SZAKDOLGOZAT

Baracsi Pál

Debrecen

2007

Debreceni Egyetem
Informatika Kar

HÁLÓZATI MENEDZSMENT ESZKÖZÖK ALKALMAZÁSA A GYAKORLATBAN

Témavezető:
Dr. Almási Béla
egyetemi docens

Készítette:
Baracsi Pál
Programtervező informatikus (Bsc)

Debrecen
2007

Tartalomjegyzék

1. Bevezetés

1. 1. Általános bevezetés

Ma már minden vállalat, szervezet rendelkezik számítógépes hálózattal, amely az intézmények tevékenységének mindennapos részévé vált. A cégek versenyképességüket különböző Internetes üzleti alkalmazásokkal próbálják növelni. Egyre inkább elterjedtté válik az e-business, így sikerességüket nagyban befolyásolja informatikai rendszerük, hálózati infrastruktúrájuk fejlettsége is. Az informatika az üzleti élet alapját képezi, ezért a folyamatos rendelkezésre állás kulcsfontosságú. A hálózati szolgáltatások nem megfelelő működése az elégedetlen ügyfelek elvesztésével, bevétel kieséssel járhat. A hálózatnak ezért Quality of Service (QoS), azaz minőségbiztosítási képességekkel kell rendelkeznie. Ráadásul a számítógépes hálózatok mérete folyamatos növekszik, ezért megfelelő felügyeletük, üzemeltetésük különösen fontos.

A dolgozatban be szeretném mutatni, a hálózati menedzsment feladatait, és hogy e feladatok megvalósításának módszereit milyen szabványok írják le. A téma feldolgozásához a magyar és külföldi irodalmat tekintem át. Ehhez szakkönyvek, internetes cikkek, és RFC dokumentumok segítségét veszem igénybe. Továbbá ismertetek néhányat a jelenleg rendelkezésre álló freeware és shareware programok közül, illetve sorra veszem, hogy azok milyen feladatokat látnak el, és hogyan segítik elő a hálózat üzemeltetését.

Dolgozatom második fejezetében a hálózati menedzsment funkcióit részletezem, úgymint a konfiguráció-, a hiba-, a teljesítmény-, a biztonság-, az elszámolás-menedzsmentet, és a felhasználói adminisztrációt. A harmadik fejezetben a fontosabb hálózat menedzsment szabványok rövid leírására, míg a negyedik fejezetben a legelterjedtebb szabvány, a Simple Network Management Protocol részletezésére kerül sor. Végül a dolgozat ötödik fejezetében az általam választott alkalmazások funkcióit, és azok használatát mutatom be.

1. 2. A hálózati menedzsment célja, feladata

A hálózat menedzselése azon folyamatként definiálható, amely lehetővé teszi a hardver, szoftver, és humán erőforrások optimális felhasználását, és koordinálását, a maximális hatékonyság és termelékenység elérése érdekében, elfogadható költségek mellett.

Tehát a hálózati menedzsment feladata nem más, mint a hálózat hatékony működésének biztosítása, és a hibák elhárítása, illetve kialakulásuk megakadályozása.

A hálózat hálózatmenedzsment céljai (lásd [11]):

- Vállalati stratégiai eszközök kézbentartása: az eszközök olcsóbbak lettek és így nagy számban jelentek meg a vállalati hálózatok minden területén. Ellenőrzés nélkül az eszközök kihasználása nem lehet optimális.
- Áttekinthetőség: a hálózatok mérete folyamatosan növekszik. A menedzsmentnek biztosítania kell a hálózat minél egyszerűbb áttekinthetőségét, különben a hibák elhárítása lehetetlenné válik.
- A szolgáltatás javítása: a felhasználó elvárja, hogy a hálózat ugyanolyan vagy még jobb színvonalat nyújtson, mint eddig.
- Különböző igények kiegyenlítése: a számítógépes hálózattól elvárják, hogy különböző üzleti igényeket elégítsen ki, mint pl.: új alkalmazások, videó-konferencia, IP-telefónia, vagy a VPN támogatása. A felhasználók különböző igényeit is ki kell elégítenie: elérhetőség, megbízhatóság, sávszélesség.
- Állásidő csökkentése: folyamatosan hozzá lehessen férni az erőforrásokhoz és a szolgáltatásokhoz, melyeket a hálózat nyújt. Az álló informatikai rendszer veszteséget okoz, ezért a magas színtű rendelkezésre állást biztosítani kell.
- Változások ellenőrzése: a változásokat, illetve változtatásokat megfelelően kell időzíteni, végrehajtani és dokumentálni, a hálózat zavartalan működése érdekében.
- Költségek ellenőrzése: a hálózattal kapcsolatos minden költségre figyelnie kell a menedzsmentnek, hogy az a lehető legkisebb legyen.

A hálózatmenedzsment egy szolgáltatás, amely számtalan eszközt és alkalmazást használ, hogy segítse a hálózat üzemeltetésével foglalkozó embereket a hálózat működésének ellenőrzésében és fenntartásában.

2. A hálózati menedzsment funkciói

Az ISO (International Standards Organization, Nemzetközi Szabványügyi Hivatal) meghatározása szerint a hálózatmenedzsment feladatait az alábbi öt funkcióra bonthatjuk (lásd [39]):

- Konfiguráció menedzsment (Configuration Management)
- Hiba menedzsment (Fault Management)
- Teljesítmény menedzsment (Performance Management)
- Biztonság menedzsment (Security Management)
- Elszámolás menedzsment (Accounting Managment)

A hálózati menedzsment sikere attól függ, milyen széles körben képes lefedni azokat a menedzsment funkciókat, melyek alapvetően a nemzetközi szabványokban rögzítettek
Ezek a funkciók természetesen szorosan kapcsolódnak egymáshoz, így a LAN menedzsment számára rendelkezésre álló eszközök sem csak egy-egy funkció megvalósítására használhatók. Az ISO nem sorolja a hálózatmenedzsment funkcióihoz, de a felhasználói adminisztráció és a hálózattervezés elősegítése is fontos feladat egy hálózat működtetésénél. Részletek tekintetében, lásd a [11] művet.

2. 1. Konfiguráció menedzsment

A konfigurációmenedzsment áll a hálózatmenedzsment középpontjában, mivel adatokat szolgáltat az aktuális konfigurációs részletekről, illetve nyilvántartja a konfiguráció változásait. Kezeli a hálózati- és rendszereszközök konfigurációit.
A konfigurációmenedzsmentnek a következő információkra van szüksége: a menedzselt objektumok, azok állapotának jellemzőire, és a hálózati összeköttetésekre vonatkozó információkra.
A konfigurációmenedzsment funkciói a következők:
A **készletnyilvántartás és topológia szolgáltatás**, melynek feladata a hardver- és szoftverkészlet kezelése, és a rendszer konfigurációs térképének karbantartása. A megfelelő készletnyilvántartás érdekében célszerű az adatokat nem megosztottan, egyszerű fájlokban

tárolni, hanem a menedzsment információs bázis (MIB) segítségével. A konfigurációs információk adatbázisa a következő adatokat kell, hogy tartalmazza:
A hálózat minden címezhető elemének fontos adatai:

- A kapcsolóelemek adatai
- Szerver és kliensoldali szoftverek kezelése (licence adatai, támogatott protokollok, és szolgáltatás-típusok)
- A forgalomirányítók konfigurációs adatbázisa
- A hozzáférési jogosultságokra vonatkozó információk, amelyek kezelését a hálózati operációs rendszerek biztosítják, de a nyomon követésükre kevés lehetőséget biztosítanak.
- A menedzselt objektumok állapota
- Különböző statisztikai és teljesítményadatok
- A hálózati események feljegyzései
- Hibacédulák (trouble ticket) információi

A pontos készletnyilvántartáshoz szükséges továbbá a **változások illetve változtatások megfelelő nyilvántartása**. Továbbá a használhatóság érdekében szükséges a megfelelő elnevezés és címzés használata, amelyet általában a hálózati operációs rendszerek biztosítanak, és a név- és címfordítás folyamatát elrejtik a felhasználó elöl. Gondoljunk csak a név szerverekre (DNS), vagy az ARP, RARP protokollokra. Az elnevezés és címzés esetén a legfontosabb kritériumok, hogy legyen könnyen átlátható, a nevek és címek egységesen legyenek megadva, és segítséget nyújtson egyedi nevek, és címek automatikus generálásával.
A konfigurációmenedzsment szintén fontos funkciója a **kábelezési rendszer nyilvántartása** és menedzsmentje. A hálózat kábelezésének dokumentálása a rendszergazda számára lehetővé teszi az egyszerűbb változtatást és hibakeresést. Ez különösen fontos, mivel a hálózati hibák jelentős része a fizikai rétegbeli hibákból adódnak. A kábelmenedzsment funkciók megvalósítására úgynevezett CMS (cable management system) termékek használhatók. Ezeknek a CMS-rendszereknek képesnek kell lennie a kábelek nyomvonalának végponttól végpontig terjedő azonosítására, a központi- és a közbülső kábelrendezők és a rack-szekrények fizikai és logikai elrendezésének szemléltetésére. Ha a rendszer képes az egyedi kábel számok megjelenítésére, esetleg automatikus generálására, akkor már a hálózat kiépítésekor használható a strukturált kábelezés megvalósításához. Szükség van továbbá a

kábelrendező helyiségben található valamennyi készülék azonosítására, a kábelrendező paneleken lévő, a kábelvégződések azonosítására használt jelzések megjelenítésére. Fontos funkció a kábelcsatornák telítettségének és kihasználtságának nyomon követése, a használaton kívüli, redundáns kábelek azonosítása. Elvárható egy CMS-rendszertől, hogy különböző típusú és célú átviteli közegeket tudjon kezelni, további információval szolgáljon a kábelcsatornák, és kábelkötegek helyéről, méretéről, és hosszáról. Egy hálózat tervezésénél egy jól használható CMS-rendszer igen hasznos lehet.

2. 2. Hiba menedzsment

A hiba menedzsment célja a hálózatban fellépő hibák érzékelése, az érintett terület meghatározása, a hiba izolálása és naplózása, az adminisztrátorok és felhasználók értesítése, és a lehetőségekhez mérten a hibák automatikus kijavítása. A hibák a hálózat leállását, vagy hibás működését eredményezhetik, amely számszerűsíthető veszteséget okoz. Ezért az ISO hálózatmenedzsment megvalósításokban erre a területre fordították a legtöbb figyelmet, és a hibamenedzsment a legjobban implementált a funkciók közül.
A hibák sikeres kezelésének természetesen elengedhetetlen előfeltétele a hálózat dokumentálása, ezért különösen fontos a konfigurációmenedzsment. A hibák gyors megoldásához a következő információkra lehet szükség:

- a hálózat topológiája
- a használt protokollok és átviteli közegek
- korábban mért sávszélesség mutatók
- és a használt alkalmazások.

Hasznos lehet, ha dokumentáljuk a korábban fellépő hibákat, és az elvégzett javításokat. A rendszeresen fellépő hibák felismerésére és elhárítására ajánlott logikai tervek készítése. Az ismeretlen eredetű hibák gyors detektálására különféle diagnosztikai eszközök használata szükséges. Továbbá előfeltétel az üzemeltetők és a felhasználók megfelelő kiképzése.
A következő felsorolás a hiba menedzsment feladatait tartalmazza:

- Állapot felügyelet: LAN–monitorok és LAN–analizátorok segítségével folyamatosan figyelemmel kísérhetők a hálózat legfontosabb állapotjelzői, az adatforgalom, és bizonyos események.

- Hibadetektálás és riasztás: Bizonyos események hatására automatikusan üzenetek generálódhatnak. A lényeges eseményekhez prioritást és határértéket kell beállítani, egy határérték átlépése vagy bizonyos prioritású események riasztást váltanak ki a hibás működés felderítése érdekében.
- A problémák meghatározása és elszigetelése: egy menedzselt objektumtól származó riasztás elindítja a hibafelderítés folyamatát. A hálózati problémákat egy ötfokozatú skála alapján lehet besorolni, részletek a [11] könyvben.
    1. Ezek a hibák általában nem technikai jellegűek, hanem a felhasználók hiányos ismereteiből adódnak. Ezeket a problémákat az információs pult (help-desk) hibadokumentációk segítségével kezeli, általában telefonon keresztül megoldhatók. Ezek a hibák 80-85%-át teszik ki.
    2. Bizonyos technikai jellegű problémák (pl.: hibás szerverműködés). Ezen problémák megoldása az információs pult, és a LAN–elemzők feladata. A hibák 5-10%-át teszik ki. Megoldásukhoz on-line adatbázisok és a felhasználói kézikönyvek használhatók.
    3. Kritikus és komplex technikai jellegű problémák tartoznak ide, melyek megoldása gyakran a szállító cég szakembereinek segítségét igénylik. A problémák 3-5%-át teszik ki, és jelentős erőforrást igényel a megoldásuk, melyhez on-line adatbázisok, felhasználói kézikönyvek, és a gyártókkal való közvetlen kapcsolat nyújthat segítséget.
    4. A hálózati alkalmazásokkal összefüggő problémák tartoznak ide (pl.: programfagyások), megoldásuk az alkalmazás fejlesztőinek a feladata, megoldásuk gyakran sok időt vehet igénybe. A hibák 1-5%-át teszik ki.
    5. Azon problémák, amelyeket csak a gyártók tudnak kezelni (pl.: operációs rendszer, firmware problémák). Megoldásukhoz a gyártó által biztosított update-ek, upgrade-ek használhatók.

A hálózati hibaelhárítás leggyakrabban használt eszközei az **ellenőrző listák** (check list). A hiba felderítésének megkezdésekor, el kell dönteni, hogy a szerverek vagy munkaállomások működési problémájáról, gerinchálózati hibáról, a kapcsolóeszközök hibájáról, vagy esetleg valamelyik munkaállomással kapcsolatos hibáról van-e szó. Ez után a megfelelő check list-et

kell kiválasztani és alkalmazni. Miután a hibát lokalizáltuk, megkezdődhet a probléma konkrét meghatározása, és javítása.

A hálózatokban előforduló leggyakoribb hibaforrások

- a huzalozással
- az interfész kártyákkal
- a hálózati kapcsolóeszközökkel
- a hálózati operációs rendszer hibáival
- adatvesztéssel

kapcsolatos. A hibák jelentős része fizikai rétegbeli hiba, ezek a hibák leginkább a hibás huzalozásból adódnak, pl.: szakadt kábelek, hibás csatlakoztatás, nem megfelelő portokat összekötő kábelek, kontakthibás kábelkapcsolat, nem megfelelő típusú kábel használata (a konzolkábeleket, a keresztkötésű és az egyenes kötésű kábeleket megfelelően kell alkalmazni), a törött, repedezett, rosszul lezárt, szétcsavarodott kábelek, a készülékek adó-vevő problémái, kikapcsolt készülékek. Az interfész kártyák hibáinak az okai általában a rosszul konfigurált interfészek, hibás órajel beállítás, esetleges hardver hibák, vagy hibás driver-ek telepítése lehet. A hálózati kapcsolóeszközök hibái adódhatnak hardver meghibásodásból, vagy hibás konfigurációból (helytelen IP-címek és/vagy alhálózati maszkok, nem megfelelő irányítóprotokoll) is.

Szerver-kliens rendszerekben a szerver adatvesztése működési hibákhoz, a hálózati szolgáltatások leállásához vezethet. Fájlszerverek esetében a felhasználói adatok elvesztése kritikus hibát jelent, ezért az adatvesztés megakadályozása különösen fontos. Adatvesztés lemez meghibásodás, áramkimaradás, jogosulatlan hozzáférés, vagy vírusfertőzés eredménye lehet. Az adatvesztés elleni védelem így nem csak a hibamenedzsment, hanem a biztonságmenedzsment feladata is, ezért itt csak a meghibásodásokból adódó adatvesztés elleni védelemre térek ki. Az adatok védelmének három leggyakoribb, és igen hatásos módja a biztonsági mentés, hibatűrő lemezrendszerek használata, és szünetmentes tápegységek (UPS) használata.

A **biztonsági mentés** tipikus eszköze a mágnesszalag, melynek előnye, hogy olcsó és nagy kapacitású (DAT – Digital Audio Tape – 24GByte), hátránya viszont, hogy az adatok szekvenciálisan kerülnek rögzítésre, és visszaállításra. A biztonsági mentések hatékony elvégzése érdekében többféle technika alkalmazható, ezek:

- a teljes,

- a növekményes,
- és a különbségi mentés.

Teljes mentés esetén, a lemezen található összes állomány átmásolódik a szalagra, növekményes mentés esetén csak a legutóbbi teljes vagy növekményes mentés óta létrehozott, vagy módosított fájlok kerülnek átmásolásra. Különbségi mentés esetén a legutóbbi teljes mentés óta létrehozott vagy módosított fájlok kerülnek át a mágnesszalagra.

Az adatok védelmének egy másik módja a **hibatűrő adattároló eszközök** használata, amit RAID (Redundant Array of Inexpensive Disks, alacsony költségű lemezek redundáns tömbje) szintek szerint szokás csoportosítani. A legelterjedtebb RAID szintek a következők:

- RAID 0: Az adatokat több lemezre osztja szét, de nem használ paritást, így csak az átviteli sebességet növeli, de nem nyújt adatredundanciát. Lemezösszefűzésnek (disk striping) is hívják.
- RAID 1: Két fajtája létezik a lemeztükrözés és a lemezkettőzés. Az előbbi az adatokat két ugyanolyan partícióra írja, de két különböző lemezre, így lényegében ez egy automatikus biztonsági mentésnek tekinthető. Hátránya, hogy a két lemez ugyanazt a lemezvezérlő kártyát használja, így annak meghibásodása esetén, mindkét lemez használhatatlan lesz. Ennek megoldására találták ki a lemezkettőzést, amely lemezvezérlő kártyából is kettőt igényel.
- RAID 5: Az adatokat és a paritást több lemezen helyezi el. Nincs szükség külön paritáslemezre, mivel a körbeforgó paritás (rotating parity) módszerét használja. Alkalmazásához legalább három megegyező méretű lemezre van szükség. Egy lemez meghibásodása esetén a többiből számolható az elveszett csík tartalma.

A RAID rendszereket szoftversen és hardveresen is meg lehet valósítani. Szoftveres megvalósítás esetén vagy az operációs rendszer nyújt támogatást, vagy speciális driver programot használnak. Hátránya, hogy a központi memóriát, illetve a CPU-t terheli, lerontván az egész rendszer teljesítményét. Hardveres megvalósítás esetén a szükséges feldolgozást a RAID vezérlő valósítja meg. További RAID szintek is léteznek, de ezek a gyakorlatban nem terjedtek el, magas költségük, illetve alacsonyabb teljesítményük miatt.

Ahhoz, hogy a hibamenedzsment teljes folyamatát koordinálni tudjuk a **hibacédulák** (trouble ticket) nagyon hasznosak lehetnek. Használatához egy adatbázisra van szükség, amely általában relációs, és kapcsolódhat a konfigurációs adatbázishoz. A problémák megoldását a

különböző funkcionális területek közötti kommunikáció biztosításával segíti elő. Egy trouble ticket rendszer a következőképpen működhet, [11] alapján: Először valamilyen hibajelentés kerül az információs pulthoz. A hibajelentés automatikusan generálódott, vagy egy felhasználó jelentette. Az információs pult elkészíti a hibajegyet, majd értesíti az illetékeseket. Ekkor a hibajegy naplózására kerül sor, és a feladat megoldásához hasonló problémákat keres az adatbázisban. Ha a problémát sikerül megoldani, akkor frissíti az adatbázist, továbbá jelentést küld a menedzsmentnek, és értesíti a felhasználókat a hiba kijavításáról. A hibák kijavításának sikerességét minden esetben teszteléssel ellenőrizhetjük.

2. 3. Teljesítmény menedzsment

A teljesítmény menedzsment célja a hálózat kihasználtságának és terhelésének a mérése, és a mért adatok különböző szempontok szerinti megjelenítése, a hálózat teljesítményének optimális szinten tartása érdekében. Ehhez a következő feladatokat kell ellátnia:

- a hálózat teljesítményére vonatkozó adatok meghatározása, teljesítménymutatók definiálása, a hálózat teljesítményének figyelése
- a mért adatok analizálása, értelmezése
- küszöbértékek meghatározása, melyeknek átlépése hibát jelent, amely riasztást vagy valamilyen művelet végrehajtását váltja ki
- a hálózat modellezése
- a hálózat optimalizálása, hangolása

A hálózat teljesítményét megjelenítő mutatók típusai: statikus, dinamikus és teljesítménymérési mutatók.
A hálózat teljesítményének statikus mutatói:

- átviteli kapacitás
- jelterjedési késleltetés
- topológia
- keretméret

A hálózat teljesítményének dinamikus mutatói:

- a hozzáférési protokoll
- felhasználói adatforgalom

- bufferek mérete
- adatütközés és újratovábbítás

A hálózat teljesítményére vonatkozó mérőszámok:

- erőforrás-használat
- átviteli- és válaszidő
- hozzáférhetőség
- a mérési adatok megbízhatósága

Teljesítménymérés (monitoring):

A hálózat szűk keresztmetszeteinek felderítése az egyik legfontosabb feladat. A LAN-analizátorok ezt a tevékenységet igen jól támogatják. Biztosítja a keretek forgalmának, eloszlásának, illetve az aktív munkaállomások számának folyamatos megfigyelését, továbbá a használt protokollok elemzését. A teljesítmény mérésének fontos kritériuma, hogy az adatgyűjtés kis többleterőforrást igényeljen.

Hálózatok hangolása (tuning):

A hálózat elemzésére és a teljesítmény javítására vonatkozó igények akkor merülnek fel, amikor a szolgáltatásra vonatkozó elvárásokat nem elégíti ki (lásd [11]). A hangolás első lépéseként teljesítménymutatókat kell meghatározni, és a szükséges információkat megfigyeléssel kell beszerezni. Ezután a felmerülő alternatívákat kell megvitatni a költséghatékonyság és a technikai megvalósíthatóság figyelembe vételével. A teljesítmény szempontjából minden hálózati komponens szűk keresztmetszetet jelenthet, ezért fontossági sorrendet kell felállítani. Ha valamilyen változtatást végzünk megfelelő mérésekkel ellenőrizni kell a teljesítménybeli javulást. A hálózat tuningolásának a következő területei lehetnek, melyről részletesebben [11] műben olvashatunk:

- Hálózati operációs rendszerek: A hálózat hatékonyságát nagymértékben befolyásolja, hogy az operációs rendszer hogyan biztosítja az adatforgalmat, milyen fájlkezelési technikát használ, és az I/O igényeket hogyan elégíti ki.
- Szerverek: A hálózatok működését nagyban meghatározzák a szerverek, melyeknél a szűk keresztmetszetet a központi egység, az I/O egység, és a lemezegységek jelentik.
- Meghajtók: Azok a szoftver rutinok, amelyek biztosítják a kapcsolódási felületet a fizikai eszközök és az operációs rendszer között. A meghajtó szoftverekkel kapcsolatos problémák kihatnak az egész hálózat teljesítményére.

- Hálózati csatolókártyák: A szerverek csatoló kártyái jelenthetik a szűk keresztmetszetet. A teljesítményt befolyásolja a hálózati kártya driver-e, buffermérete, és a szerverben elhelyezet kártyák száma.
- Munkaállomások: Szintén befolyásolják a hálózat működését, mivel a felhasználók a munkaállomáson keresztül érzékelik a hálózatot. A szerverek és a munkaállomások teljesítményét összhangba kell hozni.
- Perifériák: A legfontosabb hálózati periféria a nyomtató, sebessége szűk keresztmetszetet jelenthet. Megfontolandó, hogy önálló hálózati nyomtatót, vagy nyomtatószervert használjunk.

A hálózat teljesítményének megfigyelésére olyan eszközöket kell használni, amelyek folyamatosan figyelik az adatforgalmat, felügyelik az eszközök állapotát, a lemezhasználatot, és statisztikákat készítenek.

2. 4. Biztonság menedzsment

A biztonság menedzsment célja a hálózati hozzáférés ellenőrzése a helyi szabályozások alapján. Feladata a hálózat elleni támadások, szándékos vagy véletlen működésképtelenné tételének, bizalmas információk felhatalmazás nélküli elérésének megakadályozása.
A hálózatok biztonsági problémái a munkaállomásokhoz történő szabad fizikai hozzáférésből, és a felhasználók többletjogaiból adódnak. Nem csak a szoftveres biztonságról kell gondoskodni, hanem a fizikai biztonságról is. Ez magába foglalja a file-szerverek, hálózati kapcsolóelemek, a központi- és közbülső kábelrendezők elzárásának módját, és a hozzáférésük ellenőrzését. Az illetéktelen hozzáférést a munkaállomásokon is meg kell akadályozni, például kijelentkezéssel, vagy jelszóvédett képernyővédő használatával. A hálózat legkönnyebben hozzáférhető helyei a kábelek, mivel lehetőséget biztosítanak a lehallgatásra, új csomópont közbeiktatására, vagy a hálózati adatforgalom megfigyelésére, így lehetőséget ad jelszavak leolvasására, és fontos információk megszerzésére. Vezeték nélküli technológia esetén a hozzáférés még egyszerűbb, csupán a lefedett területen belül kell tartózkodnia a támadónak.
A hálózat biztonságának érdekében szükséges a veszélyek elemzése, melynél egy veszély-mátrix összeállítása segítséget nyújthat. Ehhez a veszélyeket osztályozni kell, ilyenek például

az illetéktelen hozzáférés, a felhasználói hibák, az alkalmazotti szabotázs, a természeti katasztrófa, a vírusfertőzés és az ipari kémkedés. Továbbá meg kell határozni a hálózat azon erőforrásait, amelyek veszélynek vannak kitéve, és osztályozni a veszélyeztetettség mértékét. A veszély-mátrix segítségével könnyebben megtervezhetők a biztonsági beruházások és azok megtérülése. Mivel nem létezik tökéletes biztonság, ezért kompromisszumot kell kötni a hálózat biztonsága és a pénzügyi befektetés között (lásd [11][12]).

A hálózatot a lehető legnagyobb mértékben védetté kell tenni a jogosulatlan hozzáférésekkel szemben. Ezt biztonsági irányelvek felállításával lehet elérni, mint például minimális jelszóhossz és jelszó elévülési idő beállításával, és annak megadásával, hogy a felhasználók pontosan mely napszakokban, illetve mely napokon jelentkezhetnek be a hálózatba. Ezeket a paramétereket a hálózati rendszergazda közvetlenül megadhatja, betartásukról a hálózati operációs rendszer gondoskodik. Az adatvédelem megsértésének felismeréséhez szükséges az átlagos aktív felhasználószám változásának figyelése, a lemezeken tárolt értékes információkra vonatkozó szokatlan hivatkozások detektálása, a nem tervezett hozzáférési jogosultság változások, valamint a megmagyarázhatatlan rendszer lefagyások figyelemmel kisérése. Az adatok védelméről bővebben lásd [5][10][11] műveket.

Ahhoz, hogy biztonságos kommunikációról beszélhessünk az adatok titkossága, hitelessége, sértetlensége, és letagadhatatlansága nélkülözhetetlen. A titkosítás az adatok védelmét szolgálja, az csak a megfelelő kulcsok birtokában fejthető vissza. A hitelesítés a kommunikációs partner azonosítására szolgál, meggyőződünk arról, hogy tényleg azzal állunk kapcsolatban, akivel hisszük. Az adat sértetlensége azt bizonyítja, hogy eredeti formájában érkezett meg, és útközben senki nem módosította. A letagadhatatlanság is nagyon fontos kritérium, hiszen biztosítja, hogy a megérkezett adatot később ne tudja letagadni a feladó. Természetesen ezek a biztonsági kérdések nem csak a számítógépes hálózatok esetén, hanem a hagyományos rendszerekben is megtalálható. Ilyenek például: a pecsétek, az aláírás, a lezárt boríték, nehezen reprodukálható minták, hologramok, hiteles másolatok használata. Ezek a jól bevált módszerek nem használhatók az elektronikus világban, így más módszereket kell keresni (lásd [10]). Ilyen módszerek például a DES (Data Encryption Standard), RSA (Rivest, Shamir, Adleman – a szerzők neve alapján), vagy a Kerberos hitelességvizsgáló protokoll.

A hálózatok biztonsági szintjét az USA Védelmi Minisztériuma által definiált TCSEC (Trusted Computer System Evaluation Criteria) szintek szerint osztályozhatjuk. A szintek D-

től A-ig terjednek, ahol a D szint jelenti a leggyengébb biztonságot, a további szintek pedig mindig hozzátesznek valamilyen megszorítást az előzőhöz.

- D - Minimal Protection (Minimális védelem): Alig vagy egyáltalán nem tartalmaz biztonsági intézkedést.
- C1 - Discetionary Security Protection (Megkülönböztetéses védelem): A felhasználók névvel és jelszóval azonosítják magukat. A felhasználók csoportokba sorolhatók. A felhasználók a tulajdonukban lévő erőforrásokkal saját maguk rendelkeznek, és jogokat (olvasható, írható, futtatható) rendelhetnek hozzájuk.
- C2 - Controlled Access Protection (Ellenőrzött hozzáférés): A C1 szintet kiegészíti a biztonsággal kapcsolatos események naplózásával.
- B1 - Labelled Security Protection (Címkézett biztonság): Az adatokhoz titkossági fokozatot rendel. A felhasználók ezt a fokozatot nem állíthatják át, ezzel megakadályozva az adatokkal való visszaéléseket.
- B2 - Structured Protection (Strukturált Védelem): Ez a szint kriptográfiai módszerek használatát írja elő, továbbá az állományokhoz biztonsági szintet jelölő címkéket rendel.
- B3 - Security Domains (Biztosított egységek): Az eszközök fizikai hozzáférését is szabályozza, és a kommunikációs útvonalak ellenőrzését is előírja.
- A - Verified Design (Ellenőrzött Tervezés): Megköveteli a rendszer biztonságának matematikai úton való bizonyítását.

2. 5. Elszámolás menedzsment

Az elszámolás menedzsment feladata a költségek és számlák ellenőrzése, ehhez meg kell határozni a költségek összetevőit, az erőforrás használat mértékét. A LAN-menedzsmentnek tisztában kell lennie a kiadásokkal, így a hálózat fenntartásának költsége meghatározható. Az elszámolás menedzsment feladata még a felhasználók hálózat használatának szabályozása, a hálózat optimális kihasználása, és az erőforrások igazságos elosztása érdekében. Ezt befolyásolják a felhasználói szokások, bizonyos szolgáltatások működéséhez szükséges erőforrások, a számlázási és az üzleti érdekek. Hogy ezt biztosítani tudja a teljesítmény menedzsmenthez hasonlóan, figyelni kell a hálózatot, és méréseket kell végezni.

Az elszámolás menedzsment legfontosabb feladata tehát a költségösszetevők meghatározása. Ezek a [11] mű alapján a következők:

- Hardver eszközök: szerverek, perifériák, csatoló elemek, munkaállomások, stb.
- Kábelek: kábelek, csatoló elemek beszerzési és fenntartási költségei
- Softver: hálózati operációs rendszerek, meghajtók, alkalmazói szoftverek, licencek
- LAN menedzsment rendszerek: menedzsment alkalmazások, megfigyelők, adatbázisok, tesztelő berendezések
- Infrastruktúra: bérelt vonal, egyéb összeköttetések, előfizetői díjak, LAN szegmensek összekapcsolása
- Emberi, személyi költségek
- Egyéb állandó költségek: épületek, bérleti díjak, karbantartási díjak
- Egyéb állandó működtetési költségek: energia, fűtés, hűtés

Az elszámolás menedzsment feladata a beszállítók és szolgáltatók számláinak ellenőrzése. A számlák tényleges feldolgozása nem a LAN-menedzsment feladata, csupán a számlák helyességének ellenőrzése, a túlszámlázások, és a késedelmes fizetésből adódó problémák elkerülése.

2. 6. Felhasználói adminisztráció

A hálózati menedzsment ISO által meghatározott feladataihoz nem tartozik a felhasználói adminisztráció, de feladata szerint talán mégis ide sorolható, ahogy ezt több forrás is teszi, pl.: [11]. A felhasználókkal kapcsolatos feladatok az ISO öt funkciójának feladatai között is megtalálhatók, de ezek nem elégítik ki teljesen a felhasználókkal kapcsolatos teendőket. Például nem adnak választ a felhasználók támogatására, vagyis munkájuk egyszerűbbé tételére, segítésére. Célja, hogy elfedje a felhasználók elől a hálózat bonyolultságát, lecsökkentse a felhasználók képzésének idejét és költségét, és ezzel csökkentse a felhasználói hibák számát (ami a hálózati hibák jelentős részét teszi ki), és ezzel a rendszergazda közbeavatkozásának igényét.
A felhasználók támogatásához elengedhetetlen a könnyen kezelhető felhasználói felület, távoli felhasználókat támogató eszközök, és információs pult biztosítása.

3. A hálózatmenedzsment szabványosítása

A hálózatok méretének növekedésével működtetésük és karbantartásuk egyre nehezebb feladattá vált, ezért nélkülözhetetlen volt egy egységes hálózat menedzselési eljárás megalkotása. Több próbálkozás is történt protokollok, szolgáltatások, és architektúrák kidolgozására, de problémát jelentett a heterogén környezet, mivel a gyártók eltérő megoldásokat kínáltak. Mivel a vezető gyártók nem szívesen adják fel saját architektúrájukat, és eddigi befektetéseiket csupán azért, hogy a szabványoknak megfeleljenek, ezért a kommunikációs szabványok elfogadása jelenthet megoldást (lásd [2][7][9][11]).
A kialakult szabványok közül a következők a legfontosabbak:

- CMIP (Common Management Information Protocol): Az ISO által kidolgozott protokoll, az OSI (Open Systems Interconnection) része. A hálózati menedzsment korábban ismertetett öt funkcióját itt definiálták.
- CMOT (Common Management Over TCP/IP): A CMIP TCP/IP feletti megvalósítása. Mivel nem készültek el időben a specifikációk, az implementációk, és a gyakorlati alkalmazhatóságot bizonyító megvalósítás, így az Internet Architecture Board (IAB) támogatása csökkent, és a fejlesztés is leállt.
- TMN (Telecommunications Management Network): International Telecommunication Union (ITU), korábbi nevén Comité Consulative Internationale de Telegraphique et Telephonique (CCITT) ajánlása. A távközlési hálózatok menedzselését írja le. Felhasználásának területei a következők: távbeszélő hálózatok, LAN és WAN adatátviteli hálózatok, ISDN és B-ISDN hálózatok, mobil hálózatok, intelligens hálózati szolgáltatások, és átviteli hálózatok (SDH)
- SNMP (Simple Network Management Protocol): Internet Engineering Task Force (IETF) által szabványosított protokoll, a TCP/IP menedzsment de-facto szabványa. Ma ez a legelterjedtebb protokoll.

Az SNMP elterjedten alkalmazott, és rengeteg SNMP alapú alkalmazás létezik, és habár a CMIP funkcionalitását tekintve sok szempontból fejlettebb, mint az SNMP, mégis nagyon kevés CMIP implementáció létezik.

4. A Simple Network Management Protocol (SNMP)

Az SNMP (Simple Network Management Protocol – egyszerű hálózat felügyelő protokoll) első verzióját 1990. májusában hozták nyilvánosságra az 1157-es RFC-ben. A felügyelettel kapcsolatos információkat tartalmazó társdokumentummal (RFC 1155) együtt az SNMP egy szisztematikus módszert adott a hálózatok figyelésére és felügyeletére. Az SNMP-ről bővebben lásd: [4][6][7][10][11] műveket.

Az SNMP az első hálózati diagnosztikára kifejlesztett protokoll az SGMP (Simple Gateway Monitoring Protocol) továbbfejlesztéséből született. (Az SGMP 1987–ben jelent meg, és a hálózati átjárók menedzselésére használták.) Az SNMP azért lett „egyszerű", mert csak átmeneti megoldásnak szánták, amit majd le lehet cserélni. De ugyanúgy, ahogy a TCP/IP egyre népszerűbb lett, és a hálózati technológia egyik alapvető szabványa lett. Egyszerűsége abban nyilvánul még meg, hogy működéséhez összeköttetés-mentes (datagram) szolgáltatást igényel, ezért bármely hálózati átviteli protokollra implementálni lehet. Idővel kiderültek az SNMP hiányosságai, ezért továbbfejlesztették, és megjelent az SNMPv2 (1993), majd az SNMPv3 (2000) is. A három változat filozófiája között nem figyelhető meg lényeges eltérés, viszont a későbbi változatok összetettebb feladatok egyszerűbb elvégzését teszik lehetővé, és fejlettebb biztonsági megoldásokat tartalmaznak. Továbbá kibővítik a távoli monitorozással (Remote Monitoring – RMON) is, amely lehetővé teszi, hogy elkülönült készülékek helyett egyetlen egységként szemléljük a hálózatot. Az SNMP-vel kapcsolatos legfontosabb RFC dokumentumok a következők:

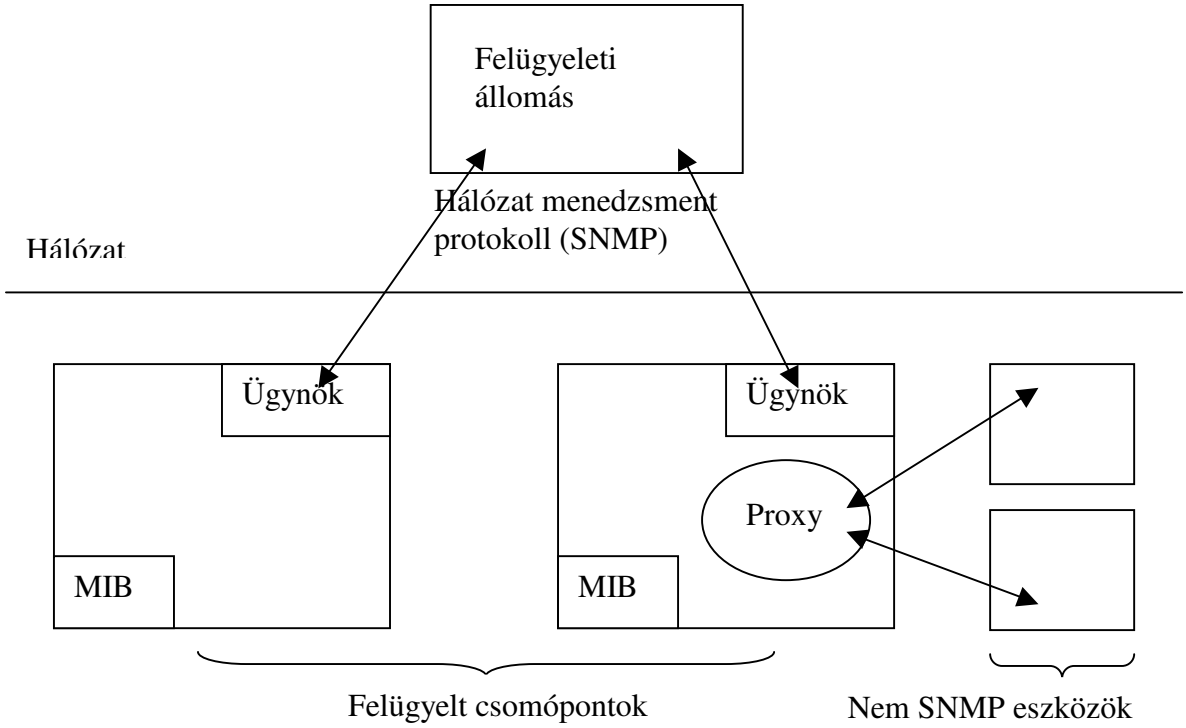
- SNMPv1:
    - RFC 1155 – A menedzsment információk struktúráját írja le
    - RFC 1157 – Magát az SNMP-t definiálja
    - RFC 1212 – A MIB definíciója
    - RFC 1213 – A TCP/IP hálózatok menedzsmentjéhez szükséges MIB
- SNMPv2:
    - RFC 1901 – Az SNMPv2 bemutatása
    - RFC 2578 – az SMIv2-t definiálja
- SNMPv3:
    - RFC 1906 – Az SNMPv3-at írja le
- RMON

- RFC 1757 – Remote Monitoring
- RFC 2021 – Remote Monitoring 2

4. 1. Az SNMP felépítése, működése

Az SNMP hálózat felügyeleti modellje négy összetevőből áll (lásd [10]):

1. Felügyelt csomópontok
2. Felügyeleti állomások
3. Felügyeleti információ
4. Felügyeleti protokoll



Felügyelt csomópont bármely eszköz lehet, amely képes állapot információt küldeni magáról, pl.: hosztok, forgalomirányítók, kapcsolók, hidak, nyomtatók. Ahhoz, hogy egy eszközt az SNMP felügyelhessen, képesnek kell lennie az SNMP ügynök (SNMP agent) futtatására. Az ügynök egy változókból álló helyi adatbázist tart fent, hogy leírja az eszköz állapotát, információkat tároljon a korábbi eseményekről, vagy megváltoztassa az eszköz működését. Az ügynök feladata a felügyeleti állomás kéréseinek kiszolgálása. Az ügynök tulajdonképpen két feladatot lát el: a felügyelt csomópont figyelését, és vezérlését. Ha a

felügyelő állomás lekérdez egy információt az ügynök vagy a már begyűjtött adatokat adja vissza, vagy a kérdés hatására szerzi be az eszköztől a szükséges információt. Általában a felügyeleti állomás bizonyos időközönként lekérdezi az eszközöket, ezt polling-nak hívják. Az ügynök a felügyeleti állomás kérése nélkül, csak csapda (trap) esemény esetén küld üzenetet. Ilyen figyelmeztető üzenetet a beállított határértékek átlépése, vagy az eszköz leállása, újraindulása válthat ki. Ez az üzenet csak azt tartalmazza, hogy valamilyen esemény történt, ez után a felügyeleti állomás feladata, hogy kiderítse az esemény okát. A eszköz vezérlése egy változó átállítását jelenti (pl.: a Cisco router-ek esetén, azt hogy töltse le a konfigurációs állományt egy TFTP szerverről, egy változó beállításával tehető meg, ez általában gyártó specifikus), ekkor az ügynök a felügyeleti állomás kérésére tudja módosítani az eszköz működését. Ez jelenti az SNMP egyik legnagyobb veszélyét, mivel az első verzióban a felügyeleti állomás csupán egy egyszerű szövegként (kódolatlanul) megadott jelszóval azonosította magát. Ez azért probléma, mert a felügyeleti állomás a csomópont működéséről bármit megtudhat, sőt módosíthatja (le is állíthatja). Ezt a későbbi verziókban már kijavították, ám ez Tanenbaum szerint, a már amúgy is bonyolult protokollt még bonyolultabbá tette.
Azért, hogy olyan csomópontokat is felügyelni lehessen, amelyek nem képesek az SNMP ügynököt futtatni, az SNMP a helyettesítő ügynököt (proxy agent) biztosítja. A proxy agent egy vagy akár több nem SNMP készüléket felügyel, kommunikál a felügyeleti állomással, az eszközzel pedig valamilyen gyártó specifikus protokoll segítségével tartja a kapcsolatot.

A **felügyeleti állomás** gyakorlatilag egy menedzsment szoftvereket futtató számítógép, amely hálózaton keresztül kéréseket küld az ügynököknek, és fogadja azok válaszait. A felügyeleti állomás, pontosabban a rajta futó menedzsment alkalmazások archiválják, dolgozzák fel, és könnyen értelmezhető formában jelenítik meg a begyűjtött információkat.

A **felügyeleti információ** alatt azokat az adatokat értjük, amelyek leírnak egy SNMP-vel menedzselhető eszközt. A felügyeleti információs adatbázis minden felügyelt készüléken megtalálható egy adatbázis-struktúra formájában. Mivel ezek az eszközök általában több gyártótól származnak, a tárolt információ felépítését pontosan definiálni kell. Ezért az SNMP minden egyes ügynök számára előírja, hogy milyen információkat kell tartalmaznia, és milyen formátumban kell azt rendelkezésre bocsátania. A felügyelt csomópontok az állapotuk

információit változókban tárolják, az SNMP ezeket a változókat objektumoknak hívja. Ez az objektumfogalom nem felel meg teljesen az objektumorientált rendszerek objektum fogalmának, mivel ezeknek az objektumoknak csak értékük van, amelyet olvasni és írni lehet, nem rendelkeznek további metódusokkal. Az összes lehetséges objektumot a MIB (Management Information Base – felügyeleti adatbázis) nevű adatstruktúrában adják meg. A MIB-t a következő részben részletesebben fogom tárgyalni.

A **felügyeleti protokoll** maga az SNMP. Az SNMP egy alkalmazási rétegbeli protokoll, melyet a felügyeleti állomás és a felügyelt csomópontok, pontosabban az ügynök közti adattovábbításra terveztek.

Az SNMP üzenetformátuma:

Version Number	Community String	SNMP PDU

Ahol a version number és a community string együtt alkotja az SNMP üzenet fejrészét, melyben a community string szolgálja az authentikációt, a felügyeleti állomás ezzel azonosítja magát. Az SNMP PDU felépítése pedig a következő:
GetRequest, GetNextRequest, SetRequest, GetResponse üzenet esetén:

PDU Type	Request ID	Error Status	Error Index	Variable Bindings

Ahol az Error status, és az Error index értéke a GetResponse üzenet kivételével mindig nulla.
A trap üzenet felépítése az első verzióban eltért a többitől, de az SNMPv2-ben már ez is megegyezik a többiével. A trap PDU SNMPv1 esetén a következőképpen néz ki:

PDU Type	Enterprise	Agent address	Generic Trap Type	Specific Trap Type	Time Stamp	Variable Bindings

A Variable Bindings felépítése pedig a következő:

OID 1	Value 1	OID 2	Value 2	…	OID n	Value n

Ahol az OID, Value párok a MIB egy objektumát, és a hozzá tartozó értéket jelentik.

A következő üzenettípusokat biztosítja az SNMP:

- GetRequest: egy vagy több változó értékének a lekérése. Az ügynök kikeresi a variable-bindings (magyarul talán kapcsolt változók) által meghatározott MIB változók értékét, és a GetResponse üzenetben válaszol a kérésre.
- GetNextRequest: hasonló a GetRequest-hez, de nem a kérésben megadott változót, hanem a lexikografikusan rákövetkezőt adja vissza. Segítségével a MIB gráf balról jobbra történő mélységi bejárását adhatjuk meg, ahol a bejárás során csak a fa levelei érdekesek számunkra.
- GetResponse: az ügynök generálja válaszul a GetRequest, GetNextRequest, és a SetRequest üzenetekre.
- SetRequest: a variable-bindings által hivatkozott objektum értékének beállítására használható.
- Trap: ezt az üzenetet a felügyelt csomópont automatikusan generálja valamilyen esemény hatására. Ilyen események lehetnek például [36]:
    - Cold Start: Hideg újraindítás - a konfiguráció módosulhatott
    - Warm Start: Meleg újraindítás - a konfiguráció nem változik
    - Link Down: az eszköz jelzi, hogy változás (hiba) történt az egyik kommunikációs kapcsolatnál
    - Link Up: a kapcsolat helyreállt
    - Authentication Failure: Jogosulatlan hozzáférés
    - EGP neighbour Loss: forgalomirányító hibajelzése
- GetBulkRequest: az SNMPv1 nem tartalmazta, csak a v2-ben kerül be. Táblázatok lekérésére (pl.: forgalomirányító tábla) használható.
- InformRequest: ez az üzenettípus is csak az SNMPv2–ben jelenik meg. A felügyeleti állomás számára teszi lehetővé, hogy egy másik felügyelővel közölje, mely változókat tartja számon.

Az SNMP összekötetés-mentes (UDP: User Datagram Protocol) szolgáltatást használ az üzenet továbbítására, mely kevesebb erőforrást igényel, és gyorsabb, mint a TCP. Viszont nem használ nyugtázást, vagyis nem megbízható, de ez nem okoz komoly problémát Az üzenetek a 161-es portot használják, kivéve a trap üzenetek, amelyek a 162-es portot.

4. 2. Management Information Base (MIB)

Az SNMP középpontjában az ügynökök által kezelt objektumok vannak, melyeket a felügyeleti állomások lekérdezhetnek, és módosíthatnak. Ezért ezeket az objektumokat gyártó független módon, szabványosan kell leírni, és a hálózaton történő továbbításukat szabványos kódolás segítségével kell biztosítani. Az SNMP ezért az ASN. 1-et (Abstract Syntax Notation One – absztrakt szintaxis jelölés) használja, amely egy szabványos objektum definíciós nyelv. Az ASN. 1 egy primitív adatdeklarációs nyelv, amelyet az ISO 8824–es nemzetközi szabvány ír le. Az SNMP nem használ minden ASN. 1-ben definiált adattípust, sőt ezeket nem is engedélyezi, viszont több új definícióval kiegészíti. Részletekért, lásd: [10] könyvet. Az SNMP a következő ASN. 1-beli egyszerű adattípusokat engedélyezi:

- INTEGER: tetszőleges hosszúságú egész
- BIT STRING: nulla vagy több bitből álló fűzér
- OCTET STRING: nulla vagy több előjel nélküli bájtból álló fűzér
- NULL: helyfoglaló
- OBJECT IDENTIFIER: az objektumokra való hivatkozást teszik lehetővé.

Az alaptípusokból a Sequence, és a Sequence Of segítségével lehet új típusokat definiálni. Az előbbivel típusok egy rendezett sorozatát adhatjuk meg (a C struktúrájához hasonlít), az utóbbival az adott egyszerű típusból álló egydimenziós tömböt definiálhatunk. Az SNMP által definiált további adattípusok a következők:

- Counter32: előjel nélküli 32 bites számláló
- Gauge32: előjel nélküli nem körbeforgó érték (miután eléri a maximális értékét, nem nullázódik le, hanem megtartja azt)
- Integer32: 64 bites CPU esetén is csak 32 bites, előjeles
- UInteger32: 64 bites CPU esetén is csak 32 bites, előjel nélküli
- Counter64: 64 bites számláló
- TimeTicks: Egy időpillanat óta eltelt idő századmásodpercekben
- Opaque: elavult, csak a kompatibilitás miatt
- IpAddress: IP cím
- NsapAddress: egy OSI NSAP cím

Az ASN. 1 átviteli szintaxis azt definiálja, hogyan történik az értékek bitsorozattá konvertálása, és hogyan tudja a fogadó ezt visszaállítani. Az SNMP az ASN. 1 BER (Basic Encoding Rules – alap kódolási szabályok) nevű átviteli szintaxisát használja. Az átvitelre kerülő értékeket a következőképpen ábrázolja:

- Azonosító
- Az adat mező hossza bájtokban
- Az adatmező

Tehát az SNMP a felügyeleti adatok leírását az ASN. 1 segítségével írja le.

A MIB egy objektumának a definíciója a következőképpen néz ki:

Az OBJECT TYPE makrónak négy kötelező paramétere van:

- SYNTAX: az objektum adattípusát adja meg, pl.: INTEGER, OCTET STRING, Counter64.
- ACCESS: az objektumhoz történő hozzáférésről ad információt. Értéke a következők egyike lehet:
    - *read-only* - csak olvasható, -ekkor a felügyeleti állomás az objektum értékét csak olvashatja, nem módosíthatja
    - *read-write* - írható, olvasható, -ekkor a felügyeleti állomás az objektum értékét módosíthatja is
    - *write-only* - csak írható, -például jelszavak esetén használható
    - *not-accessible* - nem elérhető, -kívülről nem elérhető, így a felügyeleti állomás számára sem.
- STATUS: az objektumra vonatkozik. Értéke lehet:
    - mandatory - kötelező, -ha az eszköz támogatja azt a csoportot, amelyiknek ez az objektum tagja, akkor ezt az objektumot kötelező támogatnia
    - optional - választható, -nem kötelező az eszköznek támogatnia
    - obsolete - elavult, -egy korábbi SNMP változat támogatta, de a jelenlegi már nem támogatja
    - deprecated - csökkenő fontosságú, hamarosan elavulttá válik.
- DESCRIPTION: azt írja le, hogy mi az objektum feladata. Ez a mező az embernek szól.

Következzen egy példa az 1213-as RFC dokumentumból (az Interfaces csoportból):

```
ifNumber OBJECT-TYPE
        SYNTAX  INTEGER
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
                "The number of network interfaces (regardless of their current state)
                present on this system."
        ::= { interfaces 1 }
```

Az utolsó sor, tehát a ::= utáni rész helyezi el az objektumot a fában, tehát az ifNumber az interface csoport első számú eleme lesz.

A felügyeleti információk fastruktúráját, és a MIB felépítésének szabályait az SMI (Structure Of Management Information – felügyeleti adatok struktúrája) írja le.

Ezt a hierarchikus fastruktúrát, vagyis az objektumazonosító névteret az ISO, és az ITU felügyeli, és ebben helyezkedik el az SNMP MIB. Ez a névtér globális, tehát minden név globálisan egyedi, és bármely lehetséges objektumot tartalmazhat. A fában minden élhez tartozik egy címke, és egy szám, így a csomópontok egyértelműen meghatározhatók egy címke, vagy számsorozattal. Az OBJECT IDENTIFIER pont ezt a hivatkozást teszi lehetővé.

A fa legfelső szintjén a CCITT (ITU), az ISO, és a kettő kombinációja, azaz a Joint-iso-ccitt áll, amelyekhez a 0, 1, 2 számokat rendelték ebben a sorrendben. Az ISO négy élet definiál, amelyek közül az egyik az identified-organisation nevű, amelyben található az USA Nemzetvédelmi Minisztériuma (Department. Of Defense), amely alatt található az Internet.

A fában elhelyezkedő objektumok a címkék, vagy számok ponttal elválasztott sorozatával adhatók meg. Az objektum megadását mindig a gyökértől kell kezdeni. Az objektumok címkéje és száma közötti megfeleltetés egyértelmű, ezért mindegy melyiket használjuk.

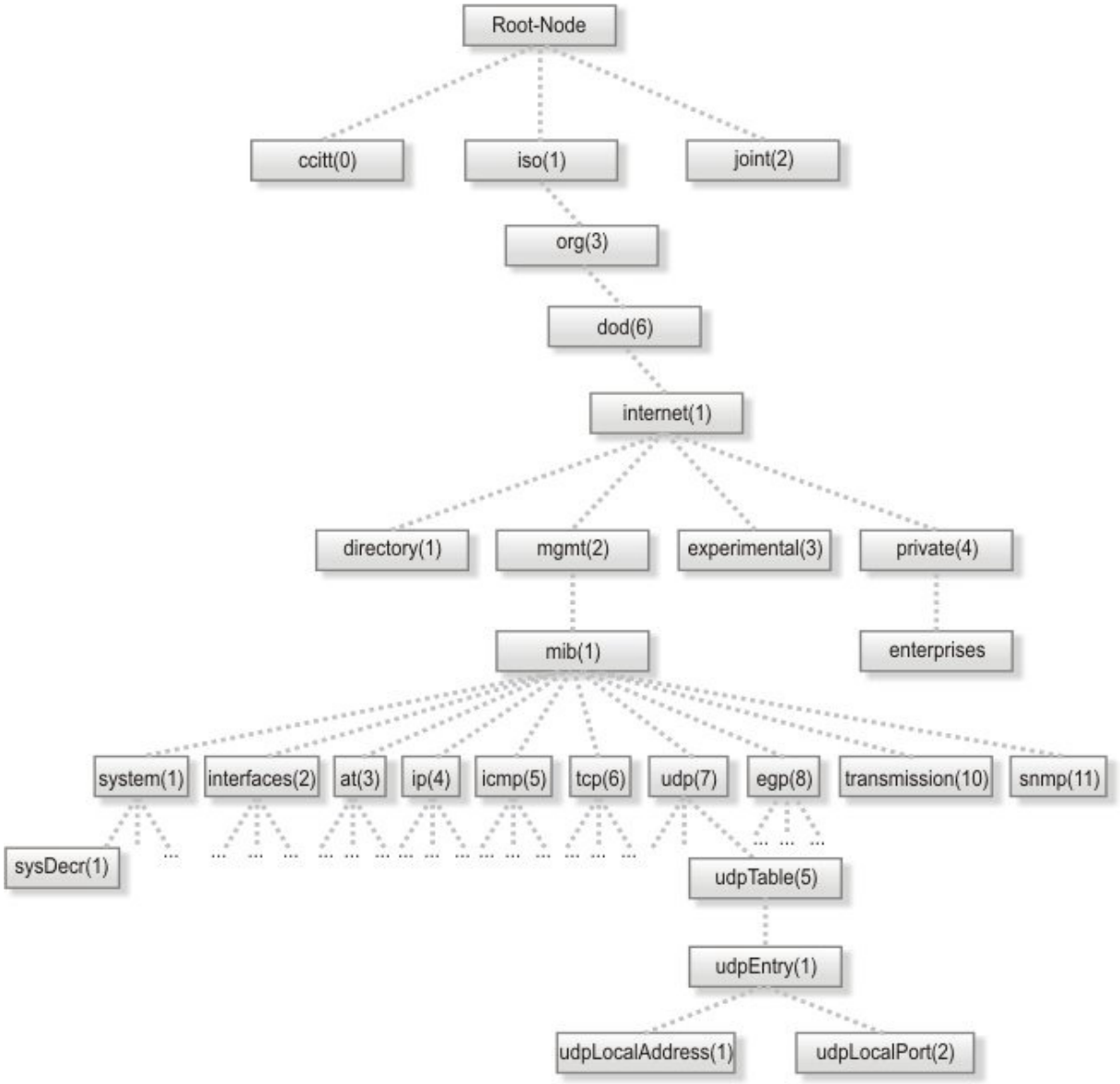
A MIB-ben található objektumok mindig a következőképpen kezdődnek:

Iso.org.dod.internet.mgmt.mib vagy számmal 1.3.6.1.2.1

Ugyanígy a fentebb bemutatott ifNumber a következőképpen hivatkozható:

Iso.org.dod.internet.mgmt.mib.interfaces.ifNumber vagy 1.3.6.1.2.1.2.1

Az objektumazonosító névtér egy részlete - amely tartalmazza a hálózat menedzsmenthez szükséges MIB-fát - az **1. ábrán** látható.



1. ábra. Az objektumazonosító névtér egy része

Az Internet alatt a következők találhatók:

1. directory (könyvtár)
2. management (menedzsment)
3. experimental (kísérleti)
4. private (privát)
5. security (biztonság)
6. snmpv2

A privát részben helyezkedik el az enterprises(1), azaz a vállalati rész. Itt az eszközgyártó cégek (pl.: cisco(9)) kapnak helyet, ahol a saját eszközeikhez állapotokat definiálhatnak.

A menedzsment részben található a mib(1) rész, pontosabban a mib-2(1) rész, mivel a MIB-I-et hiányosságai miatt ki kellett bővíteni. A MIB-II-t az RFC 1213-as dokumentum definiálja. Majdnem minden hálózati eszköz támogatja, mivel különböző gyártók eszközei esetén is általános menedzselési lehetőséget biztosít. A 1213-as RFC a felügyeleti információkat a következő csoportokra osztja:

- System (1): a felügyelt csomópont általános információit tartalmazza, ezek a következők:
    - *sysDescr* - az eszköz szöveges leírása.
    - *SysObjectID* - az eszköz gyártóspecifikus azonosítója. (hardver és agent szoftver típus)
    - *sysUpTime* - az eszköz bootolása óta eltelt idő századmásodpercekben
    - *sysContact* - az eszközért felelős személy neve (string)
    - *sysName* - az egység neve (string)
    - *sysLocation* - a csomópont fizikai helye
    - *sysServices* - egy egész szám, amelyből kiderül, hogy a hálózati egység mely OSI rétegeket támogatja.
- Interfaces (2): a felügyelt csomópont interfészeiről ad információkat. Tartalmazza az interfész sebességét, az interfész típusát, működési állapotát leíró adatokat, illetve keret- és hibaszámlálókat.
- Address Translation (3): elavult, már nem használják.
- IP (4): a hálózati rétegbe tartozó eszközök (pl.: router) menedzseléséhez tartalmaz információkat. Ilyen információk például a forgalomirányító protokollra, és a forgalomirányító táblákra vonatkozó adatok.
- ICMP (5): az ICMP (Internet Contol Message Protocol) figyelésre használható. Az ICMP feladata az IP datagramok továbbítása során előforduló hibák jelzése, jelzőüzenetek küldése. Segítségével a forrás tudomást szerez a bekövetkező hibáról. A MIB ezen objektumai az ICMP üzenetek számát adják.
- TCP (6): a TCP menedzseléséhez szükséges adatokat tartalmazza, például a kapcsolat állapotát, vagy a helyi címek és portok, távoli címre és portra való átváltását.

- UDP (7): az UDP menedzseléséhez szükséges adatokat tartalmazza, például adat é hibaszámlálókat.
- EGP (8): az EGP (Exterior Gateway Protocol – Külső forgalomirányítási protokoll) menedzseléséhez szükséges adatokat tartalmazza. Információt ad a szomszédos forgalomirányítók címéről, és állapotáról.
- Transmission (10): a csomópont helyzetét adja meg a MIB-fán belül.
- SNMP (11): Az SNMP üzenetek számáról ad információkat.

4. 3. Az SNMP előnyei és hátrányai

Előnyei:

- A hálózatmenedzsment de-facto szabványa.
- Jól alkalmazható, és igen elterjedt a használata.
- Kis erőforrásigénye megkönnyíti a hálózati eszközökbe történő implementációját.
- A nem SNMP készülékek is menedzselhetőek a proxy agentek segítségével.
- Rengeteg SNMP termék létezik, és ezek könnyen hozzáférhetők.
- A fejlesztő programcsomagok ingyenesek

Hátrányai:

- Biztonsági lehetőségei korlátozottak. Ezt igazából csak az SNMPv3 oldja meg.
- A nagytömegű adat lekérdezéseket nem támogatja megfelelően. Ezen az SNMPv2 GetBulkRequest üzenete próbál segíteni.
- A felügyeleti állomások közötti kommunikációt csak az SNMPv2 InformRequest üzenete teszi lehetővé, és ez is csak azt teszi lehetővé, hogy egy másik felügyelővel közölje, mely változókat tartja számon.
- Az összeköttetés-mentes kapcsolat miatt az üzenetek nyugtázatlanok, így a trap üzenet is, ezért nagy biztonságot igénylő rendszerekben nem használható.
- Kevés műveletet biztosít, Speciális parancsok végrehajtása meghatározott változók írásával történhet, azonban ezek a mechanizmusok nem szabványosítottak.
- Nehézkes a komplexebb feladatok megoldása.

5. Hálózati menedzsment alkalmazások

Ebben a fejezetben a jelenleg ingyenesen elérhető hálózat menedzsment alkalmazásokból fogok bemutatni néhányat. Ezek a szoftverek vagy teljesen ingyenesen használhatók (freeware), vagy kipróbálásra szánt (shareware) alkalmazások. A shareware szoftverek általában 30 napos próbaidővel, és korlátozott képességekkel használhatók. Rengeteg olyan freeware/shareware alkalmazást lehet találni, amelyeknek köze van a hálózat menedzsmenthez, vagy a hálózatok felügyeletének valamely feladatát próbálja megvalósítani. Ezek a menedzsment alkalmazások nem képesek a hálózati menedzsment összes funkcióját ellátni, többségük csupán eszközök vagy szolgáltatások figyelését, hálózati forgalom mérését, statisztikák készítését teszik lehetővé. Ezek a termékek tudásukban nem képesek felvenni a versenyt a nagy menedzsment-szoftvergyártók (IBM, HP, Novell, BMC, CA (Computer Associates)) komplex szoftver csomagjaival. Ilyen átfogó és integrált felügyeleti eszközök például a Tivoli, a ManageWise, vagy a HP Open View-ja. Viszont ezeket a rendszereket csak a nagy cégek tudják megfizetni.

Mivel a freeware/shareware eszközök csupán korlátozott képességekkel rendelkeznek, valószínűleg a hálózat figyeléséhez és üzemeltetéséhez több eszköz együttes alkalmazására lesz szükség. Az eszközök kiválasztásánál a következő szempontok érvényesülnek:

- Funkcionalitás: a hálózatmenedzsment mely funkcióit látja el, milyen képességekkel rendelkezik az adott szoftver.
- Működési kritériumok: Meghatározzák, hogy milyen környezetben képes működni az eszköz, hogyan telepíthető, és működéséhez mekkora memória- és lemezkapacitásra van szüksége.
- Használhatóság: Az eszköz használhatóságát meghatározza mennyire egyszerű a kezelése, hogyan használható, és mennyire átlátható a grafikus felhasználói felülete.
- Hatékonyság: A hálózati forgalmat figyelő alkalmazásoktól elvárható, hogy a forgalom figyelése ne járjon jelentős erőforrás használattal, a lehető legkisebb sávszélességet használják fel.
- Megbízhatóság: A menedzsment terméknek a hálózat figyelését folyamatosan el kell látnia, esetleges meghibásodása nem hathat ki a hálózat működésére.

- Dokumentáció: Egy jól használható, és megfelelően részletes dokumentáció megkönnyíti a szoftver használatát, ezzel elősegítve a még hatékonyabb hálózat felügyeletet.

Az általam választott menedzsment alkalmazások kipróbálásánál, és vizsgálatánál nem állt rendelkezésemre egy valóságban működő, változatos eszközökkel rendelkező hálózat, csupán virtuális gépekből felépített virtuális hálózat. Így a hálózatom nem tartalmazott hálózati kapcsolóelemeket (switch, router), vagy más hálózati eszközöket.
A virtuális gépek futtatásához Microsoft Virtual PC 2004-et, illetve a VMWare Workstation 30 napig ingyenesen kipróbálható shareware változatát használtam.

5. 1. SolarWinds Engineers Edition

A SolarWinds jelenleg több terméket is forgalmaz, melyeknek létezik 30 napig ingyenesen kipróbálható változata. Ezek a következők:

- Orion Network Performance Monitor
- Cirrus Configuration Management
- Engineers Edition Toolset

Léteznek további termékek is, mint például a Professional Plus Edition Toolset, vagy a Professional Edition Toolset, de az ezek által tartalmazott eszközöket az Engineers Edition Toolset mind tartalmazza. Ezek akkor jelenthetnek alternatívát, ha valamelyik terméket meg akarnánk vásárolni, mivel a kevesebb eszköz kevesebbe kerül.
Most az **Engineers Edition Toolset** nevű terméket fogom bemutatni, amely csomag 45 eszközt tartalmaz, menedzsment feladatok ellátása érdekében.
A SolarWinds által nyújtott eszközök lehetővé teszik a hálózat feltérképezését, a felderített eszközök IP és MAC címeinek, illetve MIB információinak megjelenítését, Cisco eszközök (forgalomirányítók, és kapcsolók) konfigurációs fájljainak kezelését, megadott eszközök állapotának, interfészek sebességének folyamatos figyelését. A SolarWinds az elérhető funkciókat csoportosította, és egy jól kezelhető Toolbar-on (Eszköztár) helyezte el. Így az éppen használni kívánt eszköz gyorsan, és könnyen elérhető.

A SolarWinds Toolbar felépítése a következő, amely a 2. ábrán látható:

2. ábra

- Discovery
- Cisco Tools
- Ping Tools
- Address Mgmt
- E-mail Management
- Monitoring
- Perf Mgmt
- MIB Browser
- Security
- SNMP Traps
- Miscellaneous
- Help & Web

Most következzen a SolarWinds által nyújtott eszközök közül néhány bemutatása:

IP Network Browser

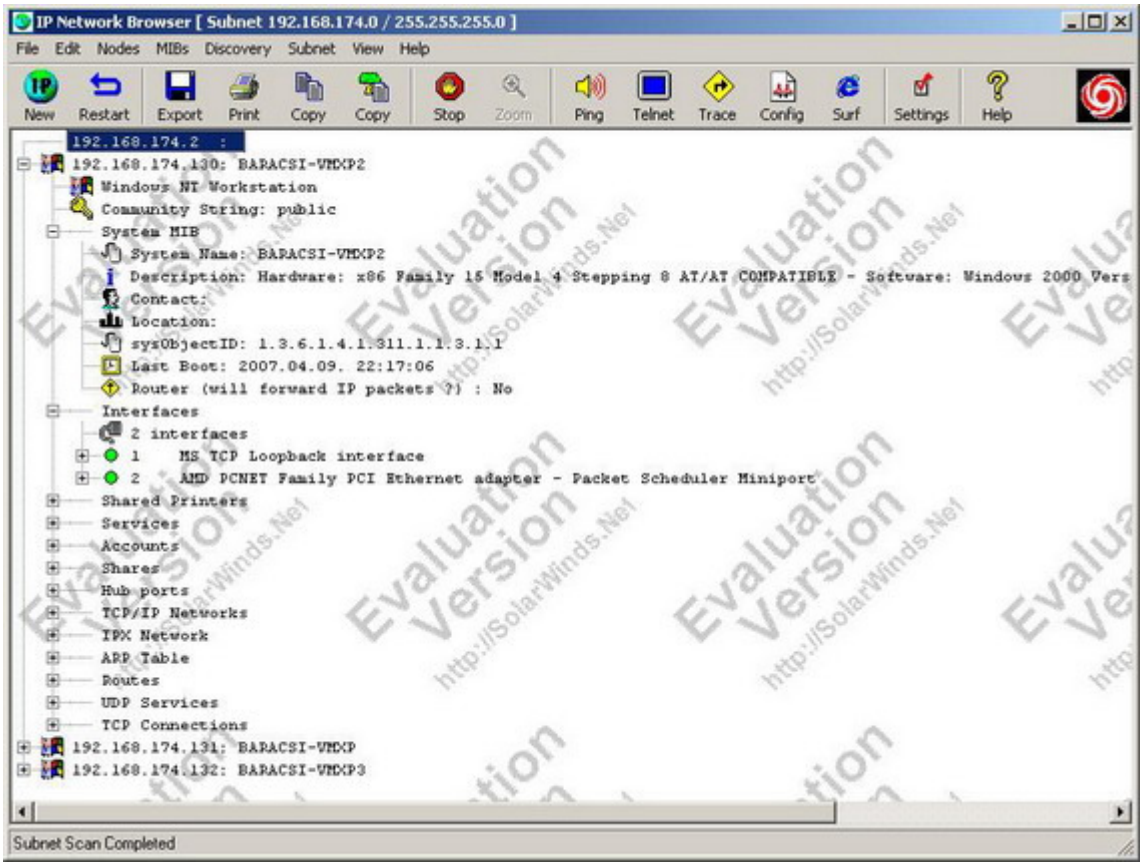
Első lépésben vagy egy hoszt nevét vagy IP-címét kell megadni, vagy egy IP-címtartományt, ami lehet egy alhálózat, vagy egy tetszőleges tartomány, amit egy kezdő- és egy bezáró IP-cím megadásával határozhatunk meg. Ezután a Netork Browser a szóba jövő IP-címeket megpingeli, és ha az válaszol, akkor megkísérli további információk begyűjtését az eszközről. Ezeket az adatokat természetesen az SNMP protokoll segítségével éri el, és ezek a MIB fában található információkat jelentik. Erről egy képernyőképet a 3. ábrán láthatunk.

SNMP Sweep

A megadott IP-címtartományban elérhető eszközök IP-címével, a MIB-fa system ágában lévő információkkal, és az eszköz DNS-nevével tér vissza.

MAC Address Discovery

Futtatásához egy alhálózat azonosítót kell megadni. Eredményül az alhálózatban elérhető eszközök fizikai címét (MAC), logikai címét (IP), DNS nevét, és a hálózati kártya gyártóját adja.



3. ábra IP Network Browser

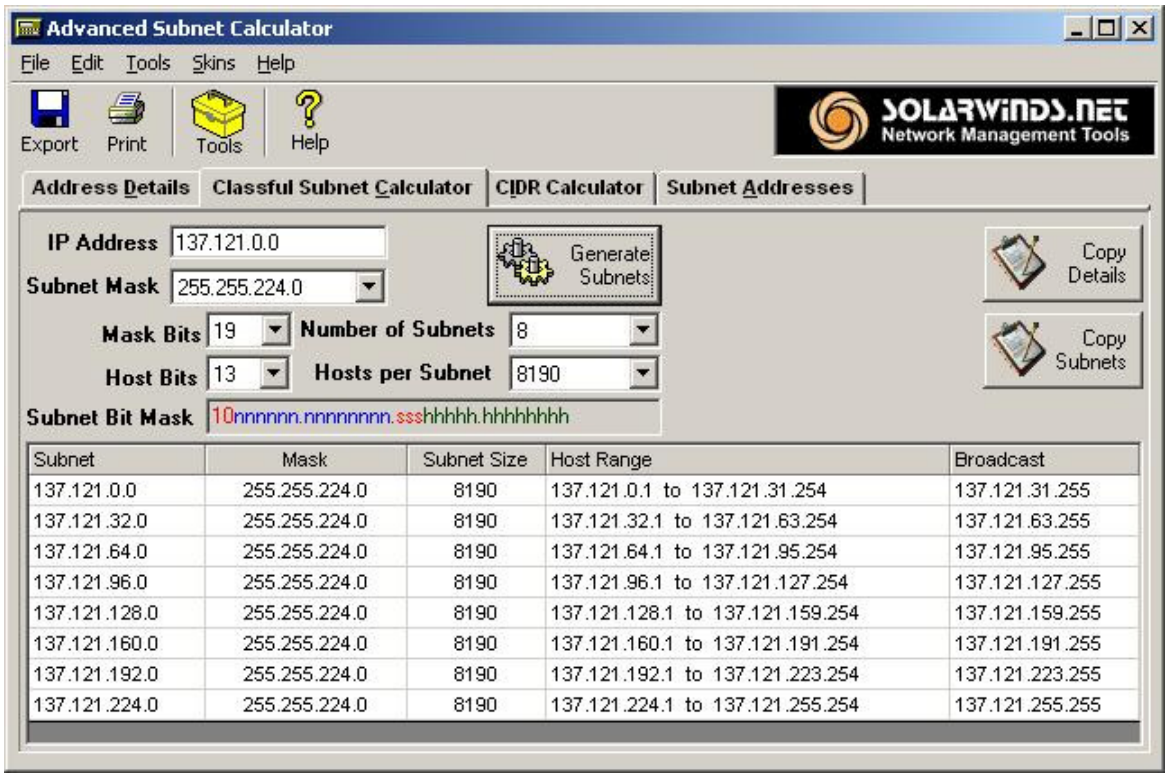
Cisco Tools

Ezek az eszközök a Cisco router-ekkel, és switch-ekkel rendelkező hálózatok esetén lehetnek nagyon hasznosak. Ezek a következők:

- Config Editor/Viewer: Használatához csupán a Cisco eszköz IP-címét, és az azonosításhoz szükséges community stringet kell megadni. A download gombbal letölthetjük a konfigurációs állományt, amit megváltoztathatunk, és az upload gombbal feltölthetünk az eszközre.
- Upload config: A kiválasztott konfigurációs állományt egy megadott TFTP-szerverről fogja letölteni a router. De használható a SolarWinds TFTP-szerver szolgáltatása is.
- Download config: A megadott router konfigurációs állományát a megadott TFTP-szerverre tölti le.
- Running vs startup config: A megadott router konfigurációs állományainak összehasonlítását teszi lehetővé.

Subnet Calculator

Alhálózatok létrehozásánál nyújthat segítséget ez az eszköz. Mind az osztályos, mind a CIDR (Classless InterDomain Routing) alhálózatra bontás módszerét ismeri, és ezt egyszerűen kezelhető, és könnyen átlátható módon biztosítja.



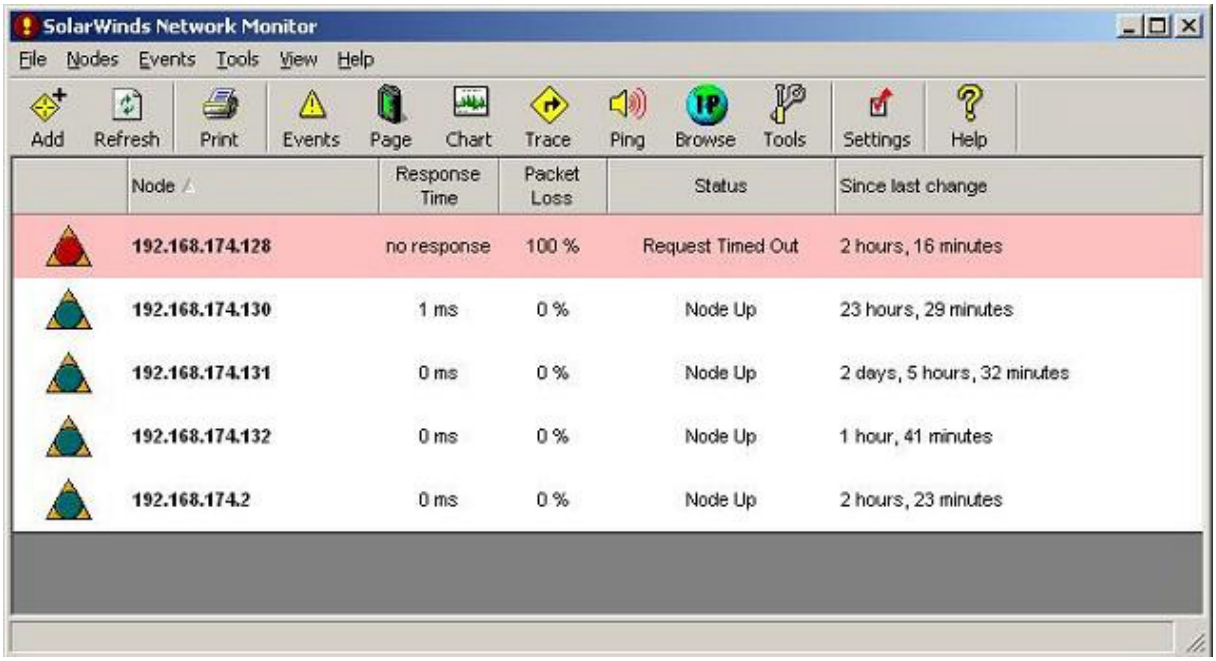
4. ábra Subnet Calculator

Csupán a rendelkezésre álló hálózati azonosítót, illetve azt kell megadni, hogy hogyan szeretnénk felbontani a hálózatot. Ezt megtehetjük a subnet mask megadásával, vagy esetleg a hálózat vagy a hosztok azonosítására használni kívánt bitek számával, vagy csak egyszerűen azt adjuk meg, hány alhálózatra van szükség, illetve alhálózatonként hány hoszt legyen. Eredményül megkapjuk a kapott hálózati azonosítókat, a hálózati maszkot, az üzenetszórásos (broadcast) címeket, illetve azt, hogy alhálózatonként hány címet oszthatunk ki, és ezeknek a címeknek a tartományát. A Subnet Calculator működéséről a 4. ábrán látható egy példa.

Network Monitor

A Network Monitor a hálózati eszközök figyelését teszi lehetővé. Használatához fel kell venni azoknak az eszközöknek az IP-címét, amelyeket figyelni akarunk. Ekkor egy listában jelennek meg a figyelt eszközök, az állapotuk megjelenítésével. Ezt az 5. ábrán láthatjuk. Sajnos a kipróbálható változatban egyszerre csak öt csomópont megfigyelése engedélyezett. Ez önmagában még nem segít sokat a hálózatot üzemeltető személyzet számára, hiszen ahhoz,

hogy bizonyos eseményekre fény derüljön folyamatosan figyelni kellene a Network Monitort.

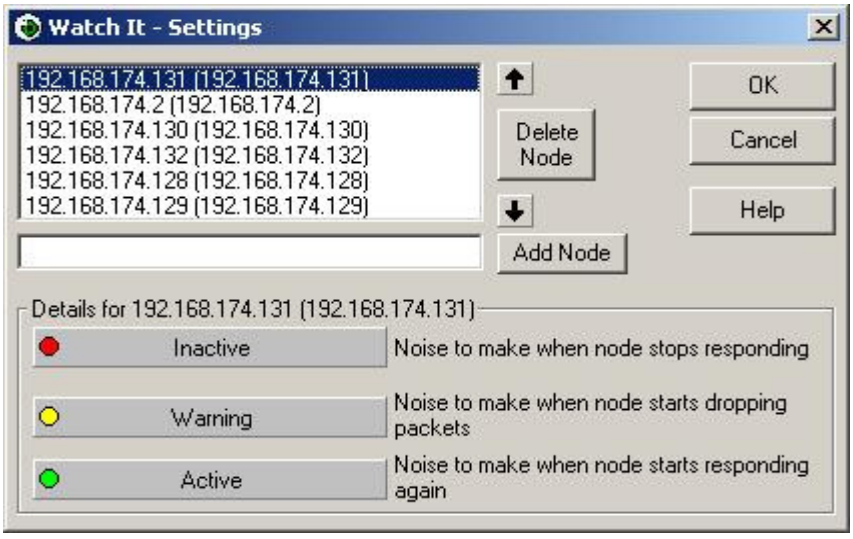


5. ábra Network Monitor

Ezért a Settings menüpont alatt megadhatunk egy e-mail címet, amelyre a megadott események bekövetkeztekor a Network Monitor automatikusan üzenetet küld. Ehhez meg kell adni az SMTP gateway IP-címét is, és az értesítések formátumát is megadhatjuk. Továbbá bizonyos eseményekhez hangjelzéseket is beállíthatunk.

Watch It!

A Solarwinds Watch It! nevű eszközével egyszerűen figyelhetjük meg a hálózat csomópontjainak állapotát. Használatához a figyelni kívánt csomópontokat fel kell venni egy listára, ez a 6. ábrán látható. Ezután képernyő jobb felső sarkában mindig látható kis állapotjelző soron kísérhetjük figyelemmel működésüket. Ezen az állapotjelző csíkon minden eszközt egy színes pont képvisel,



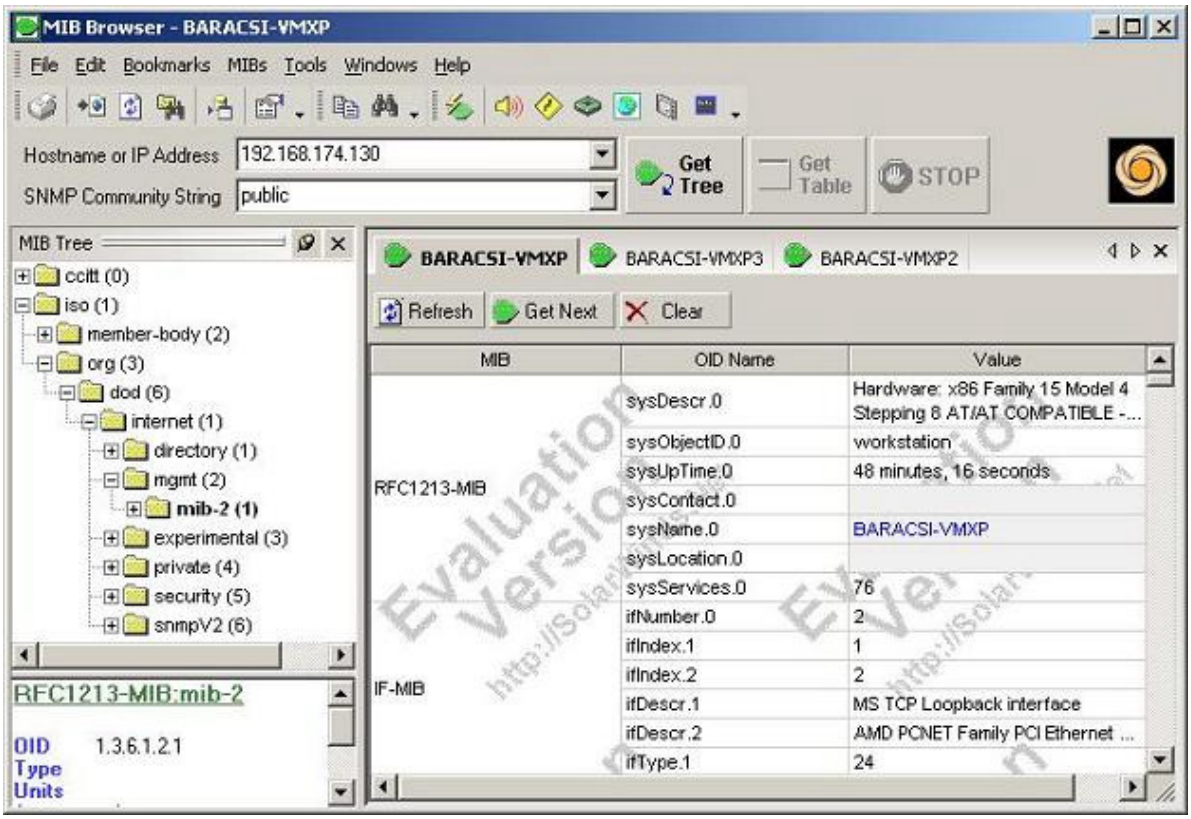
6. ábra Csomópont felvétele

melyek színe az eszköz állapotától függően három különböző színű lehet: zöld, ha az eszköz állapota aktív, piros, amikor az eszköz nem elérhető, és sárga, ha a csomópont állapota kérdéses. Ha a kurzort e csík felé helyezzük, megjelenik a teljes eszköz, ahogy az a 7. ábrán látható, így a pontok mellett a csomópontok IP-címe vagy DNS-neve is látható. Lehetőség van minden eszközhöz külön hangjelzést beállítani, a Watch It! ezzel riaszt, ha az eszköz állapota megváltozik.

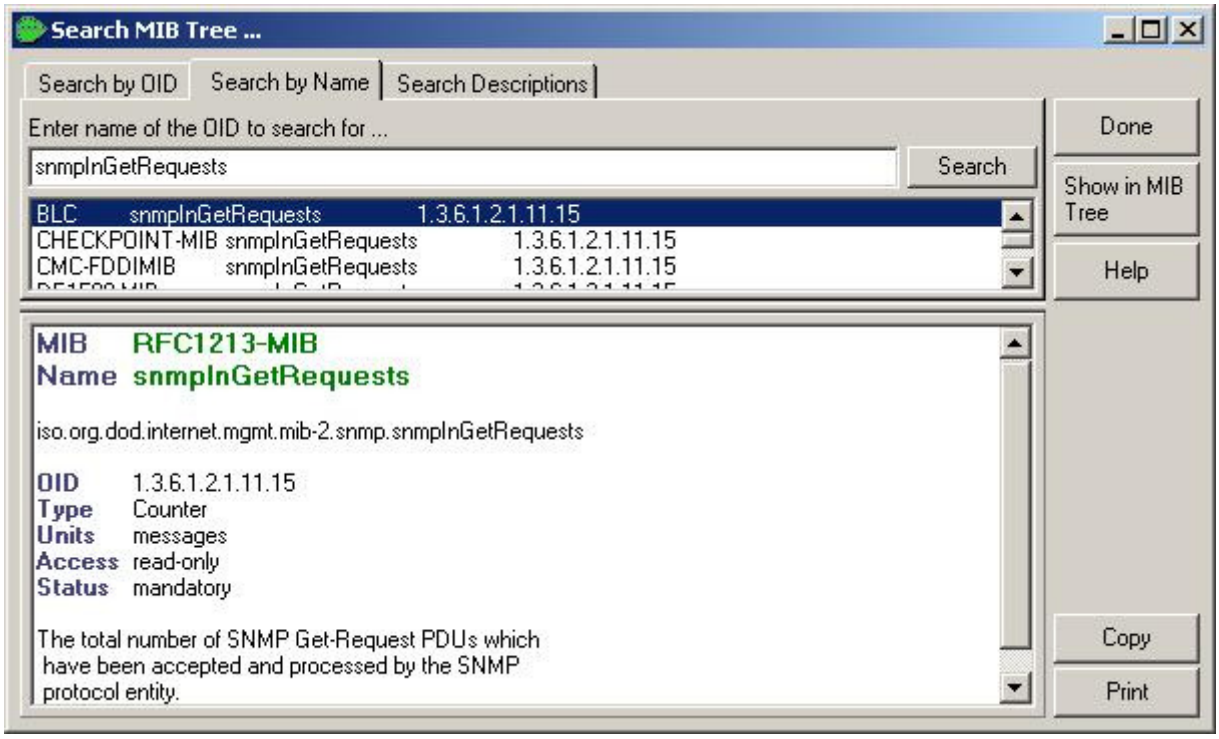
7. ábra Watch It!

MIB Browser

A MIB Browser képes az SNMP-t támogató eszközök teljes MIB-fájának lekérdezésére. Működéséhez csak a csomópont nevét vagy IP-címét, és a megfelelő community stringet kell megadni, ez a 8. ábrán látható. A lekért információk között egyszerűen kereshetünk, továbbá a MIB Browser tartalmazza a teljes objektumazonosító névtér felépítését, így az objektumokra rákereshetünk az azonosítóik, nevük, és leírásuk alapján is, ezt a 9. ábra szemlélteti . Így a MIB-fa objektumairól mindent megtudhatunk.



8. ábra MIB Browser



9. ábra Keresés a MIB-fában

A SolarWinds Engineers Edition a következő webhelyről tölthető le:

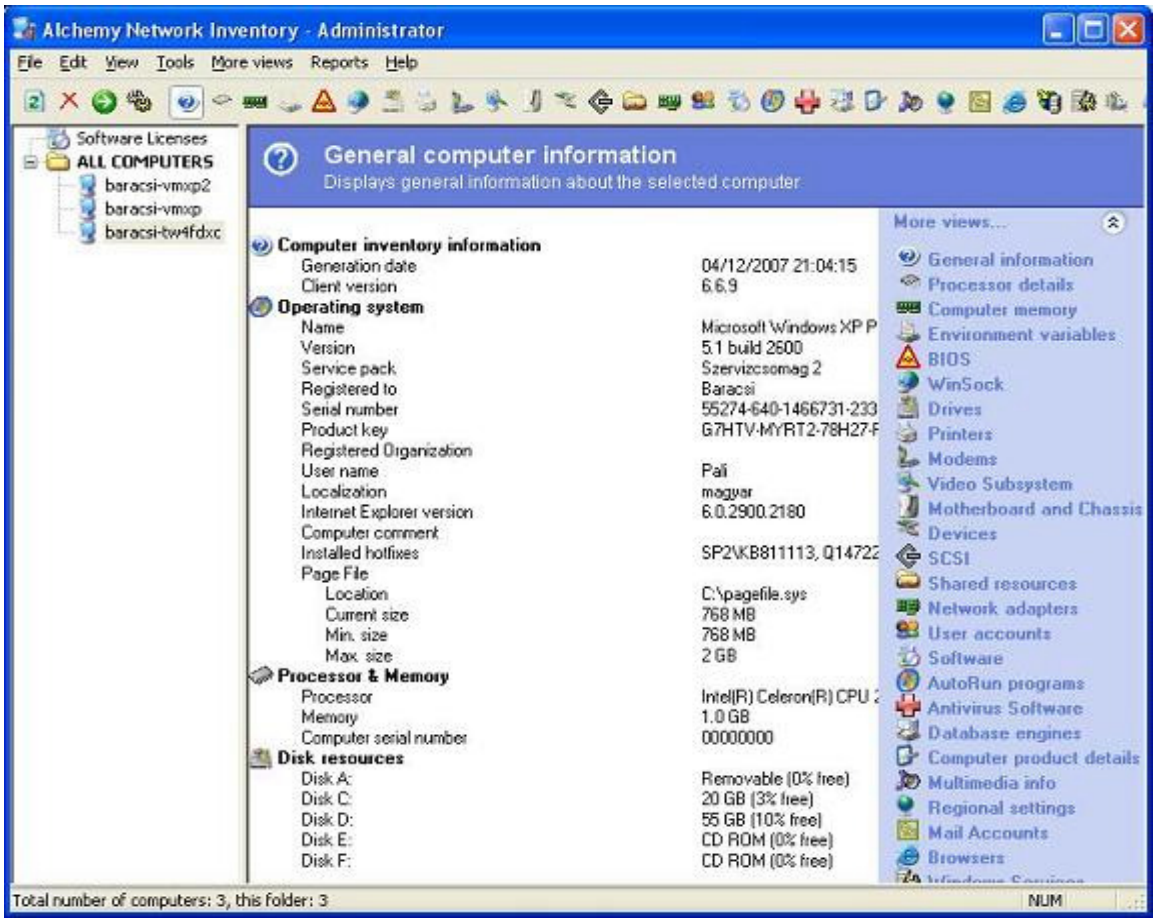
http://www.solarwinds.net/downloads/index.aspx

A SolarWinds Engineers Edition legfontosabb funkciói, és tulajdonságai összefoglalva:

- A hálózati csomópontok állapotának felügyelete, hiba esetén riasztás küldése e-mail-ben.
- SNMP támogatása, MIB információk megjelenítése.
- SNMP csapdák (trap) megjelenítése.
- Forgalomirányítók konfigurációs fájljainak kezelése.
- Hálózati interfészek forgalmának mérése.
- A hálózatban elérhető eszközök feltérképezése. Fizika, logikai címek, DNS nevek megjelenítése.
- Számos további, viszonylag egyszerűen használható eszközt biztosít, amelyek funkciójuk szerint csoportosítva könnyen megtalálhatók az eszköztárban.

5. 2. Alchemy Network Inventory 6. 6. 9

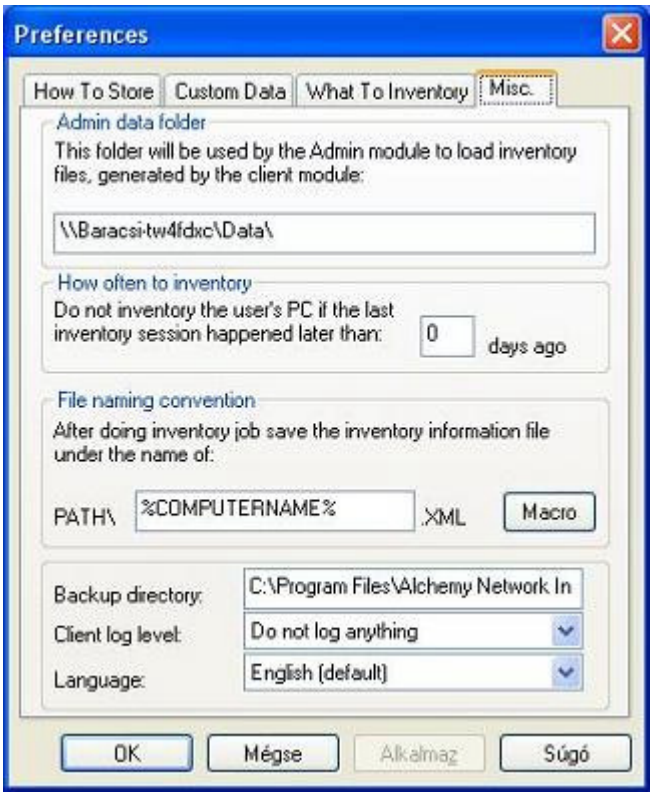
Ahogy a nevéből is lehet rá következtetni, az Alchemy Network Inventory-val a hálózat eszközeinek leltárját készíthetjük el. A hálózat számítógépeinek hardver és szoftver komponenseinek adatait így egy központi helyen tudjuk kezelni. Továbbá képes azon hálózati eszközök (router-ek, switch-ek, hálózati nyomtatók, stb.) információinak begyűjtésére, melyek támogatják az SNMP-t. A 10. ábrán látható, hogy a számítógépekről milyen információkat képes összegyűjteni.



10. ábra Network Inventory

- Hardver eszközök: alaplap, processzor, memória, merevlemezek, optikai meghajtók, hálózati kártyák, videó kártyák, nyomtatók, stb.
- Szoftverek: az operációs rendszer információi, a telepített programok, vírusirtók, licence-ek
- Az operációs rendszer egyéb információi: hálózati beállítások, felhasználók, logikai meghajtók, területi beállítások, (Windows összetevők, Internet Explorer előzmények)

Működéséhez elegendő egy adminisztrátori gépre feltelepíteni, a kliens gépek információit pedig a következőképpen lehet begyűjteni: Meg kell osztani (írási jogot is szükséges) azt a mappát, amelyikben az Alchemy Network Inventory található, vagy ennek egy másolatát. Ezen belül helyezkedik el a Data mappa, ez fogja tárolni az eszközök információit leíró XML fájlokat, és a clientcon.exe nevű fájl, amelyet a klienseknek futtatni kell, hogy lekérje az információkat. Miután megosztottuk ezt a mappát, indítsuk el a programot, és állítsuk be a File menü Preferences… pontjában a How to Store fülnél Shared Folder-nek, ezt a megosztott mappát (Data). Például, ahogy a 11. ábrán látható:



11. ábra A megosztott könyvtár beállítása

\\Baracsi-tw4fdxc\NetAssest\Data\

Ez után már csak minden a leltárba felvenni kívánt gépen le kell futtatni a clientcon.exe fájl, ezt például, így tehetjük meg:

\\Baracsi-tw4fdxc\NetAssest\clientcon.exe

Ekkor összegyűjti a számítógép információit, és a megosztott Data mappába másolja a létrehozott XML fájlt, amelynek neve a számítógép neve lesz, hacsak nem állítjuk be másképpen. Az ingyenesen kipróbálható változata a programnak egyszerre csak három gépet tud kezelni. Az Alchemy Network Inventory jól használható jelentéseket (report) tud generálni, ahol megadhatjuk, hogy mely információk kerüljenek fel a jelentésre és melyek ne. A 12. ábrán egy ilyen jelentés látható. Segítségével a hálózat számítógépeinek fontosabb adatai mindig rendelkezésre állnak, ezzel segítve a hálózati menedzsment feladatát.

Az Alchemy Network Inventory a következő webhelyről tölthető le:

http://www.mishelpers.com/network_inventory/index.html

Az Alchemy Network Inventory legfontosabb funkciói, és tulajdonságai összefoglalva:

- A hálózat hardver elemeinek legfontosabb információinak kezelése.
- Szoftverek nyilvántartása: operációs rendszerek, egyéb alkalmazások, licencek.

- SNMP támogatása.

Local users (Login)	Full name	Last logon	Number of logons
Pali		04/12/2007 19:42:12	1340
Rendszergazda		01/01/1970 01:00:00	0
Segítségnyújtó	Távoli asztal súgójának fiókja	01/01/1970 01:00:00	0
SUPPORT_388945a0	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	01/01/1970 01:00:00	0
Vendég		04/12/2007 21:02:19	0
__vmware_user__	__vmware_user__	04/12/2007 19:42:31	15

Motherboard	Manufacturer	Serial number	Revision
P4V88+		00000000	1.0

CPU name	Speed	Family.Model.Stepping	Cache (L1/L2)	Socket
Intel(R) Celeron(R) CPU 2.53GHz	2526 mHz	15.4.1	12+16/256	

Memory		
Physical: 1024 MB	Virtual: 2048 MB	Paged: 1693 MB

Physical drives	Revision	Serial	Capacity
SAMSUNG SP0822N	WA100-33	S06QJ20Y986052	74,559 Gb

CD\DVD drives	Revision
PIONEER DVD-RW DVR-110D	1.17
NERO IMAGEDRIVE2	2.26
PIONEER DVD-RW DVR-110D	1.17
NERO IMAGEDRIVE2	2.26

Logical drives	Drive Type	File system	Total bytes	Free bytes	Free %
A: ()	Removable		0,000 Mb	0,000 Mb	0,000%
C: ()	Fixed	NTFS	20,001 Gb	743,168 Mb	3,629%
D: ()	Fixed	NTFS	54,550 Gb	5,513 Gb	10,107%
E: ()	CD/DVD-ROM		0,000 Mb	0,000 Mb	0,000%
F: ()	CD/DVD-ROM		0,000 Mb	0,000 Mb	0,000%

Video subsystem				
Video adapter:	NV4_DISP		Memory: 0 MB	
Monitor:	Alapértelmezett monitor		Manufacturer: (Szabványos monitortípusok)	Resolution: 0x0
	Serial number:		Manufacturing date:	Product ID:
Display:	Resolution: 1024x768	BPP: 32	Refresh Rate: 60 Hz	

Printers	Driver	Port
> hp psc 1100 series	hp psc 1100 series	USB001

Network adapters	MAC Address	IP Address	Speed
VIA-kompatibilis gyors Ethernet-adapter - Packet Scheduler Minip	00-13-8F-21-3F-11	0.0.0.0	10 Mb/s
VMware Virtual Ethernet Adapter for VMnet1	00-50-56-C0-00-01	192.168.132.1	100 Mb/s
VMware Virtual Ethernet Adapter for VMnet8	00-50-56-C0-00-08	192.168.174.1	100 Mb/s

12. ábra A Network Inventory jelentésének részlete

5. 3. Network View 3. 51

A Network View egy igen egyszerű alkalmazás a hálózatban elérhető csomópontok felderítésére, és felügyeletére. Képes megjeleníteni a DNS, NetBIOS, SNMP, WMI (Windows Management Instrumentation) információkat, a MAC címeket, és a port scanner segítségével a használt portokat. Meg tudja jeleníteni a MIB információkat (a MIB Browser segítségével), sőt még módosítani is képes a Set művelettel, de ennek használatánál biztosnak kell lenni abban, mit állítunk át.

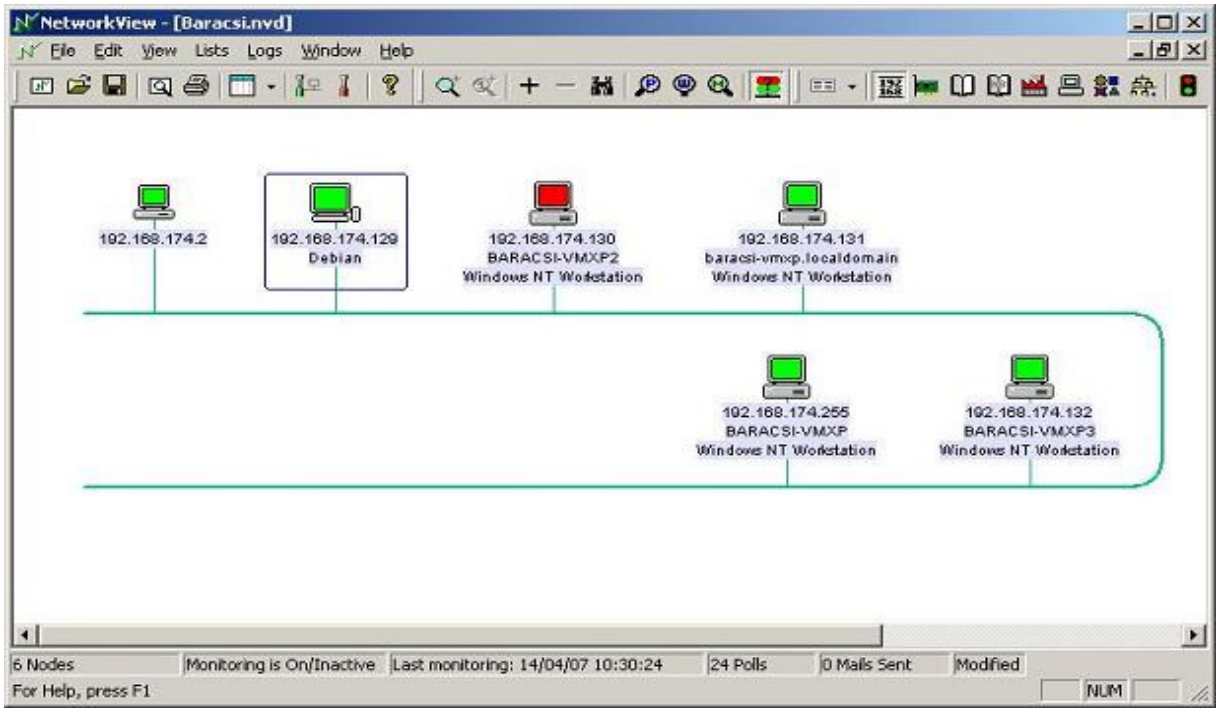
A munka megkezdéséhez egy új térképet (map) kell létrehozni (File\ New). Ekkor a hálózati csomópontok felderítésére három lehetőség kínálkozik:

- Egy megadott csomópont felderítése IP-cím alapján.
- A felderítés megadott IP-cím tartomány alapján történjen, ekkor az a tartományt meghatározó első és utolsó IP-cím szabadon megválasztható.
- Vagy egy megadott alhálózatot deríthetünk fel, amit egy hálózati azonosító, és subnet mask pár definiál.

Ekkor a Network View a lehetséges IP-címeket sorra megpingeli, és ha elérhető a csomópont begyűjti az információkat. Természetesen később is lehetséges új csomópont felvétele. Megadhatjuk a csomópont típusát, mely lehet például: munkaállomás, szerver, kapcsoló, forgalomirányító, webkamera, szünetmentes táp, nyomtató, stb. (Edit\Properties)

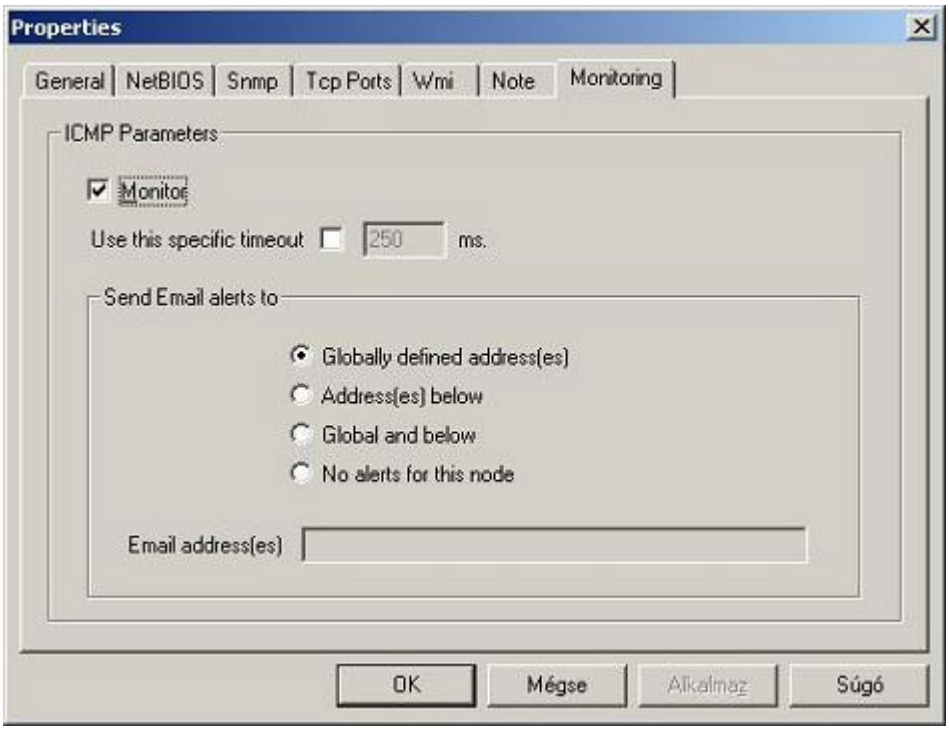
Miután feltérképeztük a hálózatban elérhető eszközöket, lehetőség van azok megfigyelésére, ha bekapcsoljuk a monitorozást, a Start/Stop Monitoring  gombbal. A Network View ICMP üzenetekkel (ping) kérdezi le a csomópontokat, és az alapján jeleníti meg az eszközök állapotát. A különböző állapotokhoz különböző színeket rendel, mint például a 13. ábrán:

- Fehér: azok a csomópontok amelyeket nem figyel, ha ki van kapcsolva a monitoring, akkor minden csomópont színe fehér (not monitored)
- Kék: a csomópont bizonytalan, vagy meghatározhatatlan állapotban van (unknown)
- Piros: a csomópont nem elérhető (down)
- Zöld: az eszköz elérhető (up)



13. ábra A Network View térképe monitorozás közben

A Network View képes riasztást küldeni egy megadott e-mail címre, ha valamelyik megfigyelt csomópont állapota nem elérhető (piros) lesz. A File\Preferences Monitoring fülénél állíthatjuk be, hogy ha az eszköz down állapotba kerül mennyi idő elteltével küldjön riasztást. Ez történhet e-mailben vagy hangjelzéssel. Az E-mail Alerts fülnél lehet megadni egy globális e-mail címet, amely alapértelmezésben minden csomópontra vonatkozik. Itt az SMTP szerver IP-címét is meg kell adni. Lehetőség van minden egyes csomópontra külön megadni, hogy figyelje-e a Network View, vagy sem. Ha igen, akkor lehetőség van beállítani, hogy az előbb említett globális címre, vagy egy egyedi e-mail címre küldje az értesítést, vagy mindkettőre, esetleg azt, hogy nem kell e-mailben értesítést küldeni (lásd 14. ábra).



14. ábra A monitorozás, és a riasztás beállítása egy csomópontra

A Network View a következő webhelyről tölthető le:

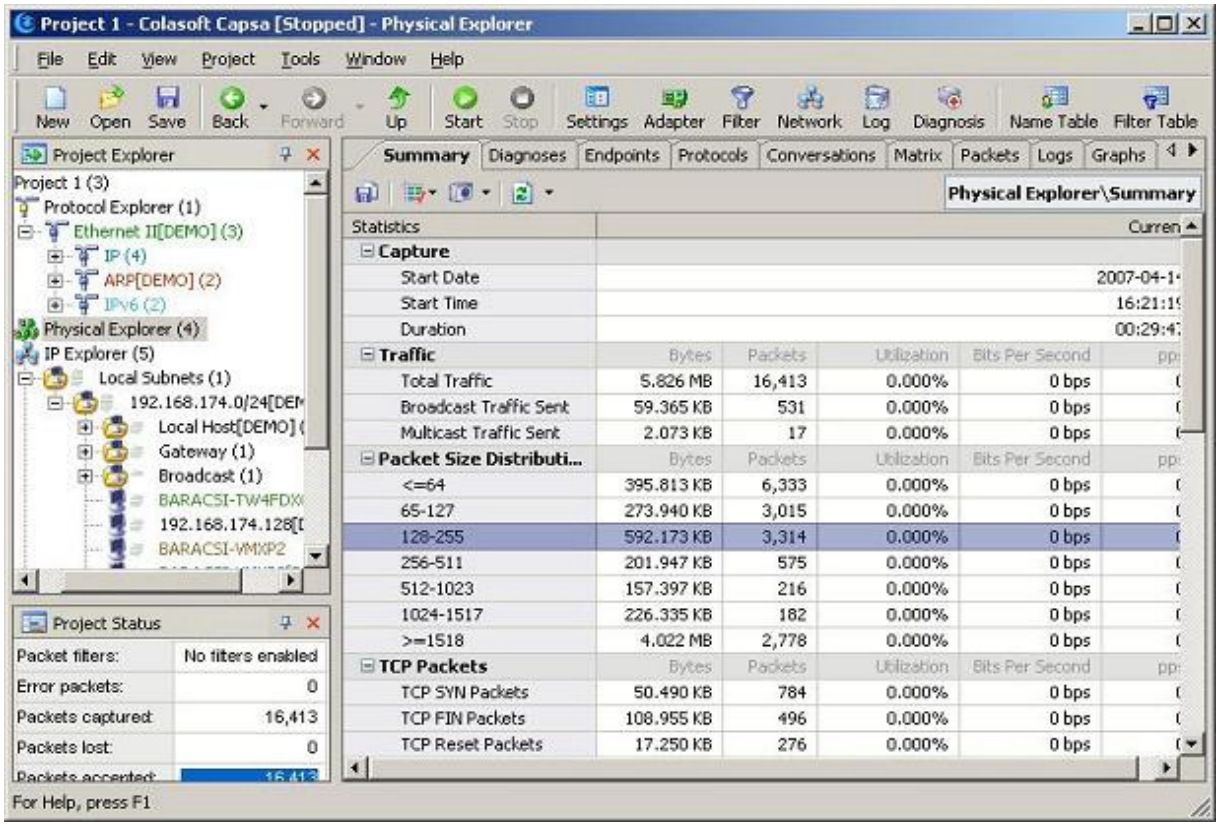
http://www.networkview.com/html/download.html

A Network View legfontosabb funkciói, és tulajdonságai összefoglalva:

- A hálózati csomópontok állapotának felügyelete, hiba esetén riasztás küldése e-mail-ben.
- SNMP támogatása, MIB információk megjelenítése.
- DNS, NetBIOS, WMI információk elérése.
- A hálózatban elérhető eszközök feltérképezése.
- Használata egyszerű.

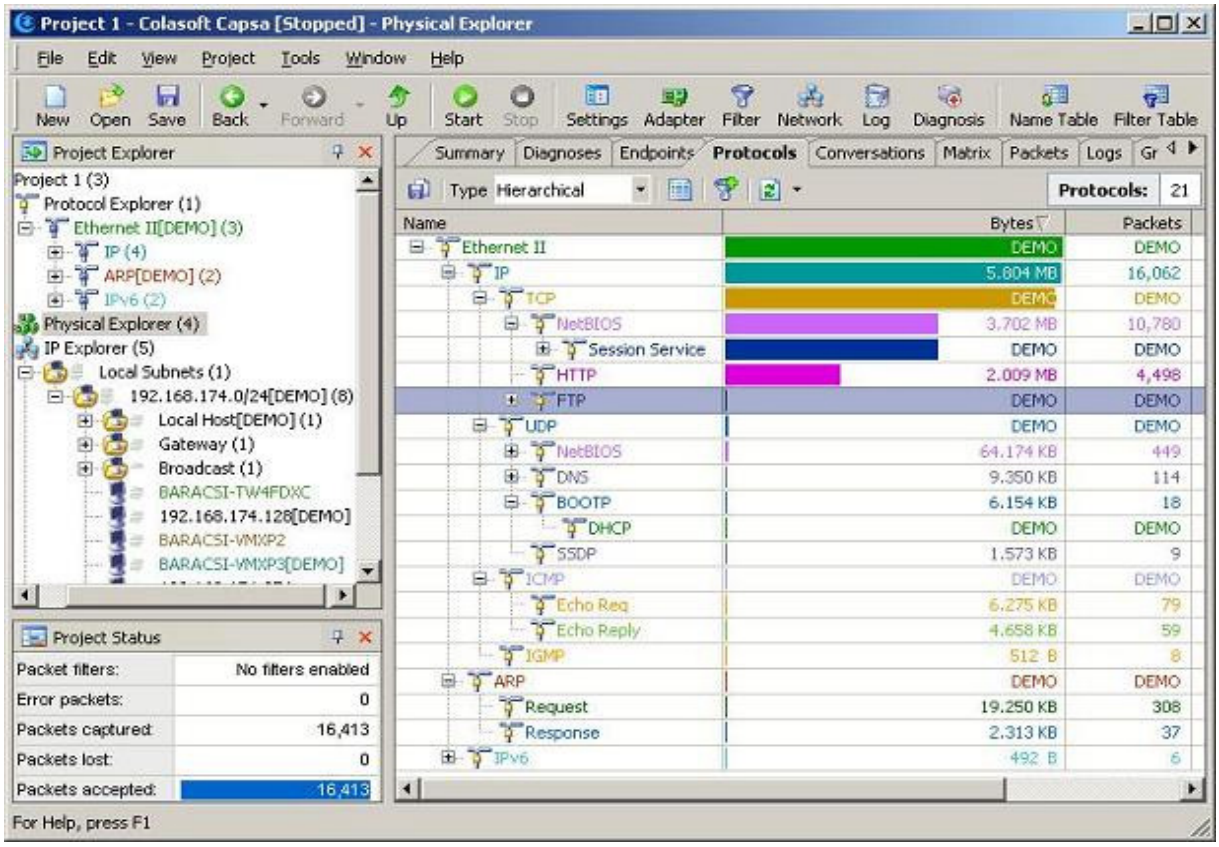
5. 4. Colasoft Capsa 6. 1 Enterprise Edition Demo

A Colasoft Capsa-val a hálózati forgalmat figyelhetjük meg, és statisztikákat készíthetünk róla, a 15. ábrán egy ilyen statisztika látható. Segítségével valós időben elemezhetjük a hálózati forgalmat, és a használt protokollokat, akár csomópontokra lebontva. Használatának megkezdéséhez egy új projektet kell indítani.



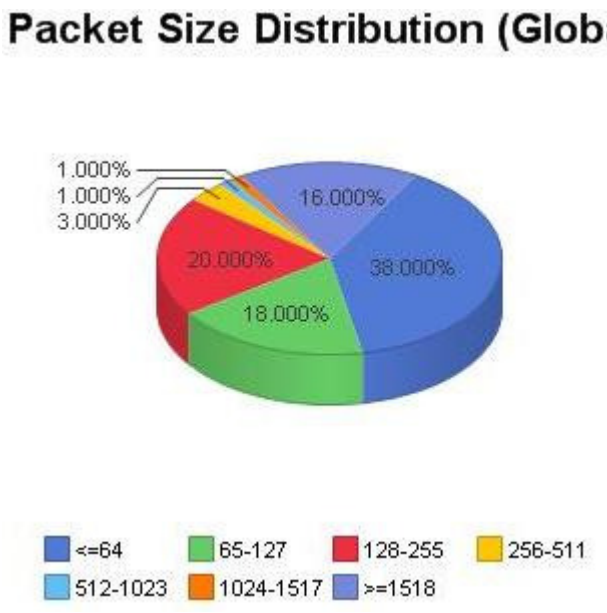
15. ábra A Colasoft Capsa statisztikái

A harminc napig ingyenesen kipróbálható változatban nem lehet elmenteni a projektet, így nem használhatjuk korábbi adatainkat, ezért a Start Capture Now gombra kattintva kezdhetjük el a hálózat monitorozását. A Demo változatban csak 30 percig figyelhetjük a hálózatot, és nem jelenik meg minden csomópontra vonatkozó információ. A figyelni kívánt csomagokra szűrőket (filter) definiálhatunk, így a számunkra érdektelen csomagok nem zavarnak. A begyűjtött adatokat a protokollok, a fizikai, és a logikai címek alapján képes csoportosítani, így nemcsak a teljes hálózatról, hanem annak egy részéről, vagy akár egyetlen csomópontról is képes információt szolgáltatni. A Capsa segítségével megjeleníthető, hogy az egyes csomópontok mennyi csomagot küldtek, és fogadtak, és hogy mely más csomópontokkal kommunikáltak, mely protokollokat használták, és milyen mértékben (lásd 16. ábra).



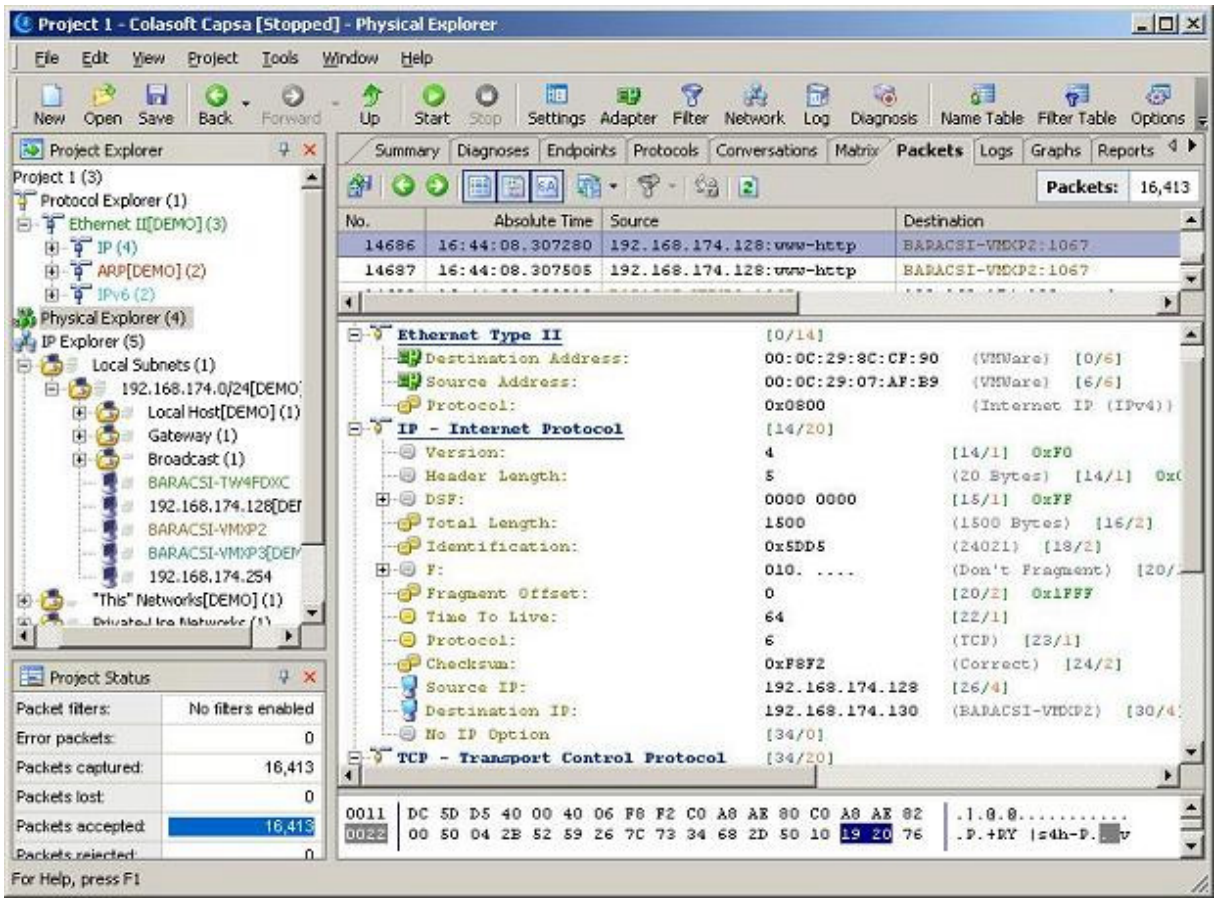
16. ábra A használt protokollok

Képes megjeleníteni a csomagok méret szerinti gyakoriságát (a 17. ábrán látható módon), az üzenetszórásos (broadcast) üzenetek, vagy az elveszett csomagok számát. Segítségével megtekinthetők a hálózati forgalomban bekövetkező hibák, illetve események is, így könnyebben felderíthetők a hálózat problémái. Segítségével az összes elkapott csomag tartalma megtekinthető, így részletesebben elemezhető (lásd 18. ábra). A csomagokat meg tudja jeleníteni hexadecimális, illetve ASCII, vagy EBCDIC formában, továbbá a csomag visszafejtésével jól látható a csomag szerkezete, illetve a beágyazás folyamata.



17. ábra A csomagok méret szerinti eloszlása

Képes a HTTP kéréseket, az SMTP üzeneteket, az FTP forgalmat, és a DNS kéréseket, illetve válaszokat logolni, így a hálózati adminisztrátor megtekintheti, hogy a felhasználók mely webhelyeket látogatták, kikkel levelezteek, vagy milyen fájlokat küldtek, illetve fogadtak FTP-n keresztül. Természetesen képes mindezen információkról jól átlátható jelentéseket (report) készíteni. Lehetőséget biztosít a tíz leggyakrabban használt protokoll, a tíz legnagyobb forgalmat generált csomópont IP-címének, vagy azon távoli eszközök IP-címeinek megjelenítésére, melyekkel a legnagyobb mértékű volt a kommunikáció.



18. ábra Egy elkapott csomag felépítése

A Colasoft Capsa a következő webhelyről tölthető le:

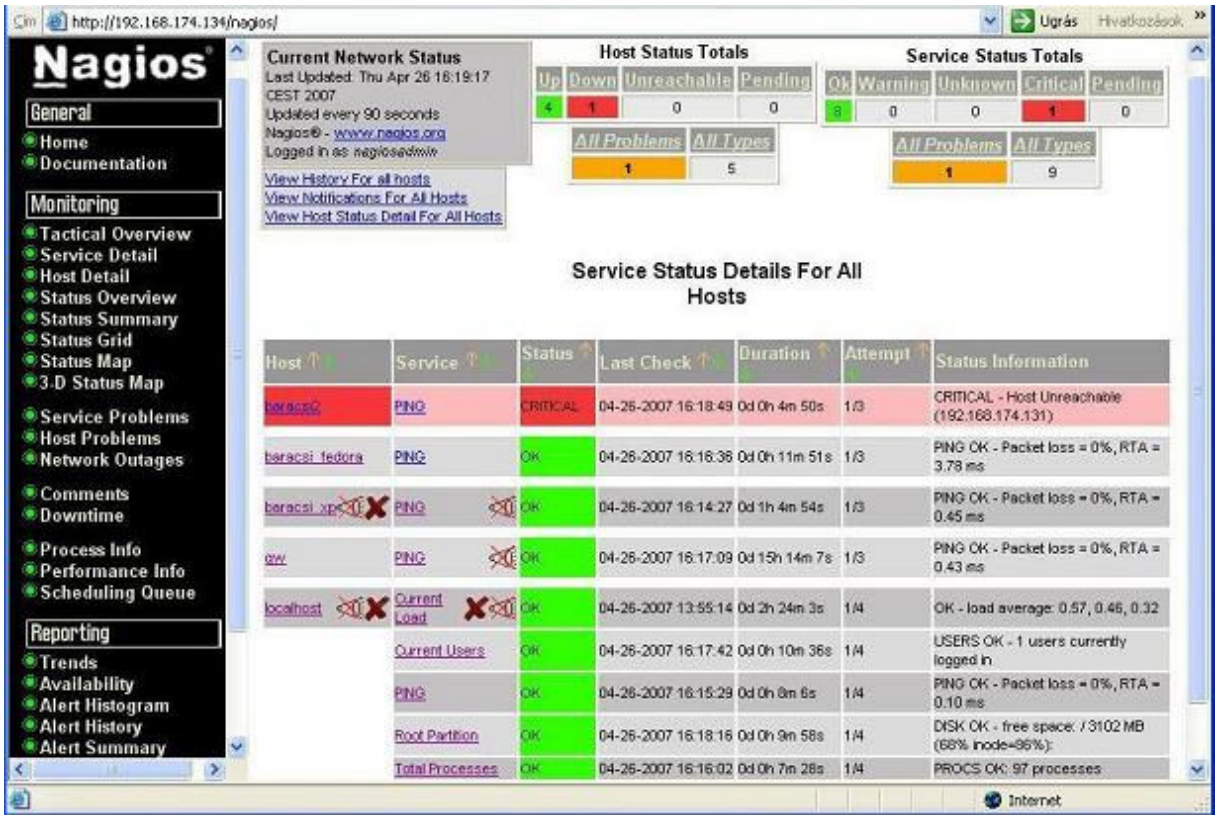
http://www.colasoft.com/download/products.php

A Colasoft Capsa legfontosabb funkciói, és tulajdonságai összefoglalva:

- Hálózati forgalom, és kommunikáció figyelése, mérése, csomagok elkapása, megjelenítése.
- A hálózati forgalom hibáinak logolása.
- HTTP kérések, SMTP üzenetek, FTP forgalom, és DNS kérések, illetve válaszok logolása

5. 5. Nagios

A Nagios az egyik legnépszerűbb nyílt forráskódú hálózat felügyeleti rendszer. A Nagios képes hálózati eszközök (szerverek, munkaállomások, forgalomirányítók, nyomtatók, stb.), és szolgáltatások figyelésére, és riasztás küldésére a felügyeleti személyeknek, ha valamely szolgáltatás nem megfelelően működik. A Nagios legfontosabb feladata a hálózati szolgáltatások (HTTP, SMTP, POP3, stb.), és a kiszolgálók erőforrásainak (processzor-, lemezterület) felügyelete. Futtatásához Linux vagy valamilyen UNIX-változat, és egy C fordító szükséges. A Nagios biztosít egy webes felületet is, melynek CGI a neve, ennek használatához szükség van egy webkiszolgáló alkalmazásra (ajánlott az Apache) is. A 19. ábrán látható, a Nagios webes felülete, és az, hogy hogyan jeleníti meg a felügyelt szolgáltatásokat.



19. ábra A CGI, és a felügyelt szolgáltatások

A Nagios telepítése a Windows-os alkalmazásokénál valamivel bonyolultabb. A forrás letölthető a http://www.nagios.org/download címről, és a telepítésről rengeteg további információ található a dokumentációban, illetve a következő helyeken: [1][40]. Sikeres telepítés után a Nagios webes felületét a következőképpen érhetjük el: http://localhost/nagios -

a Nagios-t futtató gépen, vagy http://gép_név/nagios, illetve http://IP-cím/nagios. Ekkor a telepítésnél megadott felhasználói név és jelszó megadása után megjelenik a webes felület. Ahhoz, hogy ténylegesen is használhassuk a Nagios-t, a konfigurációs fájlokban kell megadni, hogy mely eszközöket, és szolgáltatásokat felügyelje, és hogy hiba esetén kit értesítsen. Fontos megjegyezni, hogy a konfiguráció módosítása esetén újra kell indítani a Nagios-t, a következő paranccsal: /etc/init.d/nagios reload. Az összes konfigurációs állomány a /usr/local/nagios/etc könyvtárban található. A fő konfigurációs állomány a nagios.cfg, ebben adhatjuk meg a Nagios működésének főbb paramétereit. Itt lehet megadni, például a naplófájl, és az objektum definíciós fájlok elérési útját, vagy azt, hogy a Nagios mely felhasználó nevében fusson. Ezeknek az alakja a következőképpen néz ki:

- log_file=<file_name>
- cfg_file=<file_name>
- nagios_user=<username/UID>

Az objektum definíciós állományok tartalmazzák azokat az információkat, melyek alapján a Nagios tudja, hogy mit, és hogyan kell megfigyelnie. Ezekben az állományok lényegében a következőket írják le: a szolgáltatásokat, a hosztokat, az értesítendő személyzetet, ezek csoportjait, a definiált parancsokat, és az időtartamokat. Az időtartamoknak az acélja, hogy így megadhatjuk, hogy mikor figyeljen szolgáltatásokat a Nagios, és mikor ne, továbbá be lehet állítani időzített leállásokat is, így nem fog a rendszer, riasztást küldeni, amikor egy szolgáltatást szándékosan állítunk le. Hogy a Nagios-t a hálózat felügyeletére használhassuk, elegendő, ezeket az objektumokat létrehozni. De ahhoz, hogy egy igazán jól működő rendszert kapjunk, ahhoz rengeteg beállítást kell ismerni, és még több tapasztalatra van szükség. Most csak a legszükségesebb objektumok definícióját fogom ismertetni. Minden objektum definíciójában szerepelnek kötelező direktívák (ezeket félkövér betűstílussal fogom jelölni), és van, amelyeknél léteznek opcionális direktívák is.

Időtartamok definiálására példa:

define timeperiod{

timeperiod_name	***munkaido***
alias	***Munka ido***
monday	08:00-17:00
tuesday	08:00-17:00
wednesday	08:00-17:00

thursday 08:00-17:00

friday 08:00-16:00

}

Itt a hét napjai opcionálisak, és lehetőség van egy napra több időintervallum megadására is, ekkor vesszővel kell elválasztani őket.

Az értesítendő személyzet (contact), és csoport (contactgroup) definiálása:

define contact{

contact_name	***contact_name***
alias	***alias***
contactgroups	*contactgroup_names*
host_notification_period	***timeperiod_name***
service_notification_period	***timeperiod_name***
host_notification_options	**[d,u,r,f,n]**
service_notification_options	**[w,u,c,r,f,n]**
host_notification_commands	*command_name*
service_notification_commands	*command_name*
email	*email_address*
pager	*pager_number or pager_email_gateway*
address*x*	*additional_contact_address*

}

A notification_period direktíváknak már létező időtartamot kell megadni, a notification_options esetén pedig azt kell megadni, milyen esetekben küldjön értesítést ennek a személynek. Az itt szereplő betűk állapotokat jelölnek, mégpedig a következőket: d = down (kikapcsolt), u = unreachable/unknown (elérhetetlen hoszt esetén, szolgáltatás esetén ismeretlen), r = recoveries (újra válaszol), f = flapping (a hoszt vagy a szolgáltatás folyamatosan leáll, és újraindul), n = none (ismeretlen), w = warning (már átlépte a figyelmeztetés határát, de még nem kritikus érték), c = critical (kritikus, a szolgáltatás nem működik). Az addressx (az x helyébe egy számot kell írni) direktíva szolgál arra, hogyha több elérhetőséget szeretnénk megadni. A Nagios nem csak e-mail-ben, hanem SMS-ben, vagy ICQ-n, illetve MSN-en is képes riasztást küldeni. A hosztok, és szolgáltatások definíciójánál nem egy-egy konkrét személyt tudunk megadni, hanem az értesítendő személyeknek egy csoportját (contactgroups). Ez azért célszerű, mert, ha változás történik a személyzetben, nem

szükséges minden szolgáltatás esetén módosítani, hanem elég a csoport tagjait aktualizálni. Egy ilyen csoport megadása a következőképpen történik:

define contactgroup{

contactgroup_name ***contactgroup_name***

alias ***alias***

members ***members***

}

Egy csomópont (host) definiálása:

A hosztok viszonylag sok direktívával rendelkeznek, így csak a kötelezőeket, és néhány fontosabbat ismertetek.

define host{

host_name	***host_name***
alias	***alias***
address	***address***
parents	*host_names*
hostgroups	*hostgroup_names*
check_command	*command_name*
max_check_attempts	**#**
check_period	***timeperiod_name***
event_handler	*command_name*
event_handler_enabled	[0/1]
flap_detection_enabled	[0/1]
contact_groups	***contact_groups***
notification_interval	**#**
notification_period	***timeperiod_name***
notification_options	**[d,u,r,f]**
notifications_enabled	[0/1]

}

Ezen paraméterek jelentése, illetve funkciója a következő:

- Address: a csomópont IP-címe
- Parents: segítségével a hosztok hierarchiáját adhatjuk meg, így a hálózati térképen jobban látszik az eszközök kapcsolata. További jelentősége, hogyha egy csomópont

nem válaszol, akkor a Nagios először ellenőrzi, hogy a hozzá vezető úton a csomópontok elérhetőek-e, és ha kiderül, hogy már a szülője sem elérhető, akkor az adott hosztot nem tekinti hibásnak.

- Hostgroups: a hosztokat is csoportokba sorolhatjuk, hasonlóan az értesítendő személyekhez.
- Check_command: ezzel a paranccsal ellenőrizhetjük a hosztot. Értéke alapértelmezésben check-host-alive, amely a ping-nek felel meg.
- Max_check_attempts: probléma esetén ennyi alkalommal próbálja a Nagios lefuttatni az előző parancsot, mielőtt riasztást küldene.
- Check_period: milyen időközönként próbálja végrehajtani a parancsot.
- Event_handler: egy eseménykezelő megadását teszi lehetővé, ha megadunk ilyet hiba esetén először ez fog lefutni, és csak ez után kapunk riasztást a hibáról, vagy arról hogy a hiba már el is lett hárítva.
- Event_handler_enabled: értéke 0 vagy 1 lehet, attól függően, hogy engedélyezzük vagy sem az eseménykezelőt.
- Flap_detection_enabled: ha egy hoszt folyamatosan leáll, és aztán újraindul, azt a Nagios érzékeli, és nem küld folyamatosan riasztásokat.
- Contact_groups: az értesítendő személyek csoportját kell megadni.
- Notification_interval: azt adja meg, hogy hibás működés esetén milyen gyakran küldjön újabb riasztást. Ha 0-t adunk meg nem küld további riasztást.
- Notification_period: meg kell adni, hogy mely időszakokban szükséges a csomópontot figyelni. Megadásánál a már definiált időtartamok használhatók.
- Notification_options: mely állapotokról kérünk jelentést.
- Notifications_enabled: megadható, hogy kérünk-e jelentéseket, vagy sem.

A 20. ábrán látható, hogyan jelennek meg a felügyelt hosztok, és azok állapota.

Host	Status	Last Check	Duration	Status Information
baracsi2	DOWN	04-26-2007 16:16:03	0d 0h 1m 49s	CRITICAL - Host Unreachable (192.168.174.131)
baracsi_fedora	UP	04-26-2007 16:07:26	0d 0h 10m 29s	(Host assumed to be up)
baracsi_xp	UP	04-26-2007 16:16:06	0d 1h 3m 32s	(Host assumed to be up)
gw	UP	04-26-2007 16:16:06	0d 15h 12m 45s	PING OK - Packet loss = 0%, RTA = 0.27 ms
localhost	UP	04-26-2007 16:17:08	0d 2h 22m 41s	(Host assumed to be up)

20. ábra A hosztok, és azok állapota

Egy szolgáltatás (service) definiálása:

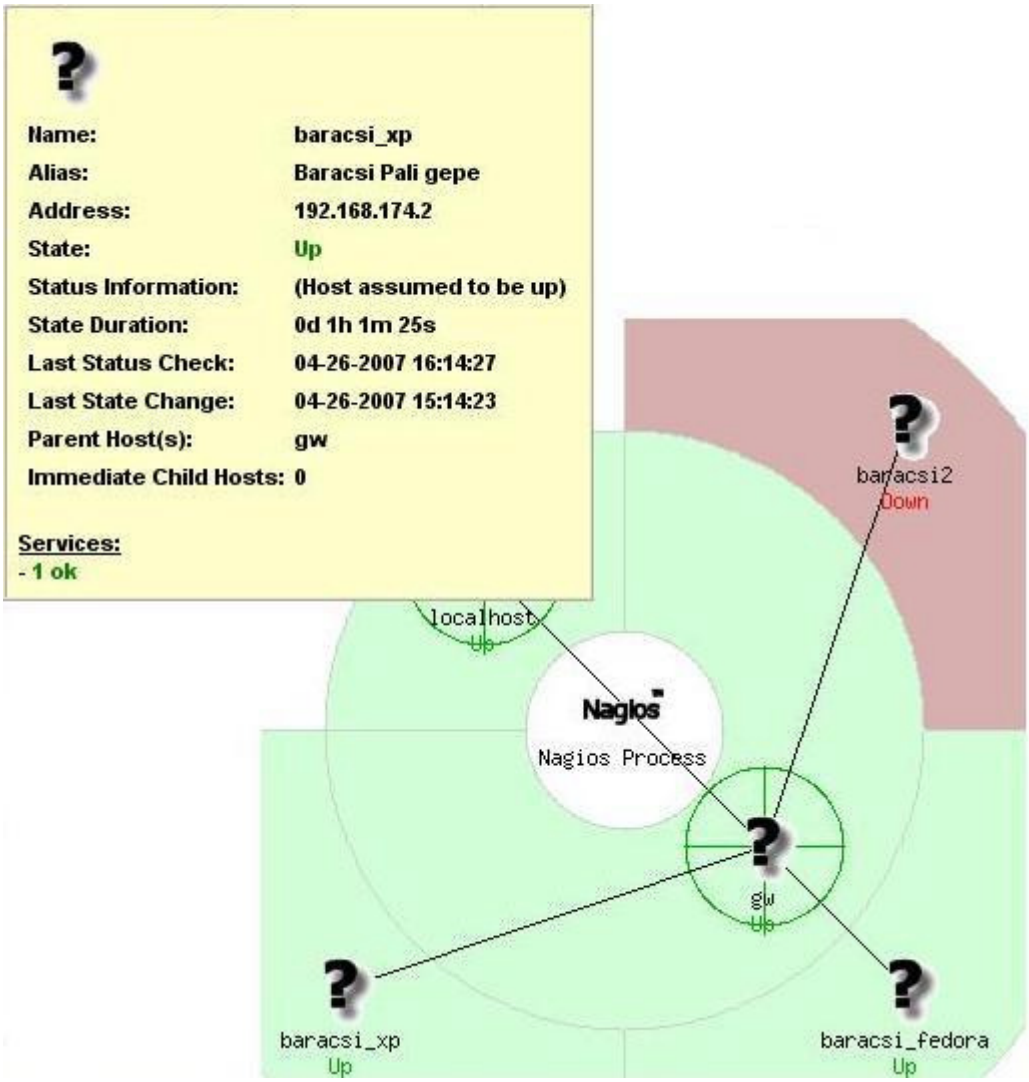
A hosztokhoz hasonlóan a szolgáltatások is sok direktívával rendelkeznek, ezért itt is csak a kötelezőket és a fontosabbakat mutatom be. Ezek jelentése megegyezik a hosztok esetén tárgyalt direktívák jelentésével. Host_name-nek annak a gépnek a nevét kell megadni, amelyiken a szolgáltatás fut.

define service{

host_name	***host_name***
service_description	***service_description***
servicegroups	servicegroup_names
check_command	***command_name***
max_check_attempts	**#**
normal_check_interval	**#**
retry_check_interval	**#**
check_period	***timeperiod_name***
event_handler	*command_name*
event_handler_enabled	[0/1]
flap_detection_enabled	[0/1]
notification_interval	**#**
notification_period	***timeperiod_name***
notification_options	**[w,u,c,r,f]**
notifications_enabled	[0/1]
contact_groups	***contact_groups***

}

Miután a felügyelni kívánt objektumokat felvettük, és újraindítottuk a Nagios-t, a webes felületen látnunk kell a hosztokat, és a szolgáltatásokat. A Nagios képes térképet (Status map) is rajzolni, melyet a hosztok szerinti hierarchia szerint határoz meg, ez a 20. ábrán látható.



20. ábra A Nagios térképe

A Nagios különféle lehetőségeket biztosít, hogy a hálózat és a szolgáltatások felügyelete hatékonyabb legyen. Például törekszik a hálózati forgalom legegyenletesebb elosztására, ezt úgy teszi, hogy a felügyelt eszközöktől nem adott időközönként egyszerre kérdezi le a szükséges információkat, hanem egyenletesen elosztva azt. Meg lehet adni, hogy mielőtt értesítést küldene a hibáról, hányszor, és milyen gyakran próbálja azt ellenőrizni. Egy eseménykezelő megadásával, akár a Nagios automatikusan megpróbálhatja elhárítani a hibát, például a szolgáltatás újraindításával.

A Nagios a következő webhelyről tölthető le:

http://www.nagios.org/download

A Nagios legfontosabb funkciói, és tulajdonságai összefoglalva:

- Eszközök, és szolgáltatások működésének figyelése.

- Hibás működés esetén riasztás küldése.
- Események kezelése, definiált parancsok segítségével.
- Megadható a felügyelt hálózati csomópontok hierarchiája.
- Hálózati térkép rajzolása.
- Plug-in-ek segítségével képes forgalomirányítók, kapcsolók, hálózati nyomtatók SNMP információinak megjelenítésére.
- Saját plug-in-ek írásával további lehetőségeket biztosít.
- Lehetővé teszi a működés, és a webes felület személyre szabását.
- Egy igazán jó konfiguráció beállításához rengeteg tapasztalat szükséges.
- Széles körben elterjedt, nyílt forráskódú alkalmazás.
- Rengeteg jól használható dokumentáció -még könyv is (lásd [1])- jelent meg hozzá.

6. Összefoglalás

Dolgozatomban a fellelhető hazai és külföldi irodalom felhasználásával ismertettem a hálózati menedzsment céljait, és hogy e célok megvalósítása érdekében milyen feladatokat lát el, illetve a leginkább elterjedt Simple Network Management Protocol-t, amely protokoll jelenleg a hálózati menedzsment de-facto szabványa. Kifejtésre került az SNMP működése, és a menedzsment információk szabványos kezelését lehetővé tevő Management Information Base felépítése. Munkám során támaszkodtam az Interneten található információkra, és a témához kötődő RFC dokumentumokra is. Továbbá bemutattam a jelenleg fellelhető számtalan freeware, és shareware alkalmazás közül, néhány legfontosabb funkcióit.

A dolgozatban szereplő eszközök egyike sem képes önállóan ellátni a hálózati menedzsment összes funkcióját, csak bizonyos feladatok elvégzésére használhatók. Az öt szoftver (SolarWinds Engineers Edition Toolset, Nagios, Alchemy Network Inventory, Network View, és Colasoft Capsa) funkciójukban eltérnek, de mindegyik segítséget nyújthat a hálózatok üzemeltetésénél. Az öt alkalmazás közül a Nagios az egyetlen, amelyik teljesen ingyenes, és mivel igen jól használható akár nagy méretű hálózatok felügyeletére is, nem véletlenül az egyik legszélesebb körben elterjedt eszköz. A másik négy alkalmazás Windows környezetben működik, használatukért fizetni kell a fejlesztőnek, a dolgozatban csupán az ingyenesen kipróbálható változatokat mutattam be, amelyek legtöbbje csak korlátozott funkcionalitással működik. A négy szoftver képességeiben teljesen eltér egymástól. Az Alchemy Network Inventory a hálózat számítógépeinek konfigurációjáról ad részletes információkat, a Network View az eszközök felderítését és felügyeletét végzi, kiegészülve bizonyos információk megjelenítésével, a Colasoft Capsa a hálózati forgalom megfigyelését teszi lehetővé, a SolarWinds Engineers Edition Toolset pedig, többféle feladat elvégzésére használható eszközkészlet.

Látható, hogy a Windows alkalmazások használata sokkal egyszerűbb a Nagios-énál, viszont kevésbé rugalmasak, nem teszik lehetővé működésük megváltoztatását, ezzel kényelmesebbé, és használhatóbbá tételét.

Belátható, hogy egy hálózat teljes körű felügyeletéhez több eszköz együttes használatára lesz szükség. Az általam bemutatott eszközök sem árukban, sem képességeikben nem veszik fel a versenyt a piacvezető cégek integrált felügyeleti rendszereivel, amelyek a nagyméretű hálózattal rendelkező vállalatoknak jelentenek megoldást.

7. Irodalomjegyzék

Könyvek:

[1] **Barth, Wolfgang:** Nagios: System and Network Monitoring. San Francisco: No Starch Press, 2006.

[2] **Clemm, Alexander:** Network Management Fundamentals. Indianapolis: Cisco Press, 2006.

[3] **Doherty, Jim; Anderson, Neil:** Otthoni hálózatok. Budapest: Panem, 2007.

[4] **Feit, Sidnie M.:** SNMP: A Guide to Network Management. New York: McGraw-Hill, 1993.

[5] **McMahon, Richard A.:** PC hálózatok a gyakorlatban. Budapest: Panem, 2004.

[6] **Simoneau, Paul:** SNMP Network Management. New York: McGraw-Hill, 1997.

[7] **Stallings, William:** SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. Boston, Mass. [etc.]: Addison-Wesley, 2000.

[8] **Steinberg, Louis A.:** Troubleshooting SNMP; Analyzing MIBs. New York: McGraw-Hill, 2000.

[9] **Subramanian, Mani:** Network Management: Principles and Practice. Boston, Mass.: Addison Wesley, 1999.

[10] **Tanenbaum, Andrew S.:** Számítógép-hálózatok. Budapest: Panem, 2004.

[11] **Terplán Kornél:** Lokális hálozatok menedzselése**.** Budapest: Panem; Maidenhead: McGraw-Hill, 1995.

[12] **Thomas, Tom:** Hálózati biztonság. Budapest: Panem, 2005.

Hálózati forrás (cikkek):

[13] **Bacun, Oliver**: Netzwerkmanagement & Internetworking. 2003. 01. 29. In http://www.it-academy.cc/article/649/Netzwerkmanagement+&+Internetworking.html Felhasználás időpontja: 2007-04-14

[14] **Bednarz, Ann; Dubie, Denise***:* Project management software can curb IT inefficiencies. 2006. 11. 15. In http://www.networkworld.com/news/2006/111506-project-management-software.html Felhasználás időpontja: 2006-11-30

[15] **Cooper, Mark**: Building a Network Management System. 2005. 03. 13. In http://freshmeat.net/articles/view/1553/
Felhasználás időpontja: 2007-04-14

[16] **Girnt József**: A Microsoft System Center az élre tör. 2006. 11. 27. In http://www.napi.hu/default.asp?cCenter=article.asp&nID=314171
Felhasználás időpontja: 2007-04-14

[17] **Girnt József**: Minden idők legtöbbet tudó NetWare-szervere. 2005. 04. 12. In http://www.napi.hu/default.asp?cCenter=article.asp&nID=242455
Felhasználás időpontja: 2007-04-14

[18] **Guerrero, David**: Network Management Monitoring with Linux. 1997. 06. 01. In http://www.linuxjournal.com/article/2140
Felhasználás időpontja: 2007-04-14

[19] **Harlan, Richard**: Network Management with Nagios. 2003. 07. 01. In http://www.linuxjournal.com/article/6767
Felhasználás időpontja: 2007-04-14

[20] **Koi Tamás**: Az Everest Ultimátuma. 2005. 04. 29. In http://prohardver.hu/cikkek/2005-04-29/everest_ultimatuma/
Felhasználás időpontja: 2006-12-12

[21] **L. Nagy Gábor :** A kis cégeké a magyar IT piac több, mint fele. 2006. 12. 14. In http://www.mfor.hu/cikk.php?article=32146&pat=15
Felhasználás időpontja: 2007-04-14

[22] **Morris, Stephen:** Workflow-Based Network Management. 2004. 07. 30. In http://www.informit.com/articles/article.asp?p=212398&seqNum=1&rl=1
Felhasználás időpontja: 2006-11-30

[23] **Seres Gábor:** Hálózatbiztonság a fotelből. 2005. 05. 13. In http://it.news.hu/cikkek/2005-05-13/halozatbiztonsag_fotelbol/
Felhasználás időpontja: 2006-12-12

[24] **Sós Éva:** Hálózati menedzsment rendszer frissítése a Magyar Telekomnál. 2006. 09. 29. In http://www.terminal.hu/cikk.php?article_id=100979
Felhasználás időpontja: 2006-11-30

[25] **Szilágyi Szabolcs**: Everest 4.0 - akár a Sidebaron is. 2007. 04. 10. In http://www.terminal.hu/cikk.php?article_id=104504
Felhasználás időpontja: 2007-04-14

[26] **Vörös Péter**: Nő a Network Associates ázsiai forgalma. 2001. 06. 15. In http://www.hwsw.hu/hir.php3?id=9931
Felhasználás időpontja: 2006-12-12

RFC dokumentumok (http://www.rfc-editor.org/):

[27] **Case, J. D., Fedor M., Schoffstall M.L.:** Simple Network Management Protocol (SNMP). 1990. In RFC1157.

[28] **Waldbusser, S.:** Remote Network Monitoring Management Information Base. 1995. In RFC1757.

[29] **Waldbusser, S.:** Remote Network Monitoring Management Information Base Version 2 using SMIv2. 1997. In RFC2021.

[30] **Case, J. D., McCloghrie, K.,Rose, M.:** Introduction to Community-based SNMPv2. 1996. In RFC1901.

[31] **Rose, M., McCloghrie, K.:** Structure and identification of management information for TCP/IP-based internets. 1990. In RFC1155.

[32] **Rose, M., McCloghrie, K.:** Concise MIB definitions. 1991. In RFC1212.

[33] **McCloghrie, K., Rose, M.:** Management Information Base for Network Management of TCP/IP-based internets:MIB-II. 1991. In RFC1213.

[34] **McCloghrie, K., Perkins, D., Schoenwaelder, J.:** Structure of Management Information Version 2 (SMIv2). 1999. In RFC2578.

[35] **Case, J. D., McCloghrie, K.,Rose, M.:** Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2). 1996. In RFC1906.

Egyéb hasznos információk:

[36] http://de.wikipedia.org/wiki/Simple_Network_Management_Protocol

[37] http://de.wikipedia.org/wiki/Abstract_Syntax_Notation_One

[38] http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[39] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm#wp1020546

[40] http://www.nagios-wiki.de/doku.php/nagios/doku/start

8. Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek, Dr. Almási Bélának, hogy időt szánt rám, és sok hasznos tanácsot adott munkámhoz.
Köszönettel tartozom mindazoknak, akik ötletekkel, tanácsokkal segítették munkámat.

Köszönöm