Debreceni Egyetem
Informatikai Kar
Informatikai Rendszerek és Hálózatok Tanszék

EGY MŰKÖDŐ KOMMUNIKÁCIÓS HÁLÓZAT ELEMZÉSE, TESZTELÉSE ÉS TOVÁBBFEJLESZTÉSÉNEK TERVEZÉSE

A DEBRECENI EGYETEM KOSSUTH LAJOS GYAKORLÓ GIMNÁZIUMÁNAK SZÁMÍTÓGÉP-HÁLÓZATA

Témavezető:	Külső témavezető:	Készítette:
Dr. Almási Béla	Kelemenné Nagy Anikó	Zsigmond Attila
egyetemi docens	informatikatanár	mérnök informatikus BSc
	DE K. L. Gyak. Gimn.	

Debrecen
2010

Tartalom

Köszönetet mondok Kelemenné Nagy Anikó tanárnőnek, külső konzulensemnek a dolgozat elkészítéséhez adott támogatásáért és a felmerült problémák megoldásában nyújtott segítségéért, Dr. Almási Béla egyetemi docens úrnak, témavezetőmnek szakmai javaslataiért, útmutatásaiért és lektori munkájáért, Dr. Orosz Péter egyetemi adjunktus úrnak gyakorlati tanácsaiért, valamint a Debreceni Egyetem Kossuth Lajos Gyakorló Gimnáziuma dolgozóinak türelmükért

1 Bevezetés

Ahogy a számítógép forradalmasította a munkavégzést, úgy reformálta meg a számítógép-hálózatok megjelenése az emberek közötti kommunikációt. Ma szinte minden intézményben találkozunk hálózattal: piaci vállalatoknál, közintézményekben, egyetemeken, iskolákban. Az internetnek, a hálózatok hálózatának létrejötte tovább növelte a felhasználási lehetőségeket és ezáltal az igényeket is. Míg a felhasználó számára az a meghatározó, hogy a hálózat működik-e vagy sem, a szakember számára az az érdekes, hogy miképpen, milyen paraméterekkel és mekkora hatékonysággal működik.

Infokommunikációs hálózatok szakirányos hallgatóként olyan témát kerestem, amely kidolgozásakor a gyakorlatban hasznosíthatom a megszerzett tudásomat, felhasználhatom a korszerű, piacképes minősítést adó Cisco és Hewlett-Packard egyetemi kurzusokon tanult ismereteimet is.

Egy működő hálózat elemzése összetett, ugyanakkor változatos és gyakorlatorientált feladat. Nehézségei is összetettségében rejlenek: az analízist, a méréseket és a fejlesztéseket úgy kell végezni, hogy azok a hálózat működését a lehető legkevésbé zavarják meg. A vizsgálat során az elemző betekintést nyer a hálózat felépítésébe és működésébe, ehhez azonban magas szintű hozzáférés szükséges. A hálózat kiválasztásakor ismerős helyszínt kerestem, ahol megelőlegezik azt a bizalmat, hogy megadják a megfelelő hozzáférést – ezért választottam volt középiskolámat, a Debreceni Egyetem Kossuth Lajos Gyakorló Gimnáziumát.

Témám kidolgozásakor arra törekedtem, hogy a hálózatot egységes egésznek tekintsem; a fizikai és logikai topológia elemzésével és a jellemzők meghatározásával, valamint az infrastruktúrát alkotó eszközök képességeinek és konfigurációjának vizsgálatával javaslatokat tegyek a továbbfejlesztésre és a hálózatbiztonság növelésére.

Dolgozatom első harmadában ismertetem az iskola hálózati infrastruktúráját és kialakításának előzményeit. Mivel nemrég új eszközöket helyeztek üzembe, először (a 2. fejezetben) említést teszek a korábbi, évekig használt berendezésekről. A 3. fejezet első része az infrastruktúrát jelenleg alkotó berendezésekről szól: a típusok felsorolása után az általuk támogatott szabványok és protokollok részletes elméleti összefoglalója következik.

A fejezet második részében az intézmény által használt alkalmazási rétegbeli szolgáltatásokat mutatom be. Szolgáltatásonként először annak elméleti háttere, általános célja kerül ismertetésre, majd az, hogyan valósul meg az adott szolgáltatás a vizsgált hálózaton. Ezután összefoglalom az intézmény hálózattal szemben támasztott elvárásait.

A második nagy egység – a 4. fejezet – a hálózat fizikai és logikai topológiájának részletes leírását, jellemzését foglalja magába, felmérve annak előnyeit és hátrányait. Ismertetésre kerülnek az alapvető tulajdonságok: a válaszidők, az útvonalak és a sebességek. Bemutatom az eszközök konfigurációját és az általam végzett forgalommérés legfontosabb eredményeit.

Az 5. fejezetben megvizsgálom a korszerűsítési lehetőségeket, kiemelve az anyagi befektetés nélkül megvalósítható fejlesztéseket. Ezek egy részét a szakdolgozat készítése során el is végeztem, a többi javaslatként szerepel, mindkét esetben indoklással. Egyes javaslatokhoz konfigurációrészletek, parancsok tartoznak, amelyek a dolgozat későbbi, referenciaként történő felhasználását segítik.

A felhasznált irodalomra való hivatkozásokat szögletes zárójelbe írt számok jelölik.

2 Történet, előzmények

2.1 Az infrastruktúra kialakítása

A gimnázium 2000-ben a Csengő utcára, a volt Bocskai laktanya területére költözött a Kossuth utcáról. Az épületek felújításával mintegy tízezer négyzetméteren kezdődhetett meg a tanítás. Az iskolában többek között 20 tanterem, 4 szaktanterem, 3 természettudományos előadó, 2 természettudományi labor, 2 idegen nyelvi labor, 3 kis csoportra méretezett idegen nyelvi szaktanterem, 2 számítástechnikai szaktanterem, 1 sportcsarnok és 3 edzőterem található, továbbá tanári dolgozók, szertárak és a könyvtár termei. *[9]*

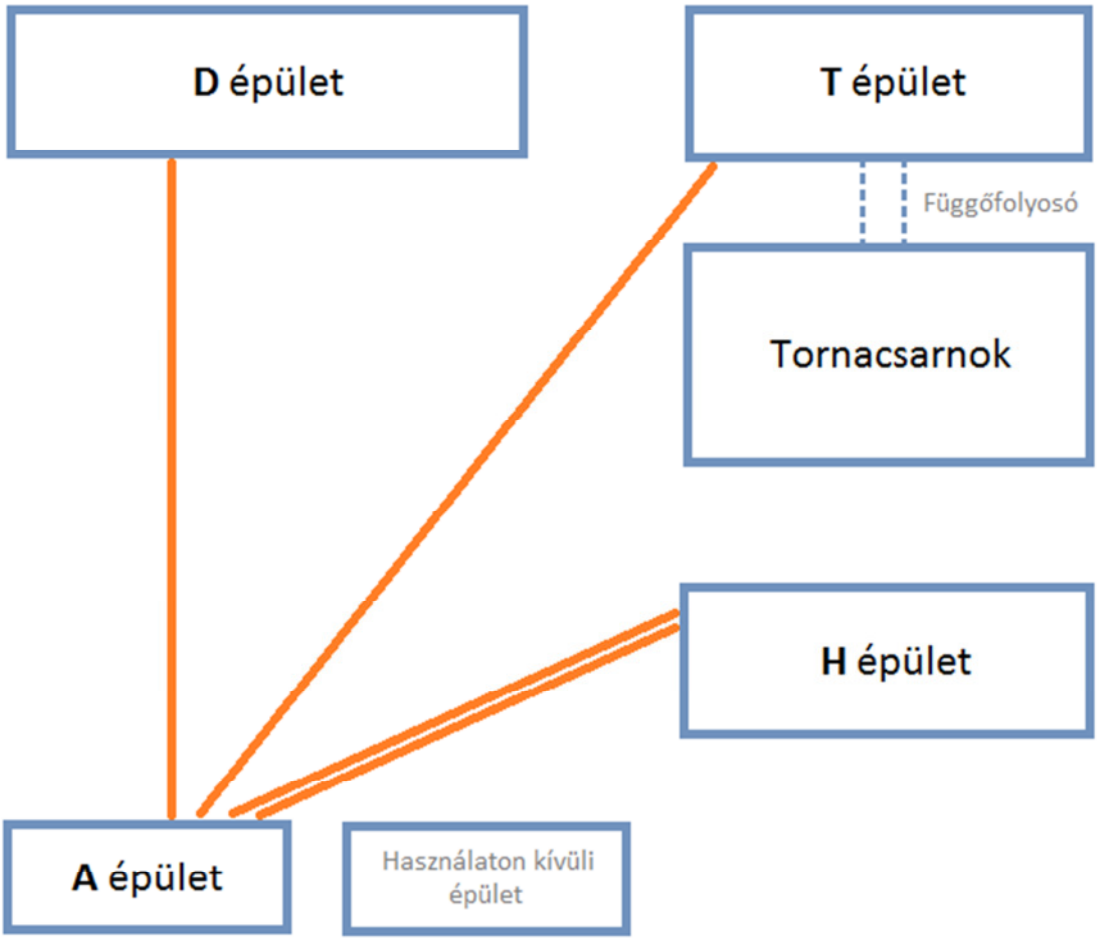
Az iskolát hat épület együttese alkotja, ezek közül az egyik egy használaton kívüli, felújításra váró épület (a leendő menza és kollégium épülete), egy másik pedig a tornacsarnok. A többi épületet mind a dolgozók mind a diákok betűkkel és nevekkel illetik, dolgozatomban ezért – az intézmény hagyományainak megfelelően és a könnyű hivatkozás végett – az igazgatóság és a porta épületét A, a természettudományi és nyelvi szaktantermeket tartalmazó főépületet D, a humán és informatikai épületet H, a testnevelő tanári szobák és öltözők épületét pedig T betűvel jelölöm.

Az igazgatási (A) épület földszintjén van a porta, a rádióstúdió, az iskolaorvosi rendelő és az iskolaszék konferenciaterme. Az első emeleten az igazgató és az igazgatóhelyettesek irodája, a titkárság és egy multimédiás tanterem (számítógép, projektor, hangrendszer) kapott helyet. A legfelső szinten a „lovagterem” található. A rack szekrényt a stúdióban helyezték el.

A testnevelési (T) épület földszintjén az öltözők és egy új tanterem (rack szekrénnyel), az emeleten pedig kondicionáló termek és tanári dolgozók vannak. Ezt az épületet függőfolyosó kapcsolja össze a tornacsarnokkal. A csarnokban gyakran bonyolítanak le városi, megyei, országos, nemzetközi sportversenyeket és más rendezvényeket.

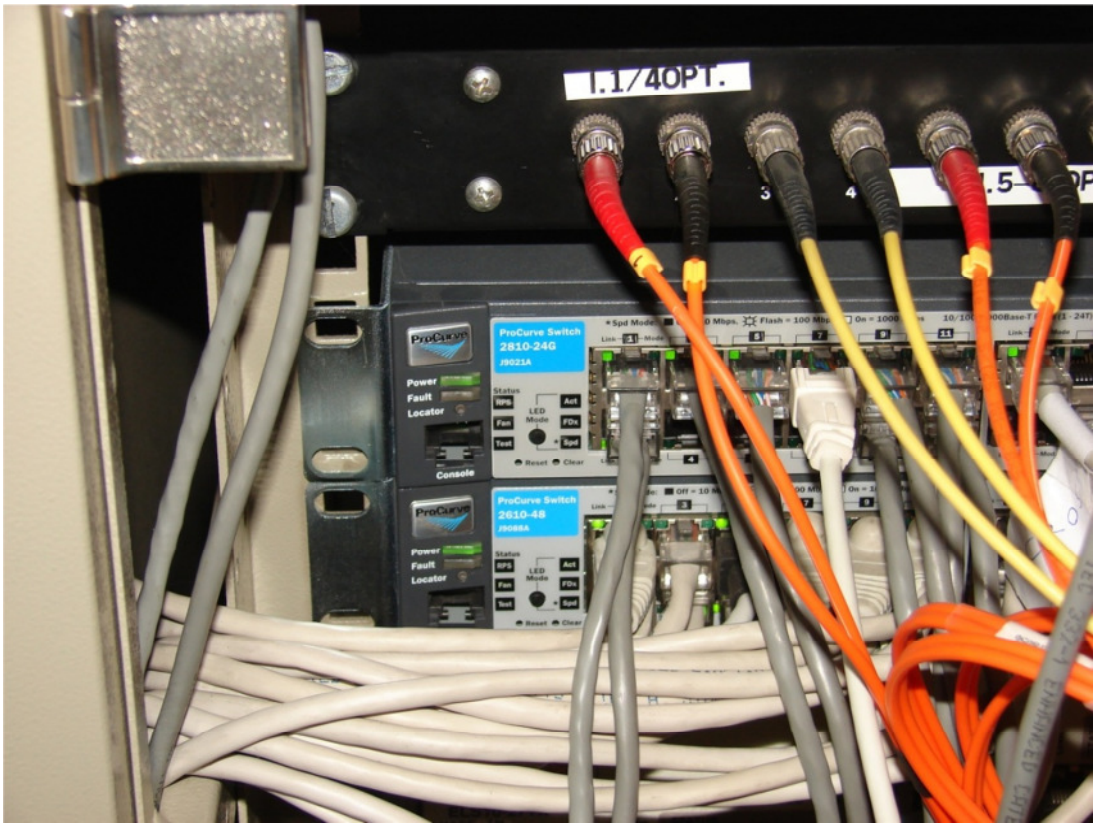
A humán (H) épületben magyar, történelem, földrajz előadótermek és tanári szobák találhatók. A könyvtár a földszinten, az informatika termek és a szerverszoba az emeleten helyezkednek el. Ebben az épületben négy rack szekrény van: egy-egy az informatika termekben és kettő a földszinten.

A D, azaz a főépület otthont ad az iskolamúzeumnak és a klubhelyiségnek (az alagsorban), a fénymásolónak, a büfének, a kémia és fizika szaktantermeknek, laboroknak, szertáraknak és tanári dolgozóknak (földszint). Mindkét emeleten általános célú tantermek és tanári szobák vannak, továbbá az első emeleten biológia előadó, a másodikon pedig idegen nyelvi szaktantermek.



A kivitelezéskor fontos szempont volt a megfelelő telefon- és számítógép-hálózat kialakítása. Ennek eredményeképpen a legtöbb helyiség – tanterem, labor, előadó, könyvtári és tanári szoba, szertár – rendelkezik egy vagy több fali RJ-11 (telefon) és RJ-45 (Ethernet) aljzattal. A számítástechnika szaktantermekbe és a könyvtár számítógéptermébe további, padlóba süllyesztett Ethernet aljzatokat és konnektorokat helyeztek, hiszen ott sokkal több hálózati végberendezés működik.

Az épületek közötti kommunikációt földalatti optikai kábelek biztosítják, amelyek az A-D, az A-T és az A-H épületek között húzódnak, utóbbi két épület között több is. Az igazgatási és a testnevelési épületben egy, a főépületben két, a humán épületben négy rack szekrény található. Minden szekrényben patch panelekbe futnak be a fali és a süllyesztett aljzatok kábelei. Az optikai kábeleket hasonlóképpen optikai patch panelekkel végződtetik, amelyekkel az épületek közötti összeköttetések akár meg is változtathatók – ahogy az a gyakorlatban történt.



2.2 A régi hálózat

Kezdetben 3Com hubok szolgáltatták a hálózat alapját. A hub fizikai rétegbeli hálózati kapcsolóelem: többportos repeater (jelismétlő), azaz egy állomás által egy adott portjára küldött jel az összes többi portján is megjelenik. A hub nem darabolja fel a hálózatot ütközési tartományokra, portjai ugyanabba az ütközési tartományba tartoznak. Ez azt jelenti, hogy a hubon egy időpillanatban egyszerre csak egy információátvitel folyhat. *[2]*

Ezeknek a huboknak nincs optikai interfészük, az épületek közötti gerinchálózatra való kapcsolódást médiakonverterekkel oldották meg.

A gimnázium internetkapcsolatát a Közháló – Sulinet biztosítja. A Sulinet végpont a humán épület földszintjén lévő rack szekrényben található, egy DSL modemet, egy Cisco 1711 NAT routert (forgalomirányítót) és egy Cisco 2950-24 típusú switchet (kapcsolót) tartalmaz. Ezek az eszközök a Sulinet felügyelete alá tartoznak, konfigurációjuk csak korlátozottan módosítható egy védett webes felületen illetve online ügyfélszolgálaton keresztül. *[4]*

A Sulinet végpont technikai dokumentációja szerint a Cisco kapcsolón alapértelmezetten 3 VLAN[1] van beállítva: publikus, privát és védett. A publikus VLAN-ba helyezhetők az internet felől elérni kívánt szerverek, a védettbe az igazgatási munkaállomások, a privátba pedig minden más végberendezés. Igény szerint választható egy másféle kiosztás: négy, úgynevezett lokális VLAN, de ezekben a Sulinet routernek nincs IP[2] címe.

Az iskola a 195.199.212.56 publikus IPv4 címtartományt használhatja 255.255.255.248 hálózati maszkkal. A publikus címeket értelemszerűen a publikus portokra kapcsolt eszközök kaphatják meg. A privát és a védett VLAN-ban a Cisco router végez címfordítást[3] és címkiosztást[4], emellett minden virtuális LAN-ban CBAC-t[5], port- és tartományszűrést valamint stateful (állapotalapú) tűzfal tevékenységeket. A védett VLAN egyedi privát IP címtartományt használ. Ebből a VLAN-ból IPsec protokoll fölött speciális sulinetes alkalmazások elérése biztosított. *[5]*

[1] Virtual Local Area Network
[2] Internet Protocol
[3] Network/Port Address Translation, NAT/PAT
[4] Dynamic Host Configuration Protocol, DHCP
[5] Context-Based Access Control

3 A jelenlegi hálózat

3.1 Eszközpark

3.1.1 Közvetítő eszközök és képességeik

A gimnáziumban 2008 őszén a hubokat új Hewlett-Packard ProCurve kapcsolókra cserélték; egy ProCurve 2810, kettő ProCurve 2626, a többi hat pedig ProCurve 2610 típusú. E kapcsolók mindegyike Layer 2-es, magasságuk 1U (rack unit). Közülük nyolcat állítottak üzembe.

A ProCurve 2810-24G eszközön huszonnégy port található, amelyek mindegyike 10/100/1000 Mbps átvitelre alkalmas. Utolsó négy portja úgynevezett „dual personality” port, azaz a hagyományos Ethernet csatlakozás helyett használható egy-egy mini-GBIC[6] modul, amellyel optikai csatlakozás (például Gigabit-SX, -LX vagy -LH) létesíthető. Ezek külön vásárolhatók meg. Az optikai modul használatakor az adott sorszámú port Ethernet interfészét szabadon kell hagyni, és fordítva. *[16]* Ez a kapcsoló a H épület földszinti rack szekrényében kapott helyet.

A ProCurve 2626 kapcsolók huszonhat porttal rendelkeznek, amelyek közül 24 Fast Ethernet (10Base-T/100Base-TX), további 2 pedig „kettős személyiségű” Gigabit Ethernet (10Base-T/100Base-TX/1000Base-T) port. *[12, 13, 14]* A számítástechnika szaktantermekben egy-egy ilyen eszköz található.

[6] Más néven Small Form-factor Pluggable, SFP

A ProCurve 2610-es sorozatból három-három darab 24 illetve 48 portos változattal rendelkezik az iskola. Ezek a portok a 2626-osokhoz hasonlóan Fast Ethernet szabványúak, de minden eszközön található még 2 db „kettős személyiségű” port. *[15]* A főépületbe egy 48 és egy 24 portos eszköz került, a testnevelési épületbe egy 24 portos, a humán épület földszintjére pedig egy 48 portos. Az igazgatási épületben eleinte egy 24 portos példány üzemelt, azonban egy villám megrongálta a tápegységét, ezért javításra vár – helyére az addig nem használt, harmadik 48 portos került.

Az adatkapcsolati rétegbeli funkciókon túl a ProCurve 2626-os és 2610-es szériájú eszközök képesek statikus IP forgalomirányításra, és lehetővé teszik hozzáférési listák[7] használatát. *[1]*

A fenti eszközök támogatják többek között a VLAN-okat (IEEE 802.1Q), a szolgáltatásminőséget[8] (IEEE 802.1p), az IEEE 802.1AB (LLDP[9]) és a 802.3ad (LACP[10]) szabványt, továbbá különböző feszítőfa-protokollokat (STP, RSTP, MST). *[11, 14, 15, 16]* Érdemes áttekinteni e szabványok és protokollok mibenlétét, működését, felhasználási területeit.

3.1.1.1 IEEE 802.1Q

Egy nagyméretű, „lapos”, nem szegmentált hálózat[11] több problémát vet fel. A broadcast üzenetek szétterjednek a teljes hálózaton jelentős adatforgalmat generálva; redundáns linkeket tartalmazó hálózatban úgynevezett „broadcast storm” alakulhat ki, mert a feladó kapcsolók a vevő kapcsolóktól egy másik interfészen visszakapják a kiküldött üzenetszórt keretet, majd kiküldik újra. A folyamat önmagát gerjeszti, ellehetetlenítve a valódi kommunikációt. *[3]*

A másik fontos probléma a biztonság. A „lapos” hálózat nem korlátozza a csomópontok számára elérhető erőforrások (szerverek, más munkaállomások, közvetítő berendezések) elérhetőségét, lehetővé teszi azok – szándékos vagy véletlen – jogosulatlan használatát. Bármely csomópont potenciálisan lehallgathatja egy másik forgalmát (különösen egy hubalapú vagy koaxiális 10Base-T hálózaton).

---

[7] Access Control List, ACL
[8] Quality of Service, QoS
[9] Link Layer Discovery Protocol
[10] Link Aggregation Control Protocol
[11] flat network

A VLAN-címkézés lehetővé teszi egy fizikai hálózat felosztását több független logikai hálózatra. A csomópontokat virtuális LAN-okba sorolhatjuk, minden VLAN külön üzenetszórási tartomány. A munkaállomások általában egy-egy VLAN-ba tartoznak, mivel többnyire nem támogatják a 802.1Q címkéket. A besorolás szinte kivétel nélkül a kapcsolókon történik, azaz a kapcsoló megfelelő portját rendeljük a VLAN-hoz (Cisco eszközön a VLAN-t a porthoz) – komoly biztonsági rést jelentene, ha ezt a feladatot a munkaállomásra bíznánk, hiszen egy támadó tetszőleges VLAN-ba helyezhetné a gépét.

A VLAN-ok kialakítása történhet földrajzi elhelyezkedés alapján, de logikai voltuk miatt a gyakorlatban ennél sokkal ésszerűbb kritériumokat fogalmazunk meg, például azonos munkakörben vagy osztályon dolgozó személyek gépét tesszük azonos VLAN-ba. A hálózaton a VLAN-ok azonosítására a tag (címke) szolgál, amely egy 4 bájtos szakasz az Ethernet keret fejrészében. A címke értékét a kapcsoló a forráscím és a hossz/típus mezők közé szúrja be. *[3]* Az „access" portokon, amelyekhez végberendezések kapcsolódnak, általában címke nélküli keretek közlekednek, míg a kapcsolók közötti portokon, ahol több VLAN forgalma továbbítódik, fontos a keretek megjelölése.

Az alábbi ábrán egy IEEE 802.1Q címke nélküli és egy címkézett Ethernet fejrész látható.

A VLAN-ok használatakor is figyelni kell azonban a lehetséges támadásokra, az egyik ilyen a kettős címkézés. Adott egy trönkport, amelynek a natív VLAN-ja a 20-as, azaz a 20-as VLAN-ba tartozó forgalmat a kapcsoló címke nélkül küldi ki a porton. Ha a támadó olyan keretet küld, amely fejrészében a 20-as és még egy másik (létező) VLAN azonosítója is szerepel, a kapcsoló a trönkporton való kiküldés előtt a keret fejrészéből kiveszi a 20-as címkét, de a másikat bent hagyja. A fogadó a másik VLAN-ba tartozó keretként érzékeli a bejövő keretet, és a megfelelő portra (vagy portokra) továbbítja. Ez a támadástípus kiküszöbölhető, ha a trönkportokon letiltjuk a natív VLAN-t, vagy olyat állítunk be, amit nem használunk. *[10]*

Bizonyos eszközök, például forgalomirányítók és szerverek (Linux) több VLAN-ba is tartozhatnak. Figyelmetlen konfiguráció esetén előfordulhat, hogy két különböző VLAN-ba

tartozó munkaállomás ezeken keresztül eléri egymást. A megoldás erre a problémára a routing tábla bejegyzéseinek felülvizsgálata és hozzáférési listák alkalmazása, továbbá a szervereken az IP forgalomirányítás kikapcsolása.

3.1.1.2 IEEE 802.1p

A hálózatok fejlődésével, növekedésével és az alkalmazások bővülésével felmerült az igény a forgalom prioritással történő ellátására, osztályozására. Különböző alkalmazások más-más kritériumokat támasztanak a kommunikációval szemben: például kis késleltetés, nagy átviteli sebesség vagy jó megbízhatóság. Az IEEE 802.1p az adatkapcsolati rétegben valósítja meg a keretek osztályozását és megjelölését egy 3 bites mező révén, amely a 802.1Q (VLAN) címkében található. Értelemszerűen csak VLAN-címkézett keretek jelölhetők meg Quality of Service értékkel. A mező értéke 0-7 között lehet, a 0 érték a jelöletlen csomagra utal (normál prioritás, „best effort" kézbesítés), de az értékek kezelésére nincs egységes implementáció.

A HP termékei 1-2 QoS érték esetén csomagokat a normálnál alacsonyabb prioritással továbbítják, a 3-7 értékűeket magasabbal. Időegység alatt a sávszélesség meghatározott százalékát allokálják a különböző osztályú kereteknek. Ezek a százalékok eszköztípusonként eltérőek, és adminisztrátor által felülbírálhatók. Ha a továbbítandó keretek száma egy adott osztályban kevés, a fennmaradó sávszélesség más osztályú keretek továbbítására használható.

A hálózati rétegben a csomagok osztályozására a Type Of Service (TOS) és a DiffServ mechanizmusok vehetők igénybe. A forgalom rangsorolása történhet a fogadó (ingress) interfész sorszáma, VLAN azonosító, TCP/UDP portszám, IP cím vagy felsőbb protokoll szerint. A különböző szempontok között precedencia van, amelyek alapján egyértelműen eldönthető a csomag prioritása. *[1]*

3.1.1.3 IEEE 802.1AB

Ez a szabvány a Link Layer Discovery Protocol (LLDP) protokollt írja le, amellyel adatkapcsolati rétegbeli eszközök (kapcsolók, forgalomirányítók, vezeték nélküli hálózati[12] hozzáférési pontok[13]) információt szolgáltathatnak magukról a szomszédos eszközöknek, és maguk is információt kaphatnak a szomszédjaikról. Az LLDP keretek élettartama általában 1,

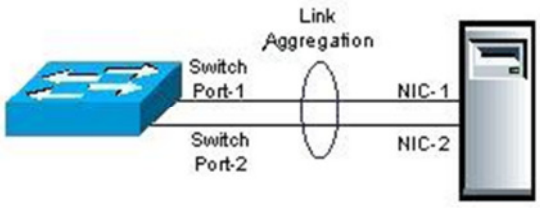
[12] Wireless Local Area Network, WLAN
[13] Access Point, AP

azaz csak a közvetlen szomszédokig jutnak el. A keretekből kinyert adatok – mint hosztnév, port sorszáma és neve – a Management Information Base-ben (MIB) tárolódnak, ahonnan lekérdezhetők például a Simple Network Management Protocol (SNMP) által.

Az LLDP nyílt protokoll, ellentétben a Cisco környezetben használt CDP-vel (Cisco Discovery Protocol). Utóbbit a ProCurve eszközök csak korlátozottan támogatják: a kereteket csak értelmezni tudják, küldeni nem. Ezek a „felderítő" protokollok a bizalomra épülnek, nem használnak hitelesítést és tartalmuk nem titkosított, így használatuk körültekintést igényel. *[1]*

3.1.1.4 IEEE 802.3ad

A Link Aggregation Protocol (röviden LACP) több fizikai kábel/port párhuzamos használatát teszi lehetővé – azaz, két hálózati eszközt, például kapcsolót több porton köthetünk össze anélkül, hogy „broadcast storm"-ot idéznénk elő. A több fizikai kapcsolatot egyetlen logikai kapcsolatként kezeljük. (A Hewlett-Packard ezt trönközésnek is nevezi.) A linkaggregációnak két célja van: a sebesség növelése és a redundancia révén magasabb rendelkezésre állás megvalósítása. Az aggregált linkeken nincs szükség feszítőfa-protokoll használatára sem – kivéve, ha két eszköz között több ilyen linket alakítunk ki.



A portok között terhelésmegosztás (load sharing) történik forrás (SA) és cél (DA) MAC[14] címpárok alapján. Egy hash függvény minden (SA, DA) rendezett párhoz (más néven beszélgetéshez) előállít egy számot, amely meghatározza, hogy az adott forgalmat mely fizikai porton kell továbbítani. Ezt a döntést a kapcsoló egymaga hozza meg, és egyirányú forgalomra vonatkozik: nincs garancia arra, hogy az azonos címek között zajló, de ellentétes irányú forgalom is ugyanazon a fizikai linken érkezik. Az algoritmus nem adaptív, azaz nem alkalmazkodik a linkek terheltségéhez. Belátható, hogy minél több különböző beszélgetés történik egy aggregált linken, annál nagyobb a valószínűsége annak, hogy a beszélgetések

[14] Media Access Control

számának eloszlása egyenletesebb lesz a fizikai interfészeken, ebből azonban nem következik az adatforgalom egyenletesebb eloszlása. A beszélgetésekhez kijelölt interfészek egy táblában tárolódnak. A döntés végleges egészen addig, amíg a kijelölt link meg nem szakad vagy a beszélgetés el nem évül (legalább 5 percig nincs adatforgalom).

A ProCurve eszközökön kétféle trönközés valósítható meg: HP és LACP. A HP megoldása statikus és nem használ protokollt. Az LACP protokoll viszont képes mind statikusan mind dinamikusan kialakítani a trönköt. A dinamikus módszer lényege, hogy az egyik eszközt aktív módra állítjuk, a passzív eszköz pedig automatikusan felismeri a trönköt, ha két vagy több interfészén megkapja az aktív eszköz BPDU-it[15] azonos fizikai forráscímről. A statikus módszer előnye, hogy megjelenik a kapcsoló konfigurációs állományában, és a trönk mint logikai interfész tulajdonságai (például az átviteli sebesség) finomhangolhatók. Dinamikus LACP esetén erre nincs lehetőségünk. Az LACP szabványt néhány szerver operációs rendszer, például a Linux is támogatja. *[1]*

3.1.1.5 IEEE 802.1D

A különböző feszítőfa-protokollok közül ebben a szabványban először a hagyományos Spanning Tree Protocol (STP) jelent meg. Megjegyzendő, hogy a szabvány nemcsak ezt tartalmazza, hanem a MAC bridge-ek működésére vonatkozó további követelményeket is.

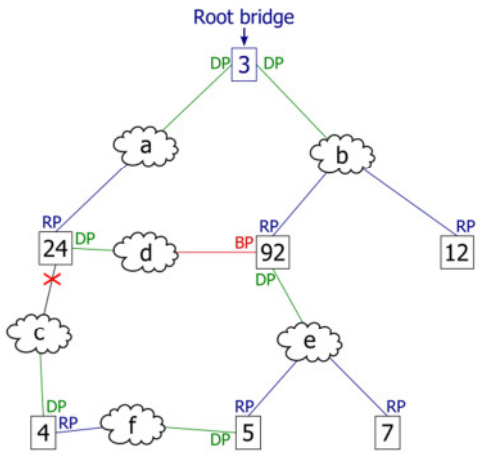
Ha egy L2-es hálózatban redundáns linkeket használunk, „broadcast storm” alakulhat ki, mivel a kapcsoló egy adott portján kapott szórt üzenetet (broadcast) minden más portján továbbít. Így a küldő kapcsolótól kapott szórt keretet a fogadó kapcsoló a redundáns linkeken visszaküldi a feladónak, az pedig ismét tovább. Ez a jelenség amellett, hogy jelentős terhelést idéz elő, meg is béníthatja a hálózatot vagy egy részét. *[3]*

Az STP adatkapcsolati rétegbeli protokoll, amely hurokmentes redundáns L2 LAN topológia kialakítására alkalmas. A hurokmentességet úgy valósítja meg, hogy feszítőfát alakít ki a hálózati csomópontok között, és letiltja azokat a linkeket, amelyek nem részei a fának. A hálózati csomópontok egy-egy gráf csúcsainak, a csomópontok közötti linkek pedig a gráf éleinek tekinthetők. A gráf feszítőfája olyan fa, amelynek élei a gráf élei, a gráf összes csúcsát tartalmazza, és kör- és hurokmentes, azaz bármely két csúcsát pontosan egy út köti össze.

[15] Bridge Protocol Data Unit

A protokoll először kiválasztja a root bridge-et. A választás a Bridge ID alapján történik, amely két számból áll: a prioritásból és MAC címből. A legkisebb prioritású kapcsoló lesz a root bridge, döntetlen esetén pedig a kisebb MAC című. A prioritást az adminisztrátor átállíthatja az alapértékről (32768), ha pl. egy kapcsolót ki szeretne nevezni root bridge-nek. Ezután minden kapcsoló meghatározza a root bridge felé vezető legkisebb költségű utat. Ehhez a többi kapcsolótól kapott BPDU-kat és saját interfészeinek adatait (pl. átviteli sebesség, sorszám) használja fel. A kiválasztott interfész lesz az adott kapcsoló root portja (RP), amely forwarding (továbbító) állapotba kerül.

A többi port állapotát könnyen meghatározhatjuk, ha a kapcsolók közötti pont-pont linkeket egy-egy hálózati szegmensnek fogjuk fel. Minden szegmenshez választunk egy designated bridge-et (a kisebb Bridge ID alapján), amelyen keresztül a szegmens kommunikál a többi szegmenssel. A designated bridge adott szegmensbe tartozó portja lesz az úgynevezett designated port (DP), a link másik vége, azaz a másik kapcsoló adott szegmensbe tartozó portja pedig a blocked port (BP). A designated portok továbbító állapotba kerülnek, a blokkolt portokon pedig csak BPDU-k haladhatnak át. A root bridge minden portja designated port (DP). *[1, 3]*



Az algoritmus minden alkalommal újra lefut, ha a hálózati topológiában változás történik – például, ha egy kapcsoló vagy link meghibásodik. Az IEEE 802.1D szabvány mai változatában a Spanning Tree protokollt a Rapid Spanning Tree váltotta fel.

3.1.1.6 IEEE 802.1w

Mivel a feszítőfa kiszámítása időigényes, felmerült az igény egy gyorsabb feszítőfa-protokollra. A Rapid Spanning Tree Protocol (RSTP) lényege, hogy az „access”[16] portok, amelyekre végberendezések kapcsolódnak, azonnal továbbító állapotba kerülnek. Ez a redundancia szempontjából nem probléma, a hagyományos STP esetén viszont gondot okozott, hogy akár 0,5-1 perc is eltelt a port továbbító állapotba kerüléséig: egy DHCP kérés esetén például időtúllépéshez vezetett. A switch-switch portokon a feszítőfa kiszámítása a hagyományos módon történik. *[1]*

Az RSTP használatakor az eszközön ki kell jelölni az „access” portokat. Ez a protokoll visszafelé kompatibilis a hagyományos Spanning Tree protokollal. Mind az STP, mind az RTSP egy LAN hálózaton belül működik, legyen az valós vagy virtuális (VLAN). Hátrányuk, hogy a redundáns linkeket nem használják ki.

3.1.1.7 IEEE 802.1s

A VLAN-ok megjelenésével szükségessé vált több feszítőfa kialakítására a kapcsolók között. Az STP és RSTP protokollok adatcsomagjai minden esetben VLAN jelölés nélkül továbbítódnak, ezért ezek a protokollok szerencsétlen esetben elszigetelhetik egymástól az azonos VLAN-ba tartozó berendezéseket. Ez kiküszöbölhető akkor, ha az összes redundáns linket hozzárendeljük az összes VLAN-hoz. *[3]*

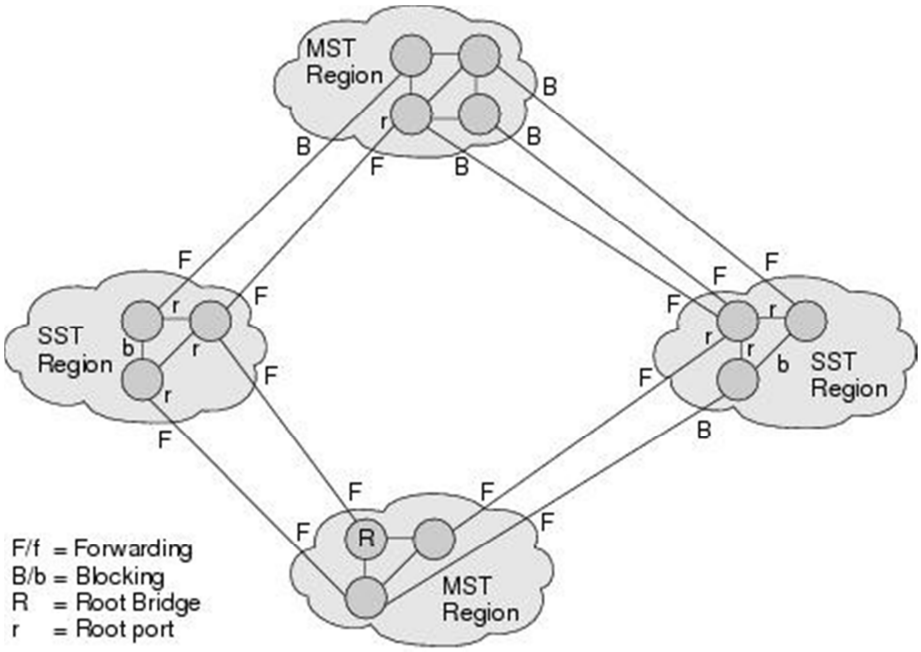
Jobb megoldás a Multiple Spanning Tree (MST), amelynek segítségével a VLAN-okat csoportokba rendezhetjük. Egy csoporthoz egyetlen MST példány tartozik, a kapcsoló pedig minden példányhoz egy-egy feszítőfát számol. *[1]* Ez azt jelenti, hogy a kapcsolók prioritásai MST-példányonként eltérőek lehetnek.

Alapesetben egyetlen MST-példány létezik, az Internal Spanning Tree (IST). Ebbe tartozik a kapcsolón definiált összes VLAN. Ha egy új MST-példányt hozunk létre, a kiválasztott VLAN-ok az IST-ből az adott példányba átkerülnek. Az alapértelmezett 1-es VLAN viszont mindig az IST-ben marad, így hibás MST-konfiguráció esetén is biztosított a kapcsoló elérése a VLAN 1-ből.

[16] Cisco PortFast, a ProCurve terminológiában „edge”

Az azonos VLAN-MST hozzárendeléssel, azonos konfigurációnévvel és revíziószámmal rendelkező kapcsolók MST régiót alkotnak. Minden eszköz csak egy régióba tartozhat. A kapcsoló egy „message digest” értéket állít elő a VLAN-MST asszociációs táblájából, és azt kiküldi a BPDU-ban. Ha egy eszköz egy adott portján a sajátjától eltérő „message digest” értéket kap, az interfészt a régiók közötti határnak tekinti.

Az MSTP együttműködik az STP és az RSTP protokollokkal az IST révén. Egy MST régió egy virtuális bridge-nek látszik az STP/RSTP[17] számára. Az MST és SST régiók mint virtuális bridge-ek egy fát alkotnak, a közös feszítőfát[18]. *[1]*



Cisco hálózati eszközökön az MST-hez hasonló a Per-VLAN Spanning Tree Protocol (PVST, PVST+) és ennek továbbfejlesztett változata, a Rapid PVST, amely ötvözi a PVST és az RSTP tulajdonságait. *[3]* Ezek minden VLAN-hoz külön interfészköltségeket és feszítőfát számolnak, amely sok VLAN esetén teljesítményigényes folyamat. Ráadásul zárt protokollok, más gyártók eszközei nem vagy csak korlátozottan támogatják. Az MST és a PVST közös előnye, hogy kihasználják a többszörös kapcsolatokat, amennyiben a VLAN-okat megfelelően rendeljük az interfészekhez.

[17] Single Spanning Tree, SST
[18] Common Spanning Tree, CST

3.1.2 Végberendezések

A Kossuth Gimnázium közel százhúsz számítógéppel rendelkezik. Ezek között vegyesen akadnak régebbi típusok és viszonylag modern, néhány éves modellek. A gépek döntő többségében Fast Ethernet-képes hálózati kártya van. Az előadótermek szinte mindegyikében van számítógép, az általános célú tantermekben ez nem jellemző. Némelyik terem fali aljzata nincs is bekötve a kapcsolóba – részben biztonsági okokból, részben pedig egyszerűen azért, mert eddig nem volt rá igény. A két számítástechnika teremben összesen körülbelül ötven, a könyvtárban tíz számítógép található, a többi munkaállomás az előadótermekben, a tanári dolgozószobákban és az igazgatóság helyiségeiben üzemel.

Jelenleg két szerver és egy dedikált tűzfal (átjáró) működik az iskolában folyamatosan, és van néhány hálózati nyomtató is. Áramszünet esetén a szerverek és a tűzfal áramellátását 2 db APC Smart-UPS 1500-XLM hálózatról kezelhető szünetmentes tápegység biztosítja. További hálózati eszközök: laptopok, digitális táblák, egyszerű (nem menedzselhető) kapcsolók.

3.1.3 Szoftverek

A munkaállomásokon szinte kivétel nélkül Windows XP operációs rendszert használnak. Néhány újabbra már Windows 7-et telepítettek. A kiszolgáló gépeken és a tűzfalon különböző GNU/Linux disztribúciók futnak (Debian és Ubuntu Server).

A személyi számítógépeken általában internetböngészőt, irodai programcsomagokat (szövegszerkesztő, táblázatkezelő, prezentációs alkalmazások) és médialejátszókat használnak, az informatika termekben továbbá nyelvoktató programokat és fejlesztőkörnyezeteket is. A helyi hálózaton belüli forgalom jelentős részét a munkaállomások és a szerverek közötti fájlátvitel teszi ki. Az internet irányú forgalmat az általános böngészés és elektronikus levelezés mellett a multimédiás alkalmazások, az iskola honlapja és a Taninform nevű iskolai ügyviteli és adminisztrációs szoftver generálják.

3.2 A hálózat funkciói

3.2.1 Szolgáltatások

A Kossuth Gimnázium hálózatán az alábbi fontosabb protokollok és szolgáltatások használatosak.

Dynamic Host Configuration Protocol (DHCP): A hálózatra csatlakozó munkaállomások részére IP címkiosztást biztosít. Az IP címmel nem rendelkező kliens feladónak a 0.0.0.0 címet állítja be, és a 255.255.255.255 globális üzenetszórási címre küldi a DHCP kérést. A szerver a címkiosztást dinamikus, automatikus vagy statikus módszerrel végezheti.

Dinamikus esetben a kliens egy meghatározott időre kapja a címet. Az idő leteltekor a cím felszabadul, és újra kioszthető (más kliensnek is). Automatikus esetben a szerver a kliens első csatlakozásakor meghatároz egy címet, és minden későbbi alkalommal azt adja a kliensnek. Statikus esetben az IP címet a hálózatadminisztrátor rendeli a kliens fizikai címéhez. *[3]*

A hálózaton a Sulinet router címkiosztása tiltott, helyette az egyik szerveren működő `dhcpd` program oszt IP címeket. A statikusan kiosztott címek listája egy egyszerű webes felületen módosítható.

Domain Name Service (DNS): Bár a Sulinet biztosít DNS szolgáltatást, az iskolában saját DNS szerver is üzemel, elsősorban a számítógépek helyi hálózaton történő könnyebb elérése céljából. A DNS rekordban szerepel a domain névhez tartozó IP cím, továbbá e-mail szerver[19] és egyéb adatok. A Kossuth Gimnáziumban a `bind` DNS szerverprogramot használják.

Network Time Protocol (NTP): Biztonsági és naplózási szempontból fontos, hogy legalább a közvetítő eszközök és a szerverek órái pontosan és összehangoltan járjanak. Az időszinkronizációs protokoll ezt teszi lehetővé úgy, hogy a pontos időt megbízhatónak tartott időszerverekről kéri le (noha maga a protokoll nem biztonságos). A megbízhatóság fokmérője a stratum: „Stratum 0" például egy atomóra, „Stratum 1" a hozzá soros vagy egyéb interfészen kapcsolódó szerver, „Stratum 2" pedig egy „Stratum 1" szerverhez szinkronizált időszerver. Az időben pontos naplóbejegyzésekkel könnyebb a hibakeresés és –elhárítás.

Az NTP protokoll előnye, hogy egy NTP kliens más kliensek számára viselkedhet szerverként is. Így csökken a magasabb stratum értékű szerverek terhelése cserébe egy kis pontatlanságért. A HP kapcsolók azonban az egyszerűsített NTP[20] protokollt ismerik: ezek nem képesek időszerverként működni. *[1]*

Lightweight Directory Access Protocol (LDAP): Ez a protokoll úgynevezett címtárszolgáltatás, főleg autentikáció (azonosítás) biztosítására használják. A gimnáziumban az `slapd` nevű LDAP-kiszolgáló a Windows munkaállomásokra, a Linux szerverekre és a levelezőrendszerbe teszi lehetővé a felhasználói bejelentkezést.

Server Message Block (SMB): Más néven Common Internet File System (CIFS). Főleg Windows-környezetben használt alkalmazási rétegbeli protokoll, amely fájlok, nyomtatók, soros portok és más erőforrások megosztására alkalmas. A szolgáltatás kliens-szerver architektúrában működik. Az iskola a gyakorlatban fájlmegosztásra és –tárolásra használja: a szerveren minden bejegyzett munkaállomásnak van egy saját védett könyvtára, amelyet írhat és olvashat, ide mentik a diákok az informatikaórai munkájukat. A tanári gépekhez szintén tartoznak ilyen könyvtárak, amelyek a Windowsban hálózati meghajtókként látszanak. Vannak továbbá megosztott könyvtárak, ahol oktatási anyagokat és programokat tárolnak.

[19] Mail Exchange, MX
[20] Simple NTP, SNTP

A könyvtárak hálózati bejelentkezéssel válnak elérhetővé, azaz a munkaállomáson a felhasználó egy közös tartományba (DOMAIN) jelentkezik be. Windows szervereken ezt az Active Directory Domain Services (korábbi nevén Active Directory illetve NT Directory) szolgáltatás biztosítja; mivel a szerverek ebben az esetben Linux alapúak, ezt a feladatot a `samba` programgyűjtemény látja el. A tartományvezérlő szerver kezeli a felhasználói hitelesítést és az engedélyeket.

Elektronikus levelezési protokollok: A Simple Mail Transfer Protocol (SMTP), a Post Office Protocol (POP) és az Internet Message Access Protocol (IMAP) a dolgozók számára biztosítja az elektronikus levelek küldését és fogadását.

Hypertext Transfer Protocol (HTTP, HTTPS): Ezen a protokollon alapul a böngészés, az iskolai honlap, a levelezőrendszer egyszerű elérése (Horde keretrendszer) és a Taninform oktatási adminisztrációs szoftver.

Secure Shell (SSH): Linuxos körökben méltán népszerű ez a protokoll, amelyet hálózati eszközök biztonságos távoli elérésére fejlesztettek ki, a titkosítatlan Telnet kiváltására. Aszimmetrikus (nyilvános kulcsú) titkosítást támogat. Többnyire kiszolgálók és kapcsolók/forgalomirányítók menedzselésére használják parancssoros felületen, de támogatja az alagutakat (tunnel) is, így a szerver egy adott portjára érkező csomagokat titkosítva továbbíthatjuk a kliensünknek vagy fordítva, akár egy harmadik IP cím portjára is. Érdemes még megemlíteni a Secure Copyt (SCP), amely a File Transfer Protocol (FTP) biztonságos alternatívája: titkosított kapcsolaton keresztül tesz lehetővé fájlküldést és –fogadást.

Tűzfal és átjáró: Habár a Sulinet végpont forgalomirányítóján számos biztonsági korlátozás be van állítva, a könnyebb adminisztráció érdekében az iskolában saját tűzfal és átjáró üzemel. Ez egy dedikált, Linuxot futtató számítógép, amelynek egyik interfésze a Sulinet switchre, másik interfésze a helyi hálózatra csatlakozik. A belső hálózat teljes WAN[21] irányú forgalma ezen a számítógépen halad át. A rátelepített `iptables` program forgalomszűrést, hozzáférés-szabályozást és IP címfordítást végez.

[21] Wide Area Network

3.2.2 Elvárások

Egy középiskolában jóval kevesebbet várnak el egy számítógép-hálózattól, mint egy nagyvállalatnál. A hálózat terhelése tanítási időn kívül, azaz hétköznap 15 óra után és reggel 7 óra előtt valamint hétvégén gyakorlatilag elhanyagolható.

A Taninform rendszer hátránya többek között, hogy rengeteg pluszmunkát jelent a tanároknak, ezért igyekeznek a velejáró adminisztrációs teendőket a szünetekben elvégezni. A Taninform webes felülete a tapasztalatok szerint önmagát tekintve sem fürge; ha ehhez hozzávesszük azt a tényt, hogy több mint száz munkaállomásra egy ADSL-kapcsolat[22] jut (amelynél a Magyarországon használt technológiák letöltési sebességének elméleti felső határa 8-24, a feltöltési sebessége pedig mindössze 1 Mbps), már meg is találtuk a leggyengébb láncszemet a hálózatban. A könyvtári számítógépterem és az iskolahonlap forgalmát pedig még bele sem számoltuk…

A LAN-forgalom hasonlóképpen egyenetlen: jelentős csúcsokat mérhetünk, ha megfigyeljük a szerverek adatforgalmát. Ezeket a csúcsokat az informatikatermek gépeiről közel egyidejűleg indított letöltések okozzák. (A tanórai internetezés ellen persze van megoldás: egy shell szkripttel pillanatok alatt letiltható a diákok gépeinek internet-hozzáférése.)

A gimnáziumban tehát nem a kiváló rendelkezésre állás a legfontosabb (persze az sem elhanyagolható), sokkal inkább a megfelelő sávszélesség. Szerencsére a hubalapú hálózatról kapcsolt hálózatra áttérés valamelyest javított az egy állomásra jutó LAN sávszélességen. Mindazonáltal kellemetlen, ha akár egy napra is leáll a helyi hálózat vagy az internetkapcsolat, ezért fontos a hibamegelőzés, a problémafigyelés és a gyors beavatkozás. Sajnos ezen a téren a középiskolák szűkös erőforrásokkal rendelkeznek, így a DE Kossuth Lajos Gyakorló Gimnáziuma is. Helyi rendszergazda és hálózatadminisztrátor híján ezeket a feladatokat az informatikatanároknak kell ellátniuk, vagy külső (például egyetemi) segítséget kell igénybe venniük.

A hálózatbiztonság tekintetében az elsődleges szempont az igazgatási és tanári számítógépeken található adatok védelme, és e gépek adatforgalmának elszigetelése. Szükséges tehát átfogó biztonsági irányelvek megfogalmazása, betartása és betartatása.

[22] Asymmetric Digital Subscriber Line

4 Elemzés és tesztelés

4.1 A hálózat fizikai és logikai felépítése

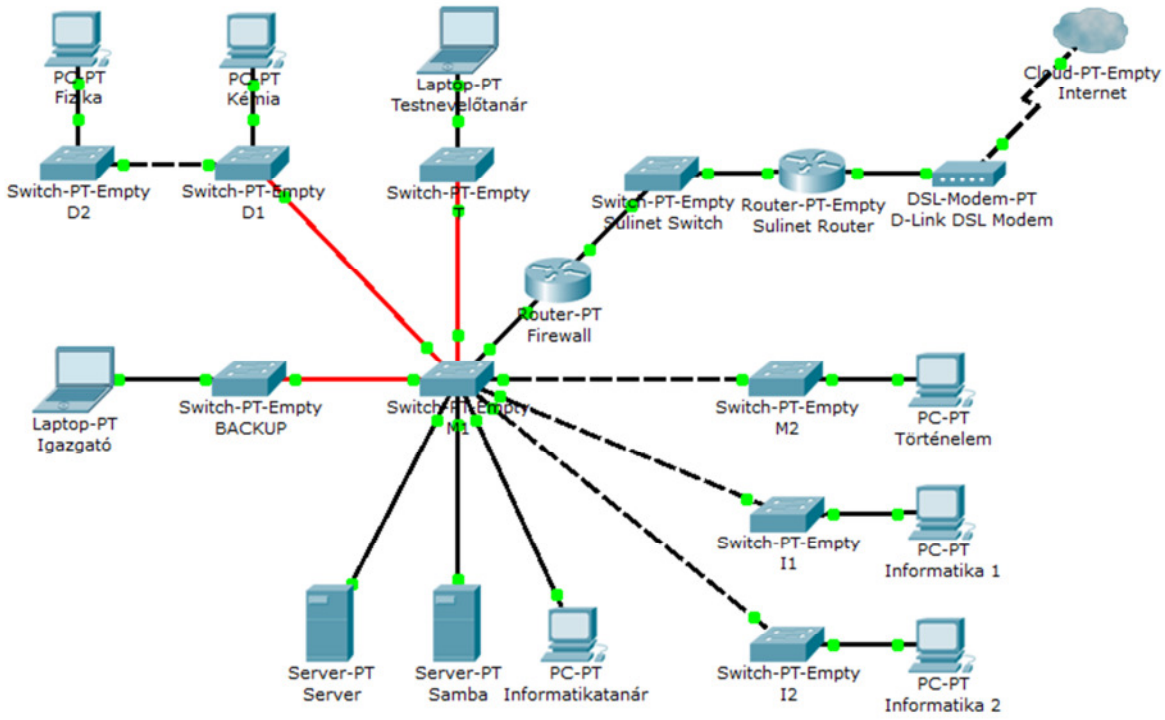
4.1.1 Gerinctopológia

Hosztnév	Típus	Hely
KOSSUTH-M1	HP ProCurve 2810-24G	H épület
KOSSUTH-M2	HP ProCurve 2610-48	H épület
KOSSUTH-D1	HP ProCurve 2610-48	D épület
KOSSUTH-D2	HP ProCurve 2610-24	D épület
KOSSUTH-BACKUP	HP ProCurve 2610-48	A épület
KOSSUTH-T	HP ProCurve 2610-24	T épület
KOSSUTH-I1	HP ProCurve 2626	H épület
KOSSUTH-I2	HP ProCurve 2626	H épület

A gimnázium hálózati gerincét a fenti nyolc kapcsoló alkotja. A KOSSUTH-BACKUP nevű az A épületben üzemel, mivel az eredetileg oda szánt eszköz meghibásodott. Az eszközök eléréséhez Telnet felületet használtam, az LLDP felderítőprotokoll adatai alapján gyorsan fel tudtam térképezni a hálózatot. Mivel az LLDP keretek élettartama 1 hop (ugrás), így egy kapcsolóról csak a hozzá közvetlenül csatlakoztatott kapcsolók látszanak. Ellenőriztem továbbá a MAC címtáblákat, amelyek bonyolultabb, több kapcsolót tartalmazó hálózatokon segíthetik a feltérképezést.

```
KOSSUTH-M1# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- ----------------------
  18        | 00 1f fe 68 45 80         50     50        KOSSUTH-M2
  19        | 00 1c 2e 05 4a 80         26     26        KOSSUTH-I1
  20        | 00 1c 2e 05 f9 c0         26     26        KOSSUTH-I2
  22        | 00 1f fe 1a 92 00         52     52        KOSSUTH-BACKUP
  23        | 00 1f fe 50 53 80         28     28        KOSSUTH-T
  24        | 00 1f fe 66 5f 00         52     52        KOSSUTH-D1
```

```
KOSSUTH-D2# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------ ------ --------- --------------------
  26        | 00 1f fe 66 5f 00        48     48        KOSSUTH-D1
```



Ahogy az ábrán látható, az épületek a H épületben található M1 switchre kapcsolódnak, noha az optikai kábelek másképp helyezkednek el a föld alatt: valójában minden épület az A épülettel van összekötve, az A épület optikai patch paneljén alakították ki a D-H, T-H és A-H összeköttetéseket. A switchek optikai interfészei 1000Base-SX üzemmódban működnek (`show interfaces brief` parancs), amely többmódusú optikai szálakat feltételez.

Az M1 minden portja 1 Gbps sebességű, ide kötötték be a két szervert és a tűzfalgépet is. (A tűzfalat forgalomirányítóként ábrázoltam, mert a Packet Tracer programban egy PC-be nem lehet több hálózati interfészt tenni.)

4.1.2 IP címzés és útvonaltáblák

A hálózati eszközök IP címei:

Eszköz neve	Interfész	IPv4 cím	Hálózati maszk
Kapcsolók	VLAN 1	192.168.10.1 - .8	255.255.255.0
Samba	eth0	192.168.11.254	255.255.255.0
Samba	eth1	192.168.10.248	255.255.255.0
Server	eth0	192.168.10.252	255.255.255.0
Firewall	eth0	195.199.212.57	255.255.255.248
Firewall	eth1	192.168.10.251	255.255.255.0
Sulinet router		195.199.212.62	255.255.255.248
Statikus DHCP		192.168.10.0	255.255.255.0
Dinamikus DHCP		192.168.11.0	255.255.255.0

A legtöbb munkaállomás a MAC címe alapján statikusan kap IP címet a Samba számítógéptől a 192.168.11.0/24 tartományból. Amelyeknek nincs regisztrálva a fizikai címe, azoknak a 192.168.10.0/24 alhálózatból oszt IP címet a DHCP.

Minden csomópont a tűzfalon keresztül éri el az internetet. A tűzfalon az `iptables` program hálózati címfordítást, csomagszűrést és további, állapotalapú tűzfaltevékenységeket végez. A regisztrált gépek alapértelmezett átjárója a Samba szerver, amelyen az IP forgalomirányítás be van kapcsolva, így a WAN irányú csomagokat a tűzfal felé továbbítja:

```
samba:/# cat /proc/sys/net/ipv4/ip_forward
1
samba:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
0.0.0.0         192.168.10.251  0.0.0.0         UG    0      0        0 eth1
```

A szerverek közül csak az egyik publikus (a Server nevű). A tűzfalon a Proxy ARP[23] engedélyezésével válik elérhetővé az internet felől. A szerver hálózati konfigurációjában egy alinterfészre van beállítva a külső IP cím:

```
server:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:22:15:8f:3b:82
          inet addr:192.168.10.252  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::222:15ff:fe8f:3b82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204395450 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139552399 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:173150076629 (161.2 GiB)  TX bytes:52130935140 (48.5 GiB)
          Interrupt:17

eth0:0    Link encap:Ethernet  HWaddr 00:22:15:8f:3b:82
          inet addr:195.199.212.58  Bcast:195.199.212.63  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:17
```

4.1.3 „Show run”

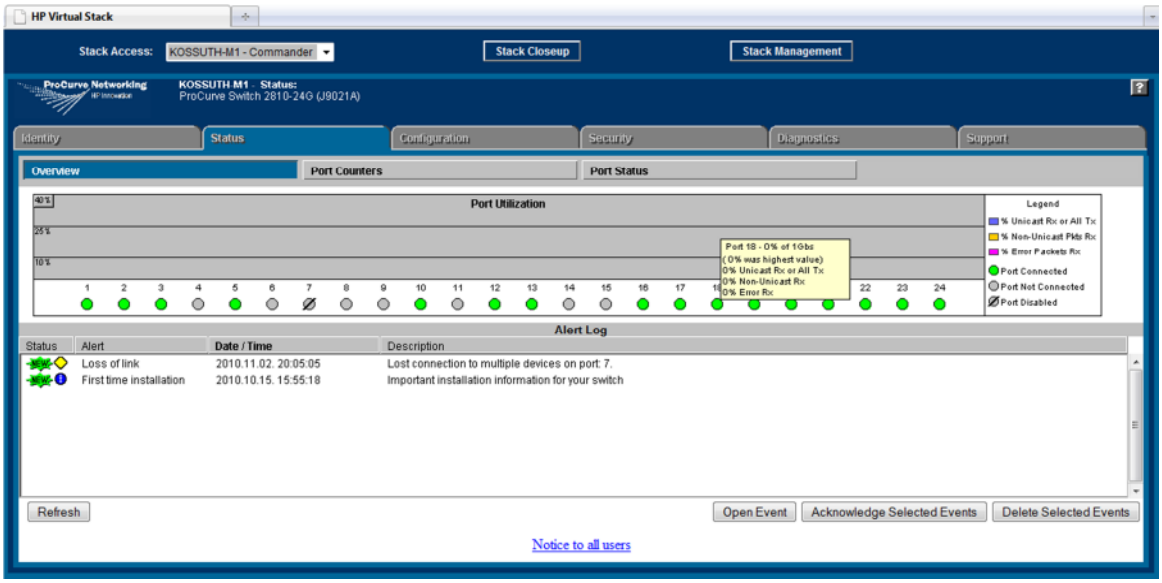
A kapcsolók konfigurációit vizsgálva kiderült, hogy szinte alapbeállításokkal működnek: csak hosztnév, jelszó, néhány SNMP információ, IP cím és alapértelmezett átjáró volt beállítva.

```
KOSSUTH-M1# show running-config

Running configuration:

; J9021A Configuration Editor; Created on release #N.11.06

hostname "KOSSUTH-M1"
snmp-server location "Magyar"
snmp-server community "public" Unrestricted
ip default-gateway 192.168.10.251
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address 192.168.10.1 255.255.255.0
   exit
stack commander "KOSSUTH"
stack member 1 mac-address 001ffe684580
stack member 2 mac-address 001ffe665f00
stack member 3 mac-address 001ffe5083c0
stack member 4 mac-address 001ffe1a9200
stack member 5 mac-address 001ffe505380
stack member 6 mac-address 001c2e054a80
stack member 7 mac-address 001c2e05f9c0
password manager
password operator
```

[23] Address Resolution Protocol

A ProCurve eszközök hasznos funkciója a „stacking”: a stackbe tartozó eszközöket egy közös, HTTP vagy HTTPS protokollt használó, Java alapú felületen adminisztrálhatjuk. Különböző tulajdonságok lekérdezését és beállítását teszi lehetővé:

- **Identitás:** hosztnév, indítás óta eltelt idő (uptime), SNMP adatok, CPU- és memóriakihasználtság, IP és MAC cím, típus, sorozatszám, szoftver verziója
- **Állapot:** hibanapló, interfészek állapota és statisztikái
- **Konfiguráció:** IP cím és átjáró beállítása, VLAN-ok, interfész-beállítások, QoS, port monitoring (egy port forgalmának másolása egy másik portra), konfigurációs fájl és szoftver-képfájlok mentése és feltöltése
- **Biztonság:** jelszavak, portbiztonság beállításai, biztonsági napló, HTTPS, SSL tanúsítványok
- **Diagnosztika:** ping (Layer 3), link-test (Layer 2), konfigurációk lekérdezése, eszköz újraindítása



A stacket egy úgynevezett Commander és több Member switch alkotja. A közös adminisztrációhoz elég a Commander webes felületét megnyitni, a Stack Closeup gombra kattintva grafikusan láthatjuk akár az egész stack tartalmát. A grafika néhány másodperces frissítéssel mutatja az interfészek állapotát, főbb tulajdonságait és kihasználtságát.

A Commander képes a hálózatba kapcsolt új eszközöket (Candidate) automatikusan hozzáadni a stackhez (auto-grab). Ez a funkció alapértelmezésben tiltott, de az egyes eszközökön is letilthatjuk a „stacking" funkciót (`no stack` parancs). A „stacking" az adatkapcsolati rétegben működik, tehát IP címet csak a Commandernek kell beállítanunk – kivéve, ha szeretnénk az eszközöket más módon (Telnet, SSH) is elérni. *[1]*

4.2 A válaszidő mérése

Csillag topológiájú kapcsolt hálózat lévén rövid válaszidőkre számítottam, és sejtésem beigazolódott. A mérésre a jól ismert `ping` parancsot használtam, amely az ICMP[24] protokollon alapul. Néhány eredmény a következőkben olvasható.

Server pingelése a fizikailag legtávolabbi kapcsolóról:

```
KOSSUTH-D2# ping 192.168.10.252
192.168.10.252 is alive, time = 1 ms
```

Server pingelése Sambáról:

```
samba:/# ping 192.168.10.252
PING 192.168.10.252 (192.168.10.252) 56(84) bytes of data.
64 bytes from 192.168.10.252: icmp_seq=1 ttl=64 time=0.284 ms
64 bytes from 192.168.10.252: icmp_seq=2 ttl=64 time=0.261 ms
64 bytes from 192.168.10.252: icmp_seq=3 ttl=64 time=0.242 ms
64 bytes from 192.168.10.252: icmp_seq=4 ttl=64 time=0.244 ms

--- 192.168.10.252 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.242/0.257/0.284/0.025 ms
```

Sulinet router pingelése Sambáról:

```
samba:/# ping 195.199.212.62
PING 195.199.212.62 (195.199.212.62) 56(84) bytes of data.
64 bytes from 195.199.212.62: icmp_seq=1 ttl=254 time=2.62 ms
64 bytes from 195.199.212.62: icmp_seq=2 ttl=254 time=2.47 ms
64 bytes from 195.199.212.62: icmp_seq=3 ttl=254 time=2.28 ms
64 bytes from 195.199.212.62: icmp_seq=4 ttl=254 time=2.28 ms

--- 195.199.212.62 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 2.288/2.418/2.625/0.145 ms
```

[24] Internet Control Message Protocol

Internetes kiszolgáló (time.kfki.hu) pingelése Sambáról:

```
samba:/# ping 148.6.0.1
PING 148.6.0.1 (148.6.0.1) 56(84) bytes of data.
64 bytes from 148.6.0.1: icmp_seq=1 ttl=55 time=28.3 ms
64 bytes from 148.6.0.1: icmp_seq=2 ttl=55 time=25.9 ms
64 bytes from 148.6.0.1: icmp_seq=3 ttl=55 time=25.1 ms
64 bytes from 148.6.0.1: icmp_seq=4 ttl=55 time=25.7 ms

--- 148.6.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 25.137/26.305/28.344/1.221 ms
```

Server pingelése az internet felől:

```
C:\>ping 195.199.212.58

195.199.212.58 pingelése - 32 bájtnyi adattal:
Válasz 195.199.212.58: bájt=32 idő=32 ms TTL=54
Válasz 195.199.212.58: bájt=32 idő=30 ms TTL=54
Válasz 195.199.212.58: bájt=32 idő=30 ms TTL=54
Válasz 195.199.212.58: bájt=32 idő=29 ms TTL=54

195.199.212.58 ping-statisztikája:
    Csomagok: küldött = 4, fogadott = 4, elveszett = 0
                          (0% veszteség),
Oda-vissza út ideje közelítőlegesen, milliszekundumban:
    minimum = 29ms, maximum = 32ms, átlag = 30ms
```

4.3 Útvonalak a hálózaton

A fenti topológiát megismerve több szűk keresztmetszetet találtam a hálózatban. A regisztrált munkaállomások egymást és a Samba (DHCP, LDAP és tartományvezérlő) szervert kapcsolt hálózaton érik el (192.168.11.0/24), míg a Server (WWW, mail, DNS) gépet és az internetet (tűzfalat) már csak a Sambán keresztül. Belátható, hogy a belső szerver és a kliensek közötti adatforgalom jelentősen zavarja a hálózaton kívülre irányuló forgalmat, hiszen ugyanazon az interfészen osztoznak. A jövőben egy gyorsabb, többtíz Mbps sebességű internetkapcsolat esetén ez az „osztozkodás” gondot jelenthet.

Mivel a hálózat topológiája majdnem „lapos” és nincs LAN forgalomirányító, az útvonal-meghatározás inkább WAN irányba érdekes. A `traceroute` parancsot a Sambán adtam ki; ha egy diák vagy tanári munkaállomásról vizsgáljuk az útvonalat, az első állomás a Samba 192.168.11.254-es címe lesz mint alapértelmezett átjáró.

```
samba:/# traceroute -s 192.168.11.254 www.index.hu
traceroute to www.index.hu (217.20.130.97) from 192.168.11.254, 30 hops max, 40s
 1  firewall (192.168.10.251)  0.296 ms  0.209 ms  0.187 ms
 2  router (195.199.212.62)  2.526 ms  2.770 ms  2.317 ms
 3  INTERNET2.ngnedi.telekom.hu (84.1.254.210)  42.810 ms  25.349 ms  24.128 ms
 4  195.199.248.225 (195.199.248.225)  26.639 ms  25.054 ms  25.071 ms
 5  195.199.248.225 (195.199.248.225)  25.221 ms  26.491 ms  24.202 ms
 6  sulinet-bix.pantel.net (195.199.254.25)  25.810 ms  25.874 ms  38.227 ms
 7  TE-1-1.core0.interware.hu (193.188.137.25)  30.680 ms  27.877 ms  44.853 ms
 8  sportgeza.hu (217.20.130.97)  26.511 ms  26.350 ms  32.049 ms
```

Az épületek közötti gigabites kapcsolatok jelenleg elegendőnek tűnnek, hiszen a fájlszerver hálózati kártyája összesen 1 gigabitet képes forgalmazni másodpercenként, és a hálózatot fájlátvitelre főleg az informatika szaktantermekben használják, ahol az I1 és I2 kapcsoló külön-külön gigabites porton csatlakozik az M1-re. A kliensszám, az igények és a felhasználási területek növekedésével azonban – akár már néhány éven belül – ez a sávszélesség esetenként kevésnek bizonyulhat.

4.4 Forgalom és terhelés

4.4.1 A mérési módszer

A hálózati forgalom figyelésére a Cacti nevű ingyenes és nyílt forrású programot használtam. A Cacti a grafikonok előállítására az RRDToolt[25], adatbázisnak a MySQL-t[26], webes felületének megvalósítására a PHP-t[27], a statisztikák lekérdezésére pedig az SNMP protokollt használja.

Az SNMP protokoll UDP adatcsomagokban továbbítja az információt. Az SNMP-képes hálózati eszközökön úgynevezett agent fut. Az adatokat összegyűjtő és naplózó szervert managernek nevezzük. Az információátvitelnek kétféle módja van: a manager rendszeresen lekérdezi az információt az agenttől (poll), esetenként pedig az agent rendkívüli figyelmeztetést (trap) küld a managernek. A trap jelezheti például egy forgalomhatár elérését, vagy utalhat meghibásodásra.

Fontos megemlíteni, hogy az SNMP 1-es 2-es verziója csomagtitkosítást nem végez, vagyis az adatforgalom lehallgatható. Az első verzió hitelesítése kimerült egy titkosítatlan szöveges

[25] Round Robin Database
[26] Structured Query Language
[27] PHP: Hypertext Preprocessor

jelszó (community string) használatában. Az eredeti SNMPv2 viszont a benne lévő új biztonsági modell bonyolultsága miatt nem terjedt el, ezért került sor az SNMPv2c kifejlesztésére. SNMPv2 alatt ma általában ezt a variánst értjük, amely biztonsági lehetőségeit tekintve jobban hasonlít az első verzióra, mint a másodikra – azaz kivették belőle az új modellt, és visszatették a community string szerinti azonosítást. Kétféle community string állítható be az SNMP-képes eszközön: csak olvasható és írható-olvasható. Előbbivel értelemszerűen csak információgyűjtésre van lehetőség, utóbbival viszont az eszköz konfigurációját is megváltoztathatjuk a manager gépről küldött parancsokkal. *[6]*

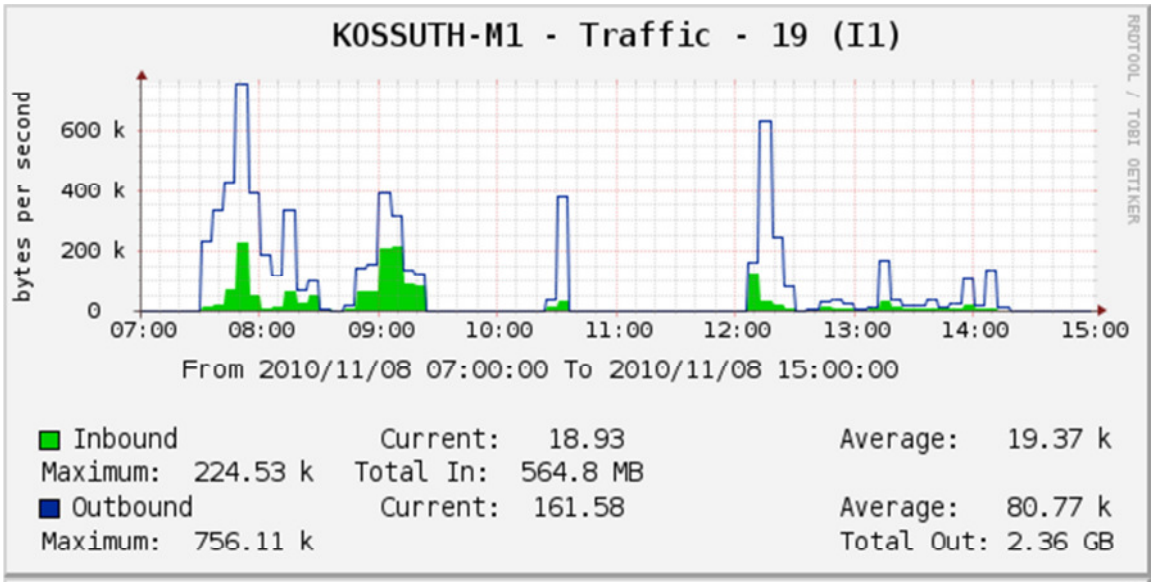
A korábban ismertetett LLDP és NTP protokollokhoz hasonlóan az SNMP is megelőlegezte a bizalmat a hálózati berendezéseknek. Ma már szükséges a forrás hitelesítése (authentication), az információ valódiságának (integrity) és bizalmasságának (confidentality) biztosítása. Az SNMPv3 képes mindezekre. *[3]*

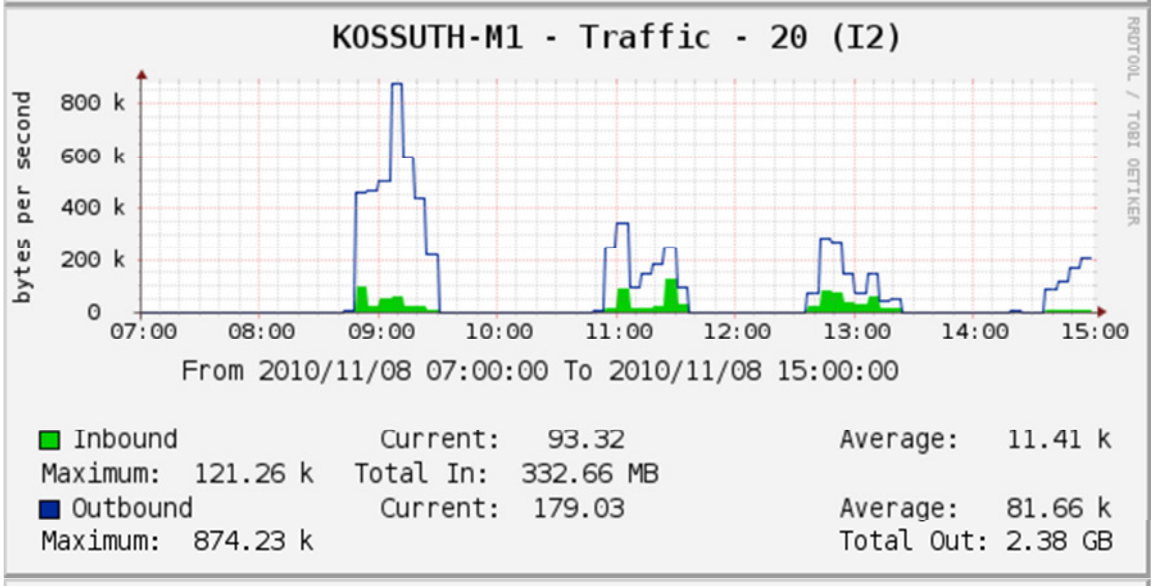
A Cactit a Server számítógépre telepítettem, és forgalommérést végeztem az M1 kapcsoló azon portjain, amelyek a többi kapcsolóhoz vezetnek. Tanítási időn kívül a forgalom elhanyagolható, az érdekes tartomány a hétfőtől péntekig reggel 7 és délután 15 óra közötti időszak. Noha a Cacti néhány percenként gyűjti be az SNMP adatokat, az RRDTool sajátossága, hogy az egyre régebbi adatokból egyre kevesebb részletet őriz meg – azaz egy korábbi nap, hét vagy hónap statisztikáit nézve már csak félórás vagy egyórás felbontású adathalmazt és grafikont láthatunk.

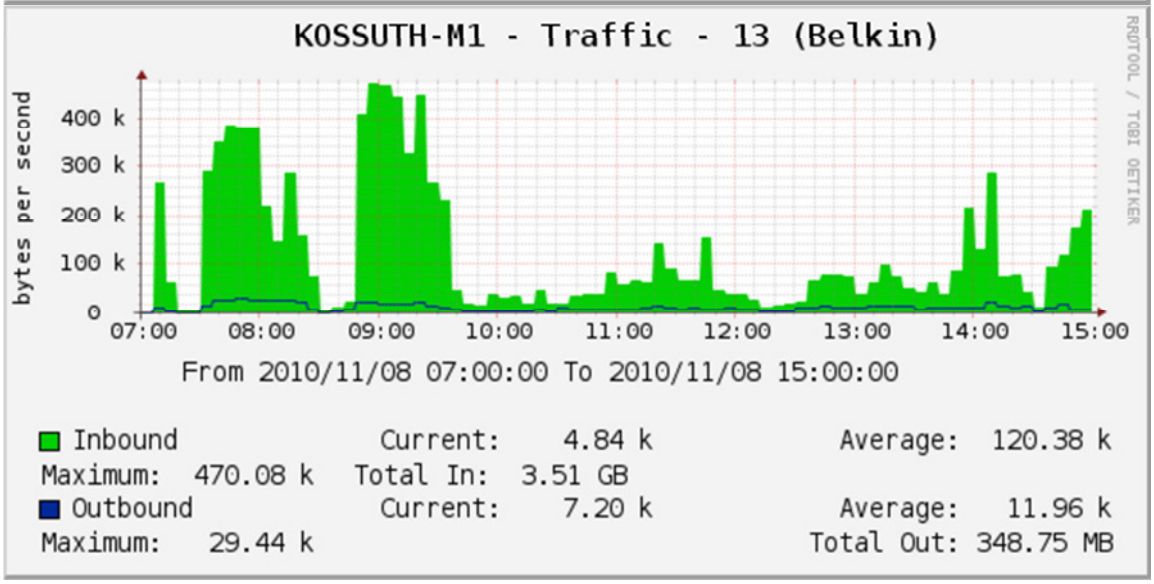
4.4.2 Eredmények

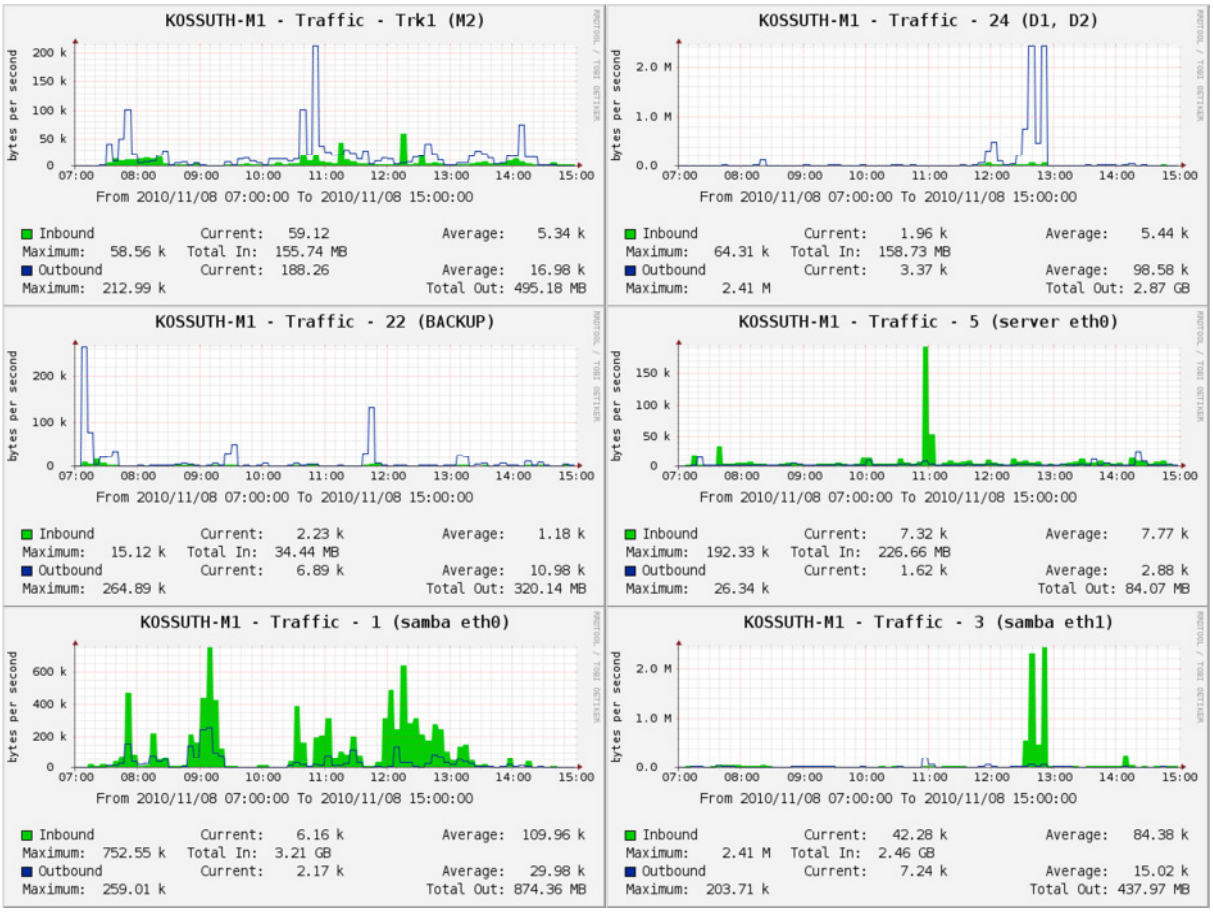
Az alábbi ábrákon a 2010. november 8-án 7-15 óra között mért adatforgalom látható; a grafikonok nevében zárójelben a „távoli” eszköz neve ill. interfésze szerepel, a bejövő (in) és kimenő (out) forgalom a név elején látható eszköz szemszögéből értendő. (A Belkin név arra utal, hogy a mérés idején a tűzfalgép merevlemez-meghibásodás miatt üzemen kívül volt, ezért a NAT és DMZ szolgáltatást átmenetileg egy ilyen márkájú SOHO[28] router biztosította.) A következő oldalon, az I1 és I2 kapcsolók forgalmi statisztikáján jól látszanak az informatikaórák okozta terhelések…

[28] Small Office/Home Office


KOSSUTH-M1 - Traffic - 19 (I1)
bytes per second
600 k
400 k
200 k
0
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
From 2010/11/08 07:00:00 To 2010/11/08 15:00:00
Inbound Current: 18.93 Average: 19.37 k
Maximum: 224.53 k Total In: 564.8 MB
Outbound Current: 161.58 Average: 80.77 k
Maximum: 756.11 k Total Out: 2.36 GB
RRDTOOL / TOBI OETIKER


KOSSUTH-M1 - Traffic - 20 (I2)
bytes per second
800 k
600 k
400 k
200 k
0
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
From 2010/11/08 07:00:00 To 2010/11/08 15:00:00
Inbound Current: 93.32 Average: 11.41 k
Maximum: 121.26 k Total In: 332.66 MB
Outbound Current: 179.03 Average: 81.66 k
Maximum: 874.23 k Total Out: 2.38 GB
RRDTOOL / TOBI OETIKER


KOSSUTH-M1 - Traffic - 13 (Belkin)
bytes per second
400 k
300 k
200 k
100 k
0
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
From 2010/11/08 07:00:00 To 2010/11/08 15:00:00
Inbound Current: 4.84 k Average: 120.38 k
Maximum: 470.08 k Total In: 3.51 GB
Outbound Current: 7.20 k Average: 11.96 k
Maximum: 29.44 k Total Out: 348.75 MB
RRDTOOL / TOBI OETIKER



Megmértem az internetkapcsolat sebességét is, klasszikus módszerrel: néhány éjszaka, amikor a hálózat nem volt terhelve, megbízhatóan gyors magyarországi Ubuntu GNU/Linux tükörszerverekről töltöttem le egy megfelelő méretű CD-kép (ISO) darabot a `wget` programmal. Az eredmény: a letöltési sebesség megközelítőleg 450 KB/s = 3,6 Mb/s.

```
root@firewall:/# wget http://ubuntu.bitmind.hu/maverick/ubuntu-10.10-server-
i386.iso
--2010-11-08 22:52:33--  http://ubuntu.bitmind.hu/maverick/ubuntu-10.10-server-
i386.iso
Resolving ubuntu.bitmind.hu... 94.125.248.123
Connecting to ubuntu.bitmind.hu|94.125.248.123|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 657735680 (627M) [application/x-iso9660-image]
Saving to: `ubuntu-10.10-server-i386.iso'

 9% [==>                                   ] 60.352.056   449K/s  eta 22m 0s  ^C
```

A feltöltési sávszélességet is ezzel a fájldarabbal mértem: SCP protokollon indítottam letöltést a saját számítógépemre. A sebesség itt erősen ingadozott, de kijelenthető, hogy a mért sávszélesség az ISP-k által alkalmazott értékeket tekintve a 192 kbps-hoz esik legközelebb.

5 A hálózat korszerűsítési lehetőségei

A továbbfejlesztés átgondolásakor azt tartottam elsődleges szempontnak, hogy az iskola a meglévő eszközök felhasználásával ingyen (de legalábbis olcsón) alakíthasson ki fejlettebb számítógép-hálózatot. Ennek ellenére – a teljesség kedvéért – több olyan módosítást és fejlesztést is fogok javasolni, amelyek anyagi befektetéssel, beruházással járnak.

5.1 Változtatások a fizikai felépítésben

Egy hálózaton mindenképp célszerű redundáns linkek (eszközök közötti többszörös kapcsolatok) létrehozása. Tekintve, hogy a kapcsolók egymástól távol, más szinten és épületben helyezkednek el, az ilyen beruházásoknak általában komoly anyagi vonzata van. Az M1 és M2 kapcsolók viszont azonos rack szekrényben találhatók, így magától értetődő volt felmérni a lehetőségeket. Két megoldás merült fel: a redundáns linkek és a linkaggregáció.

5.1.1 Redundancia és linkaggregáció

Ha redundáns linkeket alakítok ki, feszítőfa-protokollt kell használnom. E protokollok hátránya, hogy a redundáns linkek közül egy kivételével mindet letiltják, nem használják ki a rendelkezésre álló sávszélességet. Kivételek ez alól a VLAN-okra felkészített protokollok: a PVST és az MST. A különbség, hogy a PVST minden VLAN-hoz külön feszítőfát számol, az MST-ben viszont csoportokba rendezzük a VLAN-okat, és a csoporthoz készül feszítőfa. Nem elhanyagolható tény, hogy az MST működéséből következően sokkal kevésbé terheli az eszközt, mint a PVST. *[7]*

A ProCurve eszközök az MST protokollt támogatják, sőt a `spanning-tree` bekapcsolásakor ez az alapértelmezett. Érdemes legalább annyi MST példányt indítani, ahány redundáns linkünk van, és a VLAN-okat a várható forgalom alapján nagyjából egyenlően elosztani a példányok között. *[1]* Egy lehetséges konfiguráció így nézne ki az egyik eszközön:

```
KOSSUTH-M1(config)# spanning-tree
KOSSUTH-M1(config)# spanning-tree config-name KossuthMST
KOSSUTH-M1(config)# spanning-tree config-revision 1
KOSSUTH-M1(config)# spanning-tree instance 1 vlan 10 20 40
KOSSUTH-M1(config)# spanning-tree instance 2 vlan 30 50 60 70
KOSSUTH-M1(config)# spanning-tree instance 1 priority 2
KOSSUTH-M1(config)# spanning-tree instance 2 priority 1
KOSSUTH-M1(config)# spanning-tree instance 1 ethernet 17 priority 4
KOSSUTH-M1(config)# spanning-tree instance 2 ethernet 18 priority 4
```

```
KOSSUTH-M1(config)# show spanning-tree mst-config

 MST Configuration Identifier Information

  MST Configuration Name : KossuthMST
  MST Configuration Revision : 1
  MST Configuration Digest : 0x44EB1D207D38D94CD89EB9C3F88415EC

  IST Mapped VLANs : 1-9,11-19,21-29,31-39,41-49,51-59,61-69,71-4094
  Instance ID Mapped VLANs
  ----------- ------------------------------------------------------------
  1           10,20,40
  2           30,50,60,70
```

Figyelembe véve, hogy az épületek között jelenleg nincsenek redundáns linkek, inkább a linkaggregáció mellett döntöttem. Az M1-M2 között létrehoztam a meglévő mellé egy másik 1 Gbps-os összeköttetést és egy 100 Mbps-osat is. Előbbiből egy statikus LACP trönköt készítettem, utóbbin pedig csak a 60-as VLAN forgalma mehet át. (A VLAN-ok kiosztásáról részletesen a dolgozat későbbi részében lesz szó.) Ezzel a megoldással már 2 Gbps sávszélességet használhatnak a humán épületben lévő munkaállomások és szerverek, továbbá dedikált 100 Mbps-t a nyilvános (csak internetelérést engedő) VLAN forgalmára, amely hasznos lehet a jövőben.

```
KOSSUTH-M1(config)# trunk 17-18 Trk1 LACP
KOSSUTH-M1(config)# vlan 10 tagged Trk1
KOSSUTH-M1(config)# vlan 20 tagged Trk1
KOSSUTH-M1(config)# vlan 30 tagged Trk1
KOSSUTH-M1(config)# vlan 40 tagged Trk1
KOSSUTH-M1(config)# vlan 50 tagged Trk1
KOSSUTH-M1(config)# vlan 70 tagged Trk1
KOSSUTH-M1(config)# no vlan 1 untagged Trk1
KOSSUTH-M1(config)# vlan 60 tagged 21
KOSSUTH-M1(config)# show trunks

 Load Balancing

  Port | Name                               Type      | Group Type
  ---- + ---------------------------------- --------- + ----- -----
  17   |                                    100/1000T | Trk1  LACP
  18   |                                    100/1000T | Trk1  LACP

KOSSUTH-M1(config)# show lacp

                          LACP

   PORT   LACP      TRUNK     PORT      LACP      LACP
   NUMB   ENABLED   GROUP     STATUS    PARTNER   STATUS
   ----   -------   -------   -------   -------   -------
   17     Active    Trk1      Up        Yes       Success
   18     Active    Trk1      Up        Yes       Success
```

```
KOSSUTH-M1(config)# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : Management
  Management VLAN : Management

  802.1Q VLAN ID Name         Status       Voice Jumbo
  -------------- ------------ ------------ ----- -----
  1              DEFAULT_VLAN Port-based   No    No
  10             Management   Port-based   No    No
  20             Igazgatas    Port-based   No    No
  30             Tanar        Port-based   No    No
  40             Diak         Port-based   No    No
  50             Egyeb        Port-based   No    No
  60             Nyilvanos    Port-based   No    No
  70             Nyomtato     Port-based   No    No
```

Az előző parancsokon érdemes megfigyelni, hogy a Hewlett-Packard és a Cisco VLAN-besorolási módszere jelentősen különbözik. A Cisco berendezéseken az interfészekhez rendeljük a VLAN-okat: létezik „access” port, amely egyetlen VLAN-ba tartozik és trönkport több VLAN átvitelére. A HP eszközökön a VLAN-hoz rendeljük az interfészeket címkézve vagy anélkül. (Természetesen egy port címkézés nélkül csak egy VLAN-ba tartozhat.) *[1]*

Bár a kapcsoló operációs rendszere a `show trunks` parancs kimenetében terhelés-kiegyensúlyozást (load balancing) ír, a korábban ismertetett LACP és HP linkaggregációs megoldások önmagukban nem garantálják a fizikai interfészek közötti egyenlő elosztást. *[1]* A fenti konfigurációban tehát csupán terhelésmegosztásról (load sharing) beszélhetünk.

5.1.2 További javaslatok

A hálózat fizikai topológiájának korszerűsítésekor javaslom, hogy az iskola mérje fel az aktuális igényeket az intézményben, hiszen majdnem minden helyiségbe bevezethető a hálózat, mindössze a kijelölt fali aljzatok kábeleit kell a kapcsolókba bekötni. E folyamat során ajánlott felülvizsgálni a meglévő bekötéseket, a szükségteleneket megszüntetni, és a switchportok kiosztásakor ésszerű, áttekinthető sorrendet alkalmazni: az azonos VLAN-ba tartozó eszközöket szomszédos portokra helyezni (a sávszélességigény figyelembe vételével).

Érdemes megvizsgálni, hogy a szerverszobában található szünetmentes tápegységek közül elegendő-e egyetlen darab a szerverek áramellátásához. Ha igen, a másikat célszerű lenne a humán épület földszinti rack szekrénye mellé levinni, hogy az M1 és M2 kapcsolóknak és a Sulinet végpontnak biztosítsa a folyamatos működést.

A jövőben az új felhasználási területek, alkalmazások és technológiák miatt meg kell fontolni nagyobb sebességű épületközi és épületeken belüli optikai gerinchálózat kialakítását, továbbá korszerűbb közvetítő berendezések – „okosabb" (Layer 3-as) kapcsolók, forgalomirányítók, vezeték nélküli hozzáférési pontok – beszerzését.

A hatodik – jelenleg felújításra váró – épület hálózatának tervezésekor célszerű mérlegelni egy IP telefonhálózat[29] kialakításának lehetőségét. Ezzel a megoldással nincs szükség külön telefonvezetékre a falakban. Szinte minden modern készülék támogatja valamelyik Power over Ethernet szabványt (IEEE 802.3af vagy 802.3at), így PoE-képes kapcsolók alkalmazásakor a telefonok áramellátása sem jelent nehézséget.

5.2 Fokozott biztonság és hibamegelőzés

5.2.1 Biztonságos menedzsment

Mivel az eszközök a hálózat elemzésekor kvázi alapkonfiguráción működtek, mindenképpen szükségesnek tartottam néhány alapvető beállítást.

A beállítások elvégzése előtt a kapcsolók konfigurációjáról biztonsági mentést készítettem, majd szoftverüket a legújabb stabil verzióra frissítettem. *[1]* Az eredeti szoftver továbbra is elérhető, ha szükség van rá.

```
KOSSUTH-M1# copy running-config tftp 192.168.1.10 M1.txt
KOSSUTH-M1# erase startup-config
KOSSUTH-M1# copy tftp flash 192.168.1.10 N_11_25.swi secondary
KOSSUTH-M1# boot system flash secondary
```

A ProCurve eszközök más gyártók termékeihez hasonlóan out-of-band (soros port) és in-band (Telnet, SSH, HTTP) menedzselési módokat támogatnak, a biztonságos üzemeltetés miatt szükségszerű volt néhány korlátozást bevezetni. A nem biztonságos protokollokat biztonságos alternatívákra cseréltem. *[6]*

[29] Voice over IP, VoIP

Így lett Telnet helyett kizárólag SSH:

```
KOSSUTH-M1(config)# crypto key zeroize ssh
KOSSUTH-M1(config)# crypto key generate ssh rsa
KOSSUTH-M1(config)# ip ssh
KOSSUTH-M1(config)# no telnet-server
```

HTTP-ből HTTPS:

```
KOSSUTH-M1(config)# crypto key zeroize cert
KOSSUTH-M1(config)# crypto key generate cert rsa 1024
KOSSUTH-M1(config)# web-management ssl
KOSSUTH-M1(config)# no web-management plaintext
```

TFTP helyett SCP és SFTP:

```
KOSSUTH-M1(config)# ip ssh filetransfer
KOSSUTH-M1(config)# no tftp server
KOSSUTH-M1(config)# no tftp client
```

SNMPv2c-ből SNMPv3:

```
KOSSUTH-M1(config)# snmpv3 enable
KOSSUTH-M1(config)# snmpv3 restricted-access
KOSSUTH-M1(config)# snmpv3 only
KOSSUTH-M1(config)# snmpv3 user cacti
KOSSUTH-M1(config)# no snmpv3 user initial
KOSSUTH-M1(config)# snmpv3 group OperatorAuth user cacti sec-model ver3
KOSSUTH-M1(config)# no snmp-server community public Unrestricted
KOSSUTH-M1(config)# no snmp-server enable
```

Létrehoztam egy management VLAN-t is, amelybe a szerverszoba és az informatika tanári szoba tartozik. A management VLAN egy izolált virtuális alhálózat, amely a hálózat felügyeletére és hibaelhárításra használatos. *[8]*

```
KOSSUTH-M1(config)# vlan 10 name "Management"
KOSSUTH-M1(config)# vlan 10 ip address 192.168.1.1 255.255.255.0
KOSSUTH-M1(config)# vlan 10 tagged 3,5,19-20,22-24,Trk1
KOSSUTH-M1(config)# ip authorized-managers 192.168.1.0 255.255.255.0 access
manager access-method all
KOSSUTH-M1(config)# primary-vlan 10
KOSSUTH-M1(config)# management-vlan 10
```

Az eszközökön letiltottam a nem használt szolgáltatásokat, az LLDP felderítő-üzenetek küldését és fogadását a megfelelő portokra korlátoztam, és definiáltam egy bejelentkezés előtti figyelmeztető üzenetet. A tűzfalra telepítettem egy NTP időszervert, és beállítottam a szinkronizálást egy közeli „Stratum 2”-es kiszolgálóhoz. A tűzfal szolgáltatja a management VLAN-ban a pontos időt.

```
KOSSUTH-M1(config)# no cdp run
KOSSUTH-M1(config)# lldp admin-status 1-16 disable
KOSSUTH-M1(config)# banner motd "Belepes csak engedellyel! / Unauthorized access
prohibited."
KOSSUTH-M1(config)# time timezone 60
KOSSUTH-M1(config)# time daylight-time-rule Middle-Europe-and-Portugal
KOSSUTH-M1(config)# sntp server 192.168.1.10
KOSSUTH-M1(config)# sntp unicast
KOSSUTH-M1(config)# sntp 600
KOSSUTH-M1(config)# timesync sntp
```

Noha a HP eszközök „stacking” funkciója hasznos dolog, a biztonsággal szemben a könnyű kezelést tartja fontosabbnak. *[6]* Miután többszöri próbálkozással sem tudtam működésre bírni a management VLAN-ban, inkább kikapcsoltam a `no stack` paranccsal.

5.2.2 A LAN védelme

Meg kell említeni a fontosabb adatkapcsolati rétegbeli támadásokat és az ellenük való védekezési lehetőségeket.

MAC flooding: A támadás során egy portról olyan sok különböző feladó MAC címmel küldünk ki keretet, hogy a kapcsoló MAC-táblája telítődik. Ezután a kapcsoló hubként kezd viselkedni, azaz a beérkező kereteket minden portján továbbítja. A támadás eredményeképpen le tudjuk hallgatni más portok forgalmát. Védekezni ellene a `port-security` bekapcsolásával lehet: a `learn-mode` és `address-limit` paraméterekkel beállíthatjuk, hogy a választott porton hány címet „tanulhat meg” a kapcsoló, vagy magunk is megadhatjuk fixen a címeket; alkalmazhatjuk az előző kettő kombinációját is. *[1, 10]*

VLAN hopping (kettős címkézés): Ez a támadási forma a dolgozat korábbi szakaszában már ismertetett natív VLAN problémán alapul: lényege, hogy egy „access” porton kétszeresen címkézett keretet küldünk, ahol az egyik VLAN a kapcsoló trönkportjának natív VLAN-ja. Ezt a keretet a fogadó kapcsoló „rendes”, egyszeresen címkézett keretként érzékeli, és a támadó által kívánt VLAN-ba továbbítja. Megoldás a natív VLAN kikapcsolása vagy olyan natív VLAN választása, amelybe nem tartozik más switchport. *[10]*

ARP poisoning/spoofing: A támadó hamis ARP kereteket küld, amelyben az áldozat gép IP címéhez saját fizikai címét rendeli – így megpróbálja átvenni a szerepét. Ennek elkerülése érdekében célszerű konfigurálni az ARP Protection és a DHCP Snooping funkciókat. Utóbbi csak megbízható DHCP szerverek csomagjait engedi továbbítani, egyúttal a DHCP válaszok

vizsgálatával megtanulja az IP-MAC hozzárendeléseket. Az ARP Protection ellenőrzi, hogy helyes-e a hirdetett IP-MAC összerendelés, és a hamisított kereteket eldobja. *[6, 10]*

Feszítőfa-manipuláció: A támadó félrevezető BPDU-kat küld, amelyek befolyásolják a feszítőfa protokoll helyes működését. Ennek elkerülésére a megfelelő portokon aktiválni kell a BPDU-védelmet és a Root Guard funkciót. *[10]*

Egy ProCurve 2610-es kapcsoló védekezőképességei:

```
KOSSUTH-M2(config)# spanning-tree 52
 admin-edge-port       Set the administrative edge port status.
 auto-edge-port        Set the automatic edge port detection.
 bpdu-filter           Stop a specific port or ports from transmitting BPDUs,
                       receiving BPDUs, and assume a continuous fowarding
                       state.
 bpdu-protection       Disable the specific port or ports if the port(s)
                       receives STP BPDUs.
 hello-time            Set message transmission interval (in sec.) on the port.
 mcheck                Force the port to transmit RST BPDUs.
 path-cost             Set port's path cost value.
 point-to-point-mac    Set the administrative point-to-point status.
 priority              Set port priority (the value is in range of 0-240
                       divided into steps of 16 that are numbered from 0 to 15,
                       default is step 8).
 root-guard            Set port to ignore superior BPDUs to prevent it from
                       becoming Root Port.
 tcn-guard             Set port to stop propagating received topology changes
                       notifications and topology changes to other ports.
```

5.2.3 További javaslatok

További fejlesztésként implementálható egy fejlett AAA[30] központosított felhasználói adatbázissal (RADIUS[31] kiszolgáló) és többféle hozzáférési szinttel. Érdemes a kapcsolókon aktiválni az ARP-védelmet is: ez a szolgáltatás a DHCP Snooping eljárás segítségével megfigyeli a DHCP általi IP-MAC összerendeléseket. Később ezt az információt összeveti az ARP csomagokkal, a hamis csomagokat pedig kiszűri a hálózatból. *[6]* Ajánlott még beállítani a naplózást a `logging` paranccsal (Syslog szerverre) és különböző SNMP „csapdákat” (trap).

Minden hálózati eszköz jelszavát célszerű rövid időközönként új jelszóra cserélni, ügyelve a megfelelő hosszra és bonyolultságra. Rendszeresen felül kell vizsgálni a tűzfalbeállításokat, a

[30] Authentication, Authorization, Accounting
[31] Remote Authentication Dial In User Service

felhasználói adatbázist és a jogosultságokat. A visszaélések és jogviták elkerülése érdekében fontos egy részletes és pontos hálózatbiztonsági szabályzat megalkotása és betartatása, illetve a meglévő szabályzat aktualizálása. *[3]* Az eszközök fizikai védelme is elengedhetetlen, a kapcsolókon ezt szükség esetén ki lehet egészíteni a Password Clear és Factory Reset gombok letiltásával. Ez kockázatos művelet, ezért át kell gondolni, milyen alternatív helyreállító megoldások vannak.

Egy érdekesség: Ha sok eszköz között (vagy `snmp-server location` információ hiányában) szeretnénk megtalálni az éppen menedzselt eszközt, a `chassislocate` paranccsal bekapcsolhatjuk vagy villogtathatjuk a rajta lévő fényes Locator LED-et.

```
KOSSUTH-M1# chassislocate
 blink                Blink the chassis locate led (default 30 minutes).
 off                  Turn the chassis locate led off.
 on                   Turn the chassis locate led on (default 30 minutes).
```

5.3 Új logikai topológia

Egy nagyméretű hálózaton fontos szempont megfelelően kicsi üzenetszórási tartományok (broadcast domain) kialakítása. E tartományok összekapcsolását a forgalomirányítók végzik. A túl nagy tartományok elsősorban az adatkapcsolati réteg szintjén okoznak problémákat (LAN broadcast), a túl kicsik pedig feleslegesen terhelik a forgalomirányítókat. *[1]* A Kossuth Gimnázium hálózata szakdolgozatom készítésekor két üzenetszórási tartományból állt: 192.168.10.0/24 és 192.168.11.0/24. Utóbbiba a regisztrált munkaállomások, előbbibe a szerverek és a nem regisztrált, dinamikusan kiosztott IP című gépek tartoztak.

5.3.1 VLAN-ok

Ahogy egy vállalatnál vagy közintézményben, úgy egy iskolában is az ott dolgozó és tanuló személyek részére különböző beosztásokat, jogköröket definiálnak. Egy modern hálózatot is fel kell készíteni e jogosultságok betartatására, azaz szabályozni kell a hozzáférést, válaszolva azokra a kérdésekre, hogy ki mikor mihez és hogyan férhet hozzá.

A fenti két kritériumot – kis üzenetszórási tartományok és hozzáférés-szabályozás – figyelembe véve több virtuális alhálózat kialakítására tettem javaslatot. Egy ilyen alhálózatot olyan berendezések alkotnak, amelyek fizikai elhelyezkedésüktől függetlenül úgy kommunikálnak egymással, hogy azonos üzenetszórási tartományban vannak.

Egy VLAN ugyanazokkal a jellemzőkkel bír, mint egy fizikai helyi hálózat (LAN), de lehetővé teszi az eszközök együtt kezelését még akkor is, ha nem ugyanarra a kapcsolóra csatlakoznak. A hálózat átkonfigurálása – azaz az eszközök átsorolása – az eszközök fizikai áthelyezése nélkül, szoftveresen is végrehajtható. *[1, 3]*

VLAN	Név	Címtartomány	Felhasználási területek
10	Management	192.168.1.0/24	Kapcsolók, szerverek, inf. tanári szobák
20	Igazgatás	192.168.2.0/24	Igazgatás, titkárság, iskolaszék
30	Tanár	192.168.3.0/24	Tanári szobák, dohányzók, szertárak
40	Diák	192.168.4.0/24	Tantermek, inf. termek, laborok, könyvtár
50	Egyéb	192.168.5.0/24	Iskolaorvos, fénymásoló
60	Nyilvános	192.168.6.0/24	Porta, büfé
70	Nyomtató	192.168.7.0/24	Hálózati nyomtatók

Ahogy a táblázatban olvasható, ez a kiosztás nem közvetlenül a felhasználókat, hanem az intézmény helyiségeit sorolja VLAN-okba. A módszer előnye, hogy könnyen megvalósítható, hátránya, hogy a hálózati szolgáltatások védelme érdekében felhasználó-hitelesítés szükséges. Szerencsére ez az LDAP révén már adott.

Az 1-es alhálózat a szervertermet és az informatikatanári dolgozószobát tartalmazza, továbbá minden kapcsolót innen lehet adminisztrálni. A távoli elérés biztosítása érdekében a tűzfalnak is van egy IP címe ebben a hálózatban, amely alapértelmezett átjáró az internet felé. A távoli menedzsment során először SSH kapcsolatot létesítünk a tűzfallal, majd innen egy másikat a megfelelő switchre.

A 2-es alhálózat az igazgatási épület szinte minden helyiségét magába foglalja. A cél az, hogy az iskola működéséhez legfontosabb adatok biztonságban legyenek, elérésük legyen tiltott a hálózat többi részéből.

Magától értetődő elkülöníteni a tanárok és a diákok számítógépeit, erre szolgál a 30-as és a 40-es VLAN. A diák VLAN-ban ügyelni kell az IP címkiosztásra, ugyanis szükséges az, hogy az informatika tantermekben (termenként külön) letiltható legyen a tanulók számára az internet-hozzáférés. Ez a tűzfalon az `iptables` konfiguráció ideiglenes megváltoztatásával oldható meg.

Az 5-ös alhálózatba azok a szolgáltatók kerülnek, akiket védeni kell a diák számítógépektől (vírusok, férgek, támadás), de akiktől védeni kell a tanári és igazgatási VLAN-t, ugyanakkor hozzáférésük lehet a szerverekhez. A VLAN 60 speciális alhálózat, amelyből a szerverek nem, csak az internet érhető el. Az átjáró itt is a tűzfal. A jövőben használható lesz például nyílt Wi-Fi hálózathoz. A 70-es VLAN-ba kerülnek a hálózati nyomtatók, amelyeknek az igazgatási, tanári és diák alhálózatokból elérhetőnek kell lenniük.

A tűzfalnak minden VLAN-ban van IP címe (192.168.x.1, ahol x=VID/10). Ez az alapértelmezett átjáró, és hálózati címfordítást végez az internet felé. A szervereknek is minden VLAN-ban van IP címük (Samba: 192.168.x.248, Server: 192.168.x.252), kivéve a 60-asben és a 70-esben, ahonnan az M2 switch DHCP Relay funkciót végez (`ip helper-address 192.168.1.248`).

Linux kiszolgálókon az IEEE 802.1Q VLAN-ok megvalósítása nagyon egyszerű; Debian alapú disztribúciókon a címkézés támogatásához be kell töltenünk a megfelelő kernel modult a `modprobe 8021q` paranccsal (rendszerindításkori betöltéshez a `/etc/modules` fájlba be kell írnunk a `8021q` sort). Az alinterfészek kialakításához a `/etc/network/interfaces` fájlba be kell írnunk az IP címet, hálózati maszkot és opcionálisan az átjáró címét:

```
auto eth0.20
iface eth0.20 inet static
    address 192.168.2.252
    netmask 255.255.255.0
    gateway 192.168.2.1
```

Miután telepítettük a `vconfig` segédprogramot (`apt-get install vlan`), a VLAN címkézés beállításához és az alinterfész bekapcsolásához az alábbiakat kell végrehajtani, majd meggyőződni a sikeres működésről:

```
server:/# vconfig add eth0 20
server:/# ifup eth0.20
server:/# ifconfig eth0.20
eth0.20   Link encap:Ethernet  HWaddr 00:22:15:8f:3b:82
          inet addr:192.168.2.252  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::222:15ff:fe8f:3b82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7242 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1709399 (1.6 MiB)  TX bytes:798 (798.0 B)
```

5.3.2 Forgalomirányítás

A VLAN-ok között minimális forgalomirányításra van szükség, de érdemes megvizsgálni a lehetőségeket. Az átjárást biztonsági okokból korlátozni kell, amire kézenfekvő megoldás lenne néhány VACL[32]. Sajnos a jelenlegi eszközparkban a ProCurve 2810 és 2626 egyáltalán nem támogat ACL-eket, a Procurve 2610 pedig csak portszintű bejövő irányú listát kezel a VLAN-tagságra való tekintet nélkül. *[14, 15, 16]* Ahhoz tehát, hogy egy 2610-es kapcsolón korlátozzuk a VLAN-ok közötti forgalmat, a kapcsoló minden interfészére alkalmaznunk kellene a listát, ami jelentős terhelést okoz.

Sokkal egyszerűbb módszer erre a célra a tűzfalat használni. Ebben az esetben a VLAN-ok közötti forgalomirányításra[33] használható sávszélesség a huszadára csökken – 2 gigabitről 100 megabitre másodpercenként, és bele kell kalkulálni az internet irányú forgalmat is –, de ez vállalható áldozat: vegyük figyelembe, hogy ilyen jellegű forgalomirányításra gyakorlatilag csak a nyomtatók VLAN-ja miatt van szükség. Hosszú távon azonban mindenképpen ajánlott egy vagy több forgalomirányító beüzemelése.

5.3.3 DHCP

Mivel a szerverek VLAN-címkézve kapják a kéréseket, a DHCP beállítása viszonylag egyszerű. Alább látható egy részlet a Linux alapú DHCP szerver konfigurációjából (`dhcpd.conf`): A 60-as VLAN-ban a megadott tartományból ad címet, a management VLAN-ban pedig (és a többiben is a nyilvános kivételével) statikusan osztja ki az IP címeket a MAC cím alapján; a címlistát egy külön fájl tartalmazza.

```
# VLAN 60 (Nyilvanos)
subnet 192.168.6.0 netmask 255.255.255.0 {
    range 192.168.6.11 192.168.6.239;
    allow unknown-clients;
    option broadcast-address    192.168.6.255;
    option routers              192.168.6.1;
    option domain-name-servers  195.199.255.4, 195.199.255.57;
    option domain-name          "pub.klte-gyakorlo.sulinet.hu";
}
```

[32] VLAN ACL
[33] inter-VLAN routing

```
# VLAN 10 (Management)
subnet 192.168.1.0 netmask 255.255.255.0 {
    deny unknown-clients;
    option broadcast-address    192.168.1.255;
    option routers              192.168.1.1;
    option domain-name-servers  192.168.1.248, 192.168.1.252, 195.199.255.4,
195.199.255.57;
    option domain-name          "mgmt.klte-gyakorlo.sulinet.hu";
    option netbios-name-servers 192.168.1.248;
    option netbios-dd-server    192.168.1.248;
    option netbios-node-type    8;
    option netbios-scope        "";
    include                     "/etc/dhcpd.conf-mgmt";
}
```

5.3.4 DNS

A DNS szerver beállításánál a split DNS technika alkalmazható, azaz különböző IP tartományokból érkező kérésekre különböző címeket adunk vissza eredményül. Ezt úgy tehetjük meg, hogy a konfigurációs fájlban (például `/etc/bind/named.conf.local`) nézeteket (`view`) definiálunk az alhálózatoknak megfelelően, és ezekbe helyezzük a zónákat.

5.3.5 QoS

A hálózaton megvalósítható a szolgáltatásminőség, azaz a Quality of Service. A MAC alrétegben az IEEE 802.1p, a hálózati rétegben a ToS (Type of Service) és a DiffServ (Differentiated Services) megoldás alkalmazható. A 802.1p esetén a csomagok osztályozása és továbbítása a már ismertetett módon történik. A prioritás-hozzárendelés szempontjai lehetnek: VLAN ID, forrás és cél IP címe, TCP[34] és UDP[35] portszám, bejövő keret EtherType mezőjének, 802.1p címkéjének vagy IP ToS mezőjének értéke vagy az interfész sorszáma. A továbbítás súlyozott Round-Robin elven zajlik. *[1]*

Néhány gyakorlati példa ProCurve eszközökön:

- **VLAN szerint:** `vlan 20 qos priority 7`
- **IP cím szerint:** `qos device-priority 192.168.2.100 priority 7`
- **Interfész száma szerint:** `int 52 qos priority 7`

[34] Transmission Control Protocol
[35] User Datagram Protocol

További finomhangolásra nyílik lehetőség a `rate-limit` és (egyes eszközökön) a `bandwidth-min output` interfészkonfigurációs parancsokkal. A helyes működéshez a csomag prioritását a forrástól a címzettig minden állomáson biztosítani kell. *[1]*

5.3.6 További javaslatok

Későbbi fejlesztésként megfontolandó, hogy a switchportokat dinamikusan, az aktuális felhasználó alapján soroljuk be a VLAN-okba. Erre alkalmas például az IEEE 802.1X[36] szabvány, amely RADIUS szerverrel és EAP hitelesítő protokollal működik.

Fel kell készülni továbbá az IPv4 címtartomány telítődésére és az IPv6-átállásra. Bár a NAT egy időre megoldást jelent, hosszú távon az újgenerációs IP protokoll előnyösebb. Az átállás nem olcsó: új hardverekre (kapcsoló, forgalomirányító) van szükség, és a Windows XP operációs rendszert is le kell cserélni. Az IPv6 LAN és WAN előnye azonban a v6-os címek natív elérhetősége és a címfordítás szükségtelenné válása.

5.4 Vezeték nélküli hozzáférés

Az internetes szolgáltatások terjedésével – különösen az ezredforduló után – megnőtt az igény a vezeték nélküli hálózatokra. A mai egyetemi hallgatók még „tanulták” a Web 2.0-t, azaz a közösségi webet, a mostani középiskolások azonban már beleszülettek, és aktívan használják a szolgáltatásait, igénylik a világhálót mint információforrást és kapcsolattartási felületet. Nemcsak emiatt, de az iskolai dolgozók mobilitása és munkavégzésének megkönnyítése érdekében is javaslom egy WLAN kialakítását a gimnázium területén. Felhasználási terület lehet még a sportcsarnokban rendezett versenyekről (pl. megyei és országos) való közvetítés.

A lefedettséget úgy kell megvalósítani, hogy az iskolában zajló oktatást ne zavarja – azaz a tantermekből a diákok óra közben ne tudjanak rácsatlakozni a hálózatra. A hozzáférési pontokat ennek megfelelően kell elhelyezni, a jelerősséget finomhangolni, esetleg irányított antennákat alkalmazni. Áramellátásuk PoE technológiával biztosítható, ha a kábelek hossza megfelelő.

„Okos” hozzáférési pontok alkalmazásával több SSID-t[37] hozhatunk létre, például egy nyilvánost (VLAN 60), amelyből csak az internet érhető el és egy védettet a tanárok és az

[36] Port-based Network Access Control, PNAC

igazgatóság számára. Könnyen elérhető védelmet ma az IEEE 802.11i szabvány alkalmazása jelenti, azaz a WPA2-AES[38] titkosítás. Az autentikáció működhet előre megosztott kulcs[39] vagy kiterjeszthető hitelesítő protokoll[40] alapján, de ilyen környezetben inkább az utóbbi használata ajánlott.

Olcsóbb megoldásként üzemeltethetők SOHO, azaz otthoni és irodai használatra készült hozzáférési pontok is, de ebben az esetben a konfiguráció és az adminisztráció nehézkes, a VLAN- és multi-SSID támogatás kérdéses, általában a jelerősség nem állítható és az áramellátás sem oldható meg Power over Ethernettel, továbbá az átviteli teljesítménnyel is gondok lehetnek.

A Wi-Fi AP-k általam javasolt elhelyezési pontjai:

- Igazgatási épület, 1. emelet: védett
- Főépület, földszint (büfé): nyílt
- Főépület, 1. és 2. emelet („zsibongó”): nyílt
- Humán épület, 1. emelet (informatika): védett és nyílt
- Tornacsarnok: nyílt

5.5 Wide Area Network

A sebességmérés számokban mérhetővé tette azt, amiről az iskola dolgozói személyes beszélgetéseink során már említést tettek: „a hálózat lassú”. Szakszerűbben megfogalmazva: a WAN, vagyis az internetirányú le- és feltöltési sávszélesség kicsi. A Sulinet nem követte a munkaállomások számának és a felhasználói igényeknek a növekedését, így alakult ki az a helyzet, hogy a gyakorlatban 4,5 Mbps letöltési és 0,2 Mbps feltöltési sebességen száznál is több felhasználó osztozik.

Égető szükség lenne a gimnáziumban egy gyorsabb internetkapcsolatra. A Sulinet által alkalmazott ADSL-t egyre inkább felváltja az újabb, gyorsabb és megbízhatóbb optikai átvitel. Ha a pénzügyi feltételek adottak, érdemes megfontolni a szerződést egy második internetszolgáltatóval.

---

[37] Service Set Identifier
[38] Wi-Fi Protected Access, Advanced Encryption Standard
[39] Pre-Shared Key, PSK
[40] Extensible Authentication Protocol, EAP

6 Összefoglalás

Szakdolgozatom elkészítése során feladatom az volt, hogy felmérjem a Debreceni Egyetem Kossuth Lajos Gyakorló Gimnáziuma számítógép-hálózatának helyzetét, elemezzem a működését, majd a tapasztalatok alapján javaslatokat tegyek továbbfejlesztésére.

A hálózat kialakítása a 2000. évben történt, amikor a szélessávú internet-hozzáférés éppen csak terjedni kezdett Magyarországon. Ezt figyelembe véve a hálózat jelenlegi formájában a lehetőségekhez mérten fizikailag jól felépített, ám redundanciát nem tartalmaz. Noha az általam elvégzett terhelés- és forgalommérés adatai alapján az épületközi vonalak és a szerverek nincsenek teljesen kihasználva, a következő években a felhasználói igények növekedése miatt és a multimédiás oktatás elterjedésével ezek az értékek várhatóan emelkedni fognak. A jövőbeli fejlesztéseknél célszerű tehát megfontolni redundáns linkek létesítését az épületek között. E leendő kapcsolatok kihasználása megoldható feszítőfa-protokollok és linkaggregáció alkalmazásával. A rendelkezésre állás tovább növelhető a szünetmentes tápegységek jobb kihasználásával.

A vizsgált hálózat kvázi „lapos”: két üzenetszórási tartományt tartalmaz minimális átmenő forgalommal a tartományok között. A meglévő közvetítő eszközök képességei elegendők egy ilyen hálózat működtetéséhez; modern, virtuális alhálózatok optimális kialakításához azonban szükség lenne „intelligens”, Layer 3-as kapcsolókra és forgalomirányítóra. A VLAN-ok lehetővé teszik a nagyméretű hálózat felosztását kisebb üzenetszórási tartományokra, az azonos jogosultságú munkaállomások csoportosítását. A csoportok közötti forgalom szűrése hozzáférési listákkal biztosítható. A szolgáltatásminőség szabványok (QoS) lehetővé teszik a helyi hálózaton a keretek és csomagok végponttól végpontig történő előnyben részesítését, a sávszélesség biztosítását. (Internetirányú forgalom esetén ISP általi támogatás szükséges.)

A kapcsolók fizikai védelme megfelelő, a dolgozatomban ismertetett és elvégzett módosításokkal biztonságos felügyeletük is megoldott. A portbiztonság megvalósításával a hálózat védhető a leggyakoribb második és harmadik rétegbeli támadásoktól. A fokozott hálózatbiztonság érdekében érdemes bevezetni az adatbázis-alapú hitelesítést és hozzáférés-szabályozást. Jogi szempontból fontos a hálózat biztonsági szabályzatának naprakészen tartása és betartatása.

Az iskola informatikai infrastruktúrájának fejlesztése vagy a használaton kívüli épület felújítása jó alkalom lenne a IP telefon és Power over Ethernet technológiák bevezetésére. Használatuk csökkenti a kábelezési költségeket, egyúttal kezelhetőbbé teszi a hálózatot. A PoE alkalmazásával a vezeték nélküli hálózat kialakítása is olcsóbb és egyszerűbb.

Gyorsabb internet-hozzáféréssel javítható a felhasználói élmény mind az iskola dolgozói és diákjai mind a iskolahonlap látogatói szempontjából.

7 Irodalom- és forrásjegyzék

Könyvek

- Andrew S. Tanenbaum: Számítógép-hálózatok, 4. kiadás, Panem-Prentice Hall Könyvkiadó Kft., 2003
- **[1]** ProCurve Adaptive EDGE Fundamentals Student Guide (Technical Training), Version 8.41, Hewlett-Packard Development Company, 2008

Elektronikus dokumentumok (2010. november 15.)

- **[2]** Dr. Almási Béla: Számítógép-hálózatok oktatási segédanyag, 2006 http://irh.inf.unideb.hu/user/almasi/cn/halozat.pdf
- **[3]** Cisco CCNA Exploration 4.0 elektronikus tananyag (Cisco Network Academy) http://cisco.netacad.net *(védett)*
- **[4]** Sulinet – Szolgáltatás ismertető v3.0 http://www.kozhaloportal.hu/docs/KHP_SI_Szolgaltatas-ismerteto_3v0.pdf
- **[5]** Közháló Szolgáltatás Felügyelet – Végponti technikai információk http://www.kozhaloportal.hu/docs/kozhalo3_muszaki_reszletek.pdf
- **[6]** Hardening ProCurve Switches Technical White Paper http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA2-6603ENW.pdf
- **[7]** HP Multiple Instance Spanning-Tree Operation http://cdn.procurve.com/training/Manuals/3500-5400-6200-8200-ATG-Jan08-4-MSTP.pdf
- **[8]** White Paper: IronShield Best Practices – Management VLANs http://www.genesisglobalinc.com/PDF/foundry-management-vlans.pdf

Internetes oldalak

- **[9]** DE Kossuth Lajos Gyakorló Gimnáziuma – Iskolatörténet http://www.klte-gyakorlo.sulinet.hu/files/iskolatort.html (2010. május 8.)
- **[10]** Cisco VLAN Security White Paper http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0918 6a008013159f.shtml (2010. október 29.)
- **[11]** IEEE 802.1 – Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/IEEE_802.1 (2010. október 28.)

- **[12]** Fast Ethernet – Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Fast_Ethernet (2010. október 28.)
- **[13]** Gigabit Ethernet – Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Gigabit_Ethernet (2010. október 28.)

Adatlapok és technikai leírások (2010. szeptember 22.)

ProCurve Switch 2600 Series

- **[14]** DataSheet http://h10144.www1.hp.com/products/pdfs/datasheets/ProCurve_Switch_2600_Series.pdf
- Installation and Getting Started Guide http://cdn.procurve.com/training/Manuals/2600-Install-Jan08-59912165.pdf
- Management and Configuration Guide http://ftp.hp.com/pub/networking/software/2600-2800-4100-6108-MgmtConfig-Oct2005-59906023.pdf
- Access Security Guide http://cdn.procurve.com/training/Manuals/2600-2800-4100-6108-Security-Dec2008-59906024.pdf
- Advanced Traffic Management Guide http://ftp.hp.com/pub/networking/software/2600-2800-4100-6108-AdvTraff-Oct2005-59908853.pdf

ProCurve Switch 2610 Series

- **[15]** DataSheet http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA0-7397ENW.pdf
- Installation and Getting Started Guide http://cdn.procurve.com/training/Manuals/2610-InstGde-July2009-59918573.pdf
- Management and Configuration Guide http://cdn.procurve.com/training/Manuals/2610-MCG-Sept09-R_11_40-59918640.pdf
- Access Security Guide http://cdn.procurve.com/training/Manuals/2610-Security-Oct2008-59918642.pdf
- Advanced Traffic Management Guide http://cdn.procurve.com/training/Manuals/2610-AdvTrafficMgmt-Dec2007-59918641.pdf

ProCurve Switch 2810 Series

- **[16]** DataSheet
  http://h10144.www1.hp.com/products/pdfs/datasheets/ProCurve_Switch_2810_Series.pdf
- Installation and Getting Started Guide
  http://ftp.hp.com/pub/networking/software/2810-Install-May2006-59913843.pdf
- Management and Configuration Guide
  http://ftp.hp.com/pub/networking/software/2810-MgmtCfg-July2007-59914732.pdf
- Access Security Guide
  http://ftp.hp.com/pub/networking/software/2810-Security-July2007-59914734.pdf
- Advanced Traffic Management Guide
  http://ftp.hp.com/pub/networking/software/2810-AdvTrafficMgmt-July2007-59914733.pdf

Képek forrása (2010. november 11.)

5. oldal: Iskolai archívum

7. oldal: Saját készítésű ábra

8. oldal: Saját készítésű fénykép

10. oldal: http://www.senetic.com/product/J9021A

12. oldal: http://en.wikipedia.org/wiki/File:TCPIP_802.1Q.jpg

14. oldal: http://en.wikipedia.org/wiki/File:Link_Aggregation1.JPG

16. oldal: http://en.wikipedia.org/wiki/File:Spanning_tree_protocol_at_work_6.svg

18. oldal: http://www.cisco.com/en/US/i/000001-100000/65001-70000/68001-69000/68285.jpg

19. oldal: Saját készítésű fénykép

25. oldal: Saját készítésű ábra *(Program: Cisco Packet Tracer)*

28. oldal: Saját készítésű képernyőkép

33-34. oldal: Saját készítésű grafikonok *(Program: Cacti)*