Diplomamunka

Ollári László Róbert

Debrecen

2008

Debreceni Egyetem

Informatika Kar

Hálózati távadminisztrációs rendszerek

Témavezető:
Dr. Almási Béla

Készítette:
Ollári László Róbert
programtervező
matematikus

Debrecen
2008

Tartalomjegyzék

1) Hálózati távadminisztrációs rendszerek - Bevezetés

A számítógépes hálózatok kialakulásával az egy szervezeti egységbe tartozó felhasználók közötti fizikai távolság is folyamatosan növekedett. Kezdetben az egy szervezeti egységben, vagy egy munkán dolgozó felhasználók egy szobában, majd egy folyosón, egy épületben, stb. dolgoztak. Manapság már nem ritka a több 10, 100 km-nyi, vagy esetleg kontinensnyi távolság sem. A mai hálózatok ráadásul lehetővé teszik távolságtól függetlenül az online együttes munkavégzést, ezáltal a fizikai távolság nem lehet akadálya a munkatársak kommunikációjának. Így a fizikai távolság is megnövekedett.

Kezdetben számítógépen a direkt erre kiképzett szakemberek dolgoztak. Később a számítástechnika popularizálódásával egyre szélesebb rétegek kezdtek számítástechnikai eszközökön dolgozni. Ebben közrejátszott a hardver és szoftvereszközök árának csökkenése, valamint az egyre felhasználóbarátabb eszközök megjelenése. Így már luxus lett volna csak jól kvalifikált embereket foglalkoztatni, így egyre több olyan ember is bekerült ebbe a körbe, akinek kisebb-nagyobb rendszerességgel más segítségére van szüksége. A segítség szükségességének másik oka a tömegtermeléssel együtt járó minőségromlás. Eléggé gyakoriak a szoftverek „gyári hibái”, amik bizonyos használati körülmények közben derülnek ki, és az átlag felhasználó nincs felkészülve ezen hibák kezelésére.

A fenti okok miatt mindig is szükség volt kiszolgáló, támogató személyzetre. Így például emeletenként, épületenként szükség volt egy hozzáértő emberre. Esetleg több épületenként, de mivel az illetőnek mindig helyszínre kellett mennie, így a reagálás ideje egészen nagy is lehetett. Viszont a távolságok növekedésével a reakcióidő növekedését nem volt célszerű elfogadni. Így adódott az ötlet, hogy ha már egyéb okokból az informatikai eszközök számítógépes hálózattal vannak összekötve, ezt a számítógépes hálózatot távsegítségnyújtásra, illetve távadminisztrációra is lehet használni.

Egy kis kitérő. Nem véletlenül hangsúlyozom külön a távsegítséget és a távadminisztrációt. Az én értelmezésemben a távsegítség egy egyszerűbb, felhasználóközelibb tevékenység. Például rájelentkezni egy gépre és megmutatni a felhasználónak, hol találja az Aknakereső nevű programot. A távadminisztráció már egy összetettebb, felhasználótól távolabb álló tevékenység. Például egy program telepítése, vagy egy rendszertulajdonság megváltoztatása, esetleg egy hibakeresés.

Természetesen a távadminisztráció sem mindenható. A rendszereknek (operációs, hálózati) el kell érniük egy bizonyos működési szintet ahhoz, hogy egyáltalán távolról csatlakozni lehessen a végponthoz. Hiába van egy minden igényt kielégítő rendszerünk, ha nincs hálózati összeköttetés az adminisztrálandó rendszerhez, vagy például a célgép nincs bekapcsolva, áramszünet van, stb..

A távadminisztrációs rendszereket két fő csoportra bontom aszerint, hogy a felhasználó látja-e, mi történik a munkaállomásán (ezt hívják úgy a szlengben, hogy átveszik az irányítást, illetve rájelentkeznek a gépére), vagy a felhasználó tudta nélkül történik valamilyen konfigurálás a munkaállomáson. Így meg fogok különböztetni előtér és háttér távadminisztrációs rendszereket.

A könnyebb áttekinthetőség végett felállítok egy szempontrendszert is, amely szempontjainak való megfelelőségek segítségeivel objektívebben összehasonlíthatóak lesznek a vizsgált rendszerek. Milyen szempontok jöhetnek számításba? Először is a már előbb említett, leglátványosabb különbség, mit „érez” a felhasználó. További, fontos szempont lehet az alkalmazás előtt, hogy ingyenes-e az adott eszköz. Befolyásolhatja a rendszer kiválasztását, hogy mennyire platformfüggetlen, mennyire lehet széles körben alkalmazni? Mivel távoli adminisztrációról van szó, az sem mellékes, hogy a hálózaton átküldött adatok mennyire vannak biztonságban. Akár lehallgatás, akár megváltoztatás ellen. A legegyszerűbb példa: lehallgatják, ezzel ellopják az adminisztrátor jelszavát. Az utolsó szempont, a hatás gyorsasága. Azonnal érezhető, vagy esetleg valamilyen beavatkozás szükséges még? (ez általában egy újraindítás). Ez a szempont is fontos, mivel gyakorlati tapasztalataim szerint a felhasználót érzékenyen szokta érinteni, ha újra kell indítania a gépét, mivel nagyrészük nem menti rendszeresen a munkáját, és ilyenkor megnő az adatvesztés kockázata.

2) Háttér távadminisztrációs rendszerek

i) Telnet

Előre bocsátom: kaptam olyan visszajelzést, hogy a telnet nem tekinthető napjainkban távadminisztrációs rendszernek. Ebben van is igazság, hiszen egy titkosítatlan adatfolyammal kommunikáló alkalmazásról van szó. Én viszont azt a nézetet vallom, hogy amíg a világ legnagyobb hálózati eszköz gyártója (CISCO) támogatja eszközeiben a telnet-et, addig szót kell ejteni róla. Igaz, azóta már ők sem preferálják, kompatibilitási okokból támogatott a rendszer, de biztonságos LAN környezetben használható. (Én is találkoztam olyan

megoldással, hogy az adott router mellé külön fenntartottak egy adminisztrációs LAN-t, ami el volt szeparálva a nyilvános LAN-tól)

A telnet nem egy csak távadminisztrálásra kifejlesztett eszköz, viszont univerzalitása miatt arra is alkalmas. Az 1960-as évek végén dolgozták, fejlesztették ki. Akkorra jutott el olyan szintre az infomatikai fejlődés, hogy igény mutatkozott a nagy, osztott rendszerek adathálózaton keresztüli elérésére.

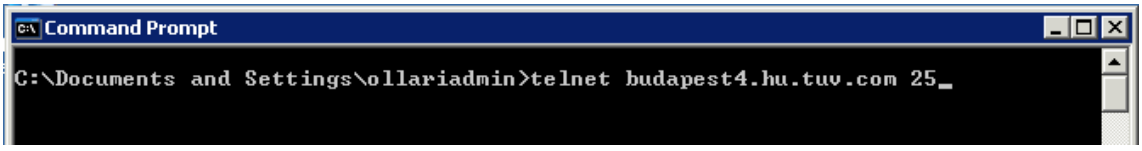
Korábban egy rendszer elérésének 2 legjellemzőbb módja volt. Vagy leült a felhasználó az eszköz konzolja elé, vagy soros vonali terminálon. Ez a soros vonali terminál egy célgép volt. Állt képernyőből, billentyűzetből, elektronikából. Ez az eszköz soros vonali interfészen csatlakozott a központi rendszerhez. Tehát ahány soros vonali terminált szerettünk volna csatlakoztatni az osztott rendszerhez, annyi interfészre és kábelre volt szükségünk. Ez a terminál tökéletesen szimulálta a gép saját konzolját, ha valaki leült elé és elkezdett dolgozni rajta, más lehetősége nem volt: megjelent az adott rendszer bejelentkeztető képernyője.

Az adathálózatok elterjedésével viszont megjelent annak is az igénye, hogy ne csak pár tíz méternyi kábel végéről, ne csak az adott rendszerhez kapcsolódó célhardverről lehessen bejelentkezni, hanem egy másik rendszerből is, számítógépes hálózaton keresztül. Ezt az igényt elégítette ki, illetve elégíti ki a mai napig a telnet. A telnet kifejlesztésének idejében a hálózatok még maximum MAN kategóriába tartoztak, vagy épületeken belül voltak kiépítve, vagy maximum egy telephelyhez tartozó épületeket kötöttek össze. Így a lehallgatással történő adatlopásra ekkoriban még nem is gondoltak, mivel a vonalak fizikai védelme erősen leszűkítette az ilyesmivel próbálkozók körét. Ezek a hálózatok több szempontból is magánhálózatok voltak. A telnet az adatokat kódolatlanul, u.n. clear text formátumban továbbítja. Ez okozta később a vesztét is. Ekkoriban még karakteres interfészeken dolgoztak a felhasználók. A soros vonali terminálóknak megfelelően tehát a telnet is byte-onként továbbította a leütött karaktereket, majd visszairányba a megjelenítendő karaktereket. Ekkor tehát a legrosszabb esetet figyelembe véve, 80x25-ös képernyő teljes frissülése esetén továbbítani kell 2000 byte-ot. Ez eléggé kis adatmennyiség, tehát a telnet nagy távolságokra történő bejelentkezés esetén, illetve kis vonalsebességnél is jól használható. Persze, mivel ekkor még a parancssori környezet volt a jellemző, kevés esetben kellett az egész képernyőt egyszerre frissíteni.

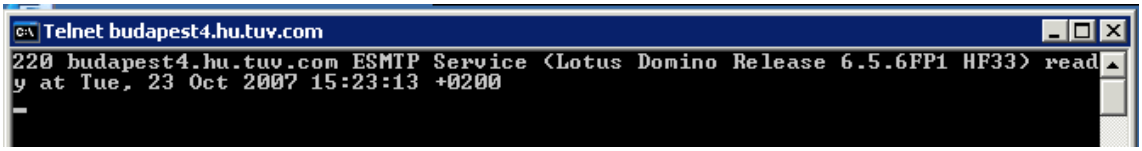
A telnet rendszer kliens-szerver arhitektúrájú. A kiszolgálón üzemelnie kell egy telnet szervernek, a kliens gépen pedig futnia kell a telnet kliens programjának. A szerveren minden

becsatlakozó klienshez létrejön egy külön session, az u.n. virtual terminal session (szimulálva a soros vonali terminálos környezetet). A kliens csatlakozáskor megadja a célrendszer címét, illetve opcionálisan a TCP/IP port számát, ahol a telnet szerver elérhető. Mivel a telnet egy széles körben használt rendszer, ezért saját szabványos port-ja van, ez a 23-as. A telnet kliensek alapértelmezés szerint erre a port-ra csatlakoznak. Paraméterként megadhatunk más port-ot is. Ekkor láthatjuk, hogy az adott port-on van-e, illetve ha kimenetében megjeleníti, a típusát is megláthatjuk egy szerviznek, mivel a telnet kliens a kapott információt közvetlenül megjeleníti.

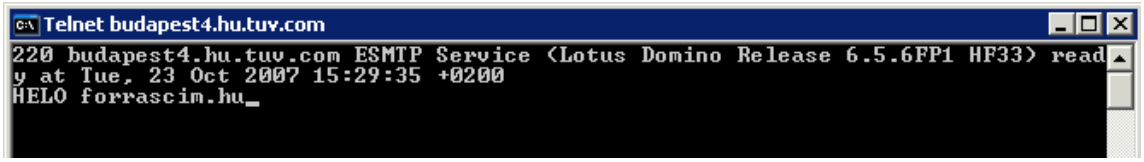
Példa: smtp szerver használata telnet klienssel (kapcsolódás a budapest4.hu.tuv.com szerver 25-ös port-jára)



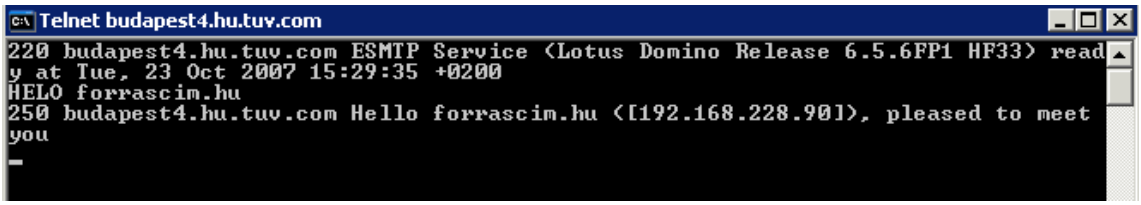
A fenti parancsot kiadva, megkapjuk egy Lotus Notes SMTP (pontosabban egy újabb verzió, az ESMTP szerver bejelentkező-képernyőjét)



Parancsokat adhatunk ki:



Amire a reakciót is láthatjuk:

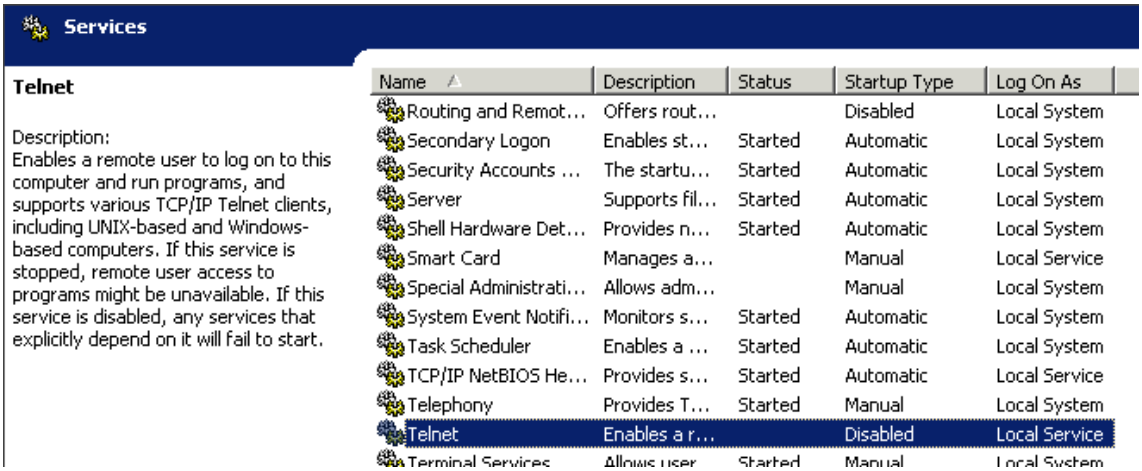


Persze felmerülhet a kérdés, hogy kapcsolódik a telnet a dolgozat témaköréhez. Úgy, hogy telnet segítségével be tud lépni a felhasználó egy távoli rendszerbe. Ha ez a felhasználó adminisztrátori jogokkal rendelkezik a távoli rendszeren, meg tudja változtatni a rendszer tulajdonságait. Alkalmazásokat tud telepíteni / törölni, jogosultságokat tud kiosztani /

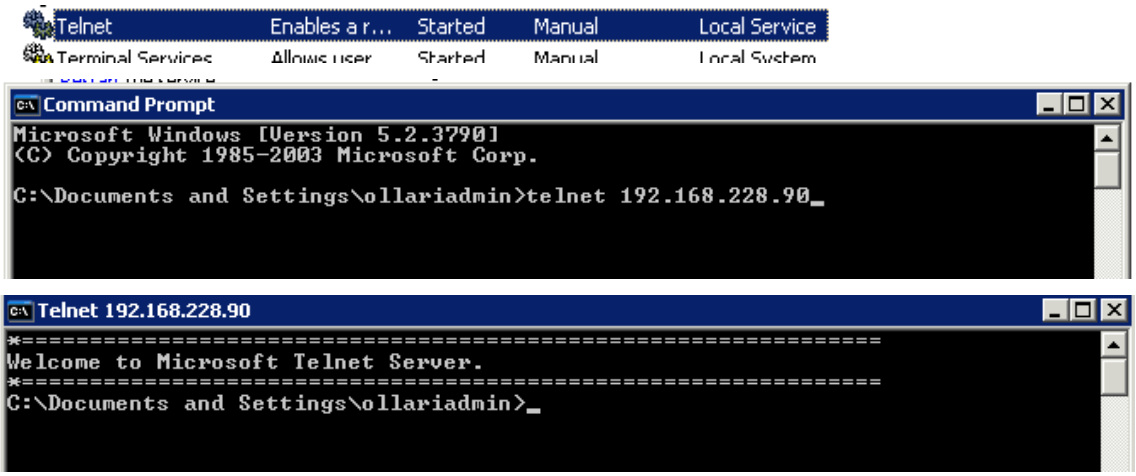
visszavonni, felhasználókat tud létrehozni. Tipikusan el tudja látni egy távoli szerver adminisztrációs feladatait. Általában kliens gépek nem szoktak telnet szervert futtatni.

Példa: telnet szerver Windows szerveren

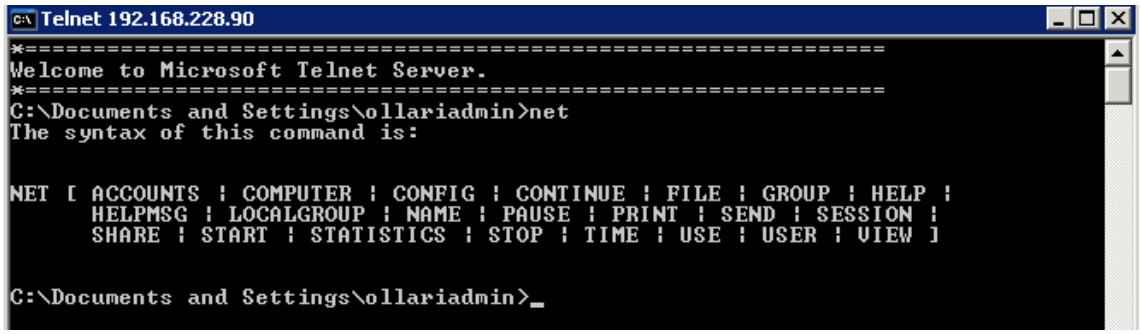
A telnet szerver a Windows szerverrendszerek beépített komponense:



Amennyiben elindítjuk, csatlakozhatunk is hozzá a klienssel:



Mivel itt Windows telnet szerverről van szó, Windows parancsokat adhatunk ki. Például a net parancsot:

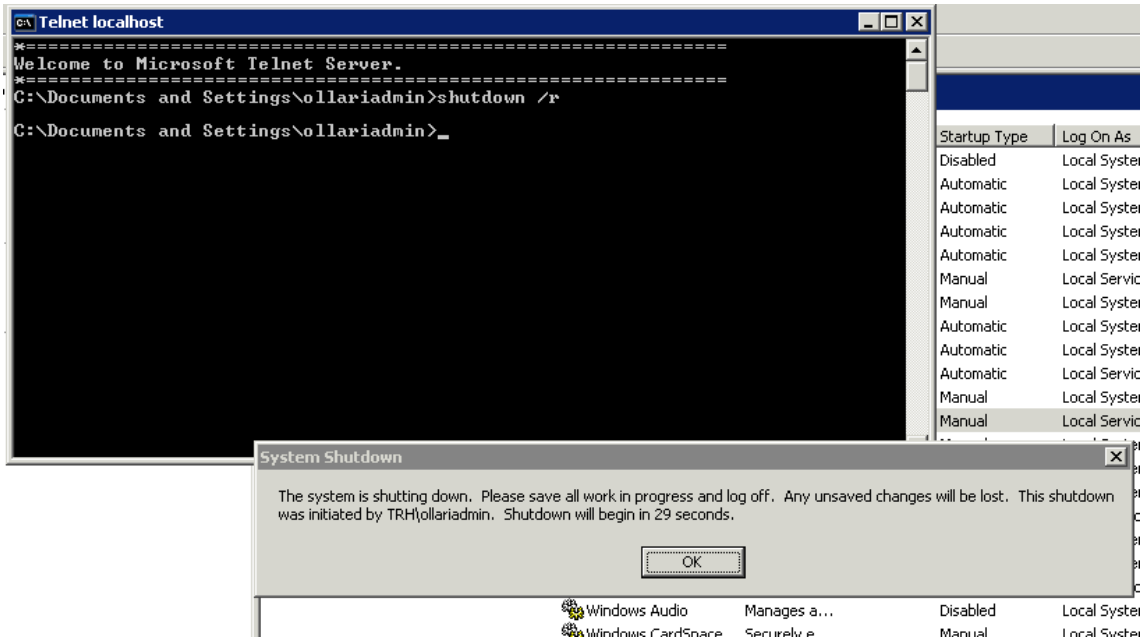


```
C:\Documents and Settings\ollariadmin>net statistics server_
```

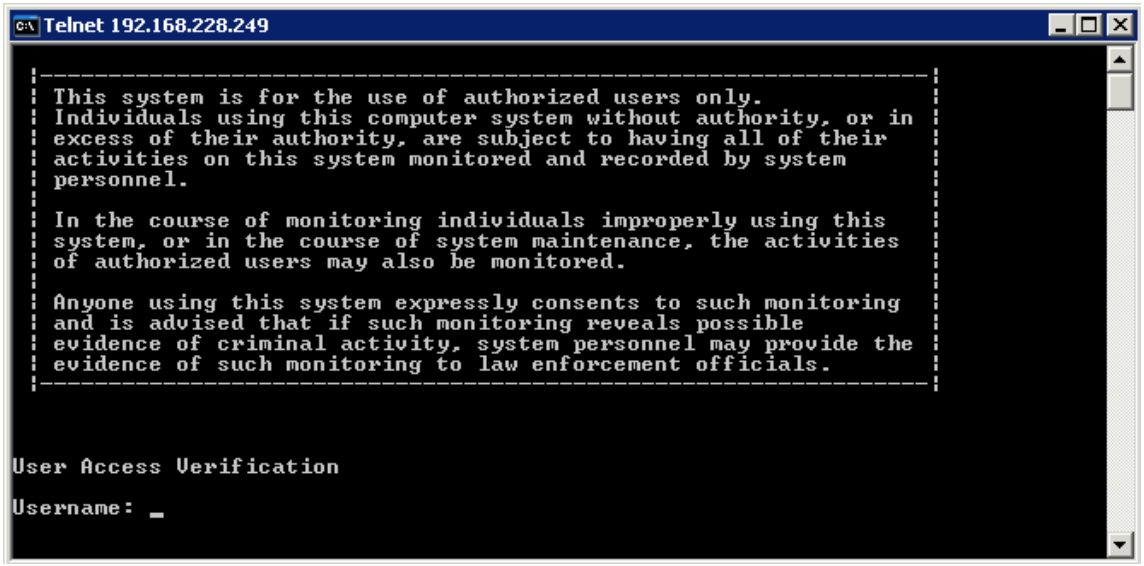
```
Telnet 192.168.228.90
Sessions timed-out                0
Sessions errored-out              0

Kilobytes sent                    51
Kilobytes received                46

Mean response time (msec)         0

System errors                     0
Permission violations             0
Password violations               0

Files accessed                    32
Communication devices accessed    0
Print jobs spooled                0

Times buffers exhausted

  Big buffers                     0
  Request buffers                 0

The command completed successfully.


C:\Documents and Settings\ollariadmin>_
```

Esetleg futtathatunk külső programokat (természetesen csak szöveges módban), vagy például újraindíthatjuk a rendszert:

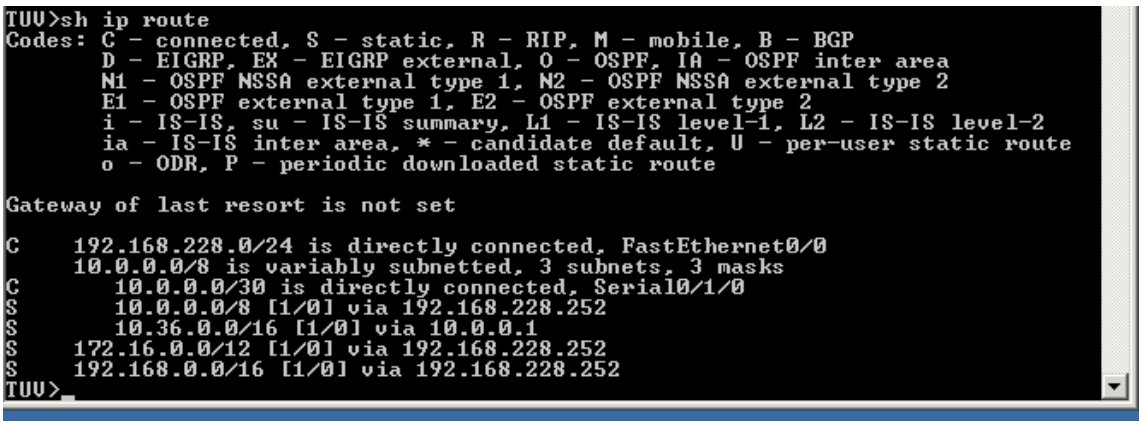
```
C:\Documents and Settings\ollariadmin>shutdown /r_
```



Példa: CISCO router adminisztrációja telnet-en keresztül



Sikeres belépés után a router teljesen manage-elhető, mivel a CISCO operációs rendszere, az IOS csak szöveges felülettel rendelkezik, így az összes konfigurációs beállítást parancsokkal tudjuk módosítani / lekérdezni. Például a routing tábla kiíratása:



ii) SSH

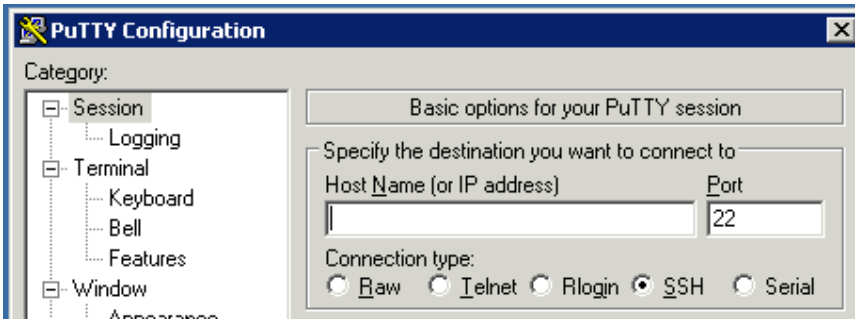
A hálózatok publikussá válásával a biztonság is egyre inkább előtérbe került. Ennek szükségességére gyakorlati példák is felhívták a figyelmet. Mivel a telnet protokoll titkosítatlanul továbbítja az információkat, jelentős biztonsági kockázatot jelent. Könnyű a publikus hálózaton lehallgatni a forgalmat, és az elkapott csomagokat összerakva, már

birtokában is vagyunk a hálózaton keresztül küldött információnak. Ez fordult elő a Helsinki Egyetemen 1995-ben. Itt tervezték meg az SSH első változatát.

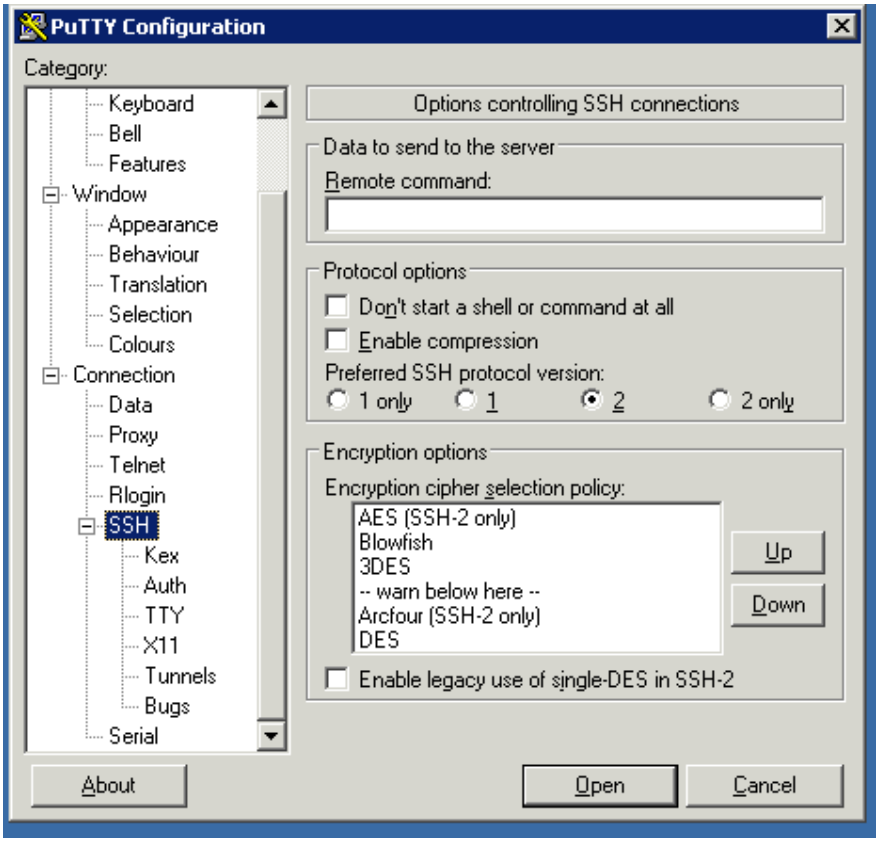
Az SSH már titkosítottan küldi az adatokat, nyilvános kulcsú titkosítást használva. Mivel a telnet kiváltására készült rendszerről van szó, megfigyelhetőek bizonyos analógiák. Az SSH is kliens-szerver architektúrára épül. Alaphelyzetben, ha egy szerverre SSH-val csatlakozunk, ekkor is egy shell indul el a szerveren, amiben ugyanazokat a parancsokat adhatjuk ki, mintha soros terminálon, vagy telnet-en keresztül lennénk belépve. Tehát ugyanazokat az adminisztrációs feladatokat is végezhetjük el.

Példa: egy népszerű Windows-os SSH kliens – PUTTY

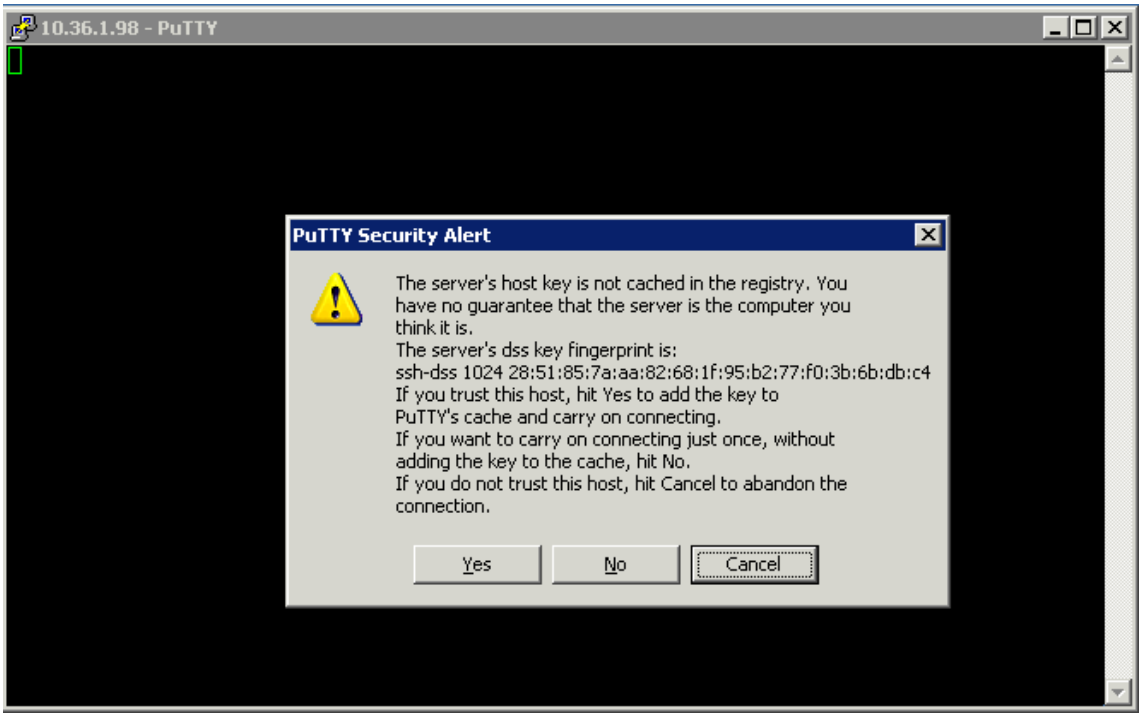
A PUTTY program nem csak SSH alapú kapcsolódásra alkalmas, de most ez a tulajdonsága az érdekes. Természetesen itt is meg kell adni a célrendszer valamilyen hálózati azonosítóját.



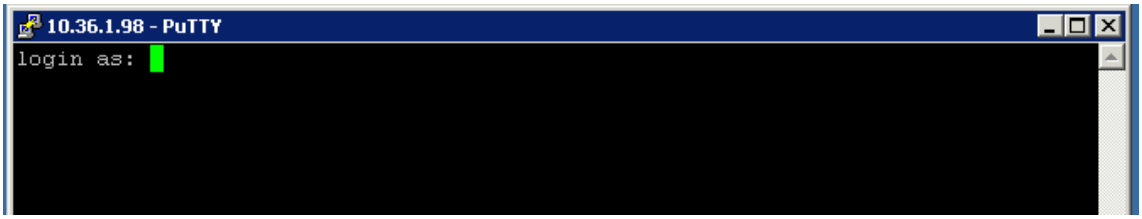
Az SSH opciók között különböző azonosítási beállítások adhatóak meg, pl. key exchange group, stb. Itt hozhatunk létre port forwarding-hoz tunnel-eket is.



Az SSH nyílt kulcsú titkosítást használ. Ennek a működési elve azon alapul, hogy minden, a kommunikációban részt vevő félnek, van egy kulcspárja. Az egyiket nevezzük nyilvános (publikus), a másikat magán (privát) kulcsnak. Ezek olyan viszonyban vannak egymással, hogy ha a küldő egy adatot letitkosít a privát kulcsával, akkor azt a fogadó csak a publikus kulcs ismeretében tudja dekódolni. Ehhez persze szükség van olyan függvényekre, amelyek egymás inverzei. A publikus kulcsot a küldő az adás előtt nyilvánosságra hozza. Ezzel a rendszerrel biztosítható, hogy az információ nem változik meg az adatátvitel folyamán (mivel ekkor e publikus kulccsal már nem lehetne visszafejteni), illetve nem lehet hamisítani a feladót (hiszen ehhez a küldő privát kulcsának az ismerete szükséges, e nélkül a visszafejtés megint nem működik). Amennyiben egy olyan szerverhez akarunk csatlakozni, aminek nem ismert a publikus kulcsa, a rendszer felajánlja, hogy elmenti:



Ezek után már egy telnet kliens belépő felületéhez hasonló képernyőt kapunk, elvégre egy shell indul el:



iii) Microsoft távadminisztrációs eszközök

A Microsoft kliensekből álló hálózatokon is lehet követni a cég politikájának fejlődését. Eljutottak az otthoni, kis hálózatoktól (amelyek kevés kliensből állnak, nem IT szakértő felhasználók a célközönség – tehát ne legyen bonyolultan konfigurálható) a nagyméretű, több szegmensből álló vállalati hálózatokhoz, melyek akár már Interneten, VPN-en keresztül is csatlakozhatnak egymáshoz. A kezdeti, kevés kliensből álló hálózatok által használt protokoll a NetBIOS. A NetBIOS hálózati protokollt használó eszközök az eddig tárgyalt rendszerektől teljesen eltérő filozófiát képviselnek. A Microsoft terméke, és mivel a Microsoft kezdetben az asztali számítógépek piacára koncentrált, ott vált piacvezetővé, az általa kifejlesztett NetBIOS

hálózati protokoll is szakít a klasszikus kliens-szerver architektúrával. Legalábbis látszólag. A NetBIOS felfogás szerint a hálózat egyenrangú kliensekből áll. Bármelyik kliensről csatlakozhatunk bármelyik kliens megosztott erőforrásához. Erőforrás lehet például egy könyvtár a háttértárolón, vagy egy nyomtató. Csatlakozáskor viszont a csatlakozást kezdeményező, megosztott erőforrást elérni akaró állomás kliens funkciót vesz fel, a megosztással rendelkező állomás pedig kiszolgálja a kérést, tehát ő a szerver. Ezek a szerepek viszont flexibilisek, feladatról feladatra változnak. A NetBIOS jelenleg már TCP/IP alapú protokollként a legelterjedtebb (mivel a TCP/IP alapú hálózatok a legelterjedtebbek), bár létezik Novell/Netware implementációja is. Kezdetben viszont egy NetBEUI nevű, saját protokollt használt, ami szintén Microsoft fejlesztés volt, és a Win95, WinNT, Windows for Workgroups operációs rendszerek használták. Az alapkoncepció az, hogy a felhasználónak semmilyen konfigurációt nem kell elvégeznie, csak csatlakoztatja a működő számítógépét a hálózatra. Persze itt sem lehet megúszni kezdeti beállítás nélkül. A munkaállomásnak meg kell mondania, hogy melyik NetBIOS csoportba tartozzon (workgroup name), és a saját nevét ezen a csoporton belül. Ezután a többi már automatikus.

Jelenleg a legelterjedtebb NetBIOS implementációk TCP/IP protokollt használnak. Ebben az esetben a működési elv a következő. Első lépésben megvásárolt a Microsoft egy hálózati tartományt (169.254.0.0/16). Mivel mindennek automatikusnak kell lennie, a munkaállomások IP cím, netmask, stb. beállításai már nem fértek bele a koncepcióba. A kliensnek viszont valahogy címet kell kapnia, hogy kommunikálni tudjon. Ez történhet például DHCP szerver segítségével. Most vegyük azt az esetet, ha nincs DHCP szerver a hálózaton (hiszen munkaállomásokból álló hálózatról beszélünk). Ekkor az operációs rendszer várakozik a DHCP szerver által kiosztandó címre, majd ha ez nem történik meg, nem kap címet, akkor a Microsoft fenntartott tartományból ad egy címet az interfésznek. Persze előbb ellenőrzi, hogy ez a cím szabad-e még a hálózaton. Ezzel a módszerrel biztosítva van, hogy a kliensek ugyanazon a logikai subnet-en is legyenek. Ezáltal megvalósítható a NetBIOS másik fő tulajdonsága, a broadcast-tal való kommunikáció. (Mivel a broadcast csomagok csak a küldővel azonos subnet-en levő csomópontokhoz jutnak el.)

A NetBIOS hálózatoknak van egy fontos üzemmódja, a tallózás. Ha ezt a funkciót elindítjuk egy munkaállomáson, az felderíti a vele egy munkacsoportban levő többi munkaállomást. Mindezt broadcast csomagok segítségével. Amennyiben megkaptuk a kívánt állomás nevét,

lekérhetjük az állomás megosztott erőforrásainak a listáját, és megfelelő engedélyek birtokában csatlakozhatunk is hozzájuk.

A NetBIOS abban az esetben is működik, ha esetleg DHCP szerver osztja a címeket a hálózati szegmensben, hiszen az így kiosztott címek is egy alhálózatba esnek, így a broadcast kommunikáció itt is működik.

Persze ez volt eddig az ideális elmélet. Az informatika rohamos fejlődésével ugyanis a hálózatok, hálózati szegmensek mérete is nőni kezdett, így az üzenetszórásos kommunikáció nem bizonyult túl robosztusnak. Képzeljük el, ha a tallózásra egy kliens válasza nem érkezik meg időben a hálózat telítettsége miatt. A tallózást kérő kliens nem fogja a hálózaton ”látni” a késett csomag gazdáját. Ennek első kiküszöbölési megoldása a főtallózó bevezetése volt. Minden szegmensen kijelölésre kerül egy kliens, aki nyilvántartja a szegmens gépeinek a listáját. Ez általában a legelsőnek bekapcsolt állomás. A főtallózó nyilvántartja a lehetséges további főtallózókat, akik átvehetik ezt a szerepet az aktuális főtallózó kilépése esetén.

A következő lépés a WINS bevezetése volt (Windows Name System). Az alap problémát az jelentette, hogy szeretnénk NetBIOS használatával másik hálózati szegmensen található megosztott erőforrásokat elérni. Itt például TCP/IP esetén arról van szó, ha egy munkacsoport gépei több TCP/IP subnet-en találhatóak, a használt broadcast csomagok nem jutnak el a másik szegmensbe. A megoldást egy WINS szerver beállítása jelenti. Ez a szerver nyilvántartja a munkacsoport klienseinek a nevét és az aktuális IP címét. A kliensen be van állítva a WINS szerver címe (akár fix-en, akár DHCP opción keresztül), így nem csak Broadcast csomagokkal „tapogatja” végig a hálózatot a többi munkaállomás után, hanem a WINS szervert is lekérdezi, milyen munkaállomások találhatóak a munkacsoportban. Illetve ha el akarunk érni egy munkaállomást, a WINS szerver szolgáltatja a névhez tartozó IP címét. A WINS szerverre a kliensek beregisztrálják magukat, így üzemeltetése nem igényel beállítást, csak fel kell telepíteni, és el kell indítani. Egyetlen beállítási lehetőség, hogy megadhatunk más WINS szervereket, amikkel információt cserél. Tulajdonképpen egy nagyon leegyszerűsített DNS szerverről van szó.

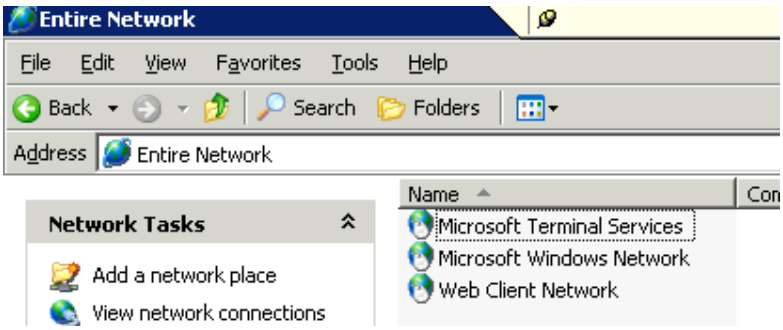
Az Active Directory szintén egy Microsoft rendszer, ezt már professzionálisabb környezethez tervezték. Szorosan integrálódik a DNS-hez, a NetBIOS-hoz, feltételez legalább egy dedikált szervert a hálózaton (domain controller), és az asztali operációs rendszereknek is a professional verziója szükséges. Segítségével központi beállításokat „küldhetünk le” a kliensekre, illetve egy adott domain tag munkaállomásról elérhetjük egy másik domain tag

munkaállomás, vagy akár szerver erőforrásait, illetve megváltoztathatjuk a rendszer tulajdonságait. Ehhez azonban előbb domain taggá kell léptetni (beléptetni a domain-be) az adott számítógépet. Innentől kezdve a munkaállomás kap egy objektumot az Active Directory tárolójában, ennek az objektumnak a tulajdonságait határozhatjuk meg távadminisztrálás esetén. Továbbá a felhasználók is kapnak egy objektumot az Active Directory-ban, ezeknek az objektumoknak a tulajdonságait állítva a munkaállomáson érvényes felhasználói környezet tulajdonságait állíthatjuk.

Még egy dolgot tartok szükségesnek megemlíteni a példák bemutatása előtt. Ez az UNC (Universal Naming Convention vagy Uniform Naming Convention). Ez egy közös szintaxist ír le, amivel meg lehet adni egy hálózati erőforrás helyét és nevét. Ez lehet egy munkaállomáson megosztott könyvtár, nyomtató, stb. Windows környezetben a szintaxis a következő: //számítógépnév/megosztott_könyvtár_neve/megosztott_erőforrás_neve . A / jelek helyett használható a \ jel is. Ezek definíció szerint egyenértékűek, de a köztudatba a \ jel használata épült be jobban, sok alkalmazás csak ezt fogadja el.

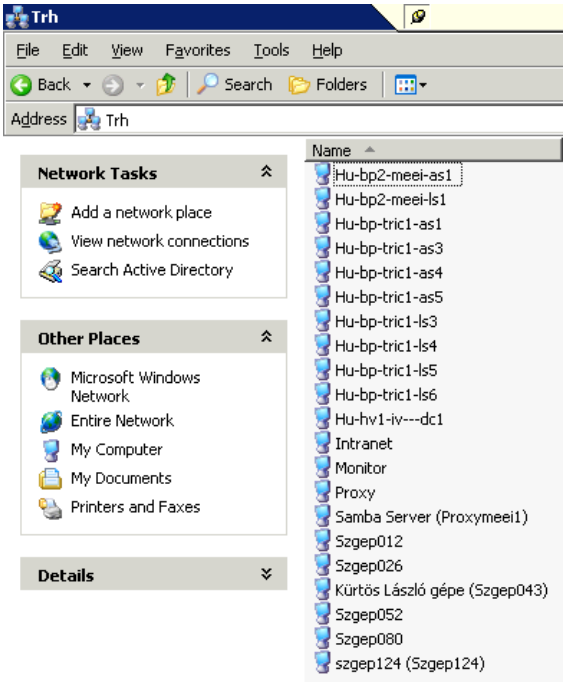
Példa: file sharing elérése NetBIOS segítségével

A kiinduló helyzet, a teljes hálózat (Hálózati helyek megnyitása - Start menüből, vagy a Saját gép ablak Cím legördülő menüjének segítségével):

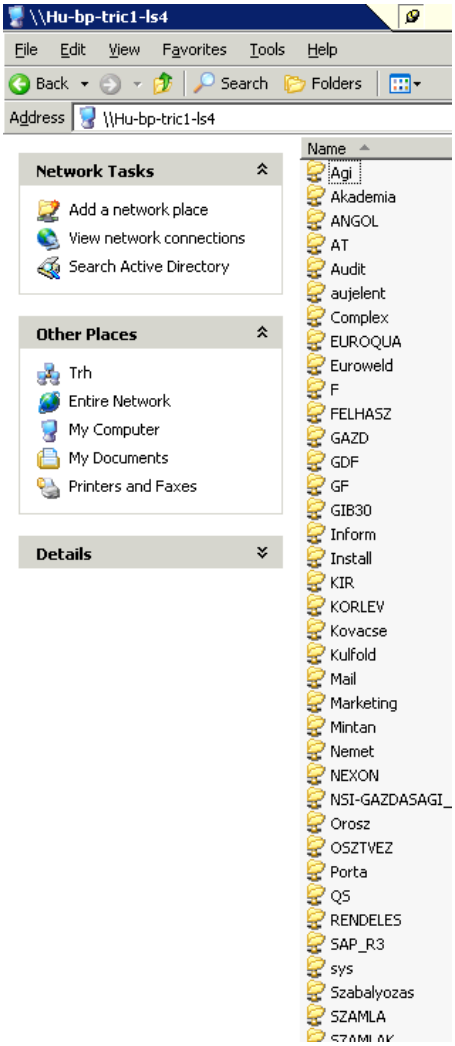


Itt a Microsoft Windows hálózatot választva a következő képet kapjuk. Itt jelen esetben több Munkacsoport látszik:

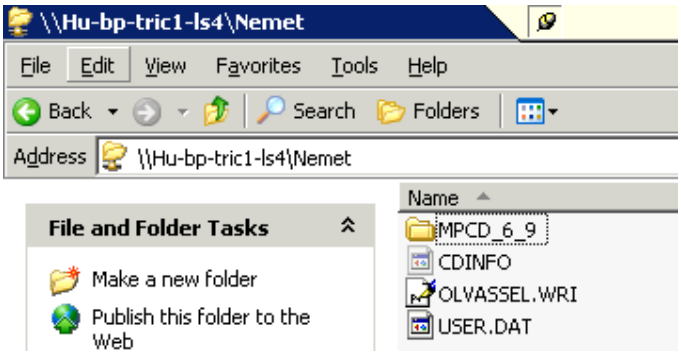
A Trh munkacsoporton duplán kattintunk. A Trh munkacsoport éppen bekapcsolt tagjai:



Ha a munkaállomás nevén kattintunk duplán, a következő képernyőhöz jutunk. Egy munkaállomás megosztott könyvtárai:



Majd egy megosztott mappát megnyitva:

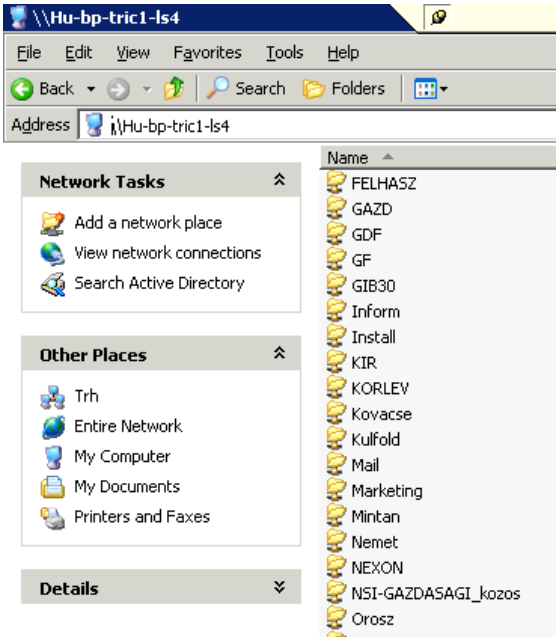


A Címsorban levő UNC elérési utat beírva a Windows tallózó ablakainak Cím mezőjébe közvetlenül is elérhetjük a megosztást. A munkaállomás neve IP címmel is helyettesíthető. Ekkor a Cím mezőbe \\IP_cím\megosztás_neve formát kell használni.

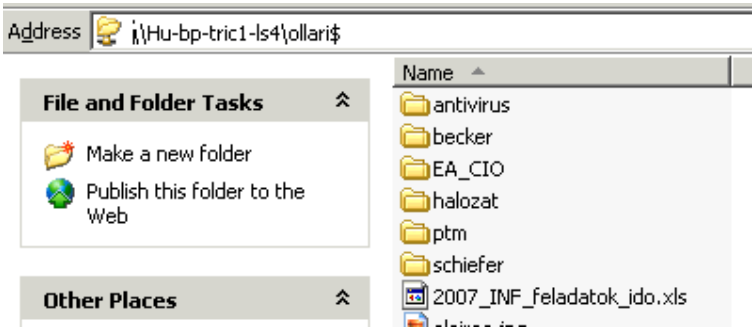
Példa: c$ megosztás, akármilyen $ megosztás

A Microsoft erőforrás megosztási rendszere ismer u.n. adminisztratív megosztást is. Minden hálózatba kapcsolt munkaállomás helyi meghajtójának gyökere meg van osztva alapértelmezettként, az adminisztrátorok csatlakozhatnak hozzájuk. Ezek a megosztások rejtettek, egy egyszerű tallózáskor láthatatlanok. Egy ilyen megosztást úgy érhetünk el, hogy a megosztási név mögé $ jelet írunk csatlakozás esetén.

Példa: itt nem látszik az ollari nevű megosztás:

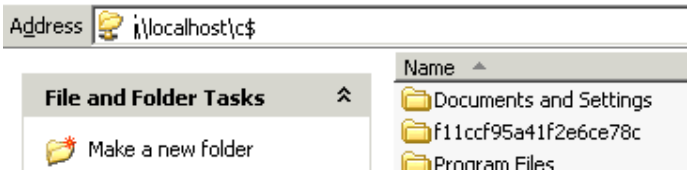


Mégis létezik (kézzel beírva a Cím mezőbe a megosztás teljes UNC nevét):



A helyzet hasonló, pl. a helyi munkaállomás c: meghajtójának megosztásával:

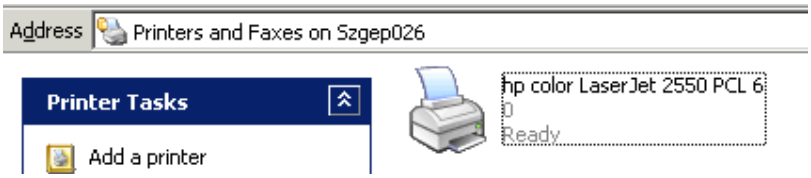
A fenti képen nem látszik a megosztott erőforrások között, mégis lehet hozzá csatlakozni.



Példa: megosztott nyomtató telepítése NetBIOS-on keresztül

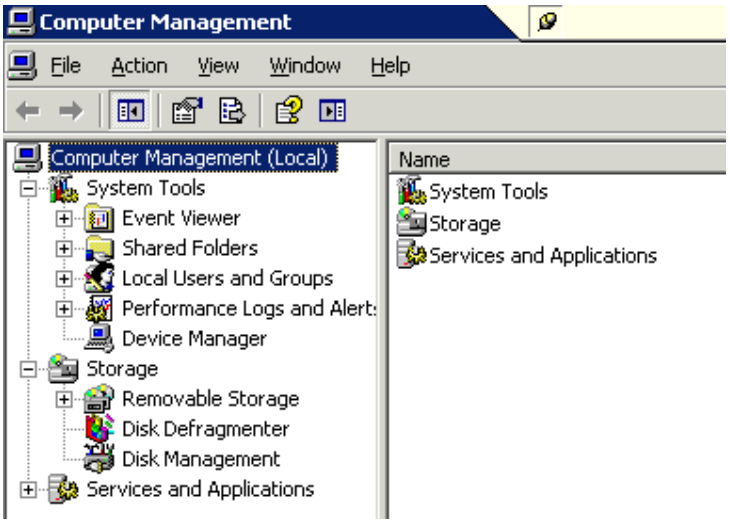
Egy munkaállomásra rájelentkezve a megosztott erőforrások között megtaláljuk a Nyomtatók és Faxok csoportot.

A Nyomtatók és Fax-ok megnyitása után megtalálhatóak a megosztott nyomtatók, amelyeken duplán kattintva már csatlakoztunk is a távoli nyomtatóhoz.

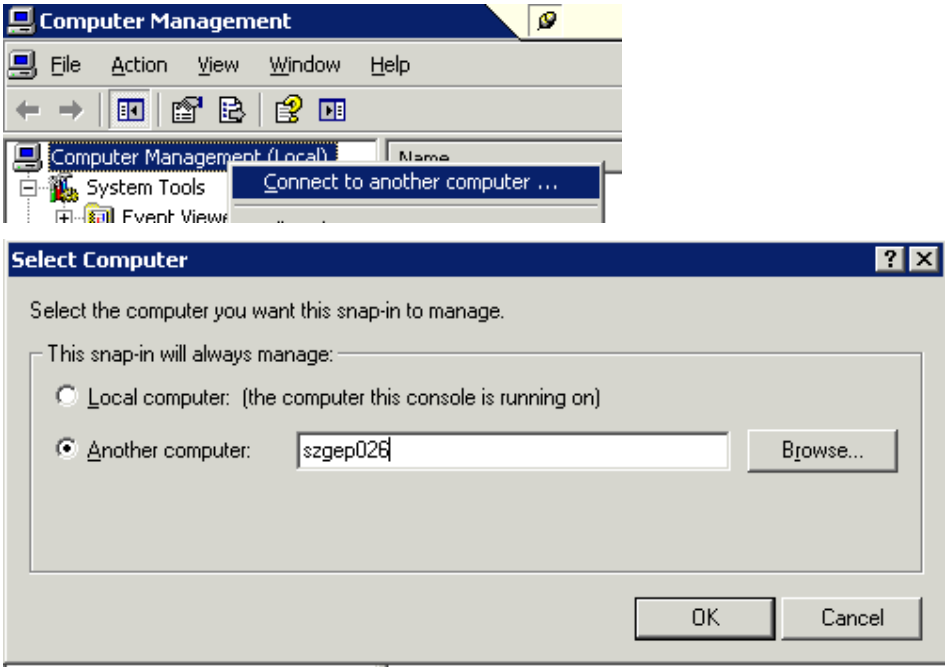


Példa: távoli gép kezelése

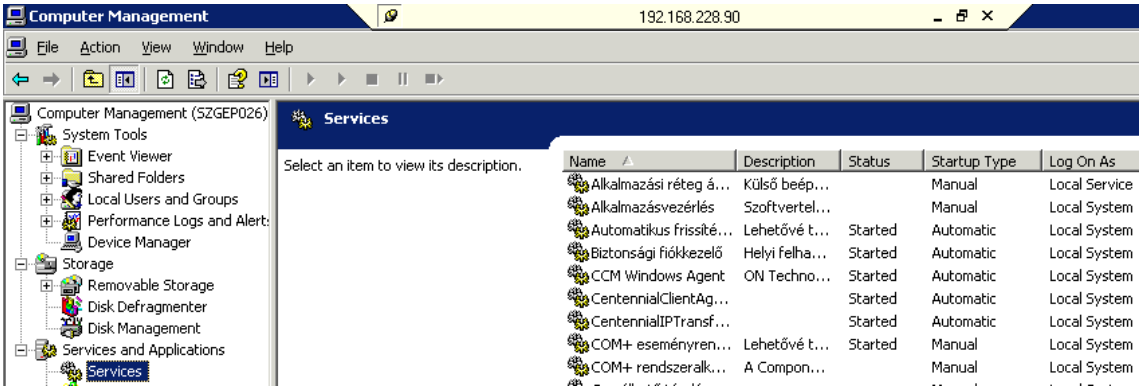
Kezdjük a Számítógép-kezelés beépülő modullal a helyi géphez csatlakozva. Ennek elérése legegyszerűbben: jobb kattintás a Saját gép ikonon, majd a Kezelés menü választása.



A fenti kép megjelenése után csatlakozzunk a távoli munkaállomáshoz. Ennek a menünek az eléréséhez szintén egy jobb kattintás szükséges a Számítógép kezelés csomóponton.

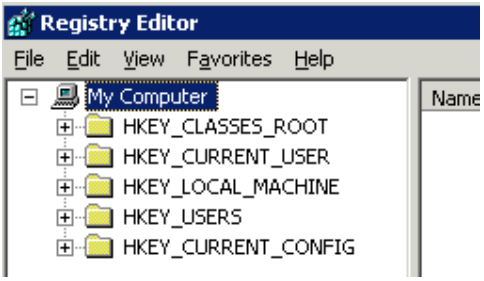


Itt a távoli gépre való csatlakozásnak több módja van. Vagy a Tallózás gomb segítségével a hálózaton levő gépeket fellistáztatjuk, vagy beírjuk a gép UNC nevét. És már kezelhetjük is, például egy távoli rendszer szervizeit. A lenti képen már csatlakoztunk az szgep026-os munkaállomáshoz, ugyanazokat a rendszertulajdonságokat látjuk, mint a kezelőpanel megnyitásakor a saját gépre vonatkozóan. Tehát a háttérben állíthatjuk a távoli rendszer tulajdonságait. (például leállíthatunk, elindíthatunk szervizeket)

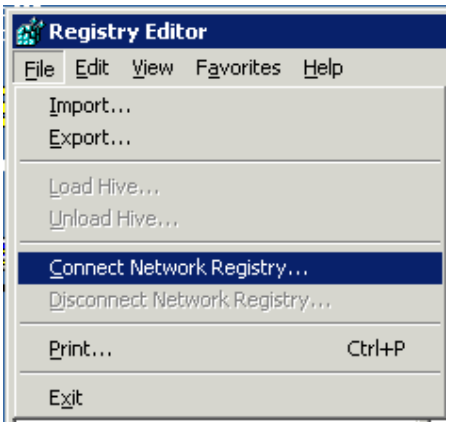


Példa: távoli registry elérése

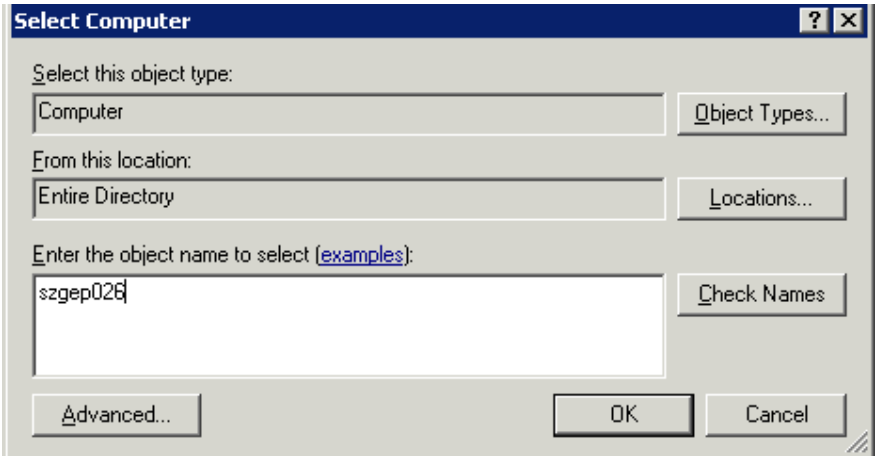
Registry Editor megnyitása a helyi gépen (regedit parancs kiadásával):

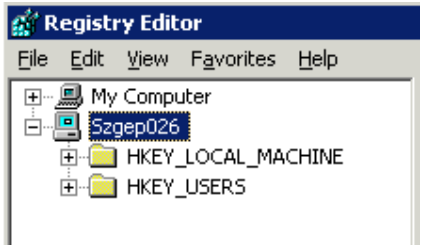


Majd csatlakozás a távoli registry-hez (A Registry editor File menüjének használatával):



Itt szintén UNC gépnév megadásával csatlakozhatunk a távoli munkaállomáshoz. Ez a panel nem a hálózatot tallózza fel, mint például a távoli számítógép kezelés, hanem Active Directory objektumok között keres.



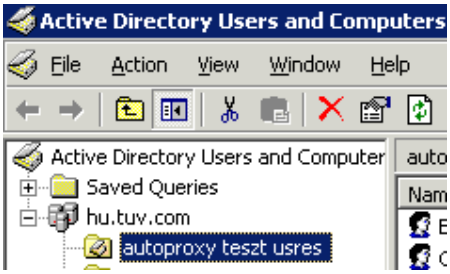


És már lehet is módosítani a távoli munkaállomás registry bejegyzéseit (persze ha a megfelelő felhasználói jogosultsággal rendelkezünk)

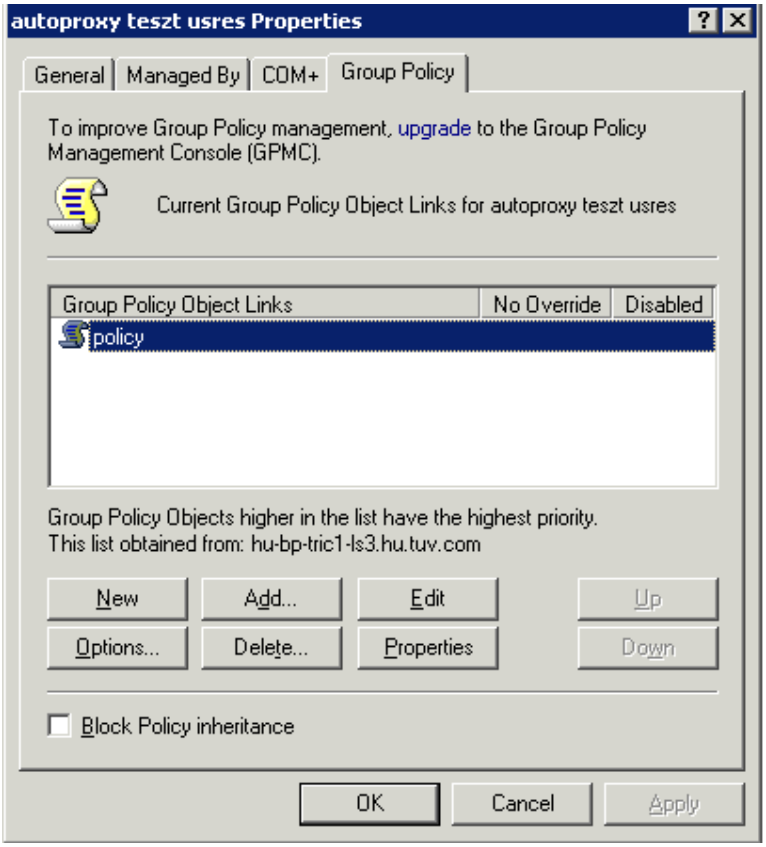
Példa: központi felhasználó-kezelés: proxy szerver beállítása

Ehhez szintén szükségünk van Active Directory-ra is. Ebben a felhasználókat csoportba szervezve, a csoportra írhatunk elő központi beállításokat, u.n. group policy-k segítségével. A példaként bemutatott beállítás az Internet Explorer által használandó proxy szerver beállítása.

Ehhez már Domain Controller szerverre van szükségünk. A szerveren a Start menü, Administrative Tools menüjében, az Active Directory Users and Computers menüt választva juthatunk el ide a legegyszerűbben. (ugyanez megoldható az mmc program indításával, és a megfelelő snap-in hozzáadásával is) A csoport (Organizational Unit) a hu.tuv.com domain alatt:

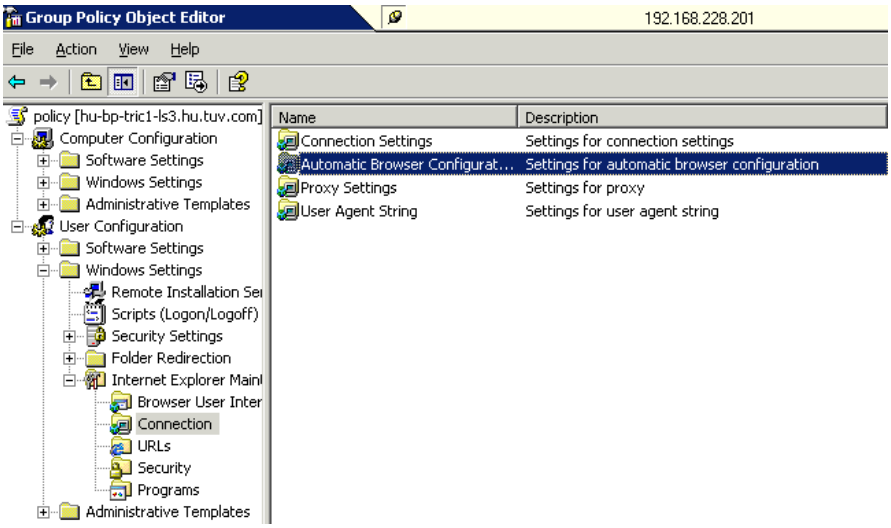


Jobb kattintás az OU-n, és a Properties menü után, a Group Policy fület választva megnézhetjük a rá érvényes group policy-t:

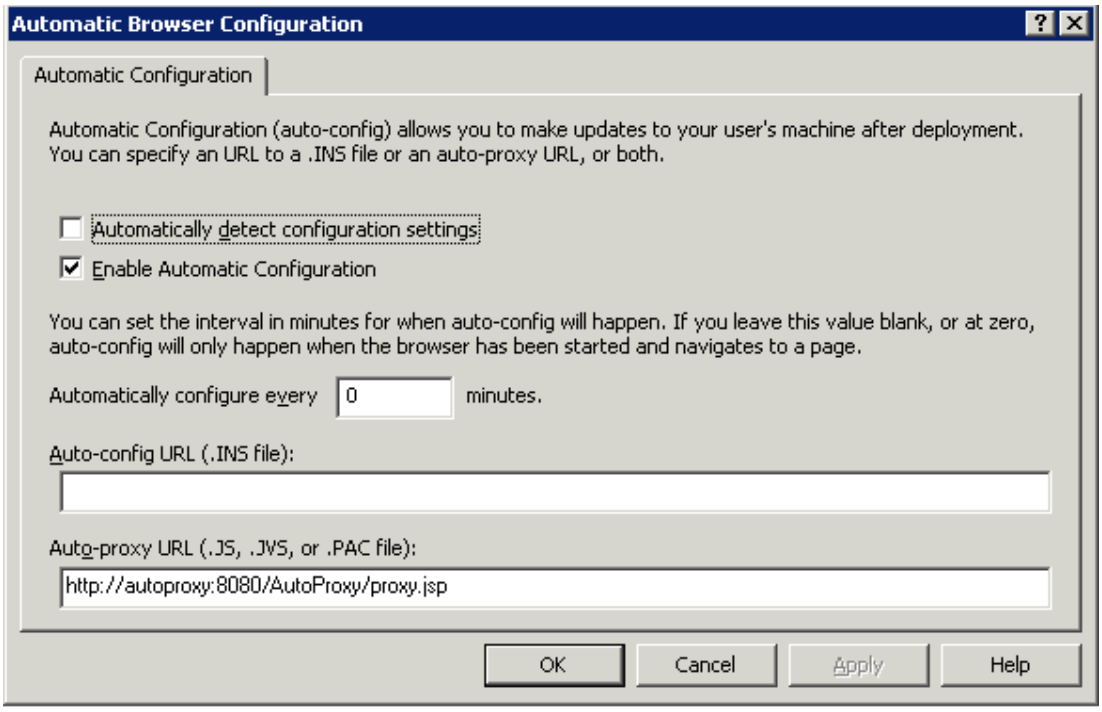


A policy-t szerkesztve, megnyílik a Group Policy Object editor. Itt fa struktúrába szervezve az adott csoportra alkalmazható beállításokat láthatjuk.

Az aktuális proxy beállítás elérése:

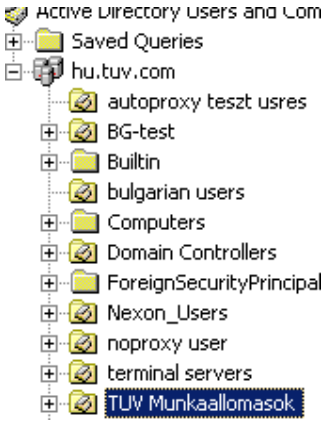


Ezt megnyitva, a proxy szerver (illetve jelen esetben egy másik szerver, ami megadja a használandó proxy szerver címét) eléréséhez szükséges információk vannak megadva. Ezek vonatkoznak az összes AD felhasználóra, akik az adott OU-ban vannak.

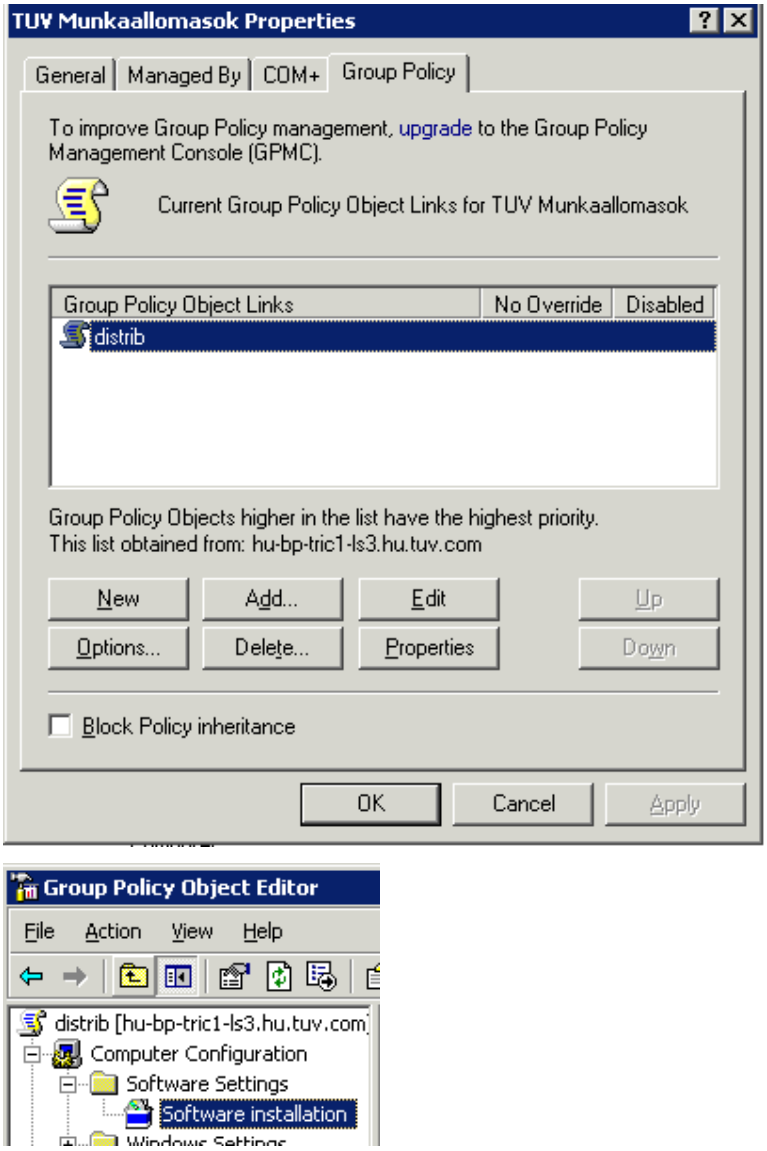


Példa: központi munkaállomás-kezelés: távoli szoftvertelepítés

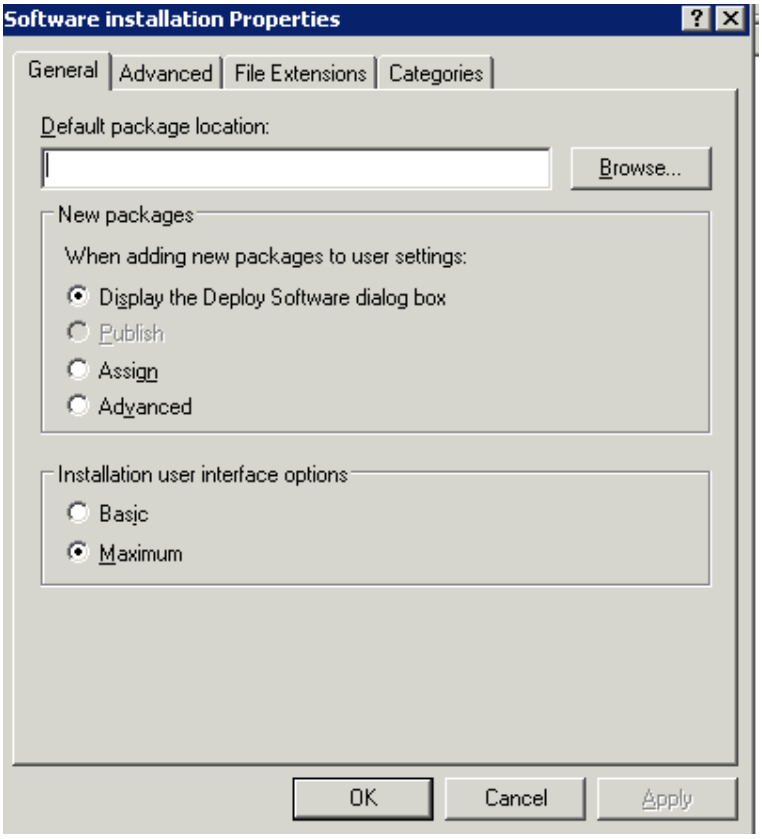
Ezt is group policy-n keresztül tehetjük meg, de itt a csoportban nem felhasználók, hanem munkaállomások vannak.



A TUV Munkaállomások OU-ra alkalmazott group policy-t nyitjuk meg szerkesztésre.



Itt megadhatjuk a telepítendő MSI csomagot, és különféle opciókat.



A fentebb tárgyalt NetBIOS-on keresztüli távoli erőforrás elérések, illetve Active Directory alapú adminisztrációs beállítások Microsoft rendszerekhez tartoznak, tehát fizetősek. Vannak köztük realtime hatásúak (szerviz leállítása), illetve késleltetett hatásúak (group policy-n keresztüli beállítás-megváltoztatás)

iv) RDP

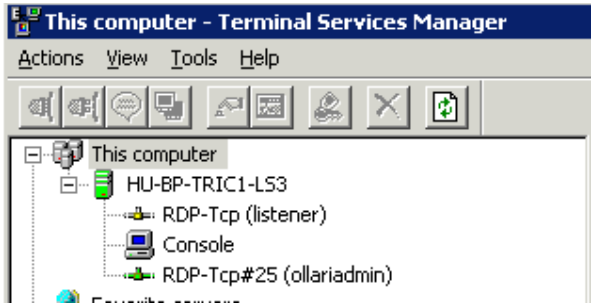
Az RDP (Remote Desktop Protocol) – lánykori nevén Microsoft Terminal Services (MSTS), szintén Microsoft rendszer. Mint a neve is mutatja, itt egy telnet-hez hasonló dologgal állunk szemben. Be lehet jelentkezni egy távoli rendszerbe, aminek a felhasználói képernyőjét (desktop) a mi munkaállomásunkon láthatjuk, kezelhetjük. Persze az azóta eltelt 30 év hozott néhány változást, így az RDP is kilépett a szöveges környezetből, már grafikus felületet tud átvinni. A fő elmélet azonban nem változott. Szükséges egy szerver, amin fut az RDP szerviz, és ami ismeri a belépni szándékozó felhasználót. A felhasználó egy kliens programmal csatlakozik a szerverhez hálózaton keresztül. A kliens programnak szüksége van a szerver elérhetőségére, valamint a port számára, ahol a szerviz található. Ez standard szerint a 3389-es, de ez módosítható a registry-ben.

A kliens program Windows 2000 és attól újabb rendszereknél az alaptelepítésben futtatható állományként megtalálható. Van azonban egy másik verziója is, a klienssel nem rendelkező munkaállomások számára. Az RDP kliens tud települni ActiveX vezérlőként is. Ehhez persze engedélyezni kell a böngészőnkben az ActiveX komponensek telepítését, de ha ezt megtettük, akkor az RDP kliens beépül a böngészőnkbe, és egy megadott Internetcímet megnyitva, ugyanazokat az RDP szolgáltatásokat tudja nyújtani, mint az önállóan futtatható RDP kliens.

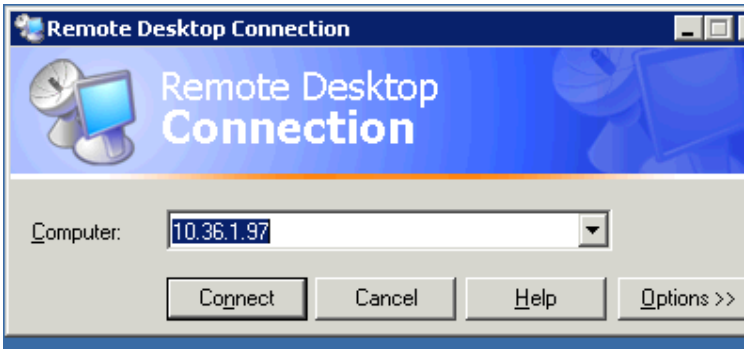
A csatlakozás sikeres végrehajtása során a felhasználó munkaállomásán megjelenik az adott szerver bejelentkeztető konzolja, ami kéri a felhasználónevet , jelszót, a beléptetési tartományt (amennyiben tartományi tag az adott szerver), és ezek után a megjelenő Windows munkafelületen bármilyen feladatot elvégezhet, amit a szerver lokális konzolján bejelentkezve – tehát adminisztrálhatja is akár a távoli rendszert.

Példa: RDP management konzol, RDP kapcsolódási folyamat

A szerver RDP session-jei. Ezeket a szerveren a Start menü, Administrative tools, Terminal Services Manager alkalmazás elindításával érhetjük el. A lokális konzolt is mutatja, valamint van egy aktív session, és egy, ami figyel az új belépőkre várva.

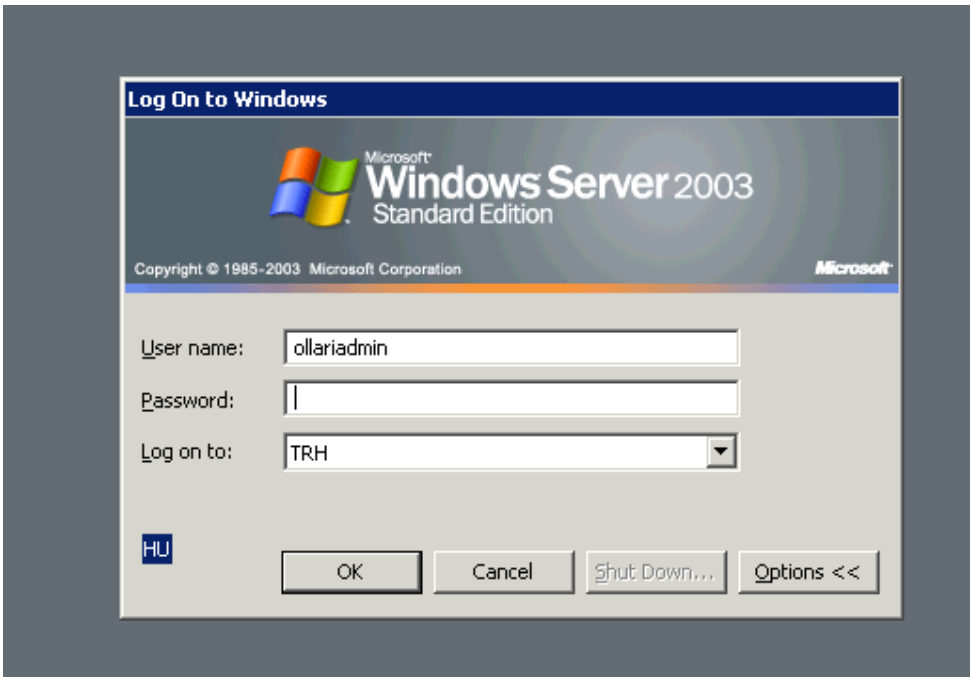


RDP kliens (vagy az mstsc parancs kiadásával, vagy Start menü- Kellékek – Távoli asztal kapcsolat menün keresztül):

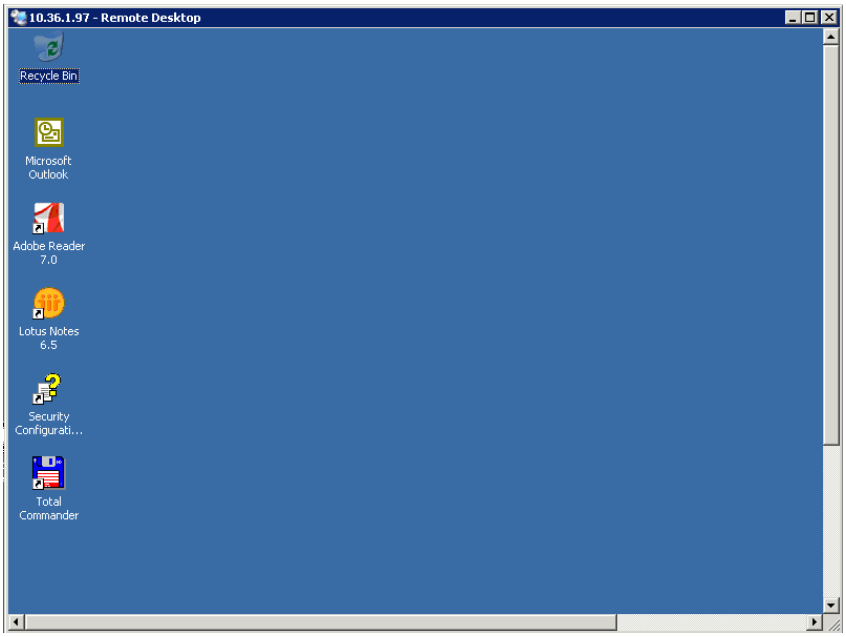


Itt meg kell adni a távoli munkaállomás elérési információját (IP cím vagy NetBIOS név)

Majd a sikeres csatlakozás után megjelenik a bejelentkeztető képernyő:



Kéri a távoli rendszer a user nevet és a jelszót, mintha lokális konzol előtt ülnénk. Majd sikeres belépés után megkapjuk a felhasználói felületünket:



Az RDP egyik „mutációja”, tehát ide tartozik, viszont nem teljesen háttér távadminisztrációs rendszer a Windows XP-be beépített távoli segítségnyújtás. Ennek használatához először a távoli munkaállomáson a felhasználónak engedélyeznie kell az adott funkciót, ami nem tesz mást, mint elindítja az RDP szervert service-ként a munkaállomáson. Ezután az

adminisztrációt végző személy csatlakozhat RDP kliensével a rendszerre. Mivel azonban egy asztali operációs rendszerről van szó, a Windows XP nem tud több user session-t kezelni. Ezt úgy oldja meg, hogy a távolról csatlakozó felhasználó a helyi session-re lép be, tehát a gép előtt ülő felhasználó akár láthatná is, hogy mi történik a gépén, de valamilyen biztonsági szempontból (például az adminisztrátorként bejelentkezett felhasználót ne tudja a user használni) a helyi konzol zárolásra kerül, amíg az adminisztrációt végző személy ki nem lép. Ezzel a módszerrel távolról el lehet mindent végezni, amit a működő operációs rendszerben helyileg el lehet.

3) Web alapú távadminisztrációs rendszerek

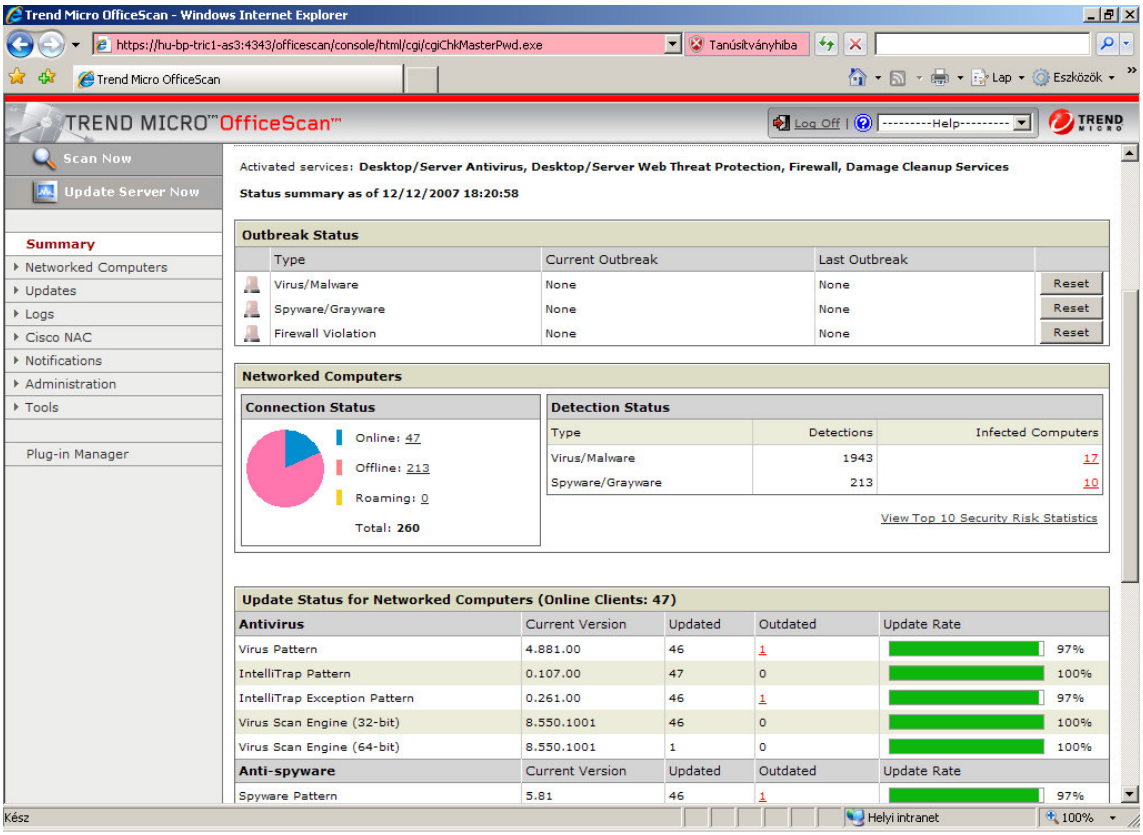
Az eddig ismertetett távadminisztrációs rendszereknek, lehetőségeknek van egy nagy hátrányuk. Speciális kliens program szükséges hozzájuk. Természetesen sok operációs rendszerbe be van építve a telnet kliens, ingyenesen le lehet tölteni a PUTTY SSH klienst, és még telepíteni sem kell, az Active Directory eszközei be vannak építve a Windows munkaállomásokba, de mi a helyzet például egy PDA-val? Ott már könnyen előfordulhat, hogy nem rendelkezünk a fenti rendszerek kliens oldali eszközeivel. Viszont az igazán modern, flexibilis távadminisztrációhoz jól jöhet egy kisméretű, hordozható, mobil internetkapcsolattal rendelkező eszköz, aminek a súlya töredéke egy notebook-nak is. Megfordítva a logikát, ha a gombhoz keressük a kabátot, felvetődik a kérdés: milyen távoli adatátviteli lehetőség, illetve kliens adott a mobil, internetkapcsolattal rendelkező eszközök nagy részén? A megoldás: webböngésző. Tehát az adminisztrálandó rendszernek rendelkeznie kell egy webfelülettel, amin keresztül a viselkedését befolyásoló változtatásokat tehetünk. Operációs rendszer szintjén ilyennel még nem találkoztam. De ha elvonatkoztatunk az operációs rendszerektől, és más számítógépes rendszereket veszünk figyelembe, az alkalmazások palettája széles. Itt most példaként a Trendmicro cég Officescan vállalati antivírus és firewall rendszerének adminisztrációs felületét szeretném megmutatni.

Ez egy fizetős rendszer, a liszenszet a kliensek száma szerint kell megvenni (hány kliensre van a program feltelepítve). A gyártó weblapja: www.trendmicro.com .

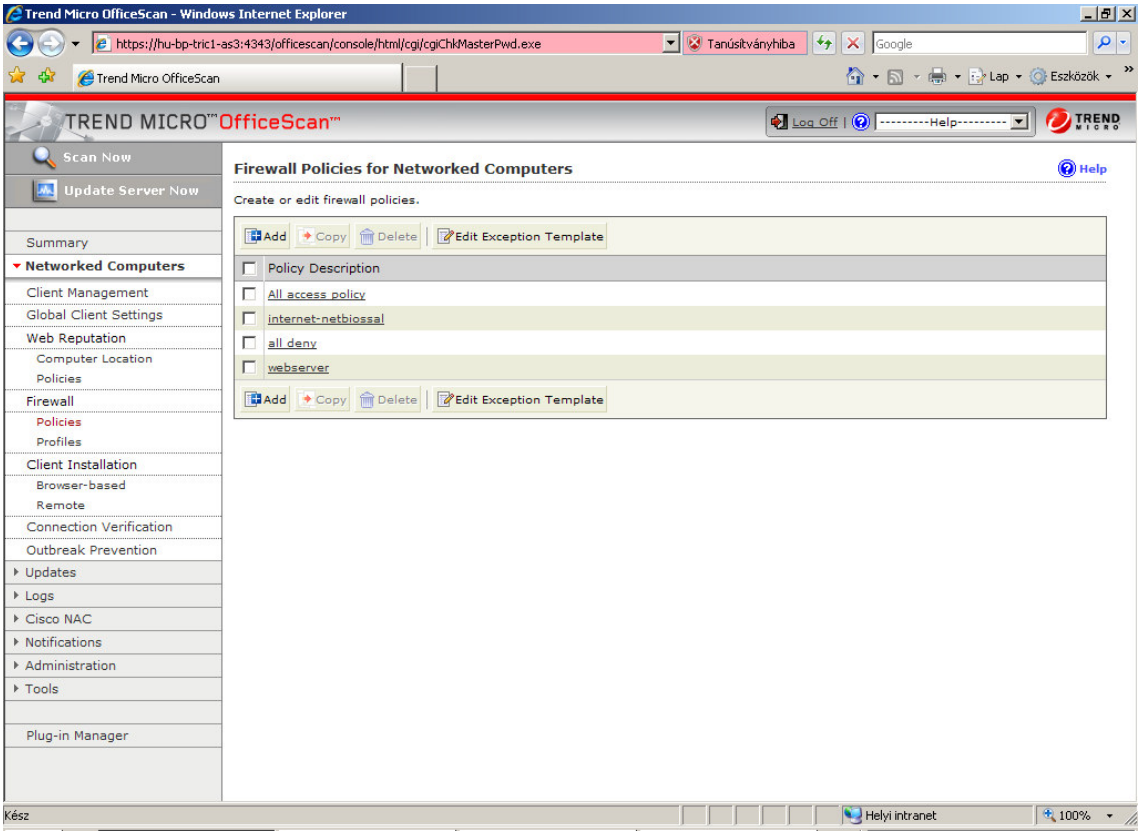
Példa: Officescan webes adminisztrációs felülete

Először csatlakozunk egy szabványos webböngésző segítségével. HTTPS protokoll használatával a szerver adminisztrációs felületéhez (professzionális rendszerről van szó)

Itt két választásunk van: vagy a link-re kattintva telepítjük az antivírus és tűzfal klienst arra a gépre, amiről megnyitottuk az oldalt, vagy a jelszó megadásával belépünk a szerver adminisztrációs weblapjára. Most ez utóbbi következik:

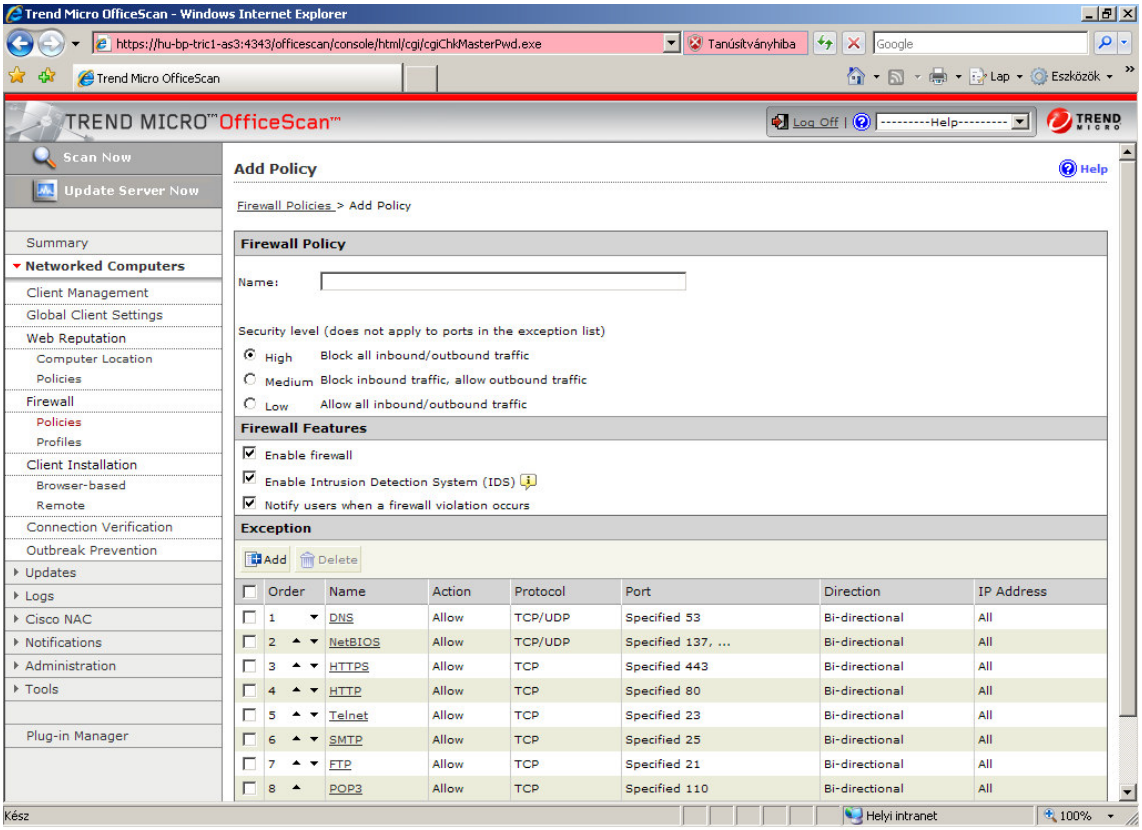


Belépés után a főképernyőn kapunk egy összefoglaló statisztikát a rendszer (szerver illetve csatlakoztatott kliensek) állapotáról. Valamint a konfigurációt módosíthatjuk, például új tűzfal-szabály felvitele. Ehhez a Networked Computers linkre (ezt kiemelném – nem csomópont, nem menü, link – hiszen WEB felületen vagyunk) kattintva a Firewall link-et kell megnyitni.



Itt a jobb oldali kezelőpanelben már egy ActiveX-es beépült program fut, amin aktív elemek (nyomógombok, rádió gombok, stb. vannak).

Majd az Add gomb megnyomása után megtekinthetjük a már meglévő tűzfal szabályokat, illetve módisíthatjuk is őket. Módosíthatjuk a sorrendet. Ez azért fontos, mert az alkalmazandó szabály kiválasztása úgy történik, hogy minden szabályhoz meg van adva egy kritériumrendszer. A kliens elkezdi az adott sorrendben végignézni a szabályokat, és az első olyan szabályt alkalmazza, aminek a kritériumait teljesíti. Az utána levőkkel már nem foglalkozik.



A fentebb bemutatott rendszert általánosítva a következőkről van szó. Van egy rendszerünk, amit távolról szeretnénk adminisztrálni. Ennek a rendszernek vannak különböző, a viselkedését befolyásoló opciói. Például Linux rendszerek esetén konfigurációs fájlok, amikben egy opció értéke igen sok esetben „Yes” vagy „No”. Az adott rendszer induláskor felolvassa a konfigurációs fájlt, és az adott opció értékének függvényében tesz valamit. A rendszer működésének távolról történő megváltoztatásához végeredményben az opció értékét kell tudnunk távolról megváltoztatni. Ezután újraindítani a rendszert, újraolvastatni vele a konfigurációt. Ha éppen nem olyan a beállítás, hogy periódikusan történik az újraolvasás. Az opció megváltoztatásához pedig egy szerver oldali alkalmazás kell, ami megjeleníti az aktuális beállítást, és meg tudjuk neki mondani, hogy melyiket változtassa meg. Ehhez a modellhez pedig egy WEB alapú kezelőfelület teljesen megfelelő a GET és POST metódusaival (tudunk vele adatot lekérni, megjeleníteni, majd adatot küldeni).

4) Előtér távadminisztrációs rendszerek

Az eddig tárgyalt háttér távadminisztrációs rendszerek természetesen nem mindenhatóak, nem alkalmasak az összes lehetséges felmerülő probléma megoldására. Sokkal inkább egy rendszeradminisztrációját segítő eszközök, és kevésbé felhasználói támogatást segítő eszközök. A felhasználói támogatás napi munkájában többször van szó olyan problémáról, ami a felhasználó tudásának hiányosságai miatt merül fel, mint a rendszer hibás működéséből származó hibáról. Tehát szükség van olyan eszközre, aminek segítségével a felhasználó meg tudja mutatni a felmerülő problémát. Persze ebben az esetben még egy olyan kamera is elég lenne, ami távolra tudja transzportálni a felvett képet. Viszont a supporter munkatársnak is tudnia kell beavatkozni a user által látott felületen, így egyszerűbben meg tudja mutatni a megoldást, mint élőszavas irányítással (kattints kétszer ballal a kék E betűre). Valamint ha szükséges, az adminisztrátor be tud jelentkezni a távoli gépére a saját profiljával, és tud pl. programot installálni.

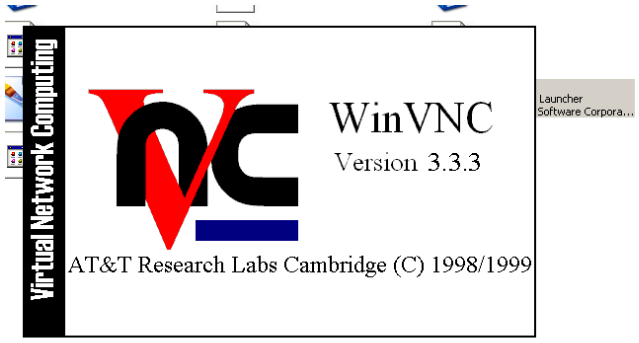
i) WinVNC

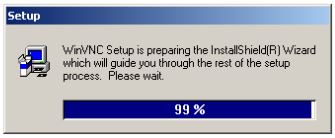
Az első bemutatandó eszköz az ingyenes VNC. A Cambridge-i Egyetemen fejlesztették ki. Kliens-szerver architektúrájú. A szerver egy service-t installál a kliensre, ehhez tudunk később a klienssel hálózaton keresztül csatlakozni.

A VNC a távoli munkaállomás képernyőjét továbbítja a kliensre, és azt a kliens külön ablakban megjeleníti. A kliens egér és billentyűműveletei viszont a távoli munkaállomásra kerülnek továbbítására, az adatkommunikáció viszont kétirányú.

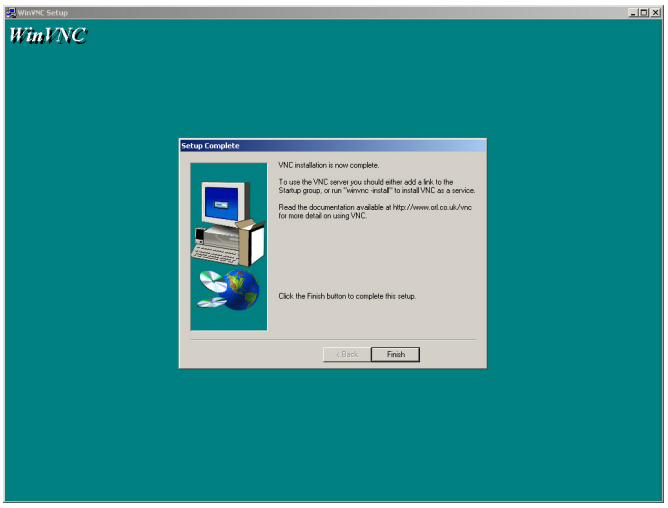
Példák

- ***VNC telepítő***





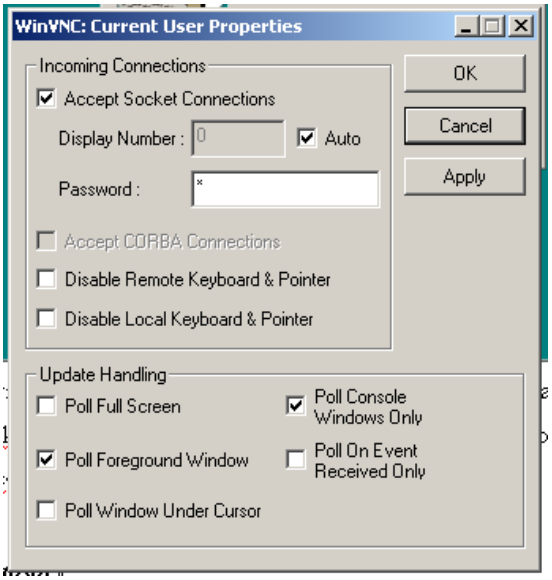
A telepítő utolsó képernyője:



Az utolsó képernyőben az az érdekes, hogy a program felhívja a felhasználó figyelmét arra, hogy ha szervizként akarja használni a VNC-t, akkor még további lépések szükségesek.

Itt tehát a távoli munkaállomáson 2 szituáció állhat fenn. Vagy automatikusan fut szervizként a VNC, és bárki bármikor csatlakozhat hozzá, vagy csak igény esetén kerül elindításra. Ez persze felveti azt a feltételt, hogy a munkaállomásnak és a felhasználónak is képesnek kell lennie igény szerint elindítani a programot. Ha állandóan fut, akkor viszont feleslegesen eszi a gép erőforrásait.

- ***VNC ikonja a task bar-on*** 
- ***VNC kliens beállításai***



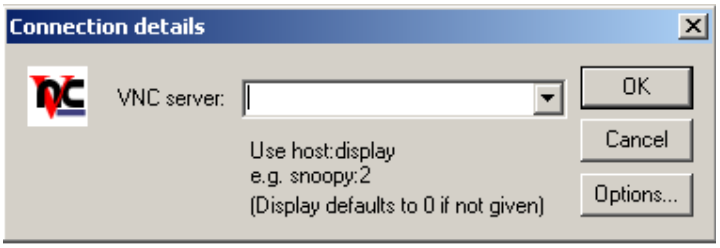
Itt megadhatjuk, fogadjon-e el egyáltalán bejövő kapcsolatokat a szerver, illetve a elfogad, akkor mi legyen a jelszó, aminek a megadásával kapcsolódni lehet.

Megadhatjuk azt is, hogy a távoli gép irányíthatja-e a helyi gép egerét, billentyűzetét.

Az Update Handling szekcióban különböző sávszélesség spórolási módszerek vannak. Például ha a Poll Full Screen előtt nincs bent a pipa, akkor csak az egérkurzor, és a körülötte levő kb. 3 cm átlójú négyzetbe eső képpontok kerülnek továbbításra. Egyébként az egész képernyő. Ez nem túl komfortos, viszont hatékony. Előfordulhat az az eset, hogy ha várunk egy kiírásra, oda-vissza kell rángatni az egeret, hogy lássuk, mikor frissül a képernyő.

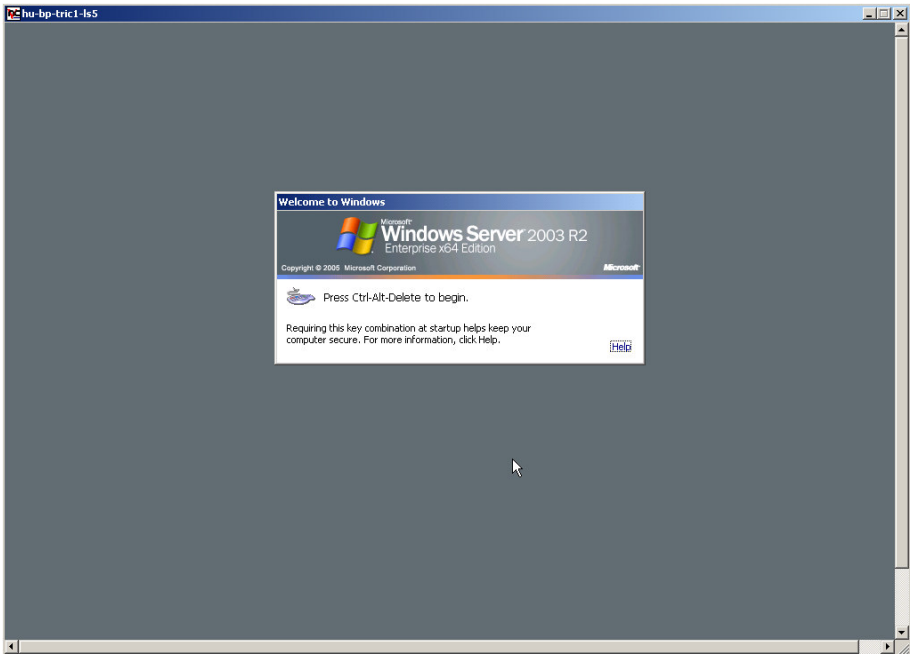
- ***Csatlakozás klienssel***

Erre külön kliensprogram, a vncviewer szolgál:

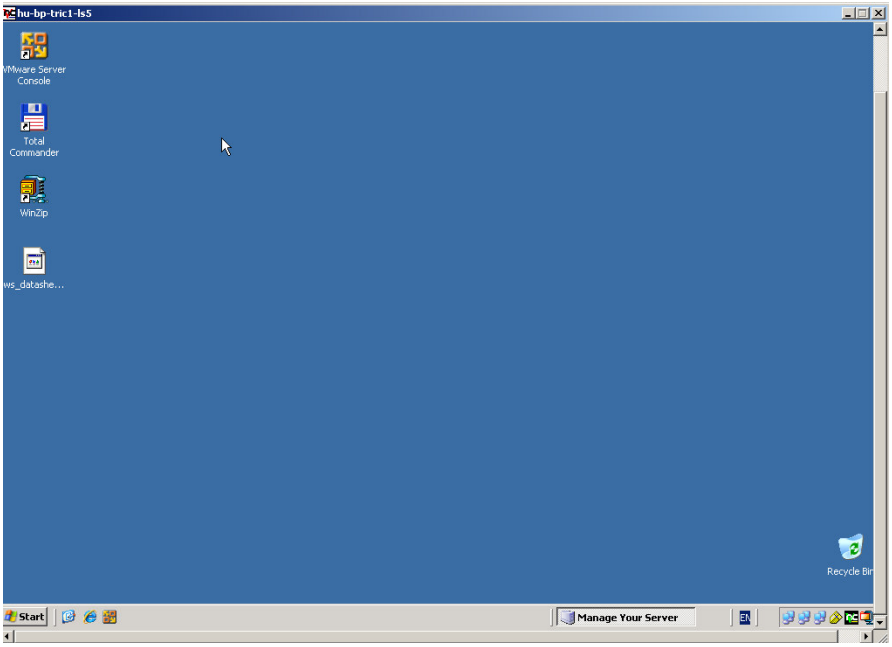


A célrendszer IP címének vagy DNS nevének megadása után, ha a kapcsolat létrejött, kéri a jelszót:

Ezután már előttünk is van a távoli rendszer képernyője:

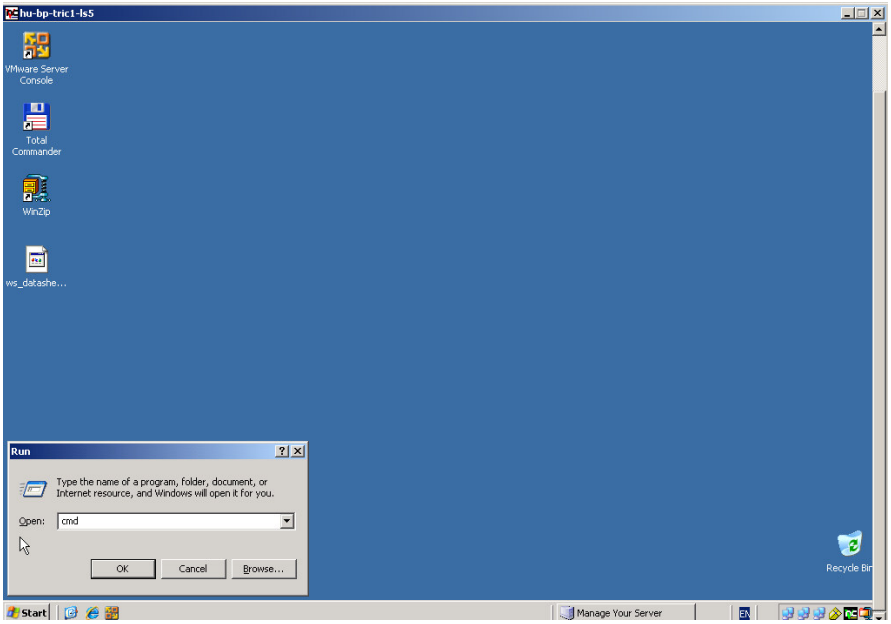


Ide belépve minden olyan, mintha az adott munkaállomás előtt ülnénk.



A képen látszik, hogy a tálcán a VNC ikonja fekete – ezzel jelzi a munkaállomás előtt ülő felhasználónak, hogy távolról valaki rájelentkezett a gépére.

Ekkor (amennyiben nincs letiltva a kliensen), egér- és billentyű-műveleteket végezhetünk.



Ezzel a szoftverrel már megvalósítható a realtime, előtér adminisztrálás / segítségnyújtás. A támogató személy látja a felhasználó képernyőjét, be tud avatkozni, nem szükséges például telefonon át keresztkérdések segítségével megállapítani az aktuális állapotot, hiszen minden látszik.

Ez a fajta távadminisztrálás szerverek esetében is jól jöhet. Például én is használok 2 olyan rendszert is, aminek az állandó futása szükséges (hogy a felhasználók bármikor tudják használni), de nem lehetséges szervizként telepíteni. Ekkor a szerveren belépve marad egy felhasználó, aki elindítja a programot. Ezt konzolon belépett felhasználóval szoktuk megtenni, mivel ide például VNC-vel fel lehet lépni később is, és hozzá lehet férni a futó programhoz.

A VNC-nek van viszont szakmai szempontból három nagy hátránya. Sajnos eléggé nagy sávszélességet igényel, így távol levő munkaállomás, vagy gyenge kapcsolat esetén a válaszidők nagyon meghosszabbodhatnak, a kapcsolat megszakadhat, illetve a kapcsolódás is meghiúsulhat. A második hátránya a nem titkosított adatátvitel. Igaz, azóta már létezik SSL titkosítást használó verziója is. A harmadik probléma a felhasználó korlátlansága. Szabadon állíthatja a VNC szerver tulajdonságait, így átállíthatja a kapcsolódási jelszót, letilthatja a billentyűzet irányítását, vagy elállíthatja a kapcsolat tulajdonságait, így meghiúsulhat a kapcsolódás is, így a távadminisztráció is sikertelen lehet, következhet a helyszíni segítségnyújtás …

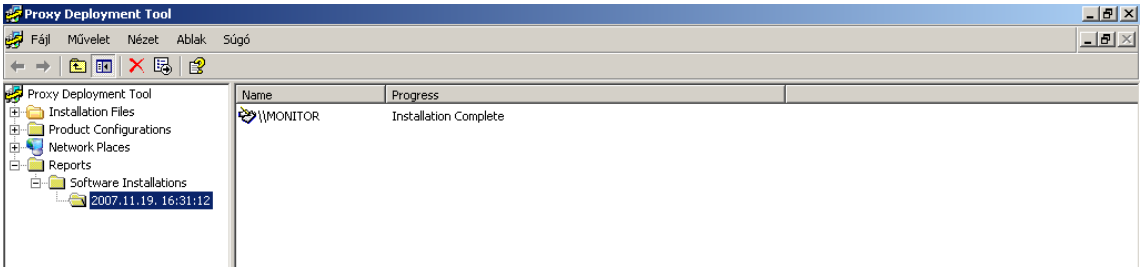
ii) Proxy Master

A Proxy Networks terméke a Proxy Master és a Proxy Host. A Proxy Networks-öt később a Symantec felvásárolta. Ezek fizetős eszközök, de az árért cserébe professzionális szolgáltatásokat is kapunk. A Proxy Master 3 alapvető programból áll: a proxy host-ból, a proxy master-ből, és a deployment tool-ból. A Deployment Tool segítségével távoli munkaállomásokra telepíthetjük fel központilag a host-ot, valamint a telepítéskor megadhatjuk a kliens pár beállítását is (csatlakozási jelszó, stb.).

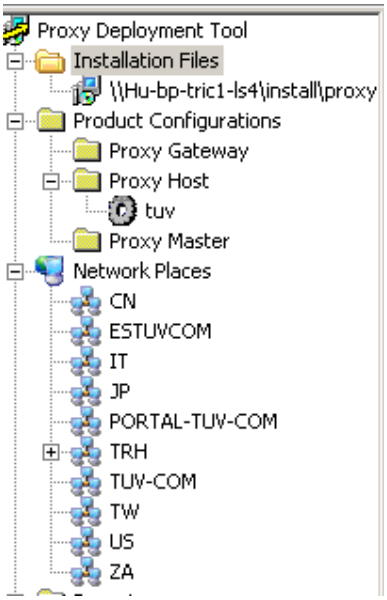
Példa: proxy deploy tool

Ez a példa azért érdekes, mert nem sok olyan szoftvert ismerek, aki saját, beépített távtelepítő modullal rendelkezik, és véleményem szerint egy nagy kiterjedésű hálózaton ez egy igen hasznos lehetőség. Nem kell odamenni minden klienshez (illetve nem kell rájelentkezni mindegyikre távolról), és nem kell egyenként telepíteni a programot.

A Proxy Deploy Tool főképernyője:

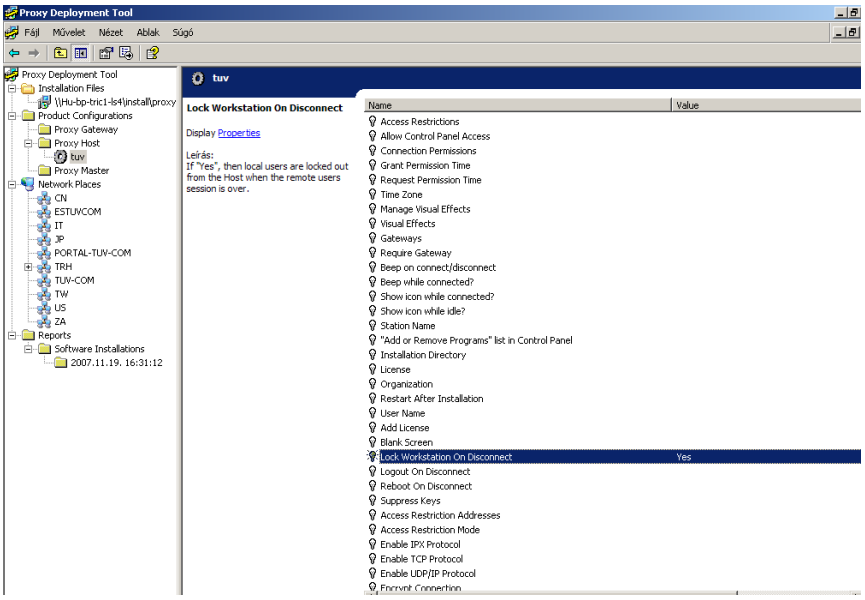


MMC szerű eszköz, de nem igazi beépülő modul, ő csak úgy tesz, mintha az lenne, valószínűleg a kezelés megkönnyítése miatt (nem kell még egy újabb felülettel megbarátkozni)

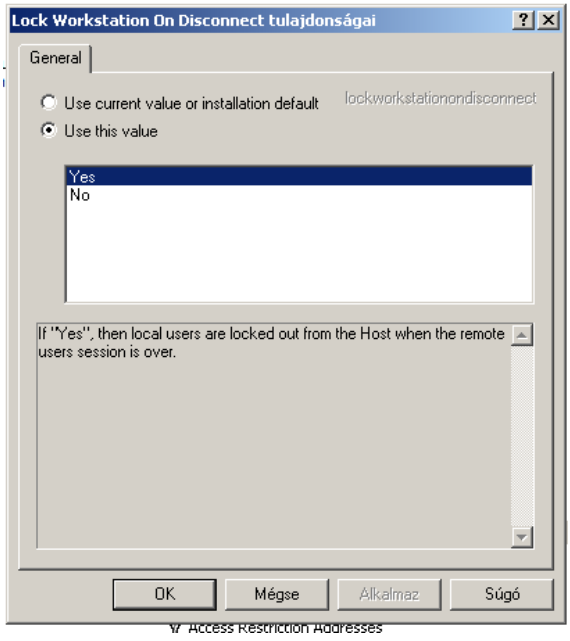


Megadjuk az install file helyét, majd a konfigurációs beállításokat. Itt nyilatkozhatunk az összes opcióról, amiket később fogok bemutatni. Ez a tool nem csak a tárgyal Proxy Host központi telepítéséhez jó, mint látszik a képen. Telepíthető vele a gyártó másik 2 szoftvere is, a Proxy Gateway, és a Proxy Master (ez utóbbi az adminisztrációs program, amit később mutatok be). Legvégül a szokásos hálózati tallózás segítségével összeválogathatjuk a klienseket, ahova telepíteni szeretnénk.

Az opciók megadása:



Ez a rész a Group Policy Object editorra hasonlít (amit már korábban tárgyaltam) Itt nincsenek olyan összetett struktúrában a lehetséges beállítások, csak 1 szint van, itt található az összes. Az opció nevén duplán kattintva megnyílik a tulajdonságainak a beállítópanelje.

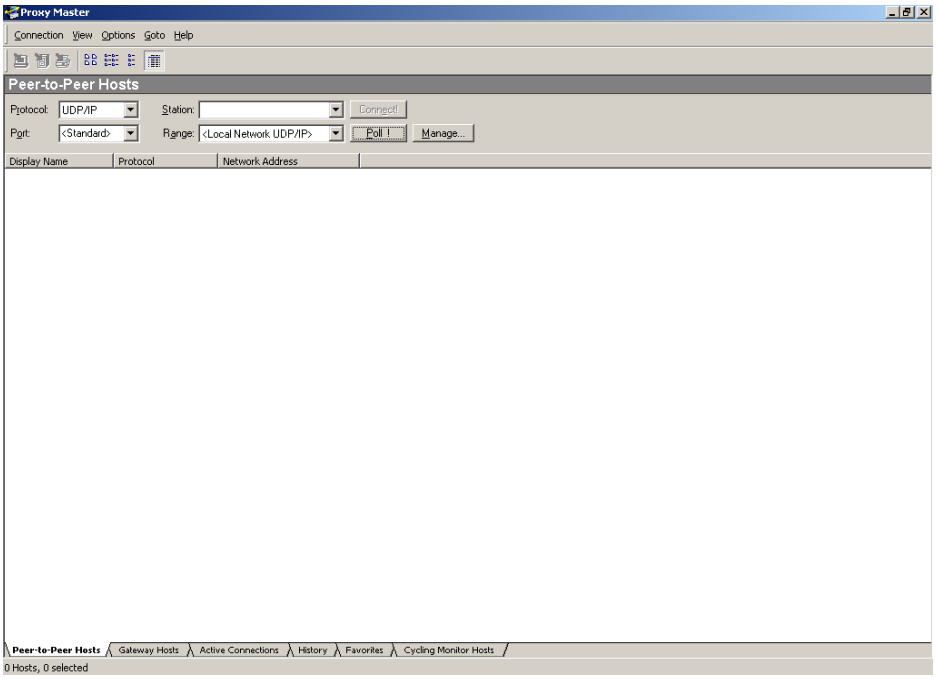


Ha megtörtént a kliens telepítése, illetve a viselkedési tulajdonságok beállítása, elkezdhetjük használni a rendszert. Következik az adminisztrációs eszköz, a Proxy Master.

A Proxy Master segítségével „felderíthetjük” egy hálózati szegmensben található Proxy Host-tal rendelkező klienseket. Így nem kell pontos névvel, vagy címmel rendelkeznünk, mint a VNC esetében. Persze amikor a listáról kiválasztjuk az adminisztrálandó klienst, akkor már rendelkeznünk kell az azonosítójával.

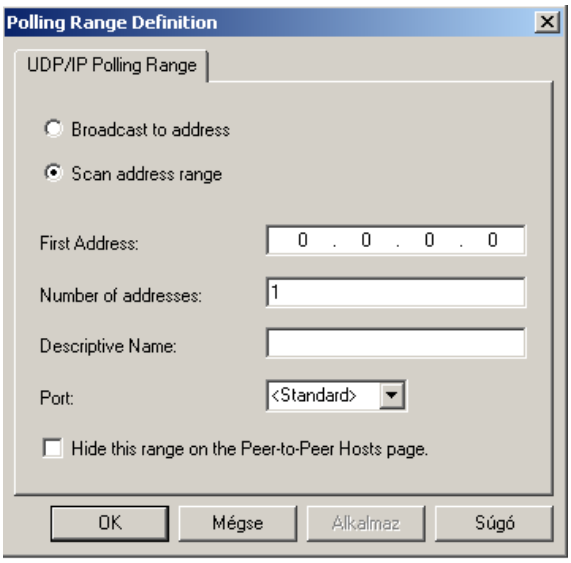
A Proxy Master futtatható program, a Start menü programjai közé telepítéskor bepakolja az ikonját, amivel elindítható a program.

A Proxy Master főképernyője:

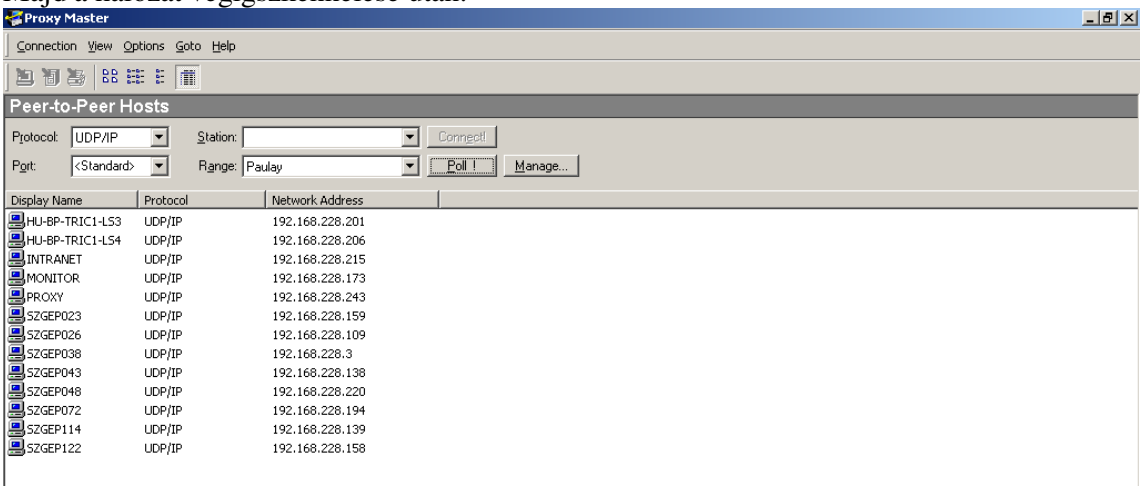


Itt a Manage gomb megnyomásával jutunk a menedzselt hálózatokat beállító menübe. Ugyanis, mint lejjebb látszódni fog, egy adott hálózati szegmensben levő bekapcsolt klienseket automatikusan meg tudjuk találni.

Példa: Proxy Master, h*álózati szegmens megadása:*

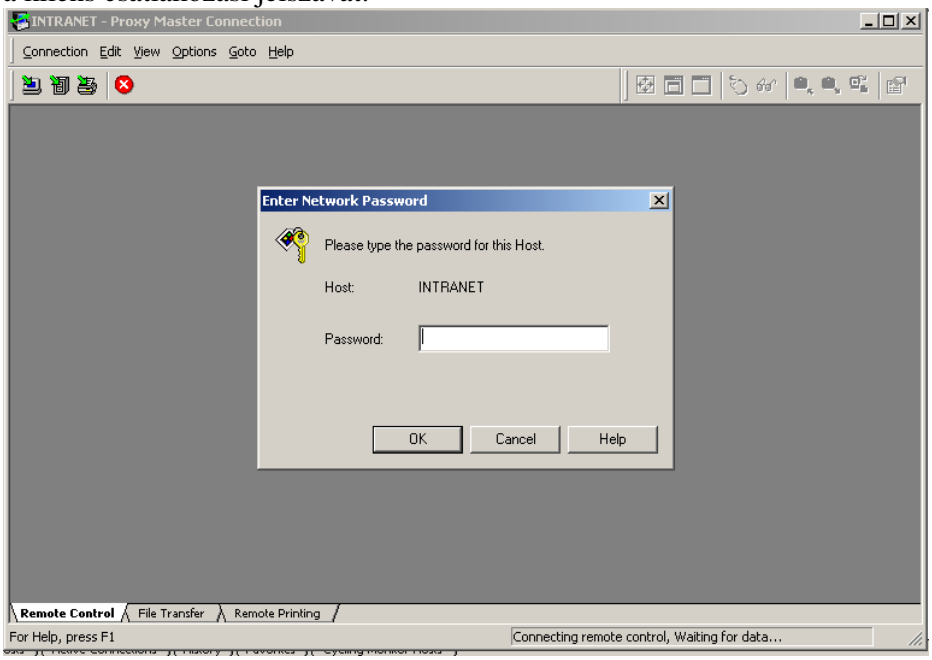


Majd a hálózat végigszkennelése után:

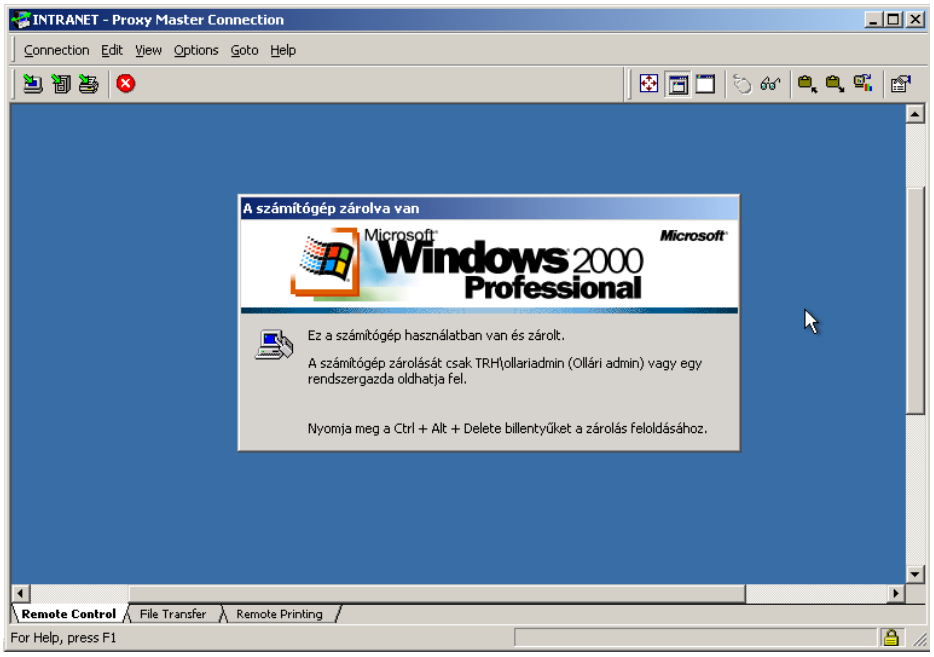


Tehát ezek a munkaállomások vannak bekapcsolva, és rendelkeznek Proxy Host-tal. Itt 2 fontos konfiguráció beállítás is érdekes lehet. Az egyik a Port mező – ha a kliens esetleg nem a standard port-on „hallgatózik”, ez is megoldható. A másik a protokoll. Nagy kiterjedésű illetve bizonytalan VPN kapcsolatokkal rendelkező hálózatok esetén választhatunk tcp/ip-t is. Igaz, ez elméletileg lassabb, viszont biztosabb. A mindennapi életben ez a saját gyakorlati tapasztalatom: VPN-en keresztül az esetek 90%-ában csak a tcp/ip életképes.

A kliens kiválasztása után a Connect gombbal indítható is a csatlakozás. Ehhez meg kell adni a kliens csatlakozási jelszavát:



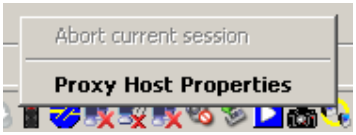
Megadjuk a csatlakozáshoz szükséges jelszót, és a Master fel is építi a kapcsolatot a Host-hoz. Megjelenik a távoli munkaállomás képernyője.



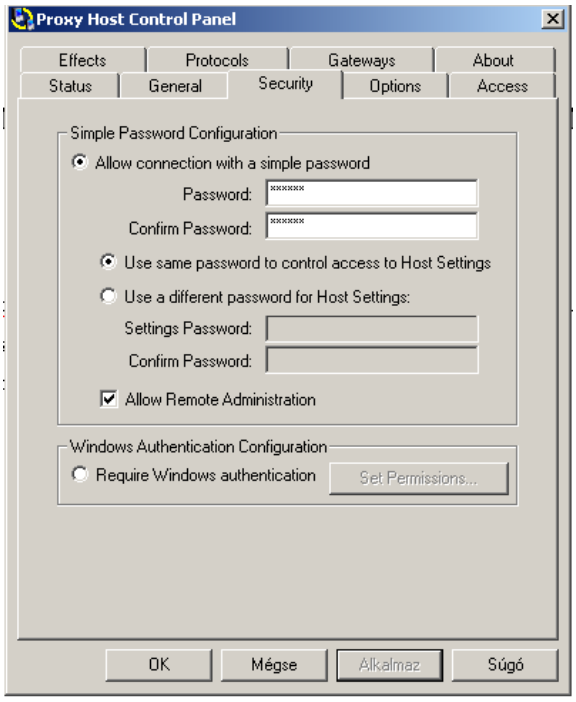
Innentől kezdve irányíthatjuk a távoli gép egerét, billentyűzetét, mintha előtte ülnénk.

A Proxy Host kliens egyik legfontosabb beállítása: bármilyen konfigurációs beállítást csak egy adminisztrációs jelszó megadása után lehet módosítani.

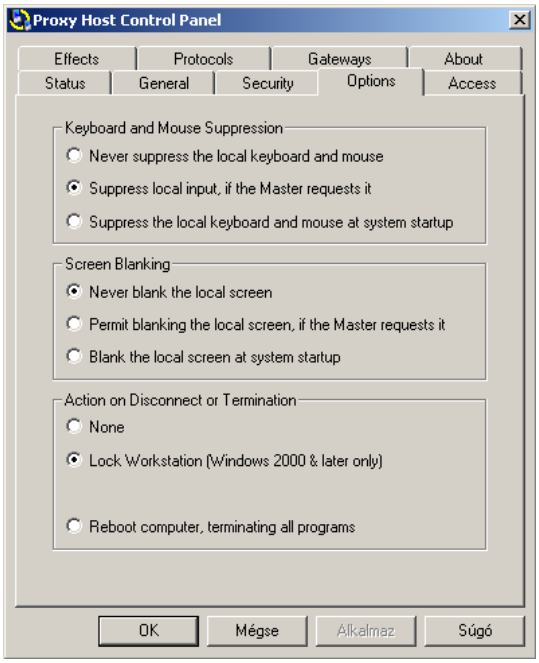
A beállítások megváltoztatásához a kliens tálcáján levő Proxy Host ikonon történő jobb kattintással juthatunk el (a Proxy Host ikonja:):



Példa: Proxy Host beállításai



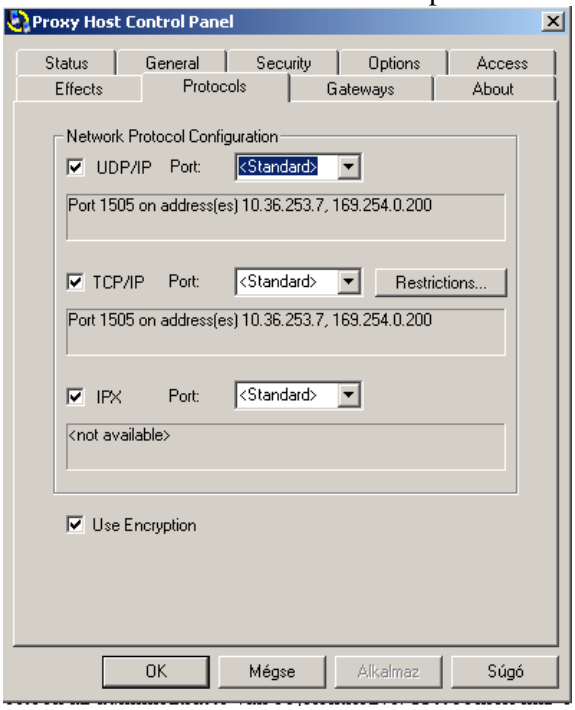
Itt választhatnánk Windows authentikációt is, ekkor csak Windows domain user / password kombinációval lehet belépni.



Itt, az Options fülön található a kedvencem, a Lock Workstation. Ez egy fontos biztonsági lehetőség. Ha megszakad a hálózati kapcsolat, akkor VNC esetén a felhasználó ott ül egy

számítógép előtt, ahová adott esetben az adminisztrátor van bejelentkezve. A többinek már csak a képzelet szab határt…
Proxy Master / Host esetén a kapcsolat megszakadásakor a munkaállomás bezárolódik, a felhasználó nem tud kezdeni semmit, max favágó módon újraindítani.

A Master-ben említett Protokoll és port beállítások:



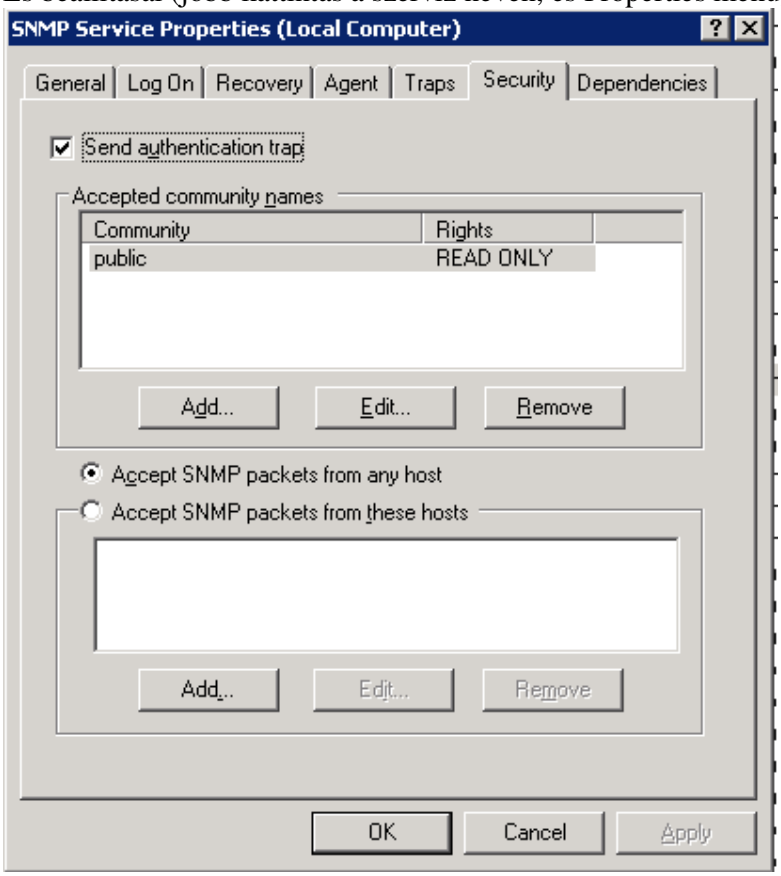
Mint már említettem, ezek a beállítások a telepítéskor központilag beállíthatóak.

5) Hálózat monitorozó protokoll – SNMP

SNMP (Simple Network Monitoring Protokoll) – mint a neve is mutatja, egyszerű hálózati monitorozásra szolgál. Pontosabban a hálózat aktív eszközeinek monitorozására. Az SNMP elterjedt eszköz, de nem kötelező szabvány – nem támogatja az összes aktív eszköz sem. Például a CISCO router-ei, a Microsoft Windows 2000-es vagy attól újabb munkaállomásai, a Watchguard 8.6-os vagy nagyobb Firebox-ai viszont ismerik.
Az SNMP a 80-as évek elején lett kifejlesztve, népszerűségéből viszont a mai napig nem veszített. Kezdetben itt is problémát okozott, hogy nem gondoltak a biztonságra, de a v2c illetve a v3-as SNMP szabványok már komolyabb biztonságot valósítanak meg. Kezdetben csak egy community string nevű jelszót kellett megadni, és már kommunikálhattunk is az eszközzel Később kapott egy felhasználói név párt is, majd a v3-ban az egész authentikációt SSL alapúra írták át.
Az SNMP alapelve a következő: a menedzselendő hálózati eszköznek vannak lekérdezhető / beállítható tulajdonságai. Ezeket úgynevezett MIB-ek tárolják. Ha pl. tudni akarjuk egy hálózati interfész forgalmát, akkor meg kell „szólítani” az adott számlálót tartalmazó MIB-et, és le kell kérni a számláló értékét. Beállításnál ugyanez a mechanizmus, csak fordítva.

Példa: SNMP szerviz Windows 2003 szerveren

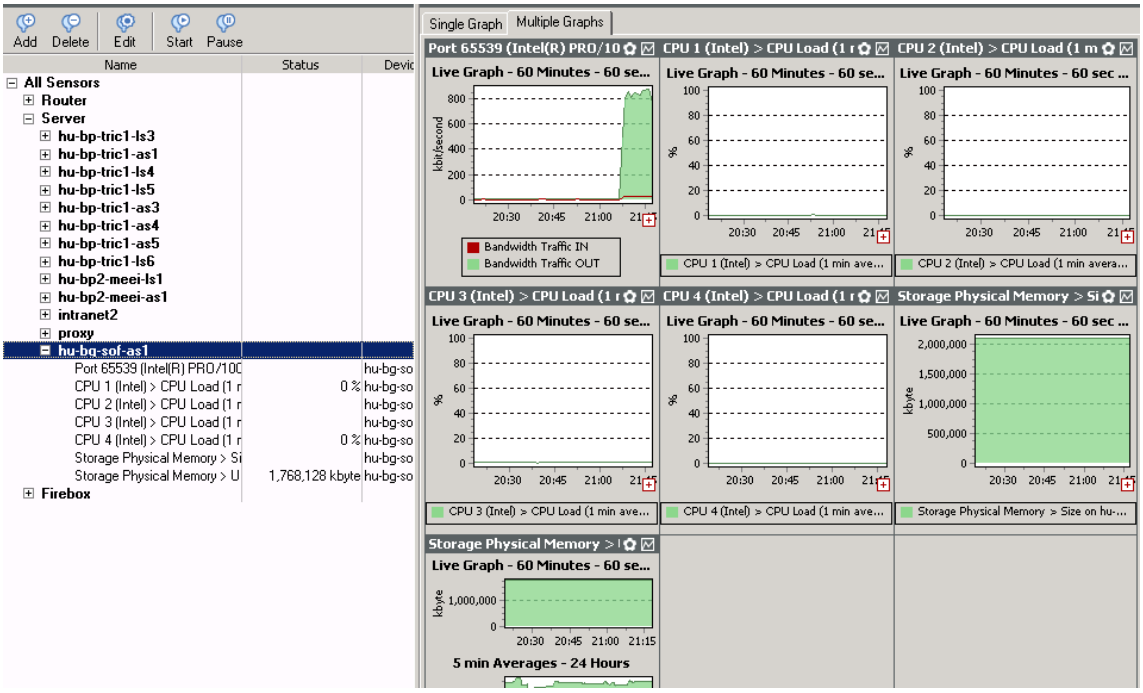
És beállításai (jobb kattintás a szerviz nevén, és Properties menü):



Itt a „public” sztring kézzel lett megadva, más is állhatna itt, de mivel ez a standard a v1 óta, megszokásból ez került beállításra. A csatlakozni szándékozó kliensnek ezt kell megadnia jelszóként.

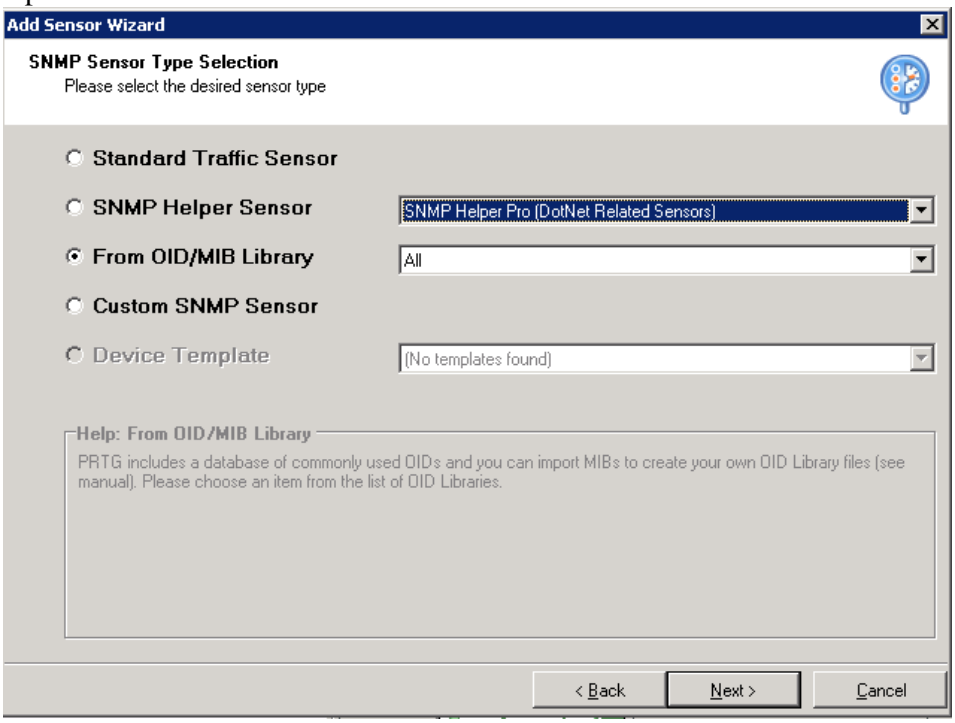
Példa: SNMP lekérdezés PRTG Traffic Grapher alkalmazás segítségével

A PRTG Traffic Grapher egy fizetős, hálózati monitorozásra szolgáló szerver eszköz. Fel lehet bele venni SNMP-t támogató hálózati eszközöket, azokat csoportokba szervezni, és az eszközök alá felvenni a különböző SNMP által lekérdezhető objektumokat.

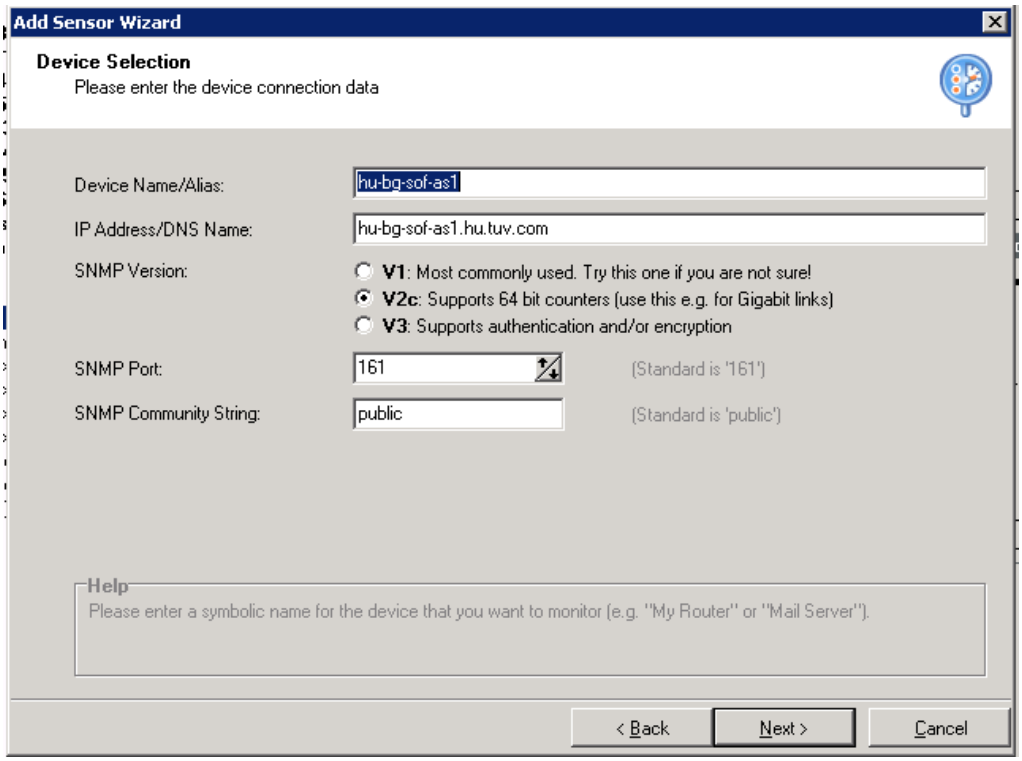


Baloldalon a hu-bg-sof-as1 szerver néhány MIB objektuma látható. Ezeket 60 másodpercenként kérdezi le a monitorozó rendszer, majd az értéket megjeleníti a jobboldali grafikonokon.

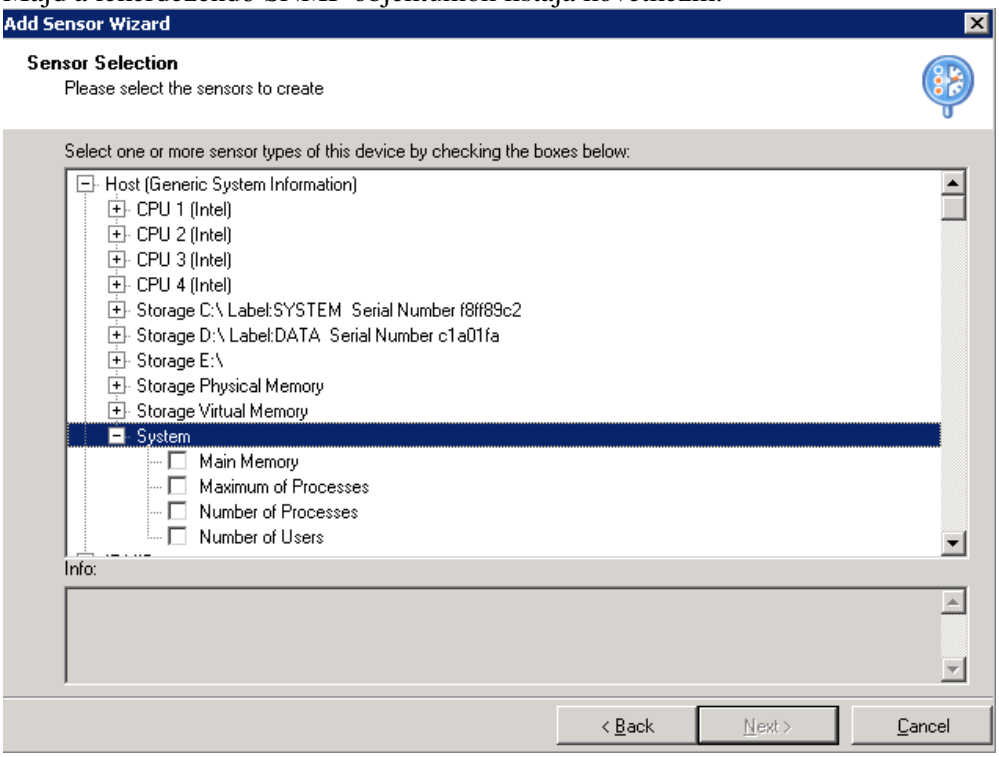
MIB objektum felvétele a rendszerbe:
Az eszköztáron levő Add gomb megnyomása után egy varázsló vezet végig a szükséges lépéseken.



Először az SNMP szenzor típusát kell megadni. Majd a monitorozandó eszköz elérhetőségét, a használandó SNMP verziót:



Majd a lekérdezendő SNMP objektumok listája következik:



A lekérdezésen és a beállításon kívül az SNMP-nek van még egy funkciója. U.n. trap-eket tud generálni. Ezek eseményfigyelők. Ha egy előre meghatározott esemény bekövetkezik, a megadott címre egy trap csomagot lehet elküldetni, amit aztán a monitorozó rendszer érzékel, és megteszi a szükséges lépéseket (például e-mail üzenet küldése).

6) Összegzés

A számítógépes hálózat nem az egyetlen „találmány" a világon, ami követ egy Murphy-törvényt. Megold egy problémát és generál több másikat. Egy újabb hibaforrás, ráadásul szakképzett személyzet is szükséges hozzá. Ezeket a generált problémákat kísérelhetjük meg elnyelni, kezelni a távadminisztrációs rendszerek egy részével. Illetve a hálózat lehetőségeit jobban kihasználhatjuk a másik részével. A hálózatok alapelveit már lerakták. A fejlődés iránya az újabb adatátviteli technikák kidolgozása felé mutat. Egyre nagyobb hangsúlyt kapnak a mobil eszközök, ezáltal a munkavégzés még hatékonyabb, a reakcióidő még rövidebb lehet. Természetesen ezek a technikák egyre bonyolultabb infrastruktúrát, egyre nagyobb szakértelmet követelnek. A hálózatok egy bizonyos szintű ismerete egyre populárisabb lesz, de az ezeken túlmutató ismeretek viszont egyre speciálisabbak és összetettebbek.

Végül térjünk vissza a bevezetésben megfogalmazott szempontrendszerre. A dolgozat szövegében nem mindenhol emeltem ki a szempontrendszernek való megfelelőséget, nem megfelelőséget. A tárgyalás során igyekeztem olyan gondolatmenetek mentén bemutatni a vizsgált rendszereket, hogy látszódjon a különböző szempontokkal levő viszonyuk.
Összefoglalásként álljon itt egy táblázat, amiben a tárgyalt rendszerek és a szempontok találhatóak.

	Közvetlen (realtime support) / nem realtime	Előtér / Háttér rendszer	Gyártófüggő / független eszközöket használ	Biztonságos / nem biztonságos	Ingyenes / fizetős
telnet	realtime	Háttér	független	nem	Általában eszközhöz adják, attól függ
ssh	realtime	Háttér	független	igen	Általában eszközhöz adják, attól függ
Microsoft Windows NetBIOS alapon elérhető megosztott erőforrások	realtime	Háttér	Microsoft	igen	Nem
Microsoft Windows Active Directory alapú rendszerek	Szükséges felhasználó oldali beavatkozás. Ez lehet ki / bejelentkezés, gépújraindítás, gpupdate parancs kiadása	Háttér	Microsoft	igen	Nem
RDP	realtime	Háttér	Microsoft	igen	Nem
WEB alapú (Officescan)	Előfordulhat olyan eset, hogy a kliensek pont akkor kérik le az új konfigurációt, amikor mentésre kerül, de ez nem jellemző	Háttér	független	Ha HTTPS, akkor igen	Általában eszközhöz adják, attól függ
VNC	Realtime	Előtér	Microsoft, de nem ők gyártották	Nem, de van secure VNC is	Van ingyenes verzió
Proxy Master	realtime	Előtér	Microsoft, de nem ők gyártották	igen	nem
SNMP (PRTG)	Rendszertulajdonságot változtat meg realtime	Háttér	független	V3 már az	Ez csak protokoll, az ezt használó eszközök közt van mindkettő.