DIPLOMAMUNKA

Balla Tamás

Debrecen

2010

Debreceni Egyetem

Informatikai Kar

Számítógépes hálózat fejlesztés a DE Műszaki Karán

Témavezető:
Dr. Almási Béla
egyetemi docens

Készítette:
Balla Tamás
Programtervező Informatika MSc

Debrecen
2010

Tartalomjegyzék

1. Bevezetés

Napjainkban azt a világot éljük, amikor a különböző informatikai szolgáltatások minősége nagyban függ az adathálózattól. A napról napra bővülő hálózati alkalmazások egyre megbízhatóbb adathálózatot, nagy sávszélességet igényelnek. Ezen felül nem lehet figyelmen kívül hagyni a szolgáltatások minőségét sem, néha szükséges a csomagok egymástól való megkülönböztetése. Nagyon jó példa erre az utóbbi időben elterjedt valamennyi VoIP, videokonferencia, streaming alkalmazás. Ezeknek a szoftvereknek a működéséhez gyakran szükség lehet dedikált sávszélességre, hogy fennakadás nélkül élvezhessék a felhasználók őket. A ma még használatos egyes analóg szolgáltatások előbb utóbb IP alapúra fognak cserélődni. A gyártók is arra törekszenek, hogy folyamatosan egyre újabb és újabb szolgáltatásokat fejlesszenek ki és értékesítsenek. Az új technológiák gyakran nem csak jobbak elődjüknél hanem sokkal költséghatékonyabbak is, ilyen például a video konferencia.

Dolgozatom egy jelenleg üzemelő nagysebességű, akadémiai hálózatot mutat be, melyet a TIOP 1.3.1 – „Természettudományi és műszaki képzés infrastruktúrájának fejlesztése” (A felsőoktatási tevékenységek színvonalának emeléséhez szükséges infrastrukturális és informatikai fejlesztések támogatása) pályázat keretein belül sikerült a mai kor elvárásainak megfelelő szintre fejleszteni.
Azért választottam ezt a témát, mivel a DE Informatikai Szolgáltató Központ dolgozójaként az utóbbi évek egyik leglátványosabb infrastruktúrai fejlesztését mutathatom be a szakdolgozatom keretén belül.

A Debreceni Egyetem Műszaki Karának hálózata idén jelentős átalakuláson esett át. Mivel az elmúlt évek során az eszközpark idejét múlttá vált, nem volt képes az egyre növekedő felhasználói igényeket kielégíteni. Igaz, a kollégium épület strukturált hálózata 2004 –ben a HEFOP 4.1.2 pályázat részeként már átesett bizonyos fejlesztéseken viszont a mostani projekt részeként tovább szélesedik a hallgatók által elérhető szolgáltatások spektruma. Ezen felül a hálózat áteresztőképessége is jelentősen megnő.

A dolgozatban végigelemezem az alapvető LAN környezetben alkalmazott technológiákat, majd a régi hálózat működését, kitérve a hiányosságokra, esetleges hibákra, hibaforrásokra, majd az új rendszert mutatom be. Ahol szükséges ott ábrákkal és képekkel teszem könnyebben érthetővé az adott témát. Az 1.számú mellékletben összeszedtem a dolgozatban szereplő rövidítések listáját is.

2. Alapvető LAN környezetben alkalmazott technológiák

2.1. Útválasztás (routing)

Az Interneten az egyik legfontosabb feladat, a csomagok továbbítása másnéven a routing. Általában a feladó és cél számítógép között nincs közvetlen fizikai kapcsolat. Ezért ha a feladó egy csomagot el akar egy címzetthez juttatni, akkor ez több számítógépen (roteren) áthalad, amíg a címzetthez megérkezik. Az út (route, vagy path) azoknak a gépeknek a sorrendje, amelyeken a datagram áthalad. Ez a folyamat pontosan úgy zajlik, mint ha több ember állna egymás mellett egy sorban, és az egyik szélső a másik szélsőnek küldene egy csomagot. A datagram-ok továbbküldését ú.n. „útválasztó" - router - eszközök végzik. Az Internet rétegnek fel kell ismernie, hogy az adott datagram melyik hálózatból jött, és el kell döntenie, hogy a melyik interfacen kell továbbküldeni. Ezt a döntést a számítógép az útválasztási táblában (routing table) tárolt információk alapján határozza meg.

A routing az a folyamat, ami során egy hálózati protokoll (3. réteg) egy csomagja a kapcsológépek (router-ek) sorozatán keresztül a feladótól eljut a címzettig. A folyamathoz szükséges, hogy a router-ek kommunikáljanak egymással, hogy döntést tudjanak hozni abban, hogy egy adott cél felé melyik irány vezet. A hálózati protokollokat (IP, IPX, AppleTalk, stb.) route-olt protokollnak, míg a router-ek egymás közötti kommunikációját bonyolító protokollt routing protokollnak nevezzük. A routing protokoll a kommunikáció módjainak lerögzítése mellett meghatározza az útvonalválasztás mikéntjét is

A router minden link-jéhez egy interface-en keresztül kapcsolódik. A csomagok kapcsolása mindig a routing tábla alapján történik, ami <cél, kimenő interface> párokból áll. A beérkezett csomagot ennek a táblázatnak a segítségével, a cél alapján többnyire egy gyors, berendezés-orientált áramkör kapcsolja a kimenetre. . A routing protokollok feladata, a routing táblát előállítsák. A protokollokat a routerben általában egy erre a célra elkülönített célprocesszor futtatja.

A hálózat topológiáját egy gráf írja le, melyben a pontok router-ek és link-ek (amelyek a rájuk kapcsolt állomásokat összefoglalóan jelentik), az élek azt fejezik ki, hogy a router kapcsolódik az adott link-re. Ebben a gráfban a routing protokol határozza meg a csomag útját. Ha több út is lehetséges, akkor a több út közül a valamilyen szemszögből nézve a legjobbat kell kiválasztani.

A kiválasztás szempontjai lehetnek:

- távközlési szabályok vagy politikai megfontolások
- az út hossza (hány link-en vezet át)
- költség
- késleltetés
- sávszélesség
- megbízhatóság (csomagveszteség)
- az adott útvonal terheltsége

A fenti szempontok valamilyen kombinációjaként adódik az útvonal. Az is lehetséges és sokszor szükséges, hogy az útvonalak között megosszuk a forgalmat, tehát nem egyiket vagy másikat priorizáljuk, hanem mindkettőt használjuk valamilyen mértékben, ezt terheléseolsztásnak (load balancing) nevezzük.

A nagy csomagkapcsolt hálózatokban (az Internetben) igen sok célpont felé kell utat ismerni. Ez nagyméretű táblázatokat eredményez, ezért célszerű az egy csoportban lévő hálózatokat összefogni és egy egységként kezelni.

2.2. Keretkapcsolás (Switching)

A switch az az eszköz mely egy számítógép-hálózat strukturáltságát, szegmentálhatóságát hatékonyabbá teszi. A bridge-ekhez hasonlítanak, annyiban térnek el egymástól, hogy a switch képes bármely két portját összekötni egymással a többi porttól teljesen függetlenül, ezáltal a maximális sávszélesség nem csökken. Általában a switcheknek van egy vagy több nagysebességű portja is. A lokális hálózatok építőeleme, feladata sokrétű és néha nagyon összetett is lehet. Feladatai közé tartozik a hálózat szegmensei közötti kommunikáció biztosítása, a hálózat terheltségének csökkentése.

A swicth képes a portjai között egymástól függetlenül is kereteket továbbítani. Tehát egy Ethernet switch 3. és 4. portja képes a teljes 100 Mbit/s-os sebességgel kommunikálni, mialatt az 5. és 6. port között szintén a maximális sebességgel futhatnak az adatok. A switch tehát igény szerint kapcsol össze két portot, ami által csökken az ütközések száma és nő a rendelkezésre álló sávszélesség.

A switchek használatával együtt elterjedt a VLAN technológia is. Ennek lényege, hogy a valóságban egymással kapcsolatot teremteni tudó sok állomás között több virtuális LAN-t definiálhatunk, amelyek egymással képtelenek a 2. rétegbeli kapcsolatteremtésre, azaz az egyik VLAN-ból nem küldhetünk keretet egy másikba. Ezzel azt a hatást érjük el, mintha több, egymástól független LAN hálózatunk lenne. A különböző VLAN-ok tagjai egymással egy 3. szintű berendezés, a router segítségével teremthetnek kapcsolatot, ekkor

a hálózati protokoll csomagját LAN keretbe csomagoljuk és a VLAN-on belül elküldjük a routernek. A router a hálózati protokoll címe alapján kiválasztja a cél-VLAN-t, azon belül a cél MAC címet, LAN keretbe csomagolja a csomagot és elküldi a célállomásnak.

Ha valamelyik állomás az épületen belül fizikailag helyet változtat, csupán a megfelelő switcheket szükséges konfigurálni. A VLAN technológiával rengeteg munkát megtakarítunk, a hálózat áttekinthetőbb, fenntartása pedig olcsóbb.

A 2. és 3. rétegbeli kapcsolási funkciót (switching és routing) egyesítve kapjuk a multilayer switcheket. Ezek portjaik bizonyos csoportjain belül a 2. szinten switching funkciót töltenek be (az egy csoportba tartozó portok tagjai 1 VLAN-nak), a csoportok között pedig routeolni képesek, ha felismerik a hálózati protokollt. A jelenlegi multiprotocol routerek általában több hálózati protokollt képesek route-olni, általában több routing protokollt (RIP, OSPF, IGRP, EIGRP…) ismerve. A multilayer switchek tipikus felhasználási területe az akadémiai hálózat.

2.3. Hálózatfelügyelet

Minél több embert szolgál ki egy számítógépes rendszer, minél több feladatot bíznak rá, annál nagyobb gondot okoz, ha valami miatt nem megfelelően működik, esetleg leáll. Az esetleges hiba okozta kár csökkentésének számos lehetőségét adják a hálózatfelügyelő eszközök, megoldások. A hálózatfelügyelő eszköz valamilyen modellt valósít meg. A modellben felügyelt objektumok vannak, amibe minden beletartozik, amit működés közben valamilyen módon meg tudunk figyelni. Maga a felügyelet folyamata a felügyelő állomáson zajlik, ahol a magas szintű alkalmazás fut, amely összegyűjti, raktározza, elemzi a hálózat működését jellemző adatokat, a berendezések állapotát mutató paraméterektől az adatforgalom számáig. A felügyelő állomást ágensek, azaz adatgyűjtő programok látják el információval.

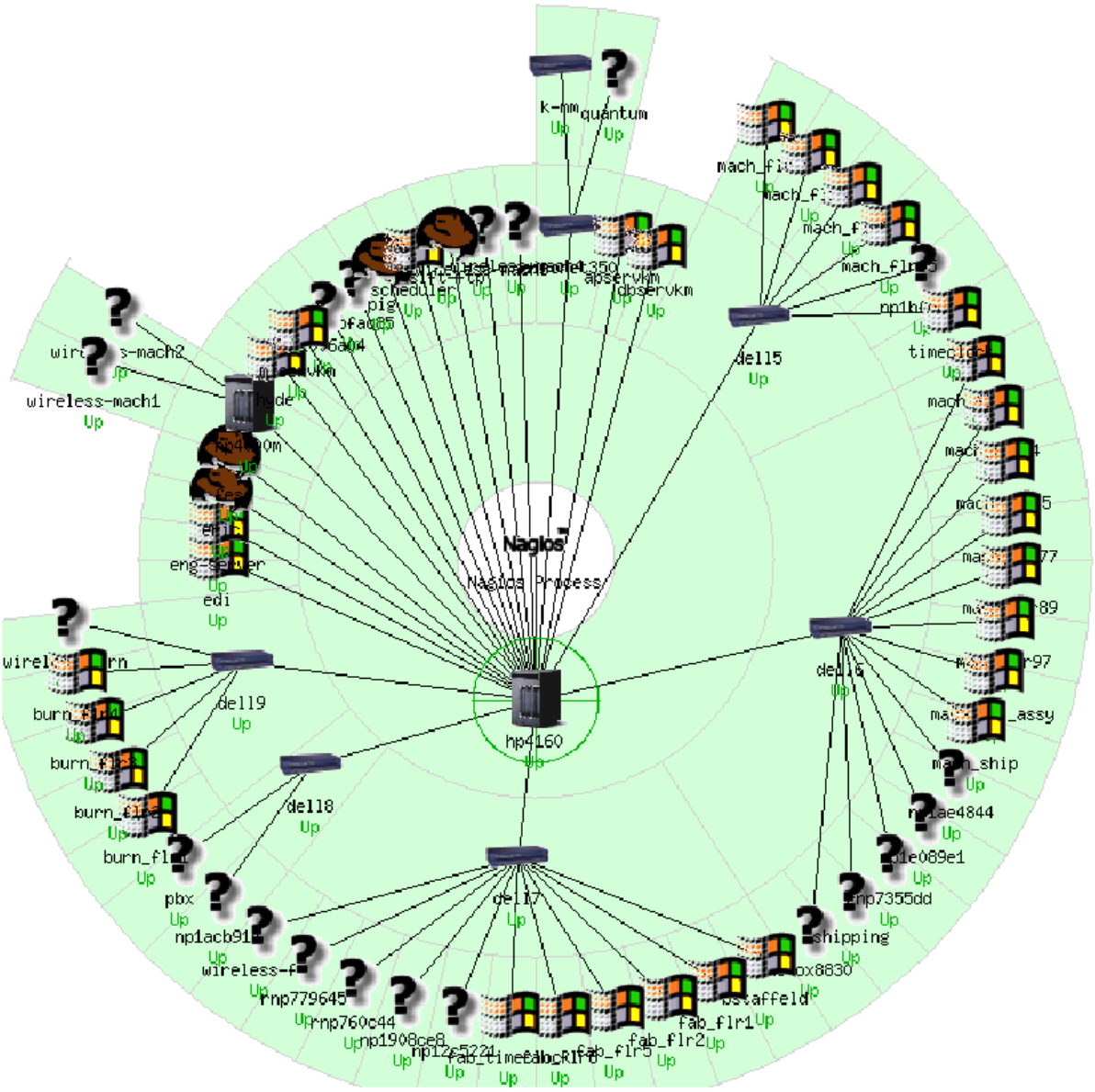
A hálózatfelügyelet érdekes területe a távoli felügyelet. Miután minden jelzést és vezérlési utasítást adatcsomagok közvetítenek, nincs szükség arra, hogy fizikailag ugyanott legyen a hálózat és a hálózatintézőt szolgáló program.

Napjainkban többféle hálózat menedzsmentre alkalmas megoldással találkozhatunk. Léteznek kereskedelmi célú szoftverek, és nyílt forrású eszközök is. Az akadémiai környezet főleg az „Open Source” megoldásokból építkezik. A következőkben röviden szeretném ismertetni ezeket a megoldásokat.

2.3.1. Nagios alapú felügyeleti rendszer

A Nagios egy hálózati szolgáltatásfelügyelő alkalmazás. Feladata, hogy figyelemmel kövesse az informatikai rendszer működését, és ha valahol rendellenességet észlel, akkor automatán értesítse az érintett személyeket. Képes több száz gép és szolgáltatás egyidejű figyelésére, többféle figyelmeztetési eljárást alkalmaz, a leggyakoribbak: e-mail, SMS, hangjelzés stb. Az üzemeltetők web és wap felületen is nyomon követhetik az egyes szolgáltatások, eszközök állapotait. Maga a program elég sokféle funkciót képes ellátni. Egyrészt képes az egyes hálózati szolgáltatások (SMTP, POP3, HTTP, NNTP, PING, stb.) figyelésére adott csomópontban, de képes a csomópontok más tulajdonságait is összegyűjteni: csomópont erőforrásai, környezete, stb. Mindezt az információt jól áttekinthető webes interfészen keresztül jeleníti meg. Az egyes csomópontok, vagy szolgáltatásaik kiesése - és helyreállása - esetén képes riasztásokat küldeni akár más-más személyeknek is (az érintett csomóponttól vagy szolgáltatástól függően). Az ilyen problémák jelentkezése esetén nem csak értesítéseket tud küldeni, hanem előre definiált lépéseket is képes tenni a probléma orvoslása végett. Akár még azt is meg lehet adni neki, hogy mikor történik üzemszerű leállás, ezekben az esetekben nem riaszt. Lehetőségünk van az egyes hálózati csomópontokat jól áttekinthető hierarchiába szervezni, amit akár 2 dimenzióban is megjeleníthetünk 1. kép. A Nagiosban lévő eszközök többféle állapotot tudnak felvenni:

- OK/UP – Minden rendben van
- WARNING – valamire figyelmeztet (pl.: ping esetében az átlagosnál nagyobb válaszidő)
- UNKNOWN – ismeretlen (pl.: az SNMP lekérdezés nem ad értékelhető eredményt)
- DOWN/CRITICAL – nem működik, kritikus hiba



1. kép – Példa a nagios 2D ábrázolására

A Nagios szoftver mivel nyílt forráskódú ingyenesen hozzáférhető a http://www.nagios.org URL –en. Nem csak a szoftvert, hanem különböző jól használható pluginekhez is hozzáférhetünk ugyanitt.

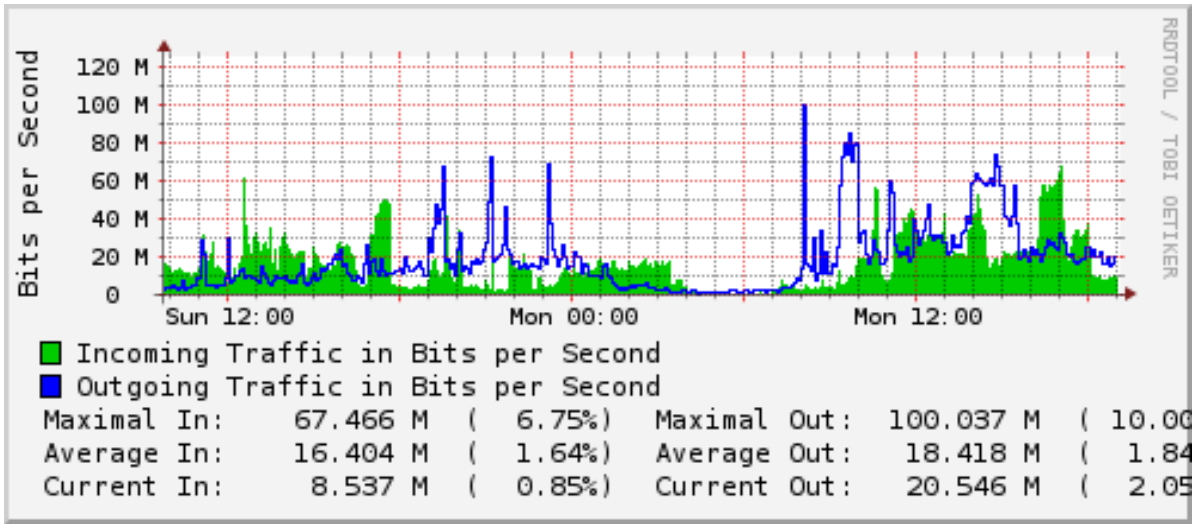
2.3.2. SNMP felügyelet MRTG segítségével

Az MRTG olyan program, amely SNMP segítségével az egyes hálózati linkek adatforgalmát képes begyűjteni, majd azt grafikonok formájában megjeleníteni. Ezen kívül akár az egyes routerek CPU felhasználását is. Saját SNMP implementációval rendelkezik, így külső SNMP-modult nem igényel. Az MRTG -vel készíthetünk grafikont az elmúlt 5 perc átlagából (daily view) , az elmúlt 30 perc átlagából (weekly view), az elmúlt 2 óra

átlagából (monthly view), és az elmúlt 1 nap átlagából (yearly view). Az MRTG nem kizárólag a Network Load -ot tudja analizálni, hanem az összes SNMP eseményt. A 2. képen láthatunk egy példát MRTG grafikonra. A szoftver ingyenesen letölthető a http://oss.oetiker.ch/mrtg/pub/?M=D weblapról.

Az MRTG legfontosabb jellemzői:

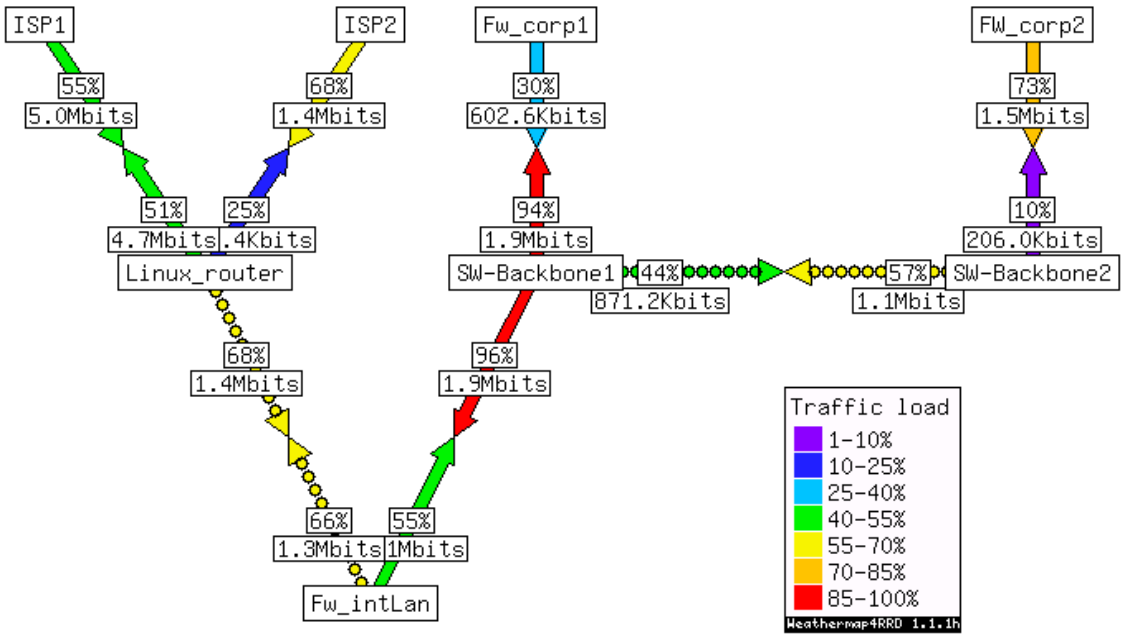
- a legtöbb UNIX és Windows platformon működik
- könnyen hordozható SNMP implementációt tartalmaz, amit teljes egészében Perlben írtak
- az MRTG logfile-jai NEM nőnek. Köszönhető ez az univerzális adatrendező algoritmusnak (rrd)
- a grafikonok közvetlenül GIF formátumba generálódnak, ehhez a GD library-t kell használni
- az MRTG által készített weblapok kinézete testre szabható
- az MRTG GNU General Public License alatt érhető el



2. kép – Példa MRTG grafikon

2.3.2.1. Network Weathermap rendszer MRTG alapokon

A Network Weathermap egy olyan program, ami az MRTG által begyűjtött adatokat képes vizualizálni (pl. hálózati linkek forgalma) dinamikus HTML dokumentumok formájában. A program lehetővé teszi IPv6 hálózatok monitorozását is. Színekkel különbözteti meg az egyes linkek terheltségét. Konfigurálása aprólékos, nagy odafigyelést igényel, viszont cserébe egy látványos eszközt kapunk, ami nagyban megkönnyíti a mindennapi üzemeltetési feladatokat. A 3. képen láthatunk egy mintát a Network Weathermap ábrái közül. A szoftver elérhetősége: http://netmon.grnet.gr/weathermap/



3. kép – Network Weathermap példa

2.4. Számítógépes hálózat energiaellátása

Nagyon sokan nem gondolnak arra, hogy az informatikai rendszerek nélkül a teljes vállalkozás működésképtelenné válik. Ezekre akkor döbbennek rá, amikor meghibásodik valami, vagy egy egyszerű áramszünet lép fel. Ennek a problémának az első lépése az informatikai struktúra energiaellátása. Nem csak a szünetmentes tápellátás biztosítása, hanem a megfelelő hálózati túlfeszültség védelem, a gépek szakaszolt energiaellátása, a szünetmentes tápegységek megfelelő karbantartása.

Egy komplex energetikai rendszer a következő fő modulokból áll:

- Túláram, és túlfeszültség végelem
- Aggregátoros betáplálás biztosítása *(nagyobb rendszerek esetén)*
- Szünetmentes tápegység

Biztosítani kell a villamos hálózat túláram védelmét ami elsősorban tűzvédelmi szempontból szükséges. Az informatikai rendszerek meghibásodásáért, hibás működéséért legnagyobb mértékben a különféle túlfeszültségekből adódó tranziensek a felelősek. Ügyelni kell rá, hogy a villamos energia ellátás lehetőleg szakaszolt módon valósuljon meg. Az áramingadozások és kimaradások problémája legkönnyebben a szünetmentes tápegységek (UPS) használatával oldható meg. A LAN-hoz ajánlott UPS mérete függ többek között az anyagi lehetőségektől, a LAN által nyújtott szolgáltatásoktól, a hálózat kimaradások gyakoriságától és az áramkimaradások jellemző időtartamától. A Műszaki Kar esetében figyelembe kell venni, azt, hogy az elektromos hálózat elég régi, a szokásosnál gyakrabban fordulnak elő áramingadozások, néha fellép egy - egy kisebb áramkimaradás is. Ezért a UPS alkalmazása elkerülhetetlen.

3. A lokális hálózat tervezési és dokumentálási folyamata

3.1. A Műszaki kar jelenlegi hálózatának ismertetése

Ahhoz, hogy megértsük miért is kell egyes eszközöket lecserélni meg kell vizsgálnunk az épület strukturált hálózatának átalakítás előtti állapotát. Maga az épület meglehetősen régi az 1960-as években épült. Az első számítógépes hálózatot körülbelül tizenöt éve építették, akkor még koaxiális kábelt használtak a kivitelezéshez. Aminek a darabjai még mindmáig megtalálhatóak az épületben. Majd ezt a rendszert felváltotta a körülbelül 7 éve újabb technológiával, UTP kábelekből megvalósított strukturált hálózat. Ez az akkori kor igényeit bőségesen kiszolgálta. Össze sem lehetett hasonlítani a koaxiális kábelezés „gyengeségeivel". Viszont a legutóbbi felújítás óta lényeges fejlesztés a kollégium kivételével sehol nem történt. Jelenleg a sok irodában küzdenek olyan problémával, hogy nincs elég végpont a PC-k meghajtására, vagy az, hogy kevés a fali ajzat, illetve ha van szabad fali ajzat, akkor az nincs „meghajtva". A meghajtó oldali eszközök közül némelyik még 10Mbit/s –os, ami már nem felel meg a mai kor követelményeinek. Mivel a hálózat forgalma egyre nő. Műszaki karról lévén szó, számításba kell venni azt is, hogy a legtöbb hallgató használ valamilyen CAD / CAM rendszert, amit egymás között illetve oktatóikkal a hálózaton cserélnek ki. Az alkalmazás által generált forrásfájlokkal nincs különösebb probléma, mivel ezek viszonylag kisebb méretű állományokat generálnak. Viszont, ha az alkalmazásokból renderelt képeket, modelleket akarjuk egymás között kicserélni a hálózaton ott már közel sem mindegy az adatátviteli közeg sebessége, mivel ezek az állományok akár több gigabájt méretűre is duzzadhatnak.

A hálózat konfigurációja az évek során nem követte a technológiai változásokat, újításokat. Még mindig a rendszergazdák osztják ki statikusan az IP címeket, melyeket Excel táblában tartanak nyílván. A címkiosztás meglehetősen rosszul van megoldva, mivel az egyes felhasználók nagyrésze publikus IP címeket használ. Ez biztonsági réseket képez az intézményi hálózaton, könnyebben elterjednek vírusok, a nagyvilág felől egyszerűbben fel tudják törni a felhasználók gépeit. Statikus címkiosztásnál az is probléma, hogy ha valaki még egy IP címet szeretne nem minden esetben fordul a helyi rendszergazdákhoz. Nincs különbség az egyes csomagok között a hálózat mindent best effort módon továbbít.

Az egyes hálózati eszközök uplinkjei nem minden esetben vannak megfelelő módon meghajtva. Mivel a legtöbbször a meghajtó eszköz nem rendelkezik elegendő nagy

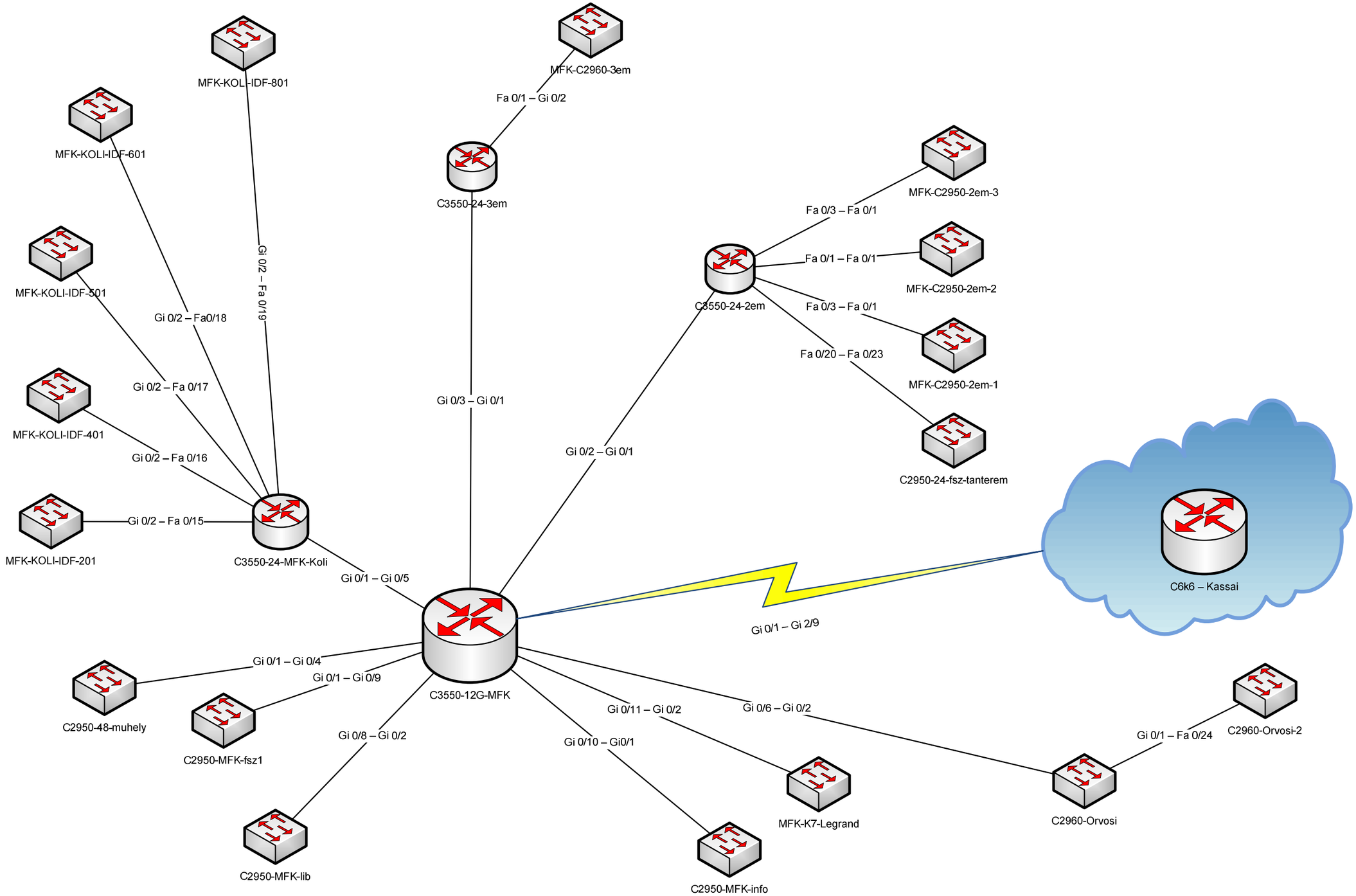
sávszélességű porttal. Gyakran előfordul, hogy egy gigabit képes eszköz csak 100Mbit es gerinckapcsolatot kap.

A hálózathasználati trendek folyamatosan fejlődnek, változnak, gyakran felmerül az igén, hogy a kar épületének egyes részein vezeték nélkül is el lehessen érni az egyetemi hálózatot. Jelenleg ez „desktop” célra készült vezeték nélküli routerekkel van megoldva, viszont ennek nagy hátránya, hogy a felhasználókat nem lehet nyomon követni.

Az 1. ábrán jól látszik a felújítás előtti hálózati topológia. Alapvetően hat részre lehet bontani:

- „Router szoba” – Itt csatlakozik be a Kassai Útról érkező gigabites kapcsolat, a szétosztás első része itt történik
- 2. emeleti rendező – A második emeletet és földszintet kiszolgáló eszközök
- 3.elemeti rendező – A harmadik emeletet kiszolgáló eszközök
- Orvosi (B) épület – A”B épületet” kiszolgáló eszközök
- Kollégium – Kollégiumi elosztó, az egyes szinti elosztók ide csatlakoznak.
- Első emeleti és földszinti helyiségeket meghajtó eszközök – Ezek az eszközök gyakorlatilag mind közvetlenül a router szobába csatlakoznak, gyakorlatilag az összes hallgatókat kiszolgáló informatikai terem, ezen kívűl ide csatlakozik még a műszaki kar szerver szobája.

A képen az is jól látszik, hogy egyes eszközök, melyek rendelkeznek gigabit ethernet portokkal néhol csak 100Mbit / s sávszélességű kapcsolatot kapnak. Ez a jelenség áll fenn a főépület 2. és 3. emeleti rendezőjében, valamint a kollégiumban.



1. ábra – A Műszaki Kar régi hálózatásnak topológiája

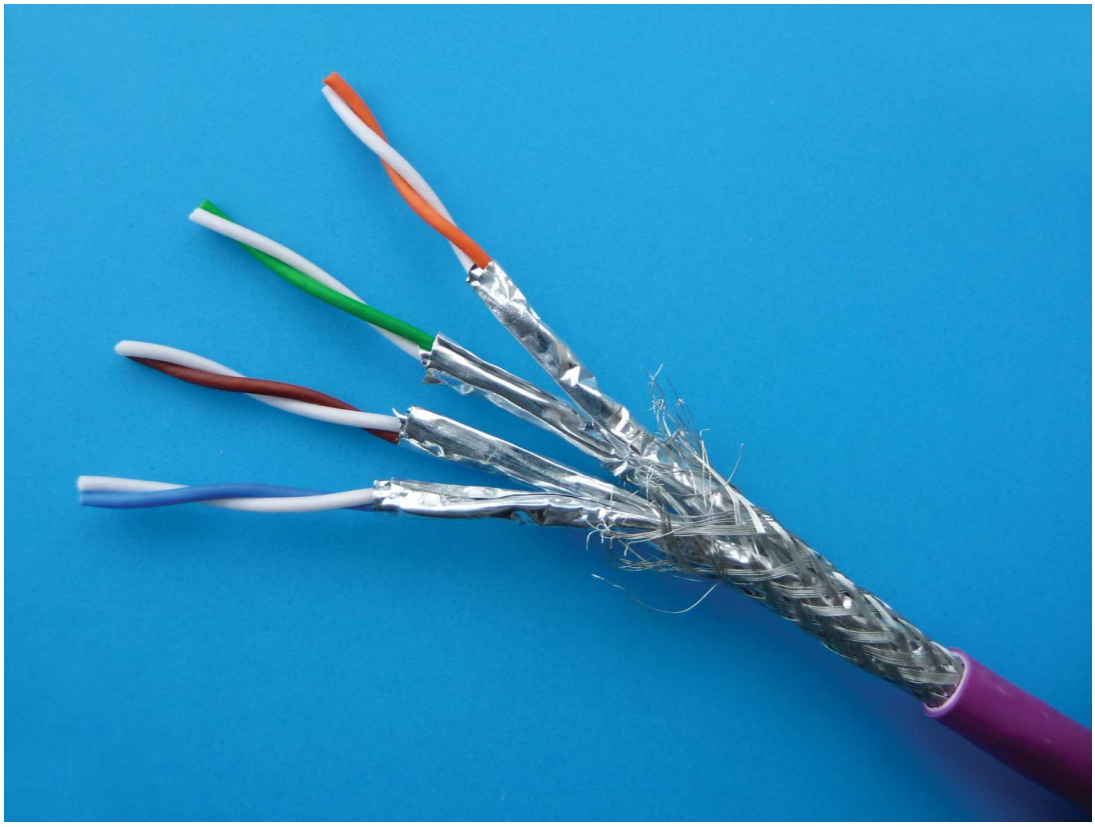
3.2. Az új hálózat tervezése és kialakítása

Ebben a fejezetben ismertetni fogom az új hálózat kialakításánál figyelembe vett szempontokat. A folyamatot három fő részre bontottam: fizikai szint, aktív eszközök, konfigurációs lépések. A tervezésnél számos tényező van amit figyelembe kell vennünk, ahhoz, hogy az új hálózat maradéktalanul megfeleljen a mai kor elvárásainak.

3.2.1. A hálózat fizikai részének továbbfejlesztése

Első lépésként a fizikai szintű fejlesztéseket kell megtervezni. Mint korábban említettem sok helyen nincs elegendő végpont, ezért ahol szükséges ott megfelelő számú sodrott érpáras végpontot kell kiépíteni. Ahol fizikai bővítésre kerül sor ott legalább CAT6a FTP minőségű kábelekre kell törekedni a sodrott érpáras kábelezésnél. Lehet, hogy ez még korainak hangzik, de 10 éve ugyanezt gondolhattuk az 1000BASE-T szabványról, ami manapság már szinte alapkövetelmény - gondoljunk a notebook-ok és a desktop PC-k integrált Gigabites csatlakozóira, az ilyen végponti sebességű switchek pedig már igen széles körben elterjedtek. Ugyan 10 Gigabites portokkal rendelkező végponti aktív eszközöknek még igen borsos áruk van, a strukturált kábelezés gondos megválasztásával felkészíthetjük hálózatunkat a jövő IT kihívásaira - a Cat6a kábelezési szabvány ugyanis a réz alapú Ethernet hálózatok esetében jól megszokott 100m-es szegmensen belül biztosít majd 10 Gigabites sebességet. Legjellemzőbb előnyei a CAT5 kábelekkel szemben:

- sűrűbben megcsavart érpárok
- a 4 érpár csavarása eltér egymástól
- az érpárokat műanyag terelő pozícionálja a kábelben
- vastagabb külső burkolat



4. kép – Cat6e kábel

Szükség van az optikai hálózat kisebb átalakítására, hogy nagyobb sávszélességet tudjunk biztosítani az egyes rack szekrényekbe. Az optikai kábeleket épületen belül, vagy épületek közötti kommunikáció céljára gyakran használjuk. Ez drágább technológia (mint a réz-vezető), de kiváló adatátviteli tulajdonságai vannak. A fényvezető kábeleknek három fő előnye van a hírközlésben használatos réz-vezetőkkel szemben: kiváló jeltovábbítás, zavarmentesség és biztonság. A jeleket kis veszteséggel továbbítják. Villamos zavarokkal szembeni érzéketlenség - A fényvezetők nemfémes jelvezetőt használnak, így nem vesznek fel és nem bocsátanak ki elektromágneses, vagy rádiófrekvenciás zavarokat (EMI, RFI). Az áthallás (szomszédos kommunikációs csatornák közötti csatolás) nem fordulhat elő, ez szintén növeli az átvitel minőségét. A fényvezető kábeleken keresztül továbbított jelek nem érzékenyek semmilyen külső zavarásra. Ez azt jelenti, hogy a tápellátás veszélyes túlfeszültsége, a közeli villámlások és a nagyfeszültségű zavarások teljesen hatástalanok.

Az optikai kábelek legfőbb előnyei és alkalmazási területei:

- függőleges kábelezés (backbone)
- épületek közötti kapcsolat
- km. nagyságrendű távolságok
- erős zavarcsökkentési igény
- nagyobb sűrűségű adatátviteli igény

Léteznek úgynevezett többutas (multimód) szálak, amik többszörös utakon vezetik a fénysugarakat. Az egyutas (monomode) szálak egyetlen útvonalon vezetik a fénysugarat. Nagyon nagy teljesítményű és nagy távolságú átvitelre van fenntartva. Az optikai kábelezésnél a Műszaki Karon törekedni kell a monomódusu legalább OS2 minőségű kábelek beépítésére, ami képes a 10Gbit ethernet átviteli sebességre. A hálózat új topológiája a 3.sz. mellékletben a 4. ábrán látható.

3.2.2. Aktív eszközök

Figyelembe kell venni mindenképpen a már működő infrastruktúrát, mivel nem minden eszköz lesz lecserélve fontos, hogy az új eszközpark a mostanival zökkenőmentesen tudjon együtt működni. Valamennyi már meglévő L3 –as szintű eszköz cserére szorul, valamint minden L2 eszköz is amelynek nincs legalább két darab 1Gbit / s sávszélességű portja. Manapság már standardnak tekintjük a 100Mbit sávszélességű portokat, ahol a Layer 2 switch nem felel meg az előbb felsorolt dolgoknak ott azokat cserélni kell.

Át kell gondolni a fizikai bővítéseket, az aktív eszközök cseréjét, bizonyos mértékben át kell strukturálni a meglévő topológiát. Javítanunk kell a hálózat áteresztő képességén, ahol lehet ott a gerinckapcsolatok sebességét növelni.

Elsőként a hálózat középső részét vizsgáltam, a jelenlegi Cisco WS-C3550-12G L3 multilayer switch meglehetősen túlterhelt, portjai telítettek. Mivel az akadémiai hálózat gerince 2007 évben a HEFOP pályázat keretében 1Gbit/s sebességről 10Gbit/s sebességre lett gyorsítva a campusok között, ezért az a cél, hogy itt is tudjuk ezt a sávszélességet biztosítani. A gyártóval egyeztetve a Cisco C6500 –as család 6504-es WAN kategóriájú moduláris switchére esett a választás.

5. kép – A Cisco C6500 kapcsolócsalád

Főbb jellemzői:

- 5U magas rackbe szerelhető kivitel
- minden 6500 platformba építhető modult támogat
- redundáns tápellátás
- SNMP támogatás
- QoS

A switch végleges felépítése a következő:

- Catalyst 6504-E-Chassis+Fan Tray

  Cisco 6500 E ház és a házhoz tartozó ventilátor egység
- Catalyst 6500 2700W AC power supply (2db)

  Az eszközbe két darab tápegységet helyezünk el, amik 2700W teljesítményűek. Ezzel biztosítjuk a redundáns tápellátást.
- Cisco Sup720-10G

  Minden 6500 szériás eszközhöz tartozik egy úgynevezett „supervisor engine” gyakorlatilag ez a switch „gondolkodó része”, ami végzi a routingot, a switchinget, biztosítja a QoS-t, alkalmazza az ACL-eket stb. Ezen felül találunk rajta két db CF kártya helyet, ami tárolhatjuk a konfigurációinkat, és a switch működéséhez szükséges operációs rendszereket (IOS) valamint két gigabit ethernet interfacet.
- WS-X6704-10GE

  Ez a kártya 4db nagy sávszélességű Xenpak modulnak biztosít helyet, ezek az interfacek képesek a 10Gbit ethernet sávszélesség biztosítására.
- WS-X6724-SFP

  A bővítő helyet ad 24db egyenként maximum 1Gbit/s sebességű SFP modulnak, amik tetszőlegesen lehetnek optikai vagy RJ45 csatolásúak.

A modulok kiválasztásánál szem előtt tartottam azt is, hogy idővel a fontosabb rendezőkbe is legyen lehetőség a 10Gbit/s sávszélességű kapcsolat eljutatására. Ezért lett kiépítve a nemrég említett OS2 monomódusú optikai kábel.

A hálózat „magja” után jöhetnek az egyes szintek rendezői. A főépület második és harmadik emeleti valamint a kollégium földszinti rendezőjébe a mostani C3550-24 portos switchek helyett Cisco WS-C3750G-24TS-S1U eszközök kerülnek. A tervek szerint ezek fogják meghejtani az előbb említett elosztókat 2Gbit/s port chenellen keresztül.

Főbb jellemzői:

- 1U magas rackbe szerelhető kivitel
- 28db 10/100/1000 port ebből 4db SFP
- Stackelhető
- SNMP menedzselhető
- QoS

6. kép – A Cisco C3750G kapcsoló

Az access szintű elérés bővítését ugyancsak a Cisco cég eszközeivel valósítottam meg. Szükség van minden rendezőben legelább egy darab 24 portos switchre. Itt a választás a Cisco WS-2960S-24TS-S eszközre esett.

7. kép – Cisco 2960 L2 switch

Főbb jellemzői:

- 1U magas rackbe szerelhető kivitel
- 26db 10/100/1000 port ebből 2db SFP / RJ45
- SNMP menedzselhető
- QoS

A kiválasztott eszközökből jól látszik, hogy mindenképpen a Cisco cég eszközeihez ragaszkodtam. Ennek a fő oka az, hogy a DE TEK hálózata homogén Cisco környezet, ezek az eszközök már bizonyítottak a konkurens gyártókkal szemben. Egy már régóta jól működő infrastruktúrát szerintem nem érdemes olyan eszközökre cserélni amivel nincsenek tapasztalataink.

Bizonyos helyeken, ahol az eszközök optikai kábellel csatlakoznak a C6504-es switchre speciális modulok behelyezésére van szükség. A C3750-es L3 switchek esetén ez SFP modullal, míg a C6504 és Kassai út között Xenpak modullal valósul meg.

8. kép - SFP modul

9. kép – Xenpak modul

Az SFP modul 1Gbit/s sebességre képes a Xenpak modul viszont 10Gbit/s –re. Fontos, hogy az érintett rendezőkbe (második emelet, harmadik emelet, kollégium) a megvalósítás során 2db SFP modul kerül beépítésre, ezáltal a gerinckapcsolat sebessége ezekbe a szekrényekbe 2Gbit/s lesz, amit port channel segítségével valósítok meg.

3.2.2.1 A régi eszközök hasznosítása

A felújítás során minden L3 szintű eszköz le lett cserélve. Mivel ezekre az új topológiában nincs szükség, az egyetem más campusain lesznek hasznosítva. Az L2 switchek maradnak az eredeti helyükön módosított konfigurációval. Összese, 1db Cisco C3550 12G és 3db Cisco C3550 24 EMI L3 multilayer switch kerülhet újra felhasználásra valamelyik más épületben vagy campuson.

10. kép - Cisco C3550 12G

11. kép – Cisco C3550 24 EMI

12. kép – Cisco C2950T 48

3.2.3. A konfiguráción tervezett módosítások

Ebben a fejezetben a főbb ismertetem az új eszközök szoftveres beállításainak főbb lépéseit.

Az új hálózatban nem kizárólag eszközcsere és fizikai szintű változtatás lesz, át kell rendezni az IP networköket is. Ki kell alakítani egy intelligens eseményvezérelt menedzsment rendszert, ami jelez, ha bárhol bármelyik eszközzel probléma van, illetve folyamatosan SNMP alapon monitorozza az egyes erőforrásokat. A hálózat logikai átszervezése is esedékes, mivel sok kisebb IP network van kiosztva vegyesen publikus és privát címosztályokból. Ennek Hátránya, hogy ahol publikus címek vannak, ott többször előfordult, hogy egyes felhasználók gépeit feltörték. A kari szervereknek kevés publikus IP cím jut, nincs külön szeparálva DMZ zóna a kiszolgálók számára, sőt a szerverek egy tartományba esnek egyes felhasználók gépeivel. Ez felvet bizonyos biztonsági kérdéseket. Az IP címek statikus kiosztását meg kel szűntetni, ezt legkönnyebben egy DHCP szerver bevezetésével lehet megoldani.

3.2.3.1. Új VLANok a DE MK hálózatán

Először az IP hálózatok „átszervezésére” kerül sor. Új VLAN –ok lesznek létrehozva, menedzsment hálózat, routing célra fenntartott hálózat, a publikus IP címosztályok le lesznek cserélve privátra (1. táblázat), a szerverek hálózata ez alól természetesen kivétel. A 2. táblázat röviden összefoglalja az új VLAN –ok nevét, azonosítóját, és funkcióját.

1. táblázat – Az IP címtartományok kiosztása

Címtartomány	Rendeltetés
10.70.70.0/28	MK routing
10.70.70.128/25	MK menedzsment
172.17.43.0/24	Kollégium
172.17.49.0/24	Hallgatói géptermek
172.17.91.0/24	Első emeleti és földszinti irodák
172.17.92.0/24	Második emeleti irodák
172.17.93.0/24	Harmadik emeleti irodák
172.17.94.0/24	B épületi irodák
193.6.145.128/26	Szerverek

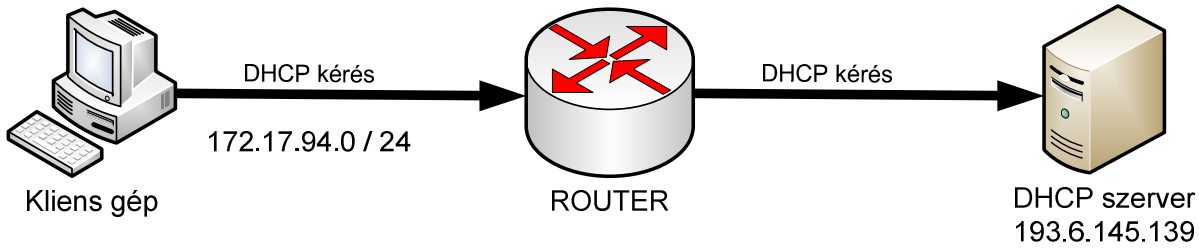
2. táblázat – Új VLANok a Műszaki Karon

VLAN id	VLAN név	Funkció
710	MK-szerverek	Kari szerverek kiszolgálása (publikus címek)
721	1em+fsz	Első emeleti és földszinti irodák
722	2em	Második emeleti irodák
731	3em	Harmadik emeleti irodák
741	B-epulet	B épületben lévő irodák
752	Borsos-Koli	Kollégiumi szobák
758	MK-Hallgatoi-Termek	Hallgatói géptermek
760	MK-routing	Routing célra fenntartott hálózat
761	MK-menedzsment	Menedzsment network

A VLAN ok konfigurációja a következőképpen néz ki:

```
!
interface Vlan741
 description ---== B epulet ==---
 ip address 172.17.94.1 255.255.255.0
 ip helper-address 193.6.145.139
!
```

A fenti konfiguráció a B épületbe definiált VLAN –ra érvényes. Egyértelműen látszik a az IP címtartomány, illetve megjelenik egy dhcp szerver specifikus sor, „ip helper-address”. Ez a parancs arra szolgál, hogy az alhálózatból érkező DHCP kéréseket továbbítsa a szerver felé. A működést a 2. ábra szemlélteti.



2. ábra – Az „ip helper-address” parancs működése

Menedzsment célra a 760 és 761 VLANok lettek létrehozva. A 760 VLAN csak routing céljára készült. A régi beállításokat kicsit továbbfejlesztve az útválasztás EIGRP protokollal valósul meg.

3.2.3.2. Az EIGRP routing protokol használata

A Cisco cég saját protokollja. Az EIGRP egy fejlett irányító protokoll, működése olyan szolgáltatásokra épül, amelyeket általában a kapcsolatállapot alapú protokollokkal társítanak. Az EIGRP jó választás olyan hálózatok számára, amelyek elsősorban Cisco forgalomirányítókat tartalmaznak.

Az EIGRP a megismert útvonalakat különleges módon tárolja. Minden útvonalhoz állapotadatokat lehet rendelni, címkézésükkel pedig további hasznos információk tárolhatók el.

Három táblát tart fenn:

- Szomszédtábla
- Topológiatábla
- Irányítótábla

Az EIGRP a következő előnyöket kínálja az egyszerű távolságvektor alapú protokollokhoz képest:

- Gyors konvergencia
- A sávszélesség hatékony kihasználása
- A változó hosszúságú alhálózati maszkok (VLSM) és az osztály nélküli, körzetek közötti forgalomirányítás (CIDR) támogatása. Az IGRP-től eltérően az EIGRP teljes mértékben támogatja az osztály nélküli IP-t, útvonalfrissítéseiben ugyanis az alhálózati maszkokat is továbbítja.
- Több hálózati réteg támogatása
- Függetlenség az irányított protokolloktól. A protokollfüggő modulok (protocol-dependent module, PDM) alkalmazása lehetővé teszi, hogy az EIGRP-t hosszú ideig ne kelljen módosítani. Az irányított protokollok fejlődése újabb protokollfüggő modulok írását teheti szükségessé, ám maga az EIGRP változatlan maradhat.

A C6504 routing beállítása:

```
!
router eigrp 65530
 redistribute static
 passive-interface default
 no passive-interface Vlan759
 no passive-interface Vlan760
 no auto-summary
 no eigrp log-neighbour-changes
 network 10.70.70.0 0.0.0.15
 network 10.70.70.128 0.0.0.127
 network 10.254.70.0 0.0.0.15
 network 10.254.70.16 0.0.0.15
```

```
 network 10.254.70.64 0.0.0.15
 network 10.254.70.80 0.0.0.15
 network 10.255.70.1 0.0.0.0
 network 172.17.44.0 0.0.0.255
 network 172.17.49.0 0.0.0.255
 network 172.17.94.0 0.0.0.255
 network 193.6.144.224 0.0.0.31
 network 193.6.145.128 0.0.0.63
!
```

Nézzük a konfiguráció főbb parancsait. A csomópont a 65530 AS –ben van, ezzel indítjuk a konfigurációt.

A „redistribute static” sor azt mondja meg, hogy a kézzel definiált statikus utakat is hírdetjük a protokolon keresztül.

A passive interface default parancs, a routerben lévő összes interfészt passzív módba rakja – természetesen az EIGRP által generált forgalomat illetően -, ezzel megakadályozzuk, hogy a routing protocol túl nagy forgalmat generáljon egyes alhálózatokban, vagy esetleg olyan irányba is küldjön információkat, amerre
nincs rá szükség.

A no-passive-interface [interface] parancs kiadásával nyílván deaktiválhatjuk az előző parancs hatását egy meghatározott interfészre, így tesszük „elérhetővé” az EIGRP-t az adott interfészen.

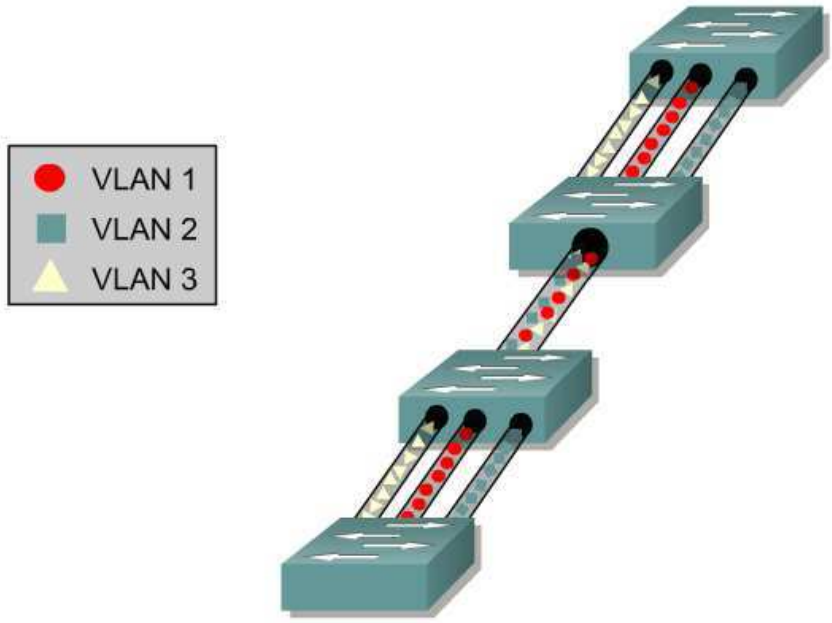
A network parancs az EIGRP egyik „alap” konfigurációs parancsa, tulajdonképpen ezzel engedélyezzük az EIGRP működését az egyes irányokba.

Alapesetben az auto summary parancs szummarizálja a routokat, így csökkentve a routing információkat, tehermentesítve ezzel a hálózatot illetve az eszközöket. Itt viszont nincs rá szükség, ugyanis csak a prefix listában meghatározott routoknak engedünk utat, nem kapunk „felesleges” routing információkat.

Ahhoz, hogy tovább csökkentsük a forgalmat, az eigrp logok cseréjét is kikapcsoltuk a no eigrp log-neighbor-changes paranccsal.

3.2.3.3. Switchport konfigurációk

A gerinckapcsolatok esetében minden eszköz uplink portjain „trunk” beállítást alkalmazunk. Előnye, hogy az ilyen interfaceken több VLAN-t is átengedhetünk. Például, ha egy switchen a hallgató terem gépei és irodai gépek is kommunikálnak, úgy a megfelelő VLAN-ba téve őket a trunk portokon keresztül egymástól szeparálva tudnak hálózati kapcsolatot létesíteni. Ezzel nem csak az skálázhatóságot javítjuk, hanem a biztonsági kockázatot is csökkenthetjük. Például egy vírustámadást sokkal könnyebb megszüntetni egy kisebb szegmensben, mint gépek tucatjait tartalmazó alhálózatban. A következő ábra a trunk működését szemlélteti leegyszerűsítve:



3. ábra – A trunk kapcsolat működése

```
!
interface GigabitEthernet1/0/8
 description 8. szint 2
  switchport trunk encapsulation dot1q
 switchport trunk native vlan 761
 switchport trunk allowed vlan 1,750,752,761,1002-1005
 switchport mode trunk
!
```

A fenti konfiguráció a kollégium 8. szintjére menő 2. számú switch gerinc kapcsolatát írja le.

Mielőtt trunk portot konfigurálunk be kell állítani az enkapszuiláció módját, ami jelen esetben dot1q. Dot1q esetén lehetőségünk van egy db VLAN-t untagged küldeni, ez jelen esetben a menedzsment VLAN a 761 –es. Célszerű explicit beállítani azokat a hálózatokat, amelyek „átfolyhatnak” a TRUNK porton, ezt a „switchport trunk allowed vlan” parancs után vesszővel elválasztva kell felsorolni.

Az access szintű kapcsolatok kialakításánál kétféle konfigurációra volt szükség. Mivel a kari hálózat a helyi rendszergazda által ellenőrzött, nincs szükség semmilyen hitelesítésre, a felhasználó csak csatlakoztatja a számítógépét, és már használhatja is. Az alábbi konfiguráció egy első emeleti L2 switch egyik portján található:

```
!
interface FastEthernet0/22
 switchport access vlan 721
 switchport mode access
 spanning-tree portfast
!
```

A beállításokban nincs semmi különös. Talán a „spanning-tree portfast” parancsról érdemes néhány szót ejteni. A parancsot érdemes minden olyan switchporton alkalmazni amelyre PC-kapcsolódik. Alkalmazását követően, a port azonnal forwarding státuszba kerül bármilyen aktivitás hatására. A parancs nélkül a switch-nek először meg kellene győződnie, hogy a port Designated Port (DP), majd ideiglenesen listening majd learning státuszba kellene azt raknia, blokkolva ezzel a forgalmat hosszú másodpercekig. Ha hálózatunkon DHCP szerverrel szolgáltatunk, akkor a kapcsoló használata szinte kötelezően ajánlott, mivel ilyenkor akár percek is eltelhetnek anélkül, hogy a gép IP címet kapna.

3.2.3.4. A kollégiumi rendszer

A kollégium esetében nem ilyen egyszerű a helyzet. A kollégisták gépeiről szükség van valamilyen nyilvántartásra. Fontos, hogy a hallgatók saját maguknak tudják regisztrálni számítógépeiket valamilyen web felületen keresztül. A régi csomópont bejelentő lapok kitöltése, már meglehetősen idejétmúlt és lassú megoldás. Be kell vezetni a hálózaton a Network Access Contol-t (NAC). Mivel homogén Cisco eszközparkról van szó, így a legegyszerűbb megoldás a VMPS (Vlan Management Policy Server) alkalmazása. Ez úgy működik, hogy a switchek portjai, nicsenek VLAN-hoz hozzá adva, de attól még access módban vannak. A portokat egy „switchport access vlan dynamic" paranccsal dinamikusra állítunk. Ilyenkor a switch ha észleli, hogy fizikai "tehát Layer 2″-es kapcsolat van akkor megnézi, hogy az kliens MAC address-e benne van-e egy adatbázisban, és milyen VLAN-ba kell tegye a port-ot, amit szintén egy adatbázisból állapít meg. Példa egy dinamikus port konfigurációjára:

```
!
interface FastEthernet0/1
 switchport access vlan dynamic
 switchport mode access
 spanning-tree portfast
!
```

A Cisco C6504 eszköz ugyan rendelkezik VMPS szerver funkcióval, viszont ez nem elég intelligens ahhoz, hogy többfajta adatbázisból kérdezzen le adatokat. Ezért egy nyíltforrású megoldást a Freeradius szervert kell alkalmazni. A Freeradius és a Cisco VMPS szerver összehasonlítása megtalálható a 3. táblázatban. A hallgatók az egyetemi hálózati azonosítójuk mellé fel tudják vinni hálózati kártyáik fizikai címét. Ha ezt megteszik, akkor a gépük regisztráltnak számít, és ezáltal jogosultak lesznek a hálózat használatára. Amennyiben gépük nincs regisztrálva abban az esetben egy korlátozott hálózatba kerülnek, ahonnan csak a NEPTUN rendszer, illetve a regisztrációs felület lesz elérhető. Ahhoz, hogy a switch kommunikáljon a VMPS szerverrel a következő beállításokat kell megtennünk:

```
!
vmps server 172.17.3.2 primary
vmps reconfirm 5
vmps retry 10
!
```

Megadjuk a VMPS szerver IP címét, majd azt is be kell állítanunk, hogy egy adott portot milyen időközönként hitelesítsen újra a rendszer. Ezek után definiáljuk a „retry” értéket, vagyis azt, hogy ha nem sikerült a hitelesítés (a szerver nem válaszolt, vagy nem sikerült hitelesíteni a portot) akkor hányszor próbálkozzon újra a hitelesítéssel a rendszer. A rendszer működését a 4. ábra szemlélteti. Ezzel a rendszerrel megoldottá válik a felhasználók nyomon követése is, ugyanis a napló fájlokból minden adat másodpercekre pontosan visszakereshető. Naplózásra kerül az adott MAC címhez kiosztott IP cím és VLAN, természetesen időbélyeggel ellátva. A freeradius szoftver aktuális verziója elérhető a : ftp://ftp.freeradius.org/pub/freeradius/ szerveren.

A kollégiumi hálózat speciális terület, jelenleg egy elég szigorú szabályozásnak van alávetve. Erre azért volt szükség, mert a hallgatók nem mindig rendeltetésszerűen használták a hálózatot. Megnőtt a P2P forgalom, elszaporodtak a vírusok, többször kaptunk bejelentést illegális tevékenységekről. Ezért arra az elhatározásra jutotta, hogy szűrő listával kell védekezni az ilyen tevékenységek ellen. Az access lista részletes konfigurációját az 2.sz. melléklet tartalmazza. Az egyetemi hálózathasználati szabályzathoz igazodva a hálózatból elérhető szolgáltatások a következők: FTP, SSH, WEB, titkosított WEB (HTTPS), különböző elektronikus levelezésre szolgáló szolgáltatások (POP3, IMAP, POP3S, IMAPS, SMTP), Skype, MSN (sajnos a Messenger webkamerás kapcsolatát ACL –lel nem lehet átereszteni), Internetes TV és rádió adások. A különböző szolgáltatások korlátozása, sajnos elég szigorú, nem teljesen elégíti ki a mai kor elvárásait, viszont ezekkel az eszközökkel szerintem ez a legjobb megoldás.

Üzemeltetés során többször szembesültünk azzal a problémával, hogy egyes portok a Spanning Tree Protocol működése végett „error-disabled” státuszba estek. Ezt a problémát előidézheti már egy hibás patch kábel használata is. Szerencsére az L2 eszközök rendelkeznek erre a célra beépített automatizmussal, tehát a későbbiekben nem lesz szükség manuális

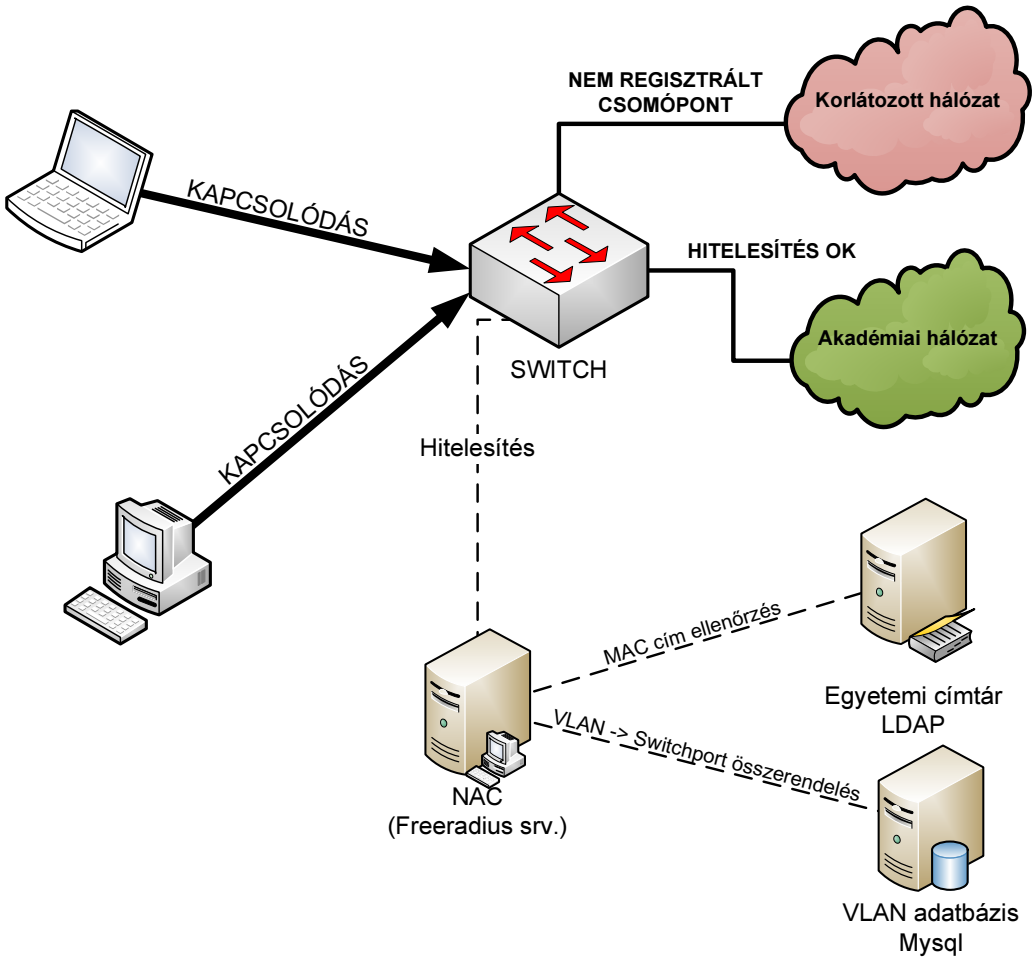
beállítások alkalmazására, hanem automatizált módon a switch képes kezelni a problémát. Összesen két parancs kiadására van szükség:

```
!
errdisable recovery cause all
errdisable recovery interval 300
!
```

Az első parancs arra engedélyezi a „recovery” automatizálást minden esetben. A második parancs pedig beállít egy időzítőt, ami megmondja a switchnek, ha hibát érzékel mennyi idő múlva engedélyezheti automatán az adott portot. Lehetne szűrni azokat az eseményeket amikor nem akarjuk, hogy az automatizmus aktív legyen. Ebben az esetben én nem ítéltem szükségesnek.

3. táblázat – Cisco VMPS szerver és Freeradius szerver összehasonlítása

Funkció	**Cisco VMPS**	**Freeradius**
VMPS domain	✓	✓
Port szintű VLAN hozzárendelés	✓	✓
VLAN hozzárendelés MAC címhez	✓	✓
Port Group kezelés	✓	✓
Vlan Group kezelés	✓	✓
LDAP támogatás	X	✓
SQL támogatás	X	✓
Egyedileg testre szabható naplózás	X	✓



4. ábra – A VMPS működése a Műszaki kar kollégiumában

3.2.3.5. QoS alkalmazása

A hálózati szolgálat minőség (QoS – Quality of Service) a hálózat azon tulajdonsága, amely segítségével ezt a forgalmat kezeli az alkalmazói program számára. Ehhez alapvető forgalomkezelési mechanizmusokra, valamint ezeket ellenőrző algoritmusokra van szükség. A QoS funkcionalitás egyrészt a hálózati alkalmazásokat, másrészt pedig a hálózati adminisztrátorokat szolgálja ki. Addig amíg a hálózati adminisztrátor korlátozza az erőforrásokat, addig az alkalmazások a az erőforrások minél szélesebb körét próbálják igénybe venni. A különböző alkalmazások egymástól eltérő követelményeket támasztanak az adatforgalmat továbbító hálózat felé. A generált forgalom erőforrás igénye időben változó és általában szükséges, hogy a hálózat megfeleljen ennek az igénynek. Bizonyos alkalmazások többé, vagy kevésbé toleránsak a forgalom késleltetésére, valamint a késleltetés változásra.

Továbbá néhány alkalmazás képes elviselni korlát alatti adatvesztést, míg mások nem. Ezek a követelmények a következő négy QoS-jellegű paraméter segítségével kerülnek kifejezésre. Sávszélesség: az alkalmazás forgalmának továbbítási sebessége; lappangási idő: az a késleltetés, amit egy alkalmazás a csomag kézbesítésénél képes elviselni; dzsitter: a lappangási idő szórása; adatvesztés: az elveszített adatok százalékos aránya. Ha végtelen méretű hálózati erőforrásainak lennének, akkor az alkalmazások forgalma a szükséges sávszéleségen, nulla lappangási idővel, nulla dzsitterrel és nulla adatvesztéssel lenne jellemezhető. Mivel azonban a hálózati erőforrások korlátosak, a rendszer bizonyos részein időtől függően az igények nem teljesíthetők. A QoS mechanizmusok az alkalmazások szolgálatigényének függvényében a hálózati erőforrások foglalásának szabályozását végzik. A priorizálás csoportjait a Class of Service technológiával a 4. táblázat szemlélteti.

4. táblázat – A forgalom priorizálása a CoS technológiával

Prioritás	Forgalaom típusa
0	Best Effort
1	Background
2	Standard (Spare)
3	Excellent Load (Business Critical)
4	Controlled Load (Streaming Multimedia)
5	Video (Interactive Media) [Less than 100ms latency and jitter]
6	Voice (Interactive Voice) [Less than 10ms latency and jitter]
7	Network Control Reserved Traffic [Lowest latency and jitter]

Switch oldalon a QoS konfigurációja nem okoz különösebb problémát, a Műszaki Kar esetében elegendő volt a központ Cisco C6504 –es eszközben alkalmazni a QoS specifikus beállásokat.

Minimálisan két parancs szükséges a QoS processz elindításához:

```
!
mls qos
!
interface [interface id]
mls qos trust cos
!
```

Az első parancs globálisan engedélyezi a QoS használatát, a második pedig az adott interfészre. Ez után a két parancs után a torlódás menedzsment már működőképes, mivel itt nagy sebességű hálózatról van szó, az automata beállítások elégségesek lesznek. Ha kisebb sávszélességgel rendelkeznénk, akkor lényegesen több paramétert kellene beállítani a sávszélesség skálázása érdekében.

4. Összefoglalás

A kivitelezés sikeres tesztelés befejeztével megállapíthatjuk, hogy egy, korunk elvárásainak megfelelő, mind sebességben, mind technológia fejlettségben előremutató kommunikációs hálózat került kialakításra. Igaz, nem sikerült minden elképzelést megvalósítani, például az épület szintű Wireless lefedettséget, de bízok benne, hogy az évek folyamán ez a szolgáltatás is beindul a Karon illetve az egyetem többi campusán is.

A régi hálózati topológiához képest történt némi változás, szerencsére a meglévő rendezőket nem kellett áthelyezni, illetve minden új eszköz belefért a régi RACK szekrényekbe.

Mind a kar mind pedig az egyes rendezők switcheinek gerinc kapcsolata jelentősen felgyorsult, a kitűzött cél, hogy minden L2 eszköz legalább 1Gbit/s és a kar 10Gbit/s sebességű hálózati kapcsolattal rendelkezzen, megvalósult. Évek elteltével akár lehetőség lesz akár a rendezőket is 10Gbit/s kapcsolattal ellátni, ennek a feltétele az új monomódusu optikai kábelezéssel megoldható.

A kollégiumban a NAC bevezetésével lényegesen felgyorsult a csomópontok regisztrációja valamint meg lett oldva a csomópontok nyomon követése és naplózása is. Ami szintén egy hosszú ideje húzódó nagy probléma volt.

A QoS bevezetésével megnyílt az út a VoIP alkalmazások zavartalan működéséhez. Ezek után nem lesz probléma a Videokonferencia rendszerek használatával, régebben többször előfordult, hogy vírusos gépek miatt ezek az alkalmazások nem működtek megfelelően. Megnyílt a lehetőség az egyetemi IP telefónia rendszerbe történő belépésre, most ha bármelyik felhasználó meglévő analóg telefon készülékét IP telefonra szeretné cserélni akkor azt nyugodtan megteheti. Az automatizál QoS Class of Service technológiával egyenlőre kielégíti a felhasználók igényeit.

Ezúton szeretnék köszönetet mondani a témavezetőmnek, hogy türelmével, tanácsaival segített a dolgozat elkészítésében.

Függelék

1.sz. melléklet: A dolgozatban szereplő rövidítések listája

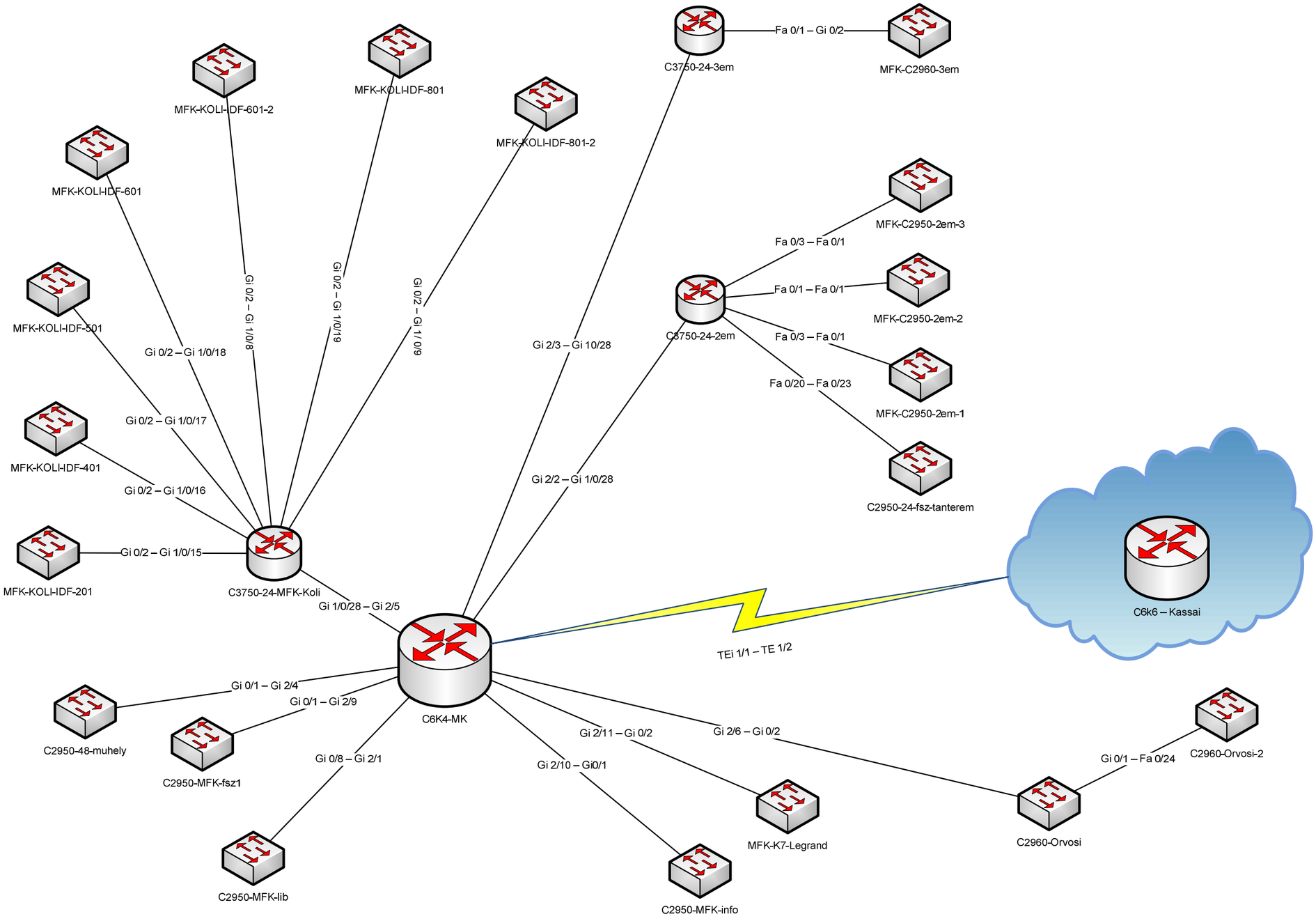
VoIP	Voice over IP
IP	Internet Protocol
TIOP	Társadalmi Infrastruktúra Operatív Program
HEFOP	Humánerőforrás-fejlesztési Operatív Program
LAN	Local Area Network
VLAN	Virtual LAN
SMTP	Simple Mail Transfer Protocol
POP3	Post Office Protocol version 3
HTTP	HyperText Transfer Protocol
MRTG	Multi Router Traffic Grapher
SNMP	Simple Network Management Protocol
UPS	Uninterruptible power supply
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
UTP	Unshielded Twisted Pair
FTP	Foil pair screened Twisted Pair
CAT5	Category 5 cable
CAT6a	Augmented Category 6 cable
WAN	Wide Area Network
QoS	Quality of Service
SFP	Small form-factor pluggable transceiver
DMZ	Demilitarized Zone
DHCP	Dynamic Host Configuration Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
NAC	Network Access Control
MAC	Media Access Control
ACL	Access control list
P2P	Peer-to-peer

2.sz. melléklet: Kollégiumi ACL konfigurációja:

```
!
ip access-list extended szures
 permit tcp any any established
 remark ===== ALTALANOS SZOLGALTATASOK =====
 permit udp any any eq domain
 permit tcp any any eq domain
 permit tcp any any eq 3128
 permit tcp any any eq ftp-data
 permit tcp any any eq ftp
 permit tcp any any eq www
 permit tcp any any eq 443
 permit tcp any any eq 22
 permit tcp any any eq 3389
 permit tcp any any eq 5900
 permit tcp any any eq 6667
 permit tcp any any eq 8000
 permit tcp any any eq 22222
 permit tcp any any eq 8082
 permit udp any any eq bootpc
 permit udp any any eq bootps
 permit tcp any any eq 8080
 remark ===== LEVELEZES =====
 permit tcp any any eq pop3
 permit tcp any any eq 143
 permit tcp any any eq smtp
 permit tcp any any eq 465
 permit tcp any any eq 993
 permit tcp any any eq 995
 remark ===== MSN MESSENGER =====
 permit tcp any any range 6891 6900
 permit tcp any any eq 1863
```

permit tcp any any eq 6901
permit udp any any eq 1863
permit udp any any eq 5190
permit udp any any eq 6901
remark ---== VISTA WIN7 KMS ==---
permit ip any host 152.66.10.214
permit ip host 152.66.10.214 any

3.sz. melléklet: A Műszaki Kar új hálózatának topológiája



5. ábra – A Műszaki Kar új hálózati topológiája

Irodalomjegyzék

[1] A Cisco cég honlapja: http://www.cisco.com/en, Megnyitva: 2010.04.10.

[2] Andrew S. Tanenbaum: Számítógép-hálózatok, ISBN: 9789635453849

[3] Cisco Press: Campus Network Design Fundamentals Dec. 2005, ISBN: 1-58705-222-9

[4] Cisco Press: NAC Appliance Aug 2007, Jamey Heary CCIE No. 7680

[5] NGC networks honlapja: http://www.ngc-networks.com, Megnyitva: 2010.04.07.

[6] Gál Zoltán, Balla Tamás (2007): A QoS hatása az infokommunikációs alkalmazásokra, Híradástechnika, Volume LXII., ISSN:0018-2028, pp. 7-16

[7] Cisco Systems: CCNA Exploration 4.0 http://www.cisco.com/web/learning/netacad/index.html, Megnyitva: 2010.04.05.