samba, MS-hoz

Info, segítség

man szekciók

1 alap
2 rendszerhívások - C
3 többi C
4 spec állományok
5 formátumok
6 játékok
7
8 rendszergazdai parancsok

man 3 printf

man -k printf

.... kulcsszavas keresés de csak az indexelt részben, szóval alapból mindenre semmi

info - szolgáltatásokról info

http://www.linuxdoc.org/

ttyS0 - ttyS31 soros portok
hd... IDE lemezek
hda
hdb
⋮

sda, sdb .. SCSI lemezek

partíciók: 1, 2, 3, 4 & 5, 6, 7 ...
primary ext. log.

fd0 (fd1, ...) floppy lemezek

zero olvasható, 0-k jönnek
null „fekete lyuk" mindent elnyel
lp0.. printer portok
tty terminál

/etc rendszerkonfigurációs fájlok
/home felhasználók könyvtárai
/lib legfontosabb library-k (mint dll)
/lost+found lost szektorok
/mnt átmenetileg mountolt kötetek
/opt programcsomagok tárolása
/proc spec. könyvtár, közvetlenül a kernelből ad információkat

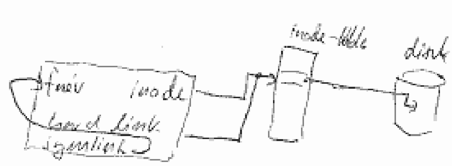
cpuinfo „fájl"
meminfo „fájl"
számok: adott process id-ja
process körny. változói

/sbin legfontosabb rendszergazda prog-k
/tmp ∀ által írható & olvasható
/var ~~logok~~ lock-ok tárolása, spool-ok
/usr

bin nem annyira alapvető prog-k
include fordításhoz
lib nem annyira alapvető lib
sbin
share egyéb, erőforrás & dokumentum
src forrás, kernelforrás
X11R6 X
local nem a disztribből hanem rendszergazdai telepítésre

Állományok

- fájl (normál) bájtsorozat
- könyvtár
- speciális (device, ilyesmi)
- link hivatkozás
  - hard link 2 fájlnév ugyanazon inode-ra mutat
  -



hard link csinálás: ln

a fájl akkor tűnik meg, ha ∀ hard linkjét töröljük

listázás inode listával ls -il

szimbolikus link: a fájlnévre mutat
készítése ln -s
Különbség: ha töröljük a hivatkozottat, törlődik
de hard link csak partíción belül
történhet.

Jogosultságok

belépéskor megkapjuk az user id-nket és
group id-nket. Az /etc/password-ből veszi
id

A rendszergazda jogait a 0-s id adja meg
/etc/group

Egy fájl csoportid-je a default group id.

jogok/attr
owner group others
d|rwx|rwx|rwx
↑
d, b, c, p
dir bin char pipe

r: olv.
w: írás
x: futtatás/használat

dir
listázható
módosítás ⇒ új bej. törlés
használat, hivatkozhat rá

módosítás: oktális jogmegadás
chmod 754 test1
owner group others
r = 4
w = 2
x = 1

vagy

chmod g-x fájlnév
csoportra x-et leveh

setuid
setgid } egy program a saját owner-ének jogaival fut,
bárki is indította.

Veszélyes, mert ha hibás, ez gyenge pontja
a rendszernek!

jele: x helyett s ill g áll

t sticky bit. Bárki írhatja/olvashatja
a tmp-t, ez viszont lehetőséget ad
arra, hogy csak én vagy a rendszer-
gazda törölhesse a fájlomat.

A spec beállítások:
4: setuid
2: setgid } ?
1: sticky

/etc

aliases : levelezéshez

at. : időzítő
at.deny : ki nem állíthat be
cron időzített feladatok
fstab : milyen fájlrendszerek
mountolódnak ?

időnként a vesélni - legyen-e check
- kritikus ?
Bminek noauto azt alapból
nem mountolja

group
gshadow } csoportinformációk

hosts név - ip hozzárendelés
inittab
Bootprocedúra
1. lilo → kernel elindul.
2. a kernel az inittab alapján indít.
levelx:
↳ lx : wait : mit indítson
respawn
megvárja a végét
újraindítja ha azt

A megadott könyvtárban levő
linkeket elő végrehajtja, ha
S-sel kezdődik a neve: start
ha K-val : stop

issue
issue.net } bejelentkezési üdvözlő szöveg

ld.so.conf
ld.so.cache } dinamikus könyvtárak
(ld van din. link)

modules.conf kernelmodul-info
profile: felhasználói bejelentkezés
alapbeállításai

skel/ kvt. új usernek ezt
másolja a könyvtárába
sysconfig hálózati beáll (ip...)
xinetd.conf internetes szolgáltatásokat
hol indítani igény szerint

mountolás
mount mit hova opciók
mount /dev/fd0
mount /mnt/floppy

df: mi van felmountolva

umount /mnt/floppy   mount leszedése

write cache van ⇒ floppyt umountolni kell

NFS mountolás

mount -t nfs avalon:/export....

Samba:

mount -t smb..

2. 2002. 02. 22

Shell

- input/output átirányítás

> fájl	kimenet átirányítás
>> fájl	kimenet hozzáfűzés
2> fájl	error kimenet
< fájl	bemenet átirányítás
<< string	a bemenetet a bill.ról olvasni a string-ig.

- parancsok kimenetének más parancs bemenetére irányítása
  |

  P du | sort -n

  disk usage sorrendezése növekvő

  különbség átirányításhoz képest
  - nem kell temporary
  - párhuzamos működés
  - kevesebb a helyszükséglet

- parancssorozat p1 ; p2 (egymás után)
  logikai kapcsolat && , ||
  ugyanúgy működik, mint C-ben.
- parancs1 \`parancs2\` visszaidézőjel
  lefuttatja & az eredményt behelyettesíti

- háttérfolyamat indítása

  parancs &

visszaad egy processz ID-t.
A ps-sel ellenőrizhetjük is.
A shellen belül sorszámozza

[shellen belül] pid

signal küldés:

kill

kill -l signal-lista

P: kill -9 | %1
           | 8450

9-es signal (KILL) küldése az 1. shellen belüli processznek vagy a 8450-es processznek

ps saját terminálom processzei
ps x összes processz

háttérbe küldés:

megállítás	CTRL+Z
háttérbe	bg %1
előtérbe	fg %1

Ajánlatos a háttérfolyamatok kimenetét fájlba tenni, mert a kimenet összekeveredik

nohup parancs &

a parancs a nohup.out-ba ír, nem a terminálra, & ha a terminált bezárjuk, nem kap HANGUP signalt.

Shell scriptek

parancsok egymásutánja szövegfájlban.
Van benne C szerű vezérlési struktúrák

x joggal lehet futtatni, vagy

sh script.

grep szűrő

grep XYZ * XYZ-t keres a könyvtárban

Használhatók egyszerű mintákban:

^ sor elejére illeszkedik
$ sor végére illeszkedik
. tetszőleges karakter
* 0 vagy több tetszőleges karakter
\ speciális karakter escape-lése
[ ] karakterhalmaz

változók shellben:

értéke : $változónév
maga a vált: változónév

pl n=`expr $n+1`

export globális környezeti v. lesz

RPM: RedHat package Management

rpm -U csomagnév

installál, vagy ha installálva volt update-l.

csomagfüggőségek is lehetnek.
több csomagot is megadhatunk & nem lesz gond ha a végeredményben a függőség teljesül

--test csak tesztel

--nodeps nem nézi a függőségeket! inkonzisztens lesz, ha nem tesszük fel a másikat sem

-q query, pl

rpm -qRp fájlnév
milyen dependency van?

rpm -qR csomagnév
milyen dependency van?

-e uninstall

-qi csomaginfo

-ql csomagfájllista

-qf fájl mely csomag része?

-qa ∀ installált csomag

rhn.redhat.com
van weben support is.

Installálás forrásból

rpm --rebuild forráscsomagból bináris csomagokat csinál.

Installálás nem rpm segítségével

tar -xzvf fájl

(x: kicsom; z: gzip fájl; v: verbose; f: csomagfájl)

configure
make
make install

Szolgáltatások

a szolgáltatások háttérprogramok (nézzük meg ps-sel)

Mikor indulnak el?

A rc.d könyvtárakban
pl /etc/rc3.d -ban

A fájlnév : S80sendmail

(S: start, K: kill; 80.-ként)

Azonos szám lehet, ekkor mindegy. (lehe szokott lenni)

chkconfig --list szolgáltatások listája
Ezzel lehet konfigurálni is.

A source-ben meglehetnek az indító scriptek, amit ilyenkor csak be kell másolni

Más lehetőség inetd vagy xinetd.
Ez igény szerint indítja el a kiszolgálót.

~~Secu~~

Security

- ~~vagy~~ ne használjunk insecure protokollt (telnet, pop3, nem anonymous ftp)
- ne indítsunk szükségtelen szolg-t.
- LISTEN-elő portok, amiket nem használunk
  netstat -ap | grep LISTEN
- firewall

Anonymous FTP

van egy FTP-user ftpuser.
Ez egy alsóm user, aminek nem lehet belépnie

a xinetd-ben engedélyezzük az ftpd-t, majd restartoljuk.
& az etc/~~ftp~~ports beállítjuk a portot

A configscriptek a /etc/ftpd-nál vannak.

Network File System

/etc/exports ban van benne, hogy nfs-en mi legyen megosztva

mit kinek milyen joggal

/exports (ro) — /exports-ot, mindenkinek read only

Az nfs RPC-n fut, nem külön listen-elő portként

Samba konfigurálás

/etc/samba/~~smb.conf~~ konfigfájl
vagy: webes

Ha titkosított jelszótovábbítást akarunk csinálni, akkor a samba jelszavakat külön fájlban tárolja, mert mindkettő egyirányú, de nem azonos. Lehet szinkronban tartani.

smbclient -L //localhost
aktuális megosztásait

mountolni is lehet

Kell tehát egy smbpasswd.
ezt a mksmbpasswd.sh </etc/passwd >smbpasswd-ből lehet legyártani

Sendmail

SMTP szolgáltatás.
Kézi konfigurálása nem jellemző
inkább a
/etc/mail/sendmail.mc
-ből fogjuk bekonfigurálni. Ezt nem igen kell általában nagyon módosítgatni
/etc/aliases
beállítható, hogy kinek passzolja az adott e-mailcímről a leveleket.
Módosítás után newaliases parancsot kell kiadni

3. 2002.03.01

Apache

/etc/httpd/conf/httpd.conf
apache config fájlja

X

/etc/X11 egér, monitor kezelés.

modeline: időzítésekkel lehet centerezni
segítség: xvidtune
Ezzel még nem-szabvány felbontást is el lehet érni

CTRL + ALT + ± ⇒ képernyőfelbontás-váltás

Viewport: lehet nagyobb képernyőterület, mint a monitor: viewport.
Többmonitoros támogatás is van

Security

1. Nem szükséges szolgáltatások kidobása az indítandók közül
2. ~~Rend~~ Biztonságos protokollokat válasszunk
3. Vigyázzunk, hogy feltegyük a javításokat
4. setuid-okat elvenni, ahol nem szüks.
   korlátozzuk a megbízható userekre a setuid-os programok elérését
5. Határ.

Firewall

1. proxy jellegű routernél van előnye + rendesen feldolgozza a protokollt.
2. Filtering: csomagszűrés adott jellemzők alapján.
   pl {forrás / cél} {cím / port} protokollok

A legegyszerűbb a legbiztonságosabb

Több firewall ~~szoftver~~ volt már

2.2 – ipchains
2.4 – iptables

ip
iptables -L

iptables fájl script
iptables -F flush
van forward, input, output:
drop → accept

ennen minden bejövő & kiszűrendő előbb...

ifconfig:
interfaces: loopback mindig van (local-host) + hálókártyák (eth0)

Kivételek: Mit engedünk:
címek !-vel negálhatunk, & kezdet: vég
megadás: IP-cím / netmask (tartományt ad meg)
IP/... ← netmask
1: minek kell egyezni
0: minek nem
IP/szám ← hány 1-es van a netmaskban

Amire nincs szabály: default policy dönt el.

ESTABLISHED: olyan csomag, ami már TCP kapcsolat része
RELATED: már meglévőhöz tartozó kapcs.
pl FTP-nél a server kapcsolódik majd, ⇒ be kell állítani, hogy engedje (vagy passzív ftp)

Lehet logolni az amúgy eldobandó ~~[illegible]~~ csomagokat.

A /etc/rc.d/init.d-ben megtalálják a beállításokat.
Ennek van egy save parancsa, ami le tudja menteni a beállításokat.

Kernel

Eredetileg azt hívták linuxnak.
Ugyan a disztribúcióban használható kernel van, pl. egy szervernél érdemes újrafordítani

főverzió . alverzió
stabil: páros
fejlesztői: ptl.

2 . 4 .

konfigurálás

menuconfig : konzolos
xconfig : x konfigurálás

make xconfig
make dep dependency-k
make clean : régi objectek törlése
make | Image : binárisított image
| zImage : gzipelt image
| bzImage : bz2-vel binárisított

make modules
make modules_install

A kész kernel megtalálható a forrás /arch/i386/boot/bzImage

be kell másolni az image-t
Azután a liloba be kell tenni.
Rebootolva lehet az új kernelt használni

Kernelmodulok

Kell egy

#define MAJOR-NUM
#define MINOR_NUM
betöltéskor meghívódik az
int init_module(), kiszedéskor a
int cleanup_module()

R/ karakter device-t akarunk csinálni

beregisztrálás:

register_chrdev
törlés
unregister_chrdev

& egy struktúrában adjuk meg, mire mit hívjon.

- open-re & close-re számlálót tartunk benn
printk: kernel-kiírás c-libraryt nem lehet használni

A memóriában az user & kernel space máshol van ⇒ copy-from-user
copy-to-user

kell a -D_KERNEL_ és a ~~-D_Module~~ -DMODULE

mknod test c 100 1
(név; típus (karakteres) opció; major num; minor num)
⇓
kész lesz a modul

insmod hellomod.o
lsmod kiírt modullista

ka127 XP-ből

8. 4.

2002.03.08

kpe/kpeuser **Windows NT**

Kovács Ernő

kovacs.erno@synergon.hu

▸ Inside Windows NT/2000 Solomon
www.win2kmag.com ® Kerosés: Russinovich
tech.net
www.netacademia.hu

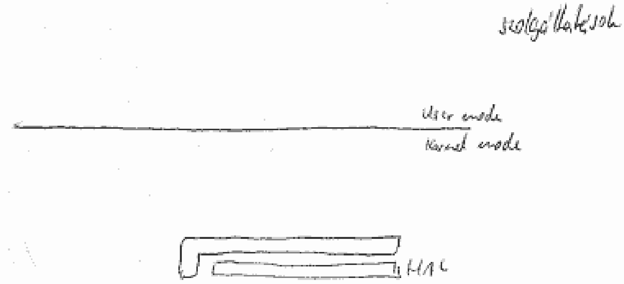
szóbeli vizsga: 1/3 linux + 2/3 WinNT

A Windows NT architektúrája

▸ vannak slide-ok

- DOS
- Windows 3.0 } grafikus kliens
  3.1 } DOS-ra

VAX szgép, VMS opre } - kit megszerezték Dave Cutlert
hogy találja ki ⇒ Windows NT 3
(nem akarták 0 1-ről)
↓
Windows NT 4.0 win95 felülettel
Volt a win95 is. Miért?
Mind több féle hardveren menjen
Tudja futtatni a DOS & Win16-os progikat
⇓
Meg kellett engedni közvetlen HW-kezelést
(→DOS) –
⇓
Nem volt tisztességes opr.
⇓
⇑
NT-n volt Hardware Compatibility List,
hogy eszerint kell: Dell, Compaq.
SW-eknek csak korlátozottabb kezelését enged,
& biztonságosabb rendszert lehetett
felépíteni



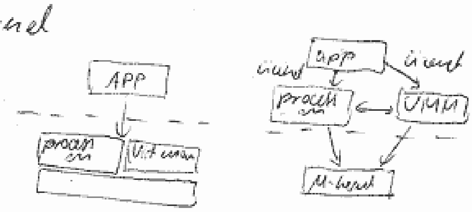
API: Application Programming Interface
Natív interface, Win32 API

- Processzormódok
  - Processzortámogatás
    Ring 0..3 (Intel)
    csak 2 (Alpha)

→ Ring 0: User mode
- Nincs közvetlen hw-kezelés
- Csak bizonyos utasítások mehetnek
- Csak bizonyos memóriaterület

→ Ring 3: Kernel mode
- Közvetlen hw engedélyezett
- teljes mem-kezelés
- teljes utasításkészlet

- Kernel



monolitikus | mikrokernel

⊕ gyors
⊖ nehéz őszerelhető
⊖ ha a kernelben hiba...

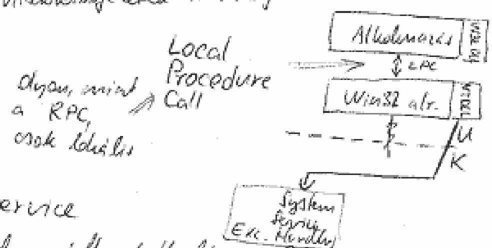
⊖ lassú, mert üzeneteket kell küldeni
⊕ biztonságosabb
⊕ szétszedhető részek

⇓
WinNT-ben kompromisszum

- Felhasználói futtató környezetek
  Linkeléskor meghívási a szolgáltatások belépési pontjait. És a futtató környezetben fordítódik
  - Op. rsz. API
  - DOS, Win16 [~~Kernel, GDI, User~~]

- Win32 (kernel32.dll, gdi32.dll, user32.dll)
- OS/2
- POSIX (psxdll.dll)

• Natív API 200-300 fv.
a futtatókörnyezetek használják.



• System service
Kernel módba kell lépni. 2E sw-megsz.
Egy System Service Table-ből választjuk ki a paraméter alapján, hogy mit kell tenni.

User módú rendszerfájlok

SERVICES.EXE	szolg. irányító processz
WINLOGON.EXE	bejelentkezési folyamat
SMSS.EXE	session menedzser
OS2SS.EXE	OS2 alr.
CSRSS.EXE	Win32 alr.
PSXSS.EXE	Posix
NTDLL.DLL	belső szolgáltatások

:

Kernel módú:

NTOSKRNL.EXE	Executive & Kernel
HAL.DLL	Hordozhatósági [?] rét. processzorfüggőségek megszüntetése α, Intel, 1, több processzor
WIN32K.SYS	3.51-ben minden grafika user módban volt. Lassú volt ⇒ kompromisszum. A Win32 alrendszer lehívása [?] jelentősen gyorsít.

• Executive
I/O menedzser dinamikusan változó része a kernelnek: eszközmeghajtók.

- Object Manager
Objektum minden, ez ~~erőforrás~~, fiz/log. erőforrás
belső struktúrája rejtett
handle ~~[?]~~ ezt tudják adni-venni
megosztás
hivatkozásszámlálás - hányan használják [?]
azonosítás.
Névtér: mint a /dev.

www.sysinternals.com Nem ajánlott a közvetlen használata a natív API-nak, ~~[?]~~... a sysinternalsnál megpróbálták feltárni

A névteret pl a Winobj - dual-lehet megnézni.

pl. a CreateFile(... "C:\readme.txt")
⇓
"\??\C:\readme.txt" lesz belőle, és a \??\C: egy link a harddisk 0-ra...
A ?? alatt vannak a linkek (symlink)

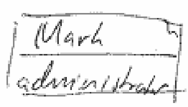
Az objektumhozzáféréseket a Security Manager Monitor ellenőrzi

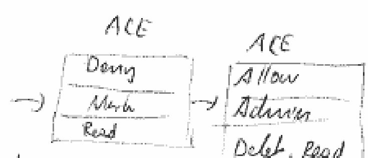
Security identifier SID (a névre [?])

access token (tartalmazza a user & csoportjai SID-jét)

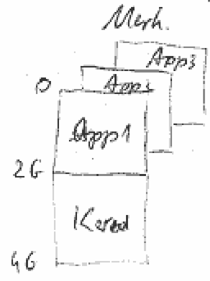
A Discretionary Access Control List-en megadni, hogy azon az objektumon az a user a műveletet végezheti-e.
A C2-es követelményekhez kellett az is, hogy legyen naplózás!!
⇓
System Access ...
-nak milyen dolgait kell logolni

Az első illeszkedést fogadja:





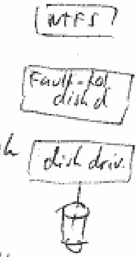
Hiába van engedélyezve neki mint admin, de le van tiltva, mint Mark.



— Virtuális Mem menedzser

fiz - log. összerendelés

- I/O menedzser
  - hw-támogatás
  - kernel módú komponensek
  - dinamikus betölt.
  - rétegezhető
  - kérés aszinkron, mehet a tovább.
  - vannak általános, MS által megírt driverben gyakran használt
  - I/O Request Packet-ben küldik a kérést, ebben minden benne van.



WDM Windows Driver Model
egységes driverfelület nem a driver W98-
W2000
WXP

- Cache manager

  a fájl egy része gyakran bemapelődik a memóriába. Hogy tényleg ott legyen & optimálja a lazy writingot, erre való a C.M. Ezért kell várni a shutdown-ra.
  Az előreolvasást (read-ahead) is intézi.

- Local Procedure Call facility
  Külön futó folyamatok közt.
  A szervernek van portja
  a kliens portot nyit & kapcsolódik.

- Process Manager

  Folyamat:
  PID (azonosító)
  Access Token „útlevél", indítójától kapja
  address map címtábla
  TID threadazonosító
  statisztikák

- Kernel
  → Szálakat ütemez, preemptív, prioritásos.
  → alapszabály: mindig a max prioritású futásra kész processz fut
  de van kivétel kiéheztetés ellen
  → megszakítás & kivételkezelés
  → szinkronizálás
  mutex szemafor [illegible]

HAL
hw-dedikált világra
absztrakt proc
verziók:
1-proc
többproc
debug

Ütemezés

Process
virtuális címtér
PID: egész szám
rendszererőforrások
minimum 1 szál
access token
nyitott kezelők

Job (Win2000-től)
folyamatok csoportosítása, hogy a proc & kernelhatásokat szabályozni lehessen. Pl. hogy az IIS ne vegyen el minden erőforrást.
- user idő
- memória (hely)
- aktív szálak száma

Szál
- az ütemezés alapja
- környezet
  regiszter
  verem (user & kernel módban)
  tároló terület
- egyedi azonosító TID

Szálütemezés
prioritásvezérelt
preemptív
processzoraffinitás (mivel szeret futni)
[NT: szimmetrikus multiproc, bármi bármelyikben futhat]
kvantum: egy thread időszelete
dispatching: ~10-15 ms-onként újraértékelik, ki fusson, ha más jön, ütemezési környezetváltás.

Prioritás 32 szint

[31 … 16] realtime processek

[15 … 1] alkalmazói programok innen indulnak, változhat, a sz. is változtatja, mi is

[0 – nullázza a felszabadított lapokat (C2-es követelmény)

Folyamatok prioritási osztályai

Idle – 4
Below normal – 6
Normal – 8
⋮

& vannak relatívak +2, +1, 0, −1, −2

– Időszeletek & Quantum

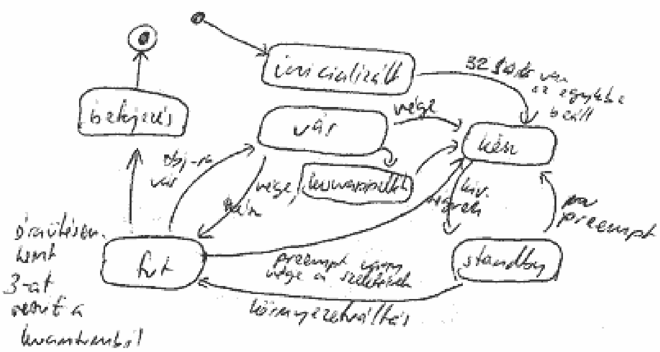
3egys / óraütés — időosztó miatt

WinNT
- NT Workst. 6e – 2ms (hátha ki szolgálja)
- NT Server 36e – 120ms
- Prioritás ↗ priority boost

Win 2000
- Változó / Fix (előtér-háttérproc köz. van-e külö)
- Rövid / hosszú (milyen kvantumhossz)
- prioritás ↗ priority boost (ennyivel nő)

A előtérben futó prog. nem a prioritást növeli, hanem csak ő futhat, csak az időszelete nő.

„Ezt szoktam szeretni kérdezni"



hogy ki jön ha a ~~…~~ ~~…~~ waitből kijönne, a prioritás adja meg
ha magasabb fut, a ready elejére (!) áll

~~…~~ a kvantumhoz nem veszti el, csak óraütéseket.

Ütemezési lehetőségek

önkéntes lemondás
- wait-be megy & büntetőpontot kap, 1 kvantumot levonnak

lejárt az időszelet
- a sor végére, ha elfogy a kvantum

preempció
- a sor elejére

Ütemezés
- új szál futásra (ready)
- abbahagyja a futást
- prioritás megváltozik
- szálaffinitás megv.

Context switch
regiszterek, ut. szám, ~~…~~ ut. szám, veremmutatók…

Szál ütemezés ~~megnyitása~~ módosítása

Időszeletnyújtás
- előtérben levő alk. időszelet ↗

Prioritásnövelés I/O mű után
- felnyomja, majd egyenként visszacsökken. Hátha bekéri & waitbe megy minél előbb.
- de nem lépi át a realtime határt

Prioritásnövelés GUI száloknál

Prioritásnövelés kiéheztetés ellen
- pár másodperce nem futott szálak ideiglenesen feldobódnak 15-re, aztán vissza. Kapnak dupla időszeletet is.

Korszerű operációs rendszerek

5. 2002.03.22.

□ Virtuális memória

Címtér 32 bit → 4 GB-os tartomány

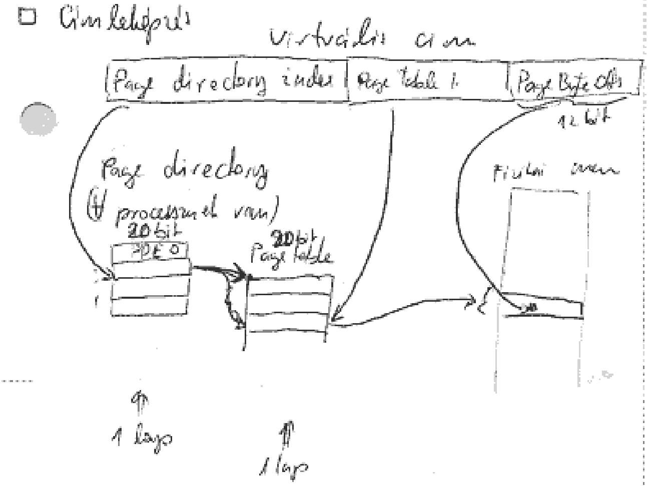
Ez logikai cím.

Mindegyik processz számára 4GB látható, ennek egy része kernel, más része user.

□ Fizikai memória

Lapokra bontják, a 4kbyte-os lapok 12 bit

□ Címleképzés



Ha az adott laphoz nincsen fizikai mem. lap, hanem van a lapozófájlban, be kell hozni

• Translation Look-Aside Buffer

asszociatív gyorstár.

Page directory ind. page table ind → page frame #

□ Address Windowing Extensions

ablakot lehet csinálni & azon keresztül bemappelni memóriát, így 4GB-os korlát feloldható

□ Physical Address Extensions

Plusz egy indirekció.

page directoryból 4 van, & az első 2 bit címzi

Így több lehet a fizikai memória

□ System Memory Pools

• Kernel:

- lapozható (minikernel, device driver)
- nem lapozható (nem lehet swappelni)

□ Laphibák (Page fault handling)

A Page Directory Entry & Page Table Entryben van valid bit. Mikor nem érvényes?

- page file
- demand zero
- transition
- unknown

Ha ilyenre hivatkozunk → laphiba-kivétel

Behozza valahová, és az új pointerekkel feltölti a táblákat. Addig ott van függőben

Page Table Entry

Page Frame Number

Flagek

Valid - (paging required?)

Owner - (kernel / user mód)

Protection - (write or read-only)

Copy-on-write (csak akkor másolja le, ha valaki módosítja)

Accessed - (hozzányúltak mostanában?) ki kell-e írni addig amíg a lap…

Dirty - (módosult-e)

□ Memória használatba vétele

• Reserve: PDE, PTE bejegyzések feltöltése
• Commit: ténylegesen fiz. mem-t foglal
• Decommit: fiz. felszab.
• Free: ténylegesen felszabadít mindent.

□ Címtartományok (Virtuális)

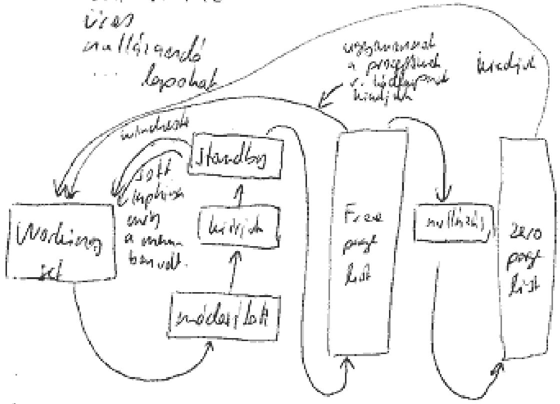
Egy fa-szerű szerkezet, megvalósítja, hogy a virtuális címtartományban hol vannak üres helyek

□ Memórialapok: Copy on write

csak olvasott mem, csak ha valamelyik módosítani akar, akkor másol

□ Working set
- Fizikai memória adott processzhez tartozó része
- minimum–maximum meghatározható
  a maximum túlléphető, ha korlátozatlan fizikai memória van.
- Page Fetch policy
  Mikor vegyem használatba a fiz. mem-t?
  - Demand paging: 2 lépésben, csak ha kell. lerak
  - Prefetching:
    Ne kelljen laphibák sorozatával indítani. Előre behoz többet
  - NT: Clustered Demand paging
    Alapjában tölti be a lapot.
    De nem biztos, hogy sorban tölt
    ⇓
    XP eltárolja, hogy milyen sorrendben szokta behozni a lapokat.
- Page Replacement Policy
  Kitől veszük el a lapot.
  - local: ~~a progra~~ ugyanattól a programtól veszi el a lapot
  - global: bárkitől
  ~~Kitől vesszük el azt~~. Melyiket vegyük el
  - FIFO
  - LRU Least Recently Used
    Accessed bit alapján: melyiket nem néztük már rég

□ Fizikai memórialapok állapotai
{Valid (active)} Dirty/Clean
Page Frame Database
Láncba fűzve
üres
nullázandó
… lapokat



Modified No Write állapot
Ne legyen automatikus kiírás

□ Memóriába ágyazott fájlok
a fájlkezelő úgy tesz, mintha, hogy a fájl tartalmát memóriába ágyazzák

Prototype PTE kell.

Megszakításkezelés

- Alaplapon ∃ interrupt controller
- Eszközmeghajtó (Device Driver) bejegyzi magát
- Interrupt service table x interrupt beérkezésekor hová ugorjunk
- Interrupt Service Routine kiszolgálja a megszakítást

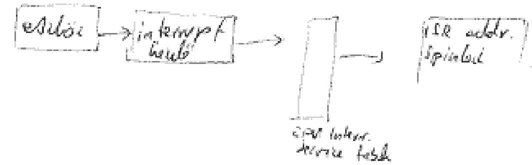
- A Windows ezt leképzi 32 megszakítási szintekre lepri le. Ezt a HAL végzi.

- Magasabb szintű megszakítás megszakíthat alacsonyabb kiszolgálórutint.
- Az idő legnagyobb részét a 0. passzívban van. Feljebb rövid időt tölthet

30. Power Fail
29 Inter Processor Interrupt
28 Clock
27 Profile-olás
26-3 Device n... 1
2 DPC/dispatcher
1 Asynchronous Proc. Call
0 Passive

HW int (30–3)
DPC/dispatcher ← ütemezés, Deferred Procedure Call: ha ide lesz, mit legyen. Ez egy queue
Asynchronous Proc. Call ← Processzek közti hívások e 10 min. egyéb így végzi

Megszakításkezelés



A tényleges feldolgozást DPC-ben adom ki, hogy ne maradjunk ezt magas szinten

Miért? Mert DPC csinálja a threadváltást.
Azaz 2 fölött ha talált olyat, ha ilyenkor page fault van, vagy
IRQL_NOT_LESS_OR_EQUAL

Korszerű operációs rendszerek 6

Kivételkezelés Exception dispatching

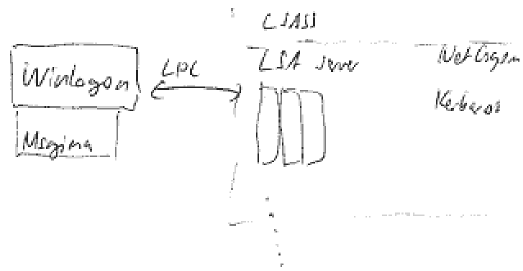
- Szoftverből indítják
- Strukturált kivételkezelés try-catch egymásba ágyazható.
- Kezeletlen kivételek (Unhandled exception)
  - User programban nem lehet, mert eleve be vannak ágyazva az NT hibakezelésbe.

Sorrend:
- Debugger, megkérdi
- Program saját catch-e
- Debugger ténylegesen
- Oprendszer

- Rendszerszolgáltatások is így történnek meg. Amikor kernel módba lép, az exception 2E meghívás. A regiszterben van, hogy melyik hívás.

Biztonság

- Security Reference Monitor
  ez dönti el, hogy az adott proc hozzáférhet-e egy erőforráshoz.
- Local Security Authority Subsystem LSASS
  Service
  biztonsági adatbázis
- Security Accounts Manager
  Service
  DB
- Active directory
- Winlogon
- Authentication packages: Kerberos
- Graphical Identification & Auth. GINA
  Ez jeleníti meg a bejelentkező ablakot
  ki lehet cserélni (ez trójaira ad lehetőséget)
- NetLogon Service hálózati belépés



SID: Security IDentifier
Változó hosszú strukturált azonosító

S-rész1-rész2-...
Verziószám
kiadó azonosító
relatív azonosító

P: Domain Admin
S-1-5-21- . . . - . . . - . . . -512
Everyone csoport
S-1-1-0
Creator owner
S-1-3-0

Amikor a felhasználó bejelentkezik, létrehoz egy access Tokent.
- SID-jei, csoportazonosítók, aminek tagja
- privilégiumai (shutdownolhat...)
  P: Backup Admin olvashat bármit
- default primary group.
  Egy létrejött doksi melyik csoporté legyen
  csoport, hogy lehessen több admin
- default DACL
  alapjogok (default)
- Lejárati idő, utána újraosztálják, nem kell emiatt ki-be lépni

Megszemélyesítés
- más nevében hozzáférünk
- bejelentkezéssel, pl. linuxos su.
- vagy bejelentkezés nélkül.

Megj.: A hívó folyamatnak átrakhatja
A megszemélyesítő foka: (a hívó folyamatnak használata)

Anonymous - csak saját
Identification - csak olvasom, nem használom
Impersonalization - belső esetben használom
Delegation - kívül is használom

Nem biztos, hogy jó magasabb jogot biztosítani egy szerverfolyamatnak ⇒ ki lehet lopni jogot a folyamatból

Biztonsági leíró - Security Descriptor

⋮

ACL: Access Control List
ACE: Access Control Entry

ACE típusok

Általános
egész objektumra
öröklődés (szülő - nem szülő)

Objektumspecifikus
egyes tulajdonságokra is van jog
öröklődik obj. típus szerint is.

Öröklődés

- új gyermek objektum létrehozásakor
- szülő jogváltozásánál ~~módosít~~ módosításakor

Öröklődjelzők:

INHERITED_ACE — öröklött tul.
INHERITED_ONLY_ACE — öröklődik, de ide nem vonatkozik, csak tovább továbbítja
CONTAINER_INHERIT — containerek öröklik
OBJECT_INHERIT — objektumok öröklik
NO_PROPAGATE_INHERIT_ACE

Naplózásjelzés

sikerest naplózzuk?
sikertelent naplózzuk?

Kanonikus sorrend (jogok)

Az első
- rám vonatkozó
- jogosultságban engedő
- + általánosra
• először explicit, utána öröklött
• először tiltó, utána eng.
• először közvetlen öröklött utána távolabbi.

2002. 03. 29

Bejelentkezés

• NT: LAN manager.
felhasználónév + 7 chr-ra hashelt jelszó
⊖ Brute force-~~al~~ szal feltörhető
⊖ Csak klienst azonosít

• Win2000, XP Kerberos
Kulcskiosztó központ Key Distr. Center
Jegyalapú, jegyet kérek, & azzal léphetek be.

- Kliens azonosítja magát & kap egy jegyet a jegykéréshez (ticket granting ticket)
AUTHENTICATION SERVICE EXCHANGE AS
- TICKET GRANTING SERVICE EXCHANGE TGS
megkéri a jegyet a szolg-hoz CS
- CLIENT SERVER EXCHANGE

K: hosszútávú kulcs
S: kapcsolatkulcs

AS

KRB_AS_REQ
{TGT kérés
K_A (adatok, időbélyeg)} ⟶ kliens hitelesítő

KRB_AS_REP
{$K_A(S_A)$, adatok ← hitelesítő
$K_{TGS}(S_A$, jegyadat)} ← TGT

TGS

KRB_TGS_REQ
{Jegyet kérek B-hez;
S_A[adatok, idő];
TGT}

KRB_TGS_REP
$K_A[S_{AB}]$, adatok
$K_B[S_{AB}$, jegyadat] — szolgáltatásjegy

CS

KRB_AP_REQ
{S_{AB}[adatok, idő],
$K_B(S_{AB}$, jegyadat)]
KRB_AP_REP
S_{AB}[idő]

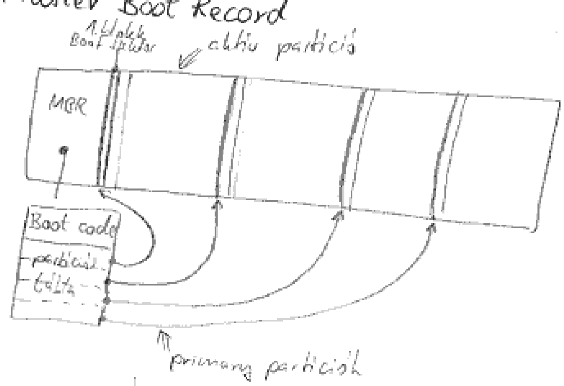
⊕ Egy ideig a jegyet még felhasználhatom, nem kell újra & újra kitelesíteni; csak néha.

Rendszerindítás

☐ Szükséges fájlok
- System partíció
  - NTLDR
  - Boot.ini
  - Bootsect.dos
  - Ntdetect.com
  - Ntbootdd.sys   Nem-BIOS-os lemezkezelés bootolás
- Boot partíció
  - Ntoskrnl.exe
  - Hal.dll
  - SYSTEM hive
  - Eszközmeghajtók

1☐ Power-on Self test
BIOS-indítás
Memória
Video
billentyűzet
stb.

2☐ Master Boot Record



3☐ NTLDR
A bootszektorban levő kód a gyökérben levő NTLDR fájlt betölti & elindítják
A BIOS lemezkezelését használja, annak korlátaival.
Ezen segít az Ntbootdd.sys

Az NT

Az NTLDR
- Real módban indul, de azonnal átvált 32-bit védettbe
- Mini-fs csak olvasható de látja a könyvtárak

☐ Boot.ini (opre. választás)
- ARC path. Hol van a partíció?
  → multi / signature / scsi ()
  ide, & BIOSsal — hova eszköz azonosító ⊛ — hanyadik (0-tól)
  → rdisk () ↑ ha scsi, hanyadik ? rajta ?
  → disk () ↑ ha ide, hanyadik rajta ?
  → partition () ↑ hanyadik partíció (1-től!)

⊛ ha signature, akkor kell neki a spec driver: Ntbootdd.sys
→ kapcsolók

5☐ Hardver detektálás (ntdetect.com)

6☐ Konfigurációválasztás
- ~~ha több konfiguráció van választhat~~
- ~~last known good~~
LastKnownGood Az utolsó jól bootoló konfighoz vissza lehet térni. akkor jó ha valaki be tudott jelentkezni.
→ Ne jelentkezzünk be ész nélkül

7☐ Kernel indítása
- Ntoskrnl.exe betöltése
- Hal.dll bet.
- Registry SYSTEM hive betöltése (registry)
- Konfiguráció (hwprofil) választás
- Eszközmeghajtók (BOOT_START)
- Ntoskrnl.exe indítása

8☐ Kernel inicializálása
- Executive rész indítása
- Eszközmeghajtók indítása (BOOT_START)
- Eszközmegh. bet + ind (SYSTEM_STAR-

• Session Manager Subsystem indítása
- BootExecute
  Amit indításkor el kell indítani, pl. checkdisk
- Win32k.sys
  → win32k.sys ← kernel módú
  → Win32 alrendszer csrss.exe ← user módú
  → winlogon
    ◦ Service Control Manager
      szolgáltatások betöltése
      (services.exe)

□ Eszközmeghajtók & szolgáltatások betöltési sorrendje
◦ Start
- SERVICE_BOOT_START (0)
- SYSTEM_START (1)
- AUTO_START (2)
- DEMAND_START (3)
- DISABLED (4)

• Group: csoportba lehet sorolni
• DependOnGroup: betölthető, ha a csoport egyik tagja már benn van
• DependOnService
  adott szolg. már elindult, akkor indulhat.

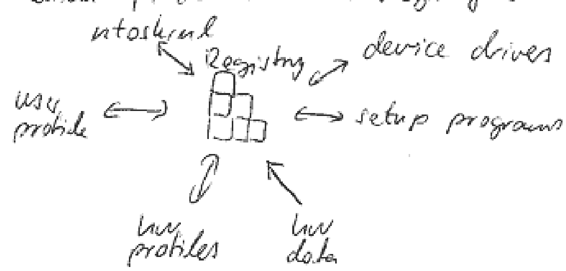
□ Hibakezelés
• Ignore (0) – semmit nem tesz
• Normal (1) – Warningot ad
• Severe (2) } – újra kell indítani
• Critical (3) }

8D Bejelentkezés
LastKnownGood

Registry

□ Configuration Manager
• Registry
• Vezérlőpult (Control Panel)
• Házirendek (Policy)
• Hardver profil (Hardware Profile)
• Felhasználói profil (User profile) ← ntuser.dat
• Registry Editor (regedit ...)

A házirend & a felhasználói profil külön fájl, de beíródik a registrybe



• Hierarchia
gyökérkulcs / kulcs / alkulcs / érték

• Adattípusok (12 db)
- REG_SZ string
- REG_EXPAND_SZ behelyettesítős %..%
- REG_LINK
- REG_DWORD 32-bites egész
- REG_BINARY

• Gyökérkulcsok
- HKEY_CLASSES_ROOT
  → fájlkiterjesztés-hozzárendelések
  → com komponensek
    GUID-okkal
    név–GUID hozzárendelés az osztályokhoz
    így lehet objektumot csinálni
  ⇒ CLSID / Guid-ok / infók a com-ról
    mit kell betölteni
    Így 2 lépésben megkapom az infót (1 név → GUID, 2 GUID → infók)
- HKEY_CURRENT_USER
  felhasználófüggő beállítások az ntuser.dat-ból.
  igazából a következőre link
- HKEY_USERS
  Aki épp bent van, meg a default.
  & mindenkinek a SID-je K. (security ID)
- HKEY_CURRENT_CONFIG
  Link a HKEY_CURRENT_MACHINE egy részére
- HKEY_PERFORMANCE_DATA
  Nincs az editorban, de olyan kéréseken hozható le

→ HKEY_LOCAL_MACHINE

→ HARDWARE

Amit indításkor az ntdetect látott, nem menti el.

→ SAM

User adatbázis (a helyi, WinNT-ben az összes)

→ SECURITY

→ SOFTWARE

Softverek konfigurációja (maga az oprs is)

→ SYSTEM *

□ Hol van a registry?

- %SystemRoot%/config-ban

HKLM/System
SAM
SECURITY
SOFTWARE
HARDWARE (ez nem íródik újra)
HKCU / UserProfile
HKU /.dat

Fájlokban vannak eltárolva.

→* System

Ebben van, hogy a rendszer elindul-e vagy nem, meg ilyesmi.
Ebből van több is → LastKnownGood

Terminal Server

- Többszörös interaktív bejelentkezés (multiple Interactive Logon)
- Vékony kliens
- Remote Desktop protocol

↓

Meg kellett többszörözni a rendszer egyes részeit.

4 Terminal Sessionok saját Win32k-t kapnak & egy másik videokezelést.

Tsharedd.dll könyvtárba rajzol, nem a monitorra.

tobb van belőle:

winlogon.exe
csrss.exe
Win32k

Persze a kódlapokat meg lehet osztani

Egyéb módosítások:

Object Manager.

Névtereket kellett kialakítani (felhasználóként külön vannak objektumok)

Registry

HKEY_USERS
HKEY_CURRENT_USER

7. 2002.04.05.

I/O alrendszer

Az I/O alrendszer

WDM WMI | PnP | Power manager | I/O manager | ← user / kernel managed
driverek
HAL ↑ ← driver

minden driverhez ∃ inf fájl.

A driverek kernel módban futnak ⇒

.cat fájlokban tárolják mit szabad t-ni

□ I/O rendszer

- I/O menedzser

Csomag alapú (IRP I/O Req. packet.) önleíró, minden benne van, ami kell

- File objektum

fájlműveletre képezi le belül, mint unixban (virt. fájlok)

- Driverek

- class driver: általánosabb funkciók, más driverek hívogatják

- port driverek: általában a MS adja, & kissé specifikusabb. (pl. hogy SCSI, ATA)
  Z disk, egér, billentyű közös funkc.

- miniport driverek: csak a hw specifikus részt kell ebbe tenni.

- Device object
  a vezérelt objektum

□ I/O request

User mode API
↓
I/O sys. services API
↓
I/O manager
↑↓ IO Request Packet
Kernel módú driver
↓
HAL rutinok
↓
HW

Az I/O kezelés aszinkron. Nem várja be az eredményt. az más dolog, hogy a programomban inkább bevárjuk.

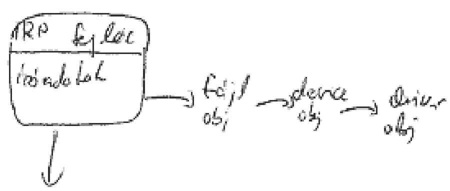
□ I/O layers: rétegszerkezet

a driverek rétegezhetők, pl a fájlrendszer támaszkodhat a lemez driverre.

Ilyenkor egy másik IO Request Packetet IRP-t küld vissza az I/O menedzsernek, ami továbbküldődik a másik drivernek.

Bejöhet még egy szint pl amikor raid szintet is beilleszthetünk (Fault Tolerant Layer)

□ IRP szerkezete



driver szerkezete

rutinok
indítókód
interruptkezelő
késleltetett végreh. rutinok

I/O completion port
Arra van, hogy blokkolhassunk.
Akik erre a portra kapcsolódnak (th adat) blokkolódik, amíg vége nincs.
LIFO módon vagy, talán azokat még nem swapolták ki.

Ha kész van az I/O, interrupt

A thread kimegy magas interrupt szintre. elvégzi a legfontosabbakat. utána ~~letolt~~ a lejjebb a szintet.
Amikor a DPC-re kerül, elvégzi a maradék műveleteket.

Visszaadja a driver az IRP-t APC hívásokban, hogy a saját magán ~~nevében~~ fejezhesse be. (callback fv)

Ha szinkron oldom meg akkor
az I/O manager, ha aszinkron akkor az user módú program callbackjét hívják.

□ Az IRP stackmérete
az IRP stack-ban épül ki.
Egy visszatérési hosszú adni, mit bennemaradunk a magasabb szintű részek is.

Szintezett IRP
Nem az előbbi IRP-hez ugyanazt nem küldi ki

Storage management

□ Storage system

disk
└ 512 bájtos szektorok
  esetleg clusterek, ha a

partíció: összefüggő diskterület
  primary: indítható
  extended

volume (kötet)
  partíciókból álló egység

drive: egy volume betűjellel
  Win32 számára

MBR part. tábla + kód

□

- Disk class driver
  - disk.sys
  - közös funkc.
- Disk port driver — közös port + miniport
  - IDE : pciidex.sys, ↓ atapi.sys
  - SCSI : scsiport.sys
- Diskte miniport driver
  - készülékfüggő, ha van.

□ Partíciók 1,2,3... 0: teljes disk

A betűjeleket a Win32 számára a \\??\ névtér biztosítja.
pl.

\\??\C: ⇒ \Device\Harddisk0\partition1\...

A konverziót az Object menedzser végzi.
Ha persze linket talál, akkor át kell adni a megfelelő drivernek

□ Hibatűrés & más dolgok ft-sys

- A fájlrendszer & disk driver közé beépül a filter driver
  - Más is bejöhet ide, pl a diskperf, azaz performance monitor.
- Spanned Volume (régen: Volume set)
  - több partíciót összevonunk 1 betű alá.
  - Max 32 lehet egy betű alatt
  - szoftveres megoldás, nem lényeges milyen disk, akár mindhakon is lehetnek.
  - NTFS-t már lehet újraformázás nélkül is bővíteni Dynamic disk esetén.
  - Kivenni már nem lehet, csak ha szétszedjük, de az egész elvész
- Mirrored Volume (régen Mirror)
  - Valójában RAID1
  - 2 db azonos partíció kell neki.
- Striped Volume (Stripe set)
  - RAID 0 3-32 lemez,
  - 64 kbyte-os egységek vannak

közös fájlrendszere van, utólag mérete nem módosítható.
(tükrözni lehet utólag)

- Raid-5 Volume Stripe set w Parity
  - minimum 3 partíció kell

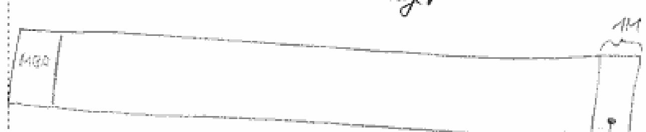
⚠ Ezek mind az NT-be beépített szoftveres megoldások, de kizárólag a Server változatokban lehet őket használni.

□ Basic disks (DOS-ból örökölt)

A legegyszerűbb dolog a
DR0 (diskből)
DP(1)0x...-0x...+2 az egyik partíciója
Partition1 link erre ↑
módosításhoz reboot kell

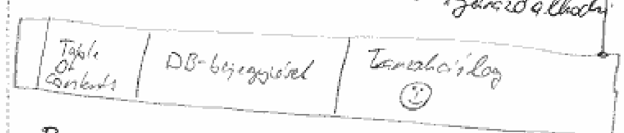
□ Dynamic Disks

Felváltja a MBR-es prim/ext dolgokat.
Nem kell reboot
LDM Logical Disk Manager



partíció DB

Van egy régi fajta ~~(mint a~~) A BIOS miatt meg kell tartani.
Ezen a partíción belül lehet „garázdálkodni"



Bejegyzések

- Disk entry
  - Alapesetben 1/disk. Külön ...-rel több is disk is együtt kezelhető
  - név, guid, ...
- Volume entry
  - Név, ID, állapot (aktív?), méret, GUID, DriveHint
- Component entry
  - Név, ID, szülő
- Partition entry
  - név, id, parent id, disk id, start, size
  - Volume

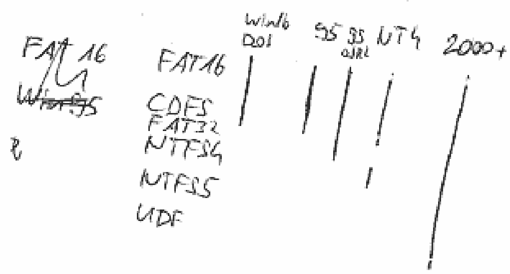
☐ Betűjelölés

- default:
  - primary M, prim S, sec M sec S
  - aktív partíciók C, D, ...
  - extended partíciókon logikai drivek
    ak G, H, I
  - maradék partíciók
    pl. L, M...

Azaz ha beteszek egy másik lemezt, nagy bajok lesznek, mert elcsúsznak.

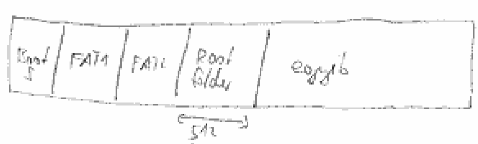
- letiltás: Disk management

☐ Fájlrendszerek:



☐ FAT16

- max 2^{16} cluster
- 512-64K / cluster
- méret 32MB - 4GB



16 bites mutató a fájl elejére a fatban, a fatban lánc

8 név
3 kiterjesztés
létrehozás
last access
last modified
size
} directory bejegyzés

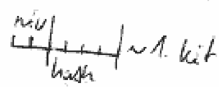
☐ FAT32

- 2^{32} clusterszám
- 512-32K clusterméret
- 512MB - 32GB formázható
  Az előbbi határt nem engedi
  max fájlméret 4GB mert nem férne be a méret mezőbe
- Hosszú fájlnevek:
  Kicsit hamis bejegyzéseket csinál
  13 karakterenként csinál bejegyzést
  unicode karakterenként.
  ~~Ezek Azt, hogy~~
  Ezeket hamis, értelmetlen attribútumkombinációval látja el, amitől a régiek nem listázzák ki.
  ⊖ limitált a gyökérkönyvtár bejegyzésszám
  – a fájlnév része
  ez meg zabálja

A rövid fájlnevekhez leszedi a pontokat ~~a maradék~~ & ~~mást~~ nem alfanumerikus karaktereket,
első 6 karakter ~ szám, kiterj.

1-4-ig.

Ha eléri a 4-et,



A 8+3 neveket NTFS-ben is generálja a régi progrok kedvéért.

☐ NTFS

512 B - 4K Cluster size
2 TB Volume size
64 bites cluster-címzés

- Beépített biztonsági rendszer, ~~ebből~~ futó rendszerről nem kiírható meg
- Több stream lehet 1 fájlban, a hivatalos default mellett neveztetett

fájlnév : streamnév

A fájlon kívülről

Word doc meg compound fájl
fájl a fájlban

• NTFS 5 óta: reparse point.
Olyasmi, mint a soft link.
Átvisz egy másik névtérbe.

• Change journal (NTFS5)
(opcionálisan)
Callback lehetőség van rá, változásra,
de a win-be nincs beépítve

• Sparse file support
Nem használt fájlrész csupa 0-val feltöltve. Gyakorlatilag csak a nem 0-s része van tárolva.

• Quota / Kvóta

• Tömörítés (transzparens)
Distributed link-tracking
(a linkek megtalálhatják az áthelyezett fájlt.)

□ NTFS4
• Metafájlok

0. $MFT — Master File Table.
Önleíró adatbázis, fájlonként 1 kbyte-os bejegyzések.
~~Töredezettség~~
Töredezettséget elkerülendő a disk elejét nem használja, amit nem kell.
Viszont a mérete monoton nő!
(bár azért a nem használtat újra felhasználja)

1. $MFTMirr — Ha A file eleje is benne van, ha kicsi, akkor az egész.
Tükrözi az első részét az MFT-nek (a metafájlok adatait)

2. $LogFile — Tranzakciólog

3. $Volume

4. $AttrDef — milyen attr. vannak

5. $ — Root dir

6. $Bitmap — Cluster map (free/used)

:

□ NTFS5

- $Extend — Opcionális dolgok
  - $ObjId — Object Id file
  - $Quota — Quota fájl
  - $Reparse
  - $UsnJrnl — Change journal
- $Secure — közös security leírók

□ MFT rekord

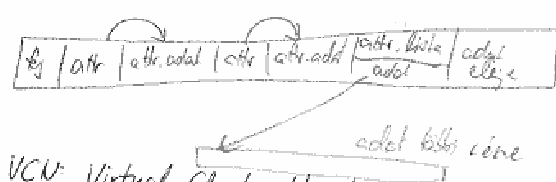
- fejléc
- attribútumok nevei & kezdőpontja
- attribútumok értékei

Rezidens attribútumok a bejegyzésben vannak, nem rezidensekre hivatkozás.
Több ~~futamból~~ is állhat (nem biztos hogy összefüggő)

NTFS attribútumok

Standard Information
szokásos info (mindig rezidens)
attriblista (milyen attrib-ok vannak & hol)
fájlnevek (rövid & hosszú, hard linkek esetén több név)
Security descriptor 4-es NT-ben, 5-ben közös helyen
adatstreamek
Object ID a distr. link trackinghez
Reparse Point.
Index Root
kezeli a könyvtárak esetén B+ fában
Bitmap — milyen clusterek foglaltak

8o 2002.06.12



VCN Virtual Cluster Number
Virtuális clusterszámozás (hányadik a fájlon belül)

LCN Logical Cluster Number
hol kezdődik a run-a & milyen hosszú

A könyvtárak az indexfákban vannak.
Ezek már név szerint rendezettek,
& itt megvan a Standard Info másolata.
Ha nem fér a bejegyzésbe, akkor ez is ki lóghat.

Security

$Security metafájlban van NTFS-ben a security információ.

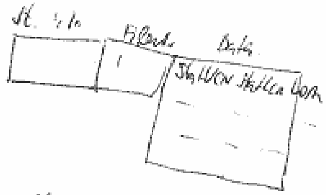
Megvan minden jelenlegi kombináció, & ha az új fájl is ilyen, akkor nem kell még egyszer létrehozni.

$SDH Security Descriptor Hash, indexelt, hashtábla, itt megkeresheted, van-e olyan, amit létre akarsz hozni

$SII ID, ami a Security Descriptor eléréséhez kell.

$SDS Security Desc Stream magukat a descriptorok

Tömörítés



16 clusteres egységet próbál tömöríteni & a futamoknál már úgy tárolja, más lesz a VCN & LCN hossz

Reparse Point

Könyvtáron v. fájlon van ilyen, & ez átmutat valahová máshová, ahol további feldolgozható a feloldás, mint egy symlink.

Mountolás is így oldható meg.

Ugyanis átadható másik partíciónak is.

Ezek

Junction (könyvtár linkelése)

Symbolic link

Az UI-n lehet mountolást csinálni, junctiont, szimbolikus linket nem lehet csinálni, csak külső utilityvel.

A FAR managerrel pl lehet hard linket is csinálni

Quota NTFS-től

Felhasználónként lehet beállítani, kötetenként

1 – ha túllépi, nem tud terjeszkedni

2 – beállítható warning level

Distributing Link Tracking

probléma: a link fájlok „alól kihúzható" a fájl.

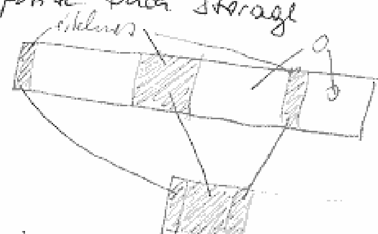
Link létrehozásakor az object ID-re hivatkozom, nem az MFT bejegyzésre.

Ha mozgatják, updateli a hivatkozásokat

alapértelmezésben kikapcsolt

! Fájlrendszerenként

Sparse Data Storage



! A töredezettség így sokkal jobban kijön!

Volume Change Tracking Journal

Egyéb adatstreamek

fájlnév:streamnév

EFS Encrypted File System

⚠ vagy titkos vagy tömör.

128 bites kulcsot generál, DESX szimmetrikus kulcs

File Encryption Key: FEK

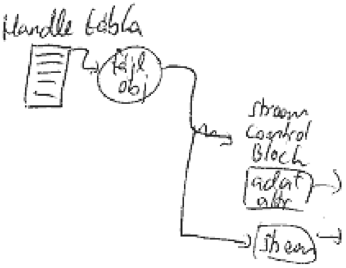
A FEK-et a felhasználó publikus kulcsával elkódolva teszi le a fájl mellé

Data Recovery Field: DRF

a FEK a Recovery Agent kulcsával is ott van

NTFS struktúrák

Handle tábla



Jogok: NTFS 4:

Full Control: a fájlokat is mindenféleképpen le lehet törölni

Csak engedélyező bejegyzések + noaccess

RWXDPO

P ← Change Permission

O ← take ownership

- Az ownernek mindig jár P jog, akkor is, ha nincs bebillentve a bit.
- Ownerséget csak venni lehet, adni nem. (nincs chown)
- A take Ownership joga mindig megvan az Administrators csoportnak

⚠ Azaz, ha elveszem, nem adhatom vissza ⇒ nyoma marad.

Standard jogok:

Könyvtárra

No Access, Read, Add, Add & Read...

Fájlra ...

A különböző csoportokhoz kapcsolódó jogok összeadódnak NTFS 4-en.

Mivel átnézte az egész ACL-t, kivéve, ha közben no accesst talál, mert akkor minden megtagadva.

De így nem lehetett személyre & jogosultságot szelektíven jogot elvenni.

NTFS 5

Sokkal több jog. Tiltó & Engedélyező is van, de pl külön 3 jog a tartalom, standard & extended attribútumra

Öröklődik, de az öröklődés blokkolható is (lehet letiltani)

Pali

Auditing: ugyanolyan mint csak nem engedélyt ad meg, mikor engedje, hanem hogy mit kell logolni

Mi lesz a jogokkal másoláskor!

~~Kötetben belül~~: a ~~szülőben~~ álló mappa jogosultságait kapja

Mi lesz mozgatáskor

Köteten belül

saját jogok megmaradnak, de az új könyvtárból öröklöl

Kötetek közt

mintha letörölném & másolnám

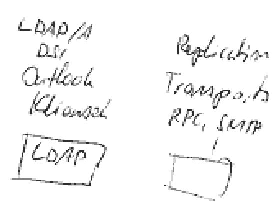
A tömörítés bit hasonlóan módosul másoláskor & mozgatáskor.

Az administrator futtathat más felhasználó nevében programot, de csak, ha megadja a jelszavát.

Active directory

Központi adatbázis, ahol a beállítások, információk (felhasználókra) tárolhatók.

Relációs adatbázis az alapja, azonban fastruktúrát mutat.



□ Active Directory objektumok

Object Class

- Users
- Groups
- Computers
- Printers

Attributes

Schema: Milyen attribútumai vannak (mi az hogy kül. obj-oknak milyen attribútumoknak kell lennie)

□ Organization Unit - olyasmi, mint a könyvtár

Ezek hierarchikusan egymásba ágyazhatók.

Egy obj Distinguished Name-je a teljes path + név

Relative Distinguished name: csak a név.

Nyilvánvalóan ezek egyediek, a RDN a saját konténeren (OU) belül egyedi, a DN pedig az egész domainban egyedi.

Egy ilyen név:

DC=hu, DC=bme, DC=aut, ~~DC~~ OU=Users, OU=Sales, OU=Managers, CN=Jane Doe

Van neki GUID-ja is, és ez nem változik ha név & a helye változhat

□ Fák & Erdők: Domainközi kapcsolatok

Egy Domain 1 egység.

Domain Controllers (DC) (Tartományi vezérlők)

tartalmazzák az Active Directoryt.

A szinkronizálást folyamatosan fenn kell tartani.

NT4-ben voltak SAM-ek, aminek a fő példánya a ~~Master~~ Primary DC-n volt, ezen módosítanak, majd értesít.

Win2k-ban viszont elosztott.

A Domain lehet (natív) (egy fajta), vagy (mixed) ha van még NT4-es domain controller is

□ Szervezeti egységek

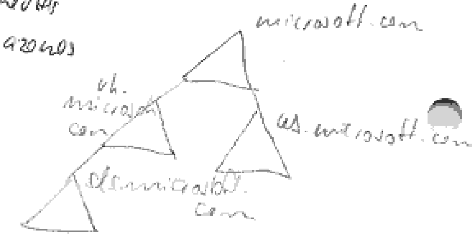
Szervezeti & biztonsági adminisztr. struktúra.

Delegálni lehet adminisztrációs jogköröket.

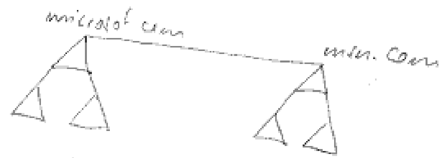
□ ~~Fák~~ Fák, (tree)

Közös névtér

séma azonos



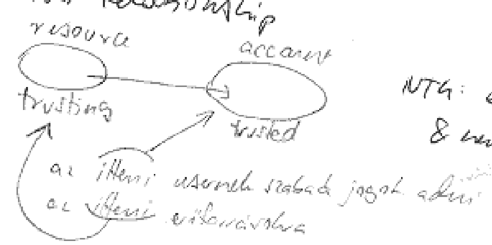
□ Erdők: különböző névtér



Common Global Catalog: a legfontosabb infókat tárolja & helyileg lehet kiolvasni

Ez közös az erdőben

□ Trust Relationship



NT4: egyirányú & nem tranzitív

NT5:

Kétirányú & tranzitív kapcsolat szülő & gyerek közt.

A többi fajtát lehet létrehozni kézi kívülre.

Az NT4-ben még nem DNS, hanem 15 karakteres NetBIOS neve volt a gépeknek.

☐ Site

Egy LAN alá tartozó hálózatrész

Minden site-ban kell min 1. domain controller

A replikáció site-on belül RPC-vel azonnal megtörténik.

A WAN-ban SMTP-vel megy, mert azt minden router átengedi, & csak időnként megy

LAN-ok között érdemes site kialakítani manuálisan megadni a replikációs útvonalait

Knowledge Consistency Checking
KCC ~~ellenőrzi~~ alapesetben kiala- kítja a repl. útvonalakat, ill. gyűri.

☐ A Global Catalog-ot ki kell jelölni
Operation Master-t is, ~~ettől~~ ezeket a fában csak 1 lehet egy erdőben
Ilyen operation masterek:
- schema master
- domain naming master
  ez hagyja jóvá, hogy ne legyen domainnév ütközés

Domainenkénti op. masterek:
- RID Master ~~Domain Master~~
  & Domain SID + RID a sec. ID.
  A RID-et a RID Master adja.
  └ Relative ID
- ~~PDC~~ PDC emulator, primary
  NT4 domain controller szerepét játssza NT4 serverek számára.

☐ Active Directory adminisztráció

☐ Csoportok

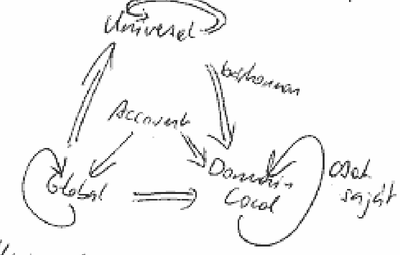
Distribution Group (csak levelezésre)
Security group (jogok is lehetnek)

☐ Group scope

Machine local (gépen lokális csoportok)
ez nem lát ki a gépből,
de tagja lehet bármilyen csoport.

Domain Local

ennek tagjai az erdőből bárki lehet.
a domain bármely gépén di- helyi hozzáférést meg lehet adni



Global & Universal csop. csak szerveren hozható létre

Replikációkor ~~&~~ a global & universal csoportok lista replikálódik, az universalnak a tartalma is.

A → G* → DL ← P

Az acc.-okat tegyem csoportokba, akár ~~...~~ többe is
a jogokat nem ~~ebbe~~ erre a csoportra adom, hanem a céldomainban csinálok csoportokat (nyomtatóhasználók)

pl: a színesnyomtató-használókba beteszem a könyvelők csoportjait.

tipikus hiba, hogy nagyon bonyolult a struktúra & valahol van egy kilógó jog, ami letilt valamit, pedig amúgy lenne jogosan.

Beépített Domain Local Groups

Users
Administrators
Guests
Account Operators
Print Operators
Server Operators
(share-k kezelése)
Backup operators
(bejelentő mentés)
Replicator

Spec. privilégiumaik vannak a teljes rendszerre
P) WS hozzáadása domainhez, stb

Beépített globális csoportok

Domain U/G/Adm
Enterprise Adm (teljes fa)
Group policy adm.
Schema admin
Domain Computers
Domain controllers
Certificate publishers

P. ha a domainban van a gép, a domain administrator bekerül a gép lok. administrators csoportjába

Speciális csoportok

dinamikusan változik, nem mi állítjuk
ACL-be felteheti de az elemeket nem mi adjuk hozzá:

- Everyone,
- Network Users – hálón keresztül, távolról
- Interactive Users – belépett a helyi gépre v. terminal s.
- Authenticated users (legalább bejelentkezve vannak)
- Service
- Principal self : aki [áthúzva] az obj-ban szerepel
- Creator / Owner : ... létrehozta ...

Active Directory jogok

Van DACL
Vannak obj.-specifikus jogok
vannak külön & egy
össze det.:
full control
read
write
create all child obj.
delete all child obj
lehet sokszor, hogy mit engedek.
Attribútumonként jogállítás lehet.

9. 2002. 04. 19.

Csoportok házirendje : Group policy
Fájlmegosztás - Shares
Nyomtatás hálózaton

Házirendek

Cél: hogy egyes beállításokat központilag adhasson meg az administrator egy csop. v tagjára

- administrative template-k
Registry beállítások alkalmazása
- security beállítások
(passw hossza / ~~...~~ lejárata ...)
- központilag menedzselt szoftver installáció (fel & le automatikusan)
- scriptek be & kijelentkezéskor
startup, shutdown, logon, logoff
- Remote Installation Services
installáció távolról
- IE maintenance
- Folder redirection
a felhasználó munkakönyvtára központi helyen legyen

Group policy object-ek szabályozzák.
Az ilyen objektumok Group Policy container-ben vannak az Active Dir.-ben.

A group policy template a megosztott sysvol könyvtárban van a domain controllerben

A group policy k
géphez kötött: gép indulásakor
felhasználóhoz k: felhaszn. bejelentk.kor

90 percenként frissül a policy (régen csak bejelentkezéskor frissült)

Policy-k megadható:
- site-ra
- domain-re
- Organization unitra

Ugyanazt a policyt több csoporthoz hozzárendelhetjük. & ugyanarra többet is.

Az Active Directoryban elfoglalt hely határozza meg, mi vonatkozik az adott elemre.
1. Site
2. Domain
3. OU-k

A későbbi beállítások felülírják a régebbit, legalábbis alapértelmezésben
egy szinten belül a policyk sorrendjét meg lehet határozni.
A scriptek bevárják az előző script végrehajt., de beállítható aszinkronra is.
A számítógép beállítások > user beáll.

- Az öröklődés blokkolható
- Megadható, hogy felülírják azokat a beállításokat (no override)

A policyra read & apply jogot is kell adni,
ill. a meg is tiltható
(deny apply groupapolicy)

DOS-os és Win16-os alkalmazások

Közvetlenül (is) használható kunt.

→ virtuális gép:
NTVDM.exe (32 bites prg.), amiben fut a MSDOS alkalmazás.
A rendszerhívásokat az 10.sys & msdos.sys helyett az ntio.sys & ntdos.sys szolgálja ki.
Virtuális Eszközmeghajtón keresztül konvertálja a közvetlen hw-kezelést rendes op.re hívásokká.
DOS-drivereket persze nem lehet alkalmazni.

Win16.
wowexec.exe, wow32 dll szimulálja a 16 bites windows hívásokat & azokat win32-es alk.-on futtatja.

Lehet 1 virtuális DOS gépet vagy több gépet indítani.
persze ezek együtt fagynak ilyenkor.
Ha külön mennek, DDE meg OLE működik, de osztott mem. nincs
⇓
Win16-os: külön-külön
DOS-os: mind ugyanabban.
Start.. /separate, van futn. nem ..: run in separate memory space
Command prompt.
Nem DOS-ablak!! Egy konzolos alkalmazás

Hálózaton megosztott erőforrások

☐ Megosztott fájlok

A könyvtárat explicite meg kell osztani & jogokat lehet adni

NT4-ben még csak engedélyező + no access volt

2000 óta {olv / módosítás / all} × {deny / allow}

A jogok NT4-ben kumulatívak voltak (vagy no access)

2000 óta az ACL kiértékelése szerint.

⚠ Ha alatta szigorúbban megint megosztjuk, akkor is az ~~teljes~~ kapcsolódás jogosultságai számítanak

☐ Ki sharelhet?

- administrator
- szervereken a server ~~admin~~ operatorok csop.
- power users
- adminisztratív (rejtett): $
  - C$ D$...
  - Admin$ C:\WINNT
  - nyomtatók
  - sysvol
  - NETLOGON belépőscriptek

☐ Hogyan kapcsolódhatunk?

- drive mappelés
  - megadása: Universal Naming Locator
  - \\szerver\sharenév\könyvtár
- explorerrel vagy Run-nal

☐ Mi van az NTFS jogokkal?

~~Először~~. A share & az NTFS jog közül a szűkebb érvényes.

☐ Sharek publikálása

- Active Directoryban elhelyezhetők hivatkozások a share-kre...

☐ Offline share

a share lemásolódik & visszaíródik

☐ Distributed File System, Dfs

logikailag egy fastruktúrába linkelhetők

☐ Hogyan történik meg a távoli fájl elérése?

Az IO managerben kiderül, hogy ez nem helyi fájl, átpasszolja egy dl-fs-drivernek, ami meg távolról szedi le.

Natív: smb: server message block

☐ Hálózati nyomtatás

print device: ahonnan a nyomtatott papír kijön

printer: sw interface

print server: itt vannak a queue-k, még akkor is, amikor a nyomtatók a hálózatra közvetlen kapcsolódnak

{print / manage documents / full}

- print: kiválasztott listában a saját feladatait kezeli
- manage documents: sorrendezés, törlés
- full: nyomtató driverek beállítások

ha megosztom, a drive-ok a szokásos kliensekre telepítődnek alpha, linux... ill ~~meg kell adni~~ kliensoldali driver kell.

printing pool.

egy printer — több printing device, feltéve, hogy van ~~fe~~ a sw. interface

□ Ugyanahhoz a fizikai nyomtatóhoz lehet több interface-t definiálni különböző beállításokkal.
P Főnök/beosztott jogok, prioritás

Nyomtatónál beállítható:
- mikor elérhető
- prioritás
- spooling:
  kinyomtatja metafájlba azonnal, de a nyomtató program addig nem engedi dolgozni

□ Hogy megy a nyomtatás?
GDI-n keresztül. A GDI a printer driver segítségével fordítja le a nyomtató nyelvére.
Bekerül a spoolba & onnan a távoli szervernek vagy a local print providerbe.
A local print provider (esetleg a távoli gépen) a bitsorozatot előáll & kijön a gépből a papír.

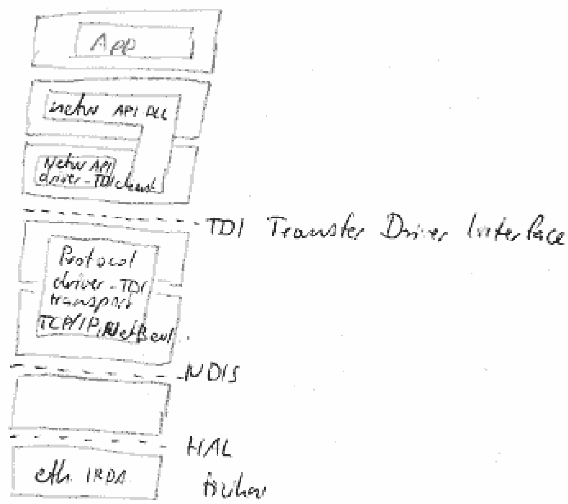
Ha a kliens nem windows 95≤, NT≤, akkor már teljesen alacsony szintig végigmegy a kliensben a feldolgozás, csak ki kell küldeni a nyomtatóra.

(Sikertelen) nyomtatás átirányítása. azonos típ. nyomtató kell, annak a UNC-jét meg kell adni & kinyomja.
2000-ben IIS service-vel http-s nyomtatási lehetőség

10

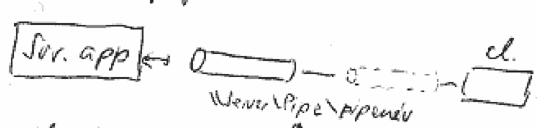
Networking

ISO/OSI
{sokszor vizsg-duma}



□ Network API
- named pipes ↔,
- mailslots →
- Windows socket
- RPC
- CIFS Common Internet File System
  smb továbbfejlesztése
- NetBIOS egyszerű BIOS-kiterjesztés

□ Named pipe



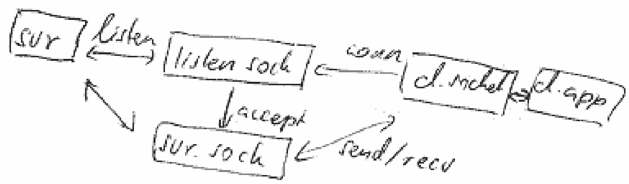
□ Mailslot

\\Server\MailSlot\AppSlot
1 kliens több szervernek is küldhet
pl. *\MailSlot\myslot

Fájlként érhető el API-ból (ugyanígy a pipe-t is, de az nw)
↳ \~~Devi~~ \Device\NamedPipe
el. egy ál-filesys-driver végzi

Windows Socket

BSD socketkezelés



Ez is fájlként képeződik le, speciális fs-driverrel.

Common Internet File Sys.

a redirectorhoz fordul, ~~majd~~ a dll, ami meglátja, hogy nem helyi fájl, ~~és~~ és a hálózati driverhez fordul

RPC

Mivel mind meg a távoli függvény, csonkot (stub) használnak.

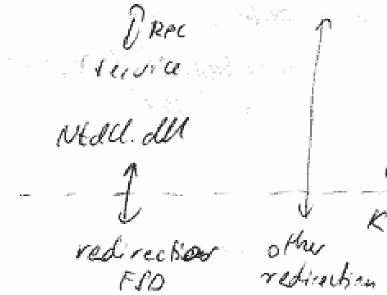
Az interface-t IDL (interface definition language) nyelven kell leírni

IDL ⇒ stub generálás ⇒ stub library

A stub helyileg helyettesíti a távoli függvényt, & a hívást átküldi a távoli csonknak. Ez a csomagolás a marshalling.

A Microsoft a RPC DCE-t valósította meg, ami eléggé szabványos & a com komponensek így működnek.

Multiple Protocol Router



Ha nincs mappelve, ~~a ren~~ kapunk UNC-t adok, a rendszer végigkérdezi a redirectorait, hogy ki tudja feloldani

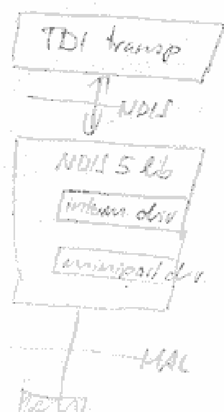
azután cachelődik

Protocol Drivers (transp., netw., drv)

- DLC IBM-es egyszerű protokoll

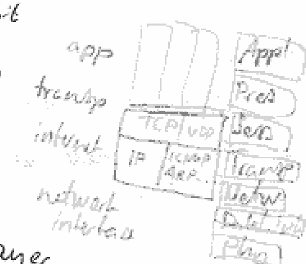
~~Network~~

- NetBEUI W for Workgroups 3.1-ben használták & nem routolható, de kihalóban van
- TCP/IP
- NWLink Netware, IPX/SPX MS-implementációja



☐ Ethernet

- síntopológia (már csak virtuálisan)
- CSMA/CD
- Ethernet frame:
  - preamble
  - dest addr. } fizikai ~~[illegible]~~ cím
  - source addr
  - T/L
  - adat
  - crc 32 bit
- token ring
- FDDI



☐ TCP-IP

- Internet layer
  - Internet protocol IP
  - Address Resolution (ARP) (IP → fizikai cím)
  - ICMP Internet Control Message Protocol
  - IGMP Internet Group Message Protocol

IP

- összeköttetésmentes host-host átvitel
- címzés
- routing
- IP packet
  - header + payload
  - → header
    - forrás
    - cél
    - azonosító
    - prot. ~~[illegible]~~ leíró
    - checksum
    - time to live
      - hány hop-ot él túl (hibásakat törli)
      - ↑ ugrás
    - minden hop-ban a time to leave
    - checksum mód. ~~[illegible]~~ újraszámolódik

Az eltérő Maximum Transmission Unit miatt a van router ~~[illegible]~~ részletezhető mögé önmagát azaz az azonosító, de a Fragmentation tárolja hogy melyik [illegible]

more fragment: van még több fragment
fragment offset: hol kezdődik a csomagban a fragment.

ARP

MAC address (eth: 6 byte)
⇕ IP
~~[illegible]~~
soft cím 6 byte

Az ARP cache tárolja a jelenleg érvényes (nagyjából használt) IP – MAC összerendelést.

ha az ARP cache-ben nincs, broadcast request (~~[illegible]~~ mindenkinek)
válasz → 6. cache-be
a ~~[illegible]~~ menti ~~[illegible]~~ a betölti a cache-jébe

ICMP

- Internet Control Message Protocol
- hibakeresésre
  - echo request
- hibajelzés
  - redirect: inkább arra küldj
  - source quench: lassabban! lassabban!
  - destination unreachable: a router nem tudja merre van

IGMP

IP Multicast Group
- dynamic
- multiple network

Message
- IGMP host membership report
- query ↰

a router megkérdezi, hogy van-e a hálózaton olyan valaki, aki ennek a csoportnak tagja

• Szállítási réteg

TCP

- kapcsolat alapú
- megbízható
- acknowledgement
- az üzeneteket szegmensekre bontja & IP-vel elküldi
- bytestream
- tcp header
  - port src, dest
  - sequence number
  - acknowledgement number
  - forgóablakos forgalomszabályozás, ablakmérete (window)
  - checksum

Jólismert TCP portok

20 FTP
21 FTP
23 Telnet
80 HTTP
22 SSH
110 POP3
25 SMTP

UDP User Datagram protocol

- összeköttetésmentes protokoll
- nem megbízható
- fejléc
  - source port
  - destination port
  - checksum

53 DNS
69 TFTP
161 SNMP
520 RIP
NFS !!

• IP cím

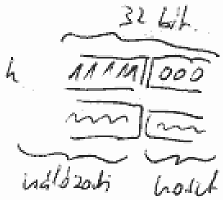
32 bites, pontozott decimális alakban

1-126. A osztály "0" + 7 + 24 bit => 126 hálózat, $2^{24}-2$ host
128.0-191.255 B osztály "10" + 14 + 16 bit => $2^{14}-1$, $2^{16}-2$
192-223 C osztály "110" + 21 + 8 bit => $2^{21}-1$, 254
D osztály "1110" multicast címek
E osztály "1111" speciális célokra
csupa 0 hálózatcím nincs
csupa 1 broadcast
csupa 0 hostcím → teljes hálózat
csupa 1 broadcast hálózaton belül

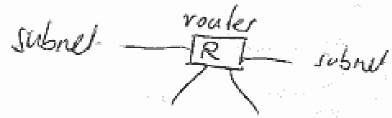
Spec: 127.0.0.1 => localhost

Kevés IP-cím van, de pl A, B hálózatok nagy része kihasználatlan

(→) subnet:



(→) supernetting
ugyanazon netmaskkal több IP
C osztályú címtartományt összevonhatók



Windowsban is van „router" routing table

- direct küldés: közvetlen, ARP-vel lekérem a címet & elküldöm LAN-on
  direct, ha (dest & netmask = src & netmask)
- indirect: dest & netmask != src & netmask
  routolni kell

route print
- network dest
- netmask
- gateway
- interface

megnézi, hogy melyik networkhöz illeszkedik legjobban, kiadja az adott lábon (interface) az adott gateway felé

metric: mennyire preferáljuk (ha több is illeszkedik)

A routerek közlik egymással, hogy kivel van kapcsolatuk.

RIP, OSPF protokollok
egész r. táblák

Speciális megoldások az IP-inség...

belső (nem routolt) címek:

10.0.0.0 /8
172.16.0.0 /12 Address
192.168.0.0 /16 Translation

11. 2002.05.03

- DHCP
  - server:
    - WindowsNT Server kell hozzá
    - része a telepítőkészletnek
    - service-ként fut
    - statikusan kell kiosztani az IP-t
    - be kell a tartományt (scope) konfigurálni.
    - Több DHCP szerver nem kommunikál egymással
  - kliens
    bármely windows 3.11<
    NT <
  - Az IP konfiguráció „kölcsönbe van" ami lejár & meg kell újítani
  - Kölcsönzés
    kérés (broadcast)
    felajánlás (∀ szervertől)
    elfogadás/elutasítás
    visszaigazolás
    - DHCPDISCOVER
      dest mac: FF... F
      source mac: saját
      dest IP 255...255
      dest IP 0.0.0.0
      client ID: saját mac
    - DHCPOFFER
      dest mac: FF...F
      source mac: svr mac
      source ip svr.ip
      offered ip
      server id svr.ip
      lease length 72 óra
      client id
    - DHCPREQUEST
      broadcasttal (!)
      visszaküldi a
      req ip,
      svr. identific.
      client identific. -t.
    - DHCPACK
      broadcasttal elküldi a svr. az összes beállítást.
  - Megújítás
    A lejárat felénél már kommunikálást kér. ~~Ha valami döbb a~~
    - DHCPREQUEST, DHCPACK
      requestet újrajátssza, de célzott üzenettel

    Ha nem sikerül, 7/8 körül újrapróbálja.

    Ha megint nem sikerül,
    broadcasttal DHCPREQUEST-től kezdi, újraküldi ugyanazt, most már bárkitől

    Ha megint nem sikerül, akkor megint újrakezdés teljesen elölről.

    Ha lejár mégis, meg kell szüntetni az IP cím használatát
  - Lejárati idő mennyi legyen
    → 72 óra a default
    → ha bőven van ip cím, akkor lehet hosszítani
      ⊕ kevesebb forg
      ⊖ lassabban frissül
    → ha kevés a cím, rövidebb időre → ha ki van kapcsolva, kiosztható másnak.
  - Scope
    - egy tól-ig tartomány, amiben lehet tetszőleges számú kizárás exclusion ranges
    - reservation: bizonyos mac-hoz hozzárendelhető ip.
    - options: egyéb kiosztott info
    - 80/20 2 server, az egyik a címek 20%-a felett rendelkezik ⇒ akkor is lesz ha a másikkal baj van
    - Superscope
      Több scope uniója
  - Címkonfliktus elkerülése kiosztás ill használatba vétel előtt ARP-al, kérésen ...

- Opciók típusai
  - default global options
  - scope options
  - class options
    - vendor classes
    - user classes
  - reserved client options
  - static configuration

  (erősödik a preced.)

- DHCP relay

  A routerek nem engedik át a dhcp-t, De ha van dhcp relay agent, akkor a router saját nevében kérdezőrküldi & visszaküldi az eredményt.

  Ez azonban nem elég, mert a másik hálózat DHCP serverének tudnia kell, hogy melyik hálózatból adjon címet.

- Windows 2000 fejlesztések
  - dhcp servertől multicast csoport létrehozásához is lehet címet kérni (MADCAP)
  - APIPA. Ha lejárt a cím, a 169.254.0.0/16 tartományból random választ címet & legalább egymást látják (ki nem)
  - Dynamic Update. DHCP-n kapott ip-hez átmenetileg DNS nevet lehet regisztrálni

ipconfig

/release
/renew
/registerdns dns-nél regisztrálni a nevüket, ha megváltoztatták

□ Wins

- NetBIOS név feloldására van. Ez a név 16 char hosszú lehet, nincs hierarchia. Az első 15 char printelhető, az utolsó a rsz. típusa.

- unique names
  - csak egy gépé lehet, pl.
  - <00> workstation service
    - E "BUDAPEST \0" megosztott nyomtató, fájl
  - <03> messenger service
    - "Budapest \0x03"
  - domain master browser
- csoportnevek:
  - <00> domainnév
  - <1C> domain controller név

☒ A gép lehet
Először cache-ben néz
B-node: ha meg akarja tudni kit keressen, broadcasttal keresi az adott névtulajt. gépet
P-node point-to-point Wins servertől
M-node (mixed) ha B nem megy, P
H-node fordítva. P először, aztán B

A LMHOSTS fájl
(system32\drivers\etc\ -ban van, ha van.

nbtstat -c cache listázása

WINS folyamata
- registering name: elsőtt üzenetben a wins servernél bejegyzi a nevét. válaszol hogy, ha elfogadja a svr.
- renewing name
- releasing name
- resolving name kérdezés, ld. fejlebb
- detecting name conflict.

Detecting name conflict:
ha bejegyezte már valaki, ellenőrzi hogy az előző címen válaszol-e az a gép?
ha nem, bejegyzi.

A WINS névbejegyzést is meg kell újítani (pár naponként)

Lecsatlakozáshoz kiregisztrálják magukat

Ha lejárt, akkor released státuszba kerül a winsben.

Ha letelik az extinction interval is, tombstone lesz belőle, amit közöl a többiekkel is (többi WINS svr) aztán később kitörli.

Verification interval
ha lejár, akkor mindenkivel egyezteti (push vagy pull, beállítástól)

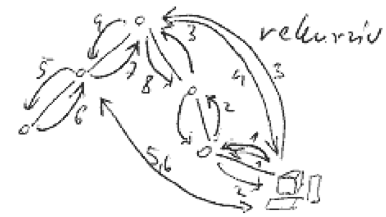
- Wins proxy
  régi kliensek csak a broadcastot ismerik
  a wins proxy elkapja & lekéri a wins servertől.
  Ez akkor érdekes, ha routeren túl van.
- Replikáció
  minden bejegyzésnek van tulajdonosa & a tulajdonos módosíthatja, a többi csak másolja.
- Wins server lehet ~~...~~ WinNT & 2000 svr.
  A server címének statikusnak kell lennie
- Wins kliens minden Windows

Domain name service

- top level domain + egyebek
- fa épül belőle.
  A fa egy szerver által lefedett része a zóna.
  - primary zone: saját jogon kezeli
  - secondary zone: zónatranszfer útján
    → van ~~hibatűrés~~
  - miért
    hibatűrés
    forgalom ↘
    terhelés ↘
  - ...

- Névfeloldás.
  - DNS név ⟷ IP cím
  - be vannak állítva a DNS szerverek

  ahol a resolver megkéri a DNS servert, hogy adja meg az ... névhez az ip-t.
  Ha az nem tudja, feljebb levőtől megkérdezi.



lehet olyan is, hogy felteszi rekurz. (iteratív)
lekéri iteratív.

load sharing
adott névhez több ip is adódhat, felváltva adogatja.

A nameserver cache-eli a ~~...~~ válaszokat. A sikertelen keresési eredmények is tárolódnak

- Resource records
  - owner
  - time to live
  - class
  - ~~typ~~ type
  - RDATA
- type:
  SOA: Start of Authority: melyik zónáért felelős
  NS: milyen nameserverek vannak
  A: közönséges bejegyzés név:ip (address)
  CNAME: más nevek ahhoz a címhez. itt nem a címre, hanem névre mutat
  MX: mailserver bejegyzés
  SRV: service rekordok WINS-t váltják ki
  PTR: visszafelé: IP → név
  Reverse Lookup zóna

° Reverse Lookup
Külön névtér:
152.66.70.4-et így kérhetjük le, hogy
4.70.66.152.in-addr.arpa
⚠ fordított bájtsorrend!

° Zone Transfer
Full/incremental
Domain esetén (active directory) a MC serverek az active dir replikációját alkalmazzák

- a kliens is beregisztrálhat: az előremutatót a kliens,
- a visszamutatót a server regisztrálja
ipconfig /registerdns
Ha engedélyezve van, akkor a DNS server is fordulhat a winshez

□ Browser

° belső hálózaton megosztások kezeli.
~~Van egy~~
° Van browser, ami nyilvántartja, hogy hol mi van megosztva.
master & backup browserek is vannak.

° Bekapcsoláskor a Master Browsernél bejelentkezik, aminek a neve "\0x01\0x01MSbrows"
Megadja neki a backup browser listát, ahonnan választ.

° A backup browserek csak időnként frissítik a db-t, & a bekapcsolt gépek csak negyedóránként jelentkeznek újra.

Ez már 2×15 perc az infoterjedés késleltetése
De egy domain esetén még a domain master browseren is keresztül kell mennie az infonak.

° A ~~brow~~ ~~browser~~ gépek közül választással dől el, ki a master browser & ~~ki a maste~~
Fontos, hogy folyamatosan frissen.
Election packet, amire licitálni lehet. Ha nem licitál senki, nyert az utolsó

° Mi határozza meg az erősorrendet
- protokollverziószám (=windows verzió)
- server > workstation
- mióta van bekapcsolva?

° NT-t konfigurálni lehet, hogy potential browser vagy never to be browser.

12.

□ NetBEUI
nem routolható szállítási protokoll
NetBIOS Extended User Interface
broadcasttal találják meg a gépek egymást. Konfig nem kell

□ NWLink NetWare IPX/SPX
Együttműködés NetWare-rel

□ Client Service for NetWare
telepíthető a gépekre,
amivel használni tudják az IPX/SPX-et és a NCP-t, ami a NetWare Core Protocol & a MS-os smb párja

☐ Gateway Service for NetWare

Az egyik gépre telepítve leshare-elhetők senb-en a NetWare server NCP-s megoldásai

⊖ Nem hatékony

- Egy felh. a NetWare felé, a gatewayen pedig windowsos jogok adhatók.

☐ File & Print services for NW

telepíteni kell az IPX/SPX protokollt, & a NCP-t server oldalon

○ Távoli adminisztráció végezhető windowsos prg-okkal

☐ Gateway beállítás

kell egy acc. a netware serverhez & megadhatók, hogy mit akarok megosztani azon.

Performance monitor

- számlálók külö. rendszerparaméterekre
- diagram (folyamatos figyelés)
- logolás
- küszöbértékek → akciók

Eseménynapló

- system log. oprendszer üzenetek
  - ⓘ tájékoztató info (service indul, megáll)
  - ⚠ Warning
  - ⊗ Error

adminisztrátorként távoli eseménynaplók is elérhetők.

- application log
  alkalmazások írhatnak ide
- security log
  bizt. eseményeket naplóz-
  ha bekapcsoljuk.
  logon, logoff-ok
  bekapcsolása policy-n keresztül
  (security settings/audit policy)
  Eseménytípusonként válogat-
  hatunk, meg sikeres/sikertelen

  Object events
  naplózza-e az azokon
  tájékozottan SACL szerinti
  (Security Audit Acces Ctrl List)
  eseményeket

anyag: sok van szerte

- slide-ok, majdnem minden kell
- egyéb írásos anyagok:
  - előadás szerint:
    → David Solomon, Mark Russinovich }
    Inside Windows 2000
    3rd edition
  - Az ő forrásuk
    Dave Cutler, az NT
    tervezője & a kódolók.
  - technet.netacademia.net

vizsgák: máj 22 8.00
máj 29 8.00
jún 5 8.00
jún 12
jún 18

www.aut.bme.hu/education/default.hu