BUDAPESTI GAZDASÁGI EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

Informatikai hálózati rendszerek fejlesztése vállalati szinten

Belső konzulens: Balogh Csaba

Külső konzulens: Tróbert József

Cseh Bence
Nappali tagozat
Gazdaságinformatikus szak
Logisztika szakirány

2019

18 57 BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

BGE GAZDÁLKODÁSI KAR ZALAEGERSZEG

NYILATKOZAT
a szakdolgozat digitális formátumának benyújtásáról

A hallgató neve: Cseh Bence
Szak/szakirány: Gazdaságinformatika szak / Logisztika szakirány

Neptun kód: JCAUI9 * A szakdolgozat megvédésének dátuma (év): 2019
A szakdolgozat címe: Informatikai hálózati rendszerek fejlesztése vállalti szinten

Belső (operatív) konzulens neve: Balogh Csaba
Külső (szakmai) konzulens neve: Tróbert József
Legalább 5 kulcsszó a dolgozat tartalmára vonatkozóan:

korszerűség, megbízhatóság, forgalomirányítás, hierarchia, protokoll

Benyújtott szakdolgozatom **nem titkosított / titkosított.**
(Kérjük a megfelelőt aláhúzni! Titkosított dolgozat esetén a kérelem digitális másolatának a szakdolgozat digitális formátumában szerepelnie kell.)

Hozzájárulok / nem járulok hozzá, hogy nem titkosított szakdolgozatomat az egyetem könyvtára az interneten a nyilvánosság számára közzétegye. (*Kérjük a megfelelőt aláhúzni!*) Hozzájárulásom - szerzői jogaim maradéktalan tiszteletben tartása mellett –nem kizárólagos és időtartamra nem korlátozott felhasználási engedély.

Felelősségem tudatában kijelentem, hogy szakdolgozatom digitális adatállománya mindenben eleget tesz a vonatkozó és hatályos intézményi előírásoknak, tartalma megegyezik nyomtatott formában benyújtott szakdolgozatommal.

Dátum: 2019. 01. 02. ..... Cseh Bence .....
hallgató aláírása

A digitális szakdolgozat könyvtári benyújtását és átvételét igazolom.

Dátum: 2019 JAN. 02 .....
könyvtári munkatárs

Budapesti Gazdasági Egyetem
Gazdálkodási Kar Zalaegerszeg
Könyvtár
8900 Zalaegerszeg
Gasparich u. 18/a
Adószám: 15329822-2-20

Tartalomjegyzék

1 Bevezetés

A 21. században a nagyvállalatok mellett a kis- és középvállalatoknál is elengedhetetlen a megfelelően és megbízhatóan működő informatikai hálózati rendszer megléte. A vállalkozások hatékony és gyors működése érdekében az informatika ezen területét maximálisan kihasználni kényszerül, hiszen az elmúlt években ugrásszerűen megnőtt az internetet használók száma, mind az üzleti területeken, mind az otthoni felhasználók tekintetében.

Az internethasználat napi gyakorlattá vált. Ennek köszönhetően a számítógépes hálózatok és a különböző informatikai technológiák fejlődése ill. a felhasználói igények növekedése folyamatosan ösztönözte az iparág egyes területeinek fejlesztéseit és fejlődését. Ez a folyamat manapság elképesztően gyorsuló tendenciát mutat. Egyik vállalat sem engedheti meg magának, hogy ezen a téren elavult eszközökkel és szolgáltatásokkal biztosítsa a kereskedést a piaci versenyszférában. Csak egy jól működő informatikai hálózat képes kielégíteni a vállalatok napi igényeit. Az internet alapfeltétel minden szervezetnél, a leg apróbb cégeket is beleértbe. Alapvető feladat biztosítani, hogy az informatikai rendszer a nap 24 órában rendelkezésre tudjon állni.

Választásom azért esett erre a témára, mert egyetemi tanulmányaim előtt már szereztem informatikai hálózattelepítői és üzemeltetői képesítést. Véleményem szerint egy rendkívül érdekes témáról van szó, amelyet tanulmányaim során a színvonalas oktatásnak és a gyakorlati órákon alkalmazott fejlett informatikai eszközöknek

1. ábra: Egy jól megtervezett informatikai hálózat elengedhetetlen a vállalatok számára
Kép forrása: https://proftec.hu/informatikai-halozat-epites/ Letöltés dátuma: 2018. 11. 27.

köszönhetően sikerült alaposan megkedvelnem. Ennek tükrében különösen tisztában vagyok, hogy vállalati szinten nélkülözhetetlen a hatékonyan, hibamentesen és nem utolsó sorban biztonságosan működő informatikai hálózat megléte.

A dolgozat címe rávilágít annak témájára, de felhívnám a figyelmet, hogy nem egy konkrét informatikai hálózat fejlesztése a célom, hanem egy általános (vállalati) számítógépes rendszer optimális felépítése, annak korszerű kialakítása. A dolgozat egymásra épülő fejezetekből áll, – az első felében szeretném bemutatni az informatika ezen területét érintő, nélkülözhetetlen fogalmakat, meghatározásokat. Ezt követően kerül előtérbe a hálózatok megfelelő tervezése, kialakítása, ill. hogy hogyan tudjuk azt optimalizálni, javítani, korszerűsíteni. A dolgozat végén jelentős figyelmet szenteltem a hálózati biztonságra, hiszen az adatvesztés és a hekkertámadások nagyon komoly károkat okozhatnak. Súlyosabb esetben ez kihathat a vállalat teljes működésére is, veszélyeztetve ezzel annak tevékenységét. Mivel a hálózatok megfelelő működését egyre több tényező befolyásolja az összetettségüknek köszönhetően, különösen fontos, hogy az ezt felügyelő rendszergazda naprakész legyen bárminemű probléma elhárításával kapcsolatban. Ennek köszönhetően nagyon fontosnak tartom a hibaelhárítás gyors menetét, hiszen egy kis informatikai probléma is elegendő ahhoz, hogy a cég működése leálljon. Kisebb, nagyobb problémák bármikor felüthetik a fejüket, mindenféle előjel nélkül, viszont amennyiben folyamatosan végezünk karbantartást, a súlyosabb gikszereket biztosan elkerülhetjük. Egy külön fejezet keretében természetesen a hibaelhárítás menetével is fogunk foglalkozni. A dolgozat zárásaként egy saját készítésű hálózatot fogok bemutatni, alkalmazva a téma során elhangzottakat.

Mivel a nagyon sok eszme a témával kapcsolatban sajnos nem fér bele a terjedelembe, ezért az általam legfontosabbnak tartott gondoltatok a mellékletek közt szerepelnek. Az olyan témaköröknél, amikhez még tartozik információ, rendszerint utalni fogok. A dolgozatban számos idegen kifejezés, rövidítés, meghatározás szerepel, ezért ezek külön ABC sorrendben összegyűjtve megtalálhatóak a dolgozat végén lévő szójegyzékben.

Összességében elmondható, hogy egy nagyon összetett témáról van szó, amelyet a legjobb tudásom szerint igyekszem érthetően és világosan bemutatni. A dolgozatot az évek során szerzett jártasságomra alapozva, hiteles segédanyagokra támaszkodva állítottam össze.

2 Informatikai hálózat fogalma, kialakulása

Mióta a számítógépek történetét az 1940-es évektől kezdődően generációkra osztjuk, az azóta eltelt évek alatt a számítógépek, ill. maga az informatika óriási mértékű fejlődésen ment keresztül. Különösen igaz ez az 5. generációs informatikára, amely kijelenthető, hogy napjainkban már exponenciális mértékben fejlődik, gyakorlatilag évről-évre valami újat hoznak piacra a fejlesztők. Ebben a hirtelen kialakult, okostelefonok és egyéb okoseszközök világában a keresleti igény olyan mértékben megnőtt, hogy a világ egyik legmagasabb profitot termelő ágazatává nőtte ki magát.

Tulajdonképpen elmondható, hogy mi emberek informatika nélkül már nem is tudnánk élni, – a technológia globálisan az egész társadalomra hatással van. Természetesen a számítógépes hálózatokra szintén érvényes ez az állítás, amely az informatika ágazataként, – vele együtt járta be a szamárlétrát.

2.1 Számítógépes hálózatok kialakulása: Az informatikai hálózatok 'Big Bang-je' egészen az 1960-as évekre nyúlik vissza. Akkoriban még csak egymástól független számítógépek léteztek. Amikor szükség volt utasítások, adatok átvitelére egyikről a másikra, azt csak az azokat kezelő emberek tudták elvégezni. Idővel megnőtt az igény az összeköttetések kialakítására, hogy közös erőforrást, adatbázist, háttértárolót tudjanak használni. A világ első hálózatát az USA-ban alakították ki, amely egy katonai, kísérleti célból jött létre. A hidegháborús időszak alatt kézenfekvő volt megoldást találni egy esetleges támadás miatti információvesztés megoldására. Úgy gondolták, ha több csomópontot sikerül összekapcsolniuk egymással, úgy egy-egy pont megsemmisülése esetén az információs rendszer sértetlen marad. A 60-as évek végére sikerült megépíteni a világ első hálózatát az ARPANET-et, amely telefonfonalon keresztül működött. Ez annyira bevált, hogy az évek során egyre többen kapcsolódtak hozzá (főleg oktatási, kutatási intézmények). „*1973-ban fejlesztették ki a hálózati protokolloknak nevezett kommunikációs szabványokat, melyek lehetővé tették a bővítést, újabb gépek bekapcsolását. A kezdetben néhány gépet összekötő zárt rendszerből a bővítés lehetőségét magában hordozó nyílt rendszer lett.*"[1]

[1] Forrás: http://www.viszki.sulinet.hu/tananyagtar/informatika/Kapin/9_evfolyam/internet.htm, Letöltés dátuma: 2018. 11. 17.

Az évek során egyre több hálózat kapcsolódott össze egymással, amíg kialakult a globális rendszer ma ismert változata, az Internet.

2.2 Informatikai hálózat fogalma: Az eddigiek alapján elmondhatjuk, hogy a számítógépes hálózat egy olyan speciális rendszer, amelyben a számítógépek és az informatikai eszközök egymással kommunikációs kapcsolatban állnak.
Ennek a technológiának számos előnye van:

- Kommunikáció
- Megbízhatóság
- Biztonságos adattárolás
- Erőforrás megosztás
- Költségkímélés
- Megosztott munkavégzés

2.3 Hálózati kommunikáció: Ahogy azt a nyelvtan érettségire megtanultuk, a kommunikáció létrejöttéhez biz. tényezőkre van szükség. Gondolok itt: adó, vevő, csatorna, üzenet, kód. A számítógépes hálózatok esetén sincs ez másként, hiszen a munkaállomások nagyon hasonló módon kommunikálnak egymással, mint az emberek. Ennek következtében az informatikai hálózatoknál ezeket a feltételeket szintén meg kell teremtenünk. Vegyük sorjában a legfontosabb összetevőket:

2.3.1 Munkaállomások: Minden olyan számítógépet és egyéb informatikai eszközt, amely csatlakozik a hálózathoz, állomásnak, vagy hostnak hívunk. Ezek jelentik az adókat és vevőket, amelyek kommunikálnak egymással. Ahhoz, hogy egy számítógép kommunikációs képességgel bírjon, elsősorban az ehhez szükséges szoftverekkel kell, hogy rendelkezzen. Ezeket a hálózatkezelési programokat az operációs rendszer rendszerint tartalmazza. Vezetékes összeköttetések esetén, fizikai szempontból nélkülözhetetlen a hálózati csatoló, vagy kártya megléte (NIC - Network Interface Controller). A csatoló segítségével lehet a hálózati kábelt csatlakoztatni az állomáshoz. Főleg régebben volt jellemző, hogy a kártyákat a számítógépek alapból nem tartalmazták, így azt külön meg kellett vásárolni, de manapság már az alaplapokban integráltan megtalálható.

2.3.2 Átviteli közeg: Amikor mi emberek beszélünk egymással, akkor a hanghullámok az adótól a vevőig a levegőn keresztül jutnak el. Légüres térben, mint pl. az űrben nagyon nehézkes lenne a beszélgetés, hiszen ott nincs kommunikációs csatorna,

amely továbbítaná az információt. Az informatikában a csatornát a vezetékes (kábelezés) és vezeték nélküli (elektromágneses hullámok) átviteli forma jelenti. (Ezekről részletesen beszélni fogunk a 9. és 10. fejezetben).

2.3.3 Üzenet: Az informatikában a számítógépek kettes (bináris) számrendszer alapján működnek. Maguk az üzenetek azok az információs csomagok, amelyek eljutnak a forrástól a célig. Bitekből épülnek fel, amely az adatmennyiség legkisebb egysége. Hasonlóan, mint amikor postai úton levelet küldünk, az üzenetek (Ethernet) keretbe, majd a keretek beágyazva az (IP) csomagba kerülnek. (Ezekről szintén lesz szó az 5. és 6. fejezetben.)

2.3.4 Kód: A hálózati kommunikációban a közös kód elengedhetetlenül fontos, ez jelenti a munkaállomások közös nyelvét. Ebben az esetben beszélünk protokollokról (szabványokról), amelyek lehetővé teszik a hálózat résztvevői számára a kommunikációt.

2.3.5 Hálózati eszközök: Az előző négy pont a hálózat megvalósításának alapfeltételei voltak. Ezen felül egy hálózat megfelelő működéséhez szükség van olyan berendezésekre, amelyek szabályozzák, irányítják az adatforgalmat. Ezeket hálózati eszközöknek szoktuk nevezni (Pl. kapcsoló, forgalomirányító). (A hálózati eszközöket a 7. és 8. fejezetben fogjuk taglalni.)

3 Főbb hálózati osztályozási szempontok

Az informatikai hálózatokat sokféle szempontból tudjuk csoportosítani.

3.1 Kiterjedés szerinti csoportosítás: Manapság az Internet sok kisebb, különálló hálózatot foglal magába. Ezeknek a mérete nagyon eltérő lehet, a benne lévő végfelhasználók függvényében. A rendszerek nagysága szerint a következőkről beszélünk:

3.1.1 PAN (Personal Area Network): A PAN-ok, másnéven személyi hálózatok a legkisebb méretű informatikai hálózatok. Amikor pl. összekapcsoljuk a telefonunkat a számítógépünkkel, rendszerint PAN-t hozunk létre. Tehát ide tartozik minden olyan eset, amely során a végfelhasználói eszközöket egy helyiségben közvetlenül összekapcsoljuk egymással.

3.1.2 LAN (Local Area Network): A LAN-ok, másnéven helyi hálózatok az Internet kis méretű informatikai hálózatai. Rendszerint egy épületen belüli hálózatról van szó, (vállalatok, intézmények saját hálózatai) amelyek napjainkban már szinte minden háztartásában megtalálhatóak. Kiterjedése a néhány száz méterig terjed.

3.1.3 MAN (Metropolitan Are Network): Főleg a városi hálózatok sorolhatók ebbe a csoportba, de MAN-nek hívjuk a LAN-okat összekötő egységet is. „*Egy ilyen hálózatban az alhálózatokon keresztül akár több tízezer számítógép összekapcsolása is megvalósulhat.”*[2]

3.1.4 WAN (Wide Area Network): A városi hálózatoknál a WAN-ok jóval nagyobbak, ebben az esetben nagykiterjedésű hálózatokról beszélünk. „*Kiterjedése pár kilométertől kezdve az egész Földre is kiterjedhet. Jobbára több szervezet birtokában van.”*[3]

3.1.5 GAN (Global Area Network): A legnagyobb, globális méretű, gyakorlatilag az egész Földet átölelő hálózatról beszélünk ebben az esetben. „*Minden korlátozás nélkül minden kommunikációs eszköz összeköttetése beleérthető. Akár a műholdas kommunikáció, akár az űreszközök kommunikációs kapcsolatai (pl. Mars szondák, vagy a világegyetem távoli végtelenjébe indított űrszondák).”*[4]

Kiterjedés szerint egy másik csoportosítás is létezik, amely az 1 sz. mellékletben található!

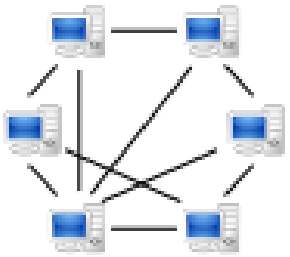
3.2 Hálózati modellek: Az informatikai rendszereket az erőforrás megosztás, ill. az azokhoz történő hozzáférés alapján kétféle csoportba szoktuk sorolni.

3.2.1 Egyenrangú hálózatok (Peer-to-peer): Az egyenrangú hálózatok nem rendelkeznek a szolgáltatásokat ellátó központi szerverrel, így a bennük lévő munkaállomások egyszerre viselkednek ügyfélként és kiszolgálóként egyaránt. Nagyon kis méretű hálózatoknál szokták alkalmazni ezt a fajta megoldást, mert telepítése könnyen és olcsón megvalósítható. A nagyobb, összetettebb hálózatoknál azonban számos hátránya van. Minél több állomással rendelkezik egy Peer-to-peer hálózat, annál lassabb működésre lesz képes, hiszen az összes

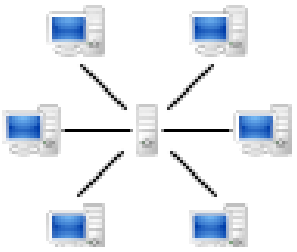
[2] Forrás: http://centroszet.hu/tananyag/szoftver/a_a_hlzatok_mret_szerinti_felosztsa.html, Letöltés dátuma: 2018. 11. 17.
[3] Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.
[4] Forrás: : http://centroszet.hu/tananyag/szoftver/a_a_hlzatok_mret_szerinti_felosztsa.html, Letöltés dátuma: 2018. 11. 17.

munkaállomás egymás erőforrásait használja. Ezen felül nehéz kialakítani biztonságos hálózatot, az eszközök nem lesznek megfelelően védve az Internet felöli támadásoktól.

3.2.2 Ügyfél-kiszolgáló alapú hálózatok: A leggyakrabban ügyfél-kiszolgáló típusú hálózatokkal találkozunk. Ebben az esetben adott a kiszolgálást nyújtó központi szerver, amely rendszerint egy nagyteljesítményű számítógépnek felel meg. Nyilvánvalóan költségesebb kivitelezéssel bír, mint egy egyenrangú rendszer. Egy jól kialakított hálózatban a központi szerver a nap 24 órájában rendelkezésre áll a vele összeköttetésben lévő munkaállomásokkal. Az erőforrás megosztás itt lényegesebb gyorsabb, és megfelelő konfigurációval nagyon biztonságossá tehetők. Talán az egyedüli hátránya, hogy a kiszolgáló meghibásodása esetén az egész rendszer megbénul. *„A kiszolgálók kezeléséhez és karbantartásához jól képzett szakemberekre van szükség, ami növeli a hálózat üzemeltetésével kapcsolatos kiadásokat.”*[5]



2. ábra: Egyenrangú hálózat
Kép forrása: https://hu.wikipedia.org/wiki/Peer-to-peer, Letöltés dátuma: 2018. 11. 27.

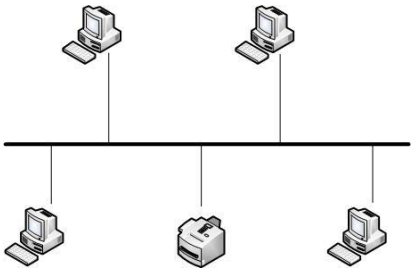


3. ábra: Ügyfél-kiszolgáló alapú hálózat
Kép forrása: https://hu.wikipedia.org/wiki/Peer-to-peer, Letöltés dátuma: 2018. 11. 27.

3.3 Hálózati topológiák: A hálózatok kiépítésének a rendszerét hívjuk topológiának. Logikai és fizikai topológiát különböztetünk meg. A hálózattervezés folyamán nélkülözhetetlen a topológiai térkép elkészítése, logikai és fizikai értelemben. (A hálózattervezéről a 12. fejezetben fogunk beszélni). A logikai topológia a hálózat eszközeinek a kommunikációját mutatja meg. Rendszerint ide tartozik az IP címzés, a forgalomirányítás menete és a hálózati biztonság (Pl. tűzfalas védelem). A fizikai topológia az eszközök fizikai elhelyezkedéseit, azok összeköttetéseit (Pl. kábelezés, hozzáférési pontok) tartalmazza.

[5] Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.

3.4 Fizikai topológia típusai



4. ábra: Busz topológia
Kép forrása: https://www.tankonyvtar.hu/en/tartalom/tamop425/0005_24_szamitogepes_halozatok_scorm_02/2352_hlzati_topolgia_szerinti_csoportosts.html
Letöltés dátuma: 2018. 11. 27.

3.4.1 Busz (sín) topológia: Főleg régebben volt jellemző ez a topológia típus az olcsó és egyszerű alkalmazása miatt, manapság viszont már elavultnak számít. A kommunikációban résztvevő állomások közvetlenül vannak csatlakoztatva a gerinchálózathoz. A gerinchálózatot alkotó buszkábel mindkét végén lezárják, hogy ne ismétlődjön a jel. Főbb hátránya, hogy biztonsági szempontból nem elég megbízható, és a buszkábel szakadása esetén a hálózat megbénul.

3.4.2 Gyűrű topológia: A gyűrű topológiában az állomások egy gyűrű (kör) alakú logikai formában vannak csatlakoztatva, az-az a hostok a szomszédaival állnak kapcsolatban. Nagy hátránya, hogy nem elég biztonságos, mivel az információ az állomásokon halad keresztül ill. bármely host meghibásodása esetén az egész hálózat működésképtelen lesz.

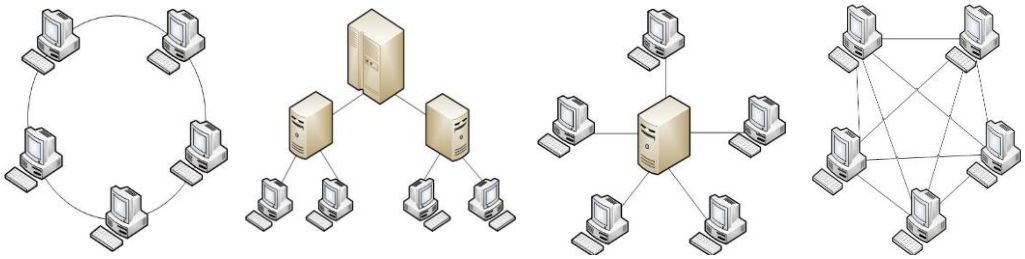
3.4.3 Fa topológia: Ebben a rendszerben a karácsonyfához hasonlóan az állomások egy hierarchikus szerkezet szerint szerepelnek. A kiszolgáló rendszerint a ’fa csúcsán’ helyezkedik el, amelyre ’ágakként’ kapcsolódik a többi eszköz. A külön ágak külön alhálózatot alkotnak. Biztonságosabb és megbízhatóbb működéssel bír, mint az előbbi típusok. Kábelhiba, vagy egy állomás meghibásodása esetén a hibatartomány csak arra az ágra terjed ki.

3.4.4 Csillag topológia: Ebben a típusban az állomások már nem egymáshoz kapcsolódnak, hanem egy központi berendezéshez. „*A központi berendezés szerepét általában egy kapcsoló vagy vezeték nélküli hozzáférési pont látja el.”*[6] Rengeteg vállalat csillag topológia szerint építi ki a hálózatát, hiszen a hostok meghibásodása esetén azok semmilyen hatással nincsenek a hálózat működésére.

3.4.5 Háló topológia: A háló topológia a legmegbízhatóbb mind közül, hiszen a hálózat összes eszköze kapcsolatban áll a többivel. A többszörös útvonalak magasszintű redundanciát biztosítanak, de nagyon komplexé teszik a rendszert, ezért a kiépítésük is messze a legdrágább megoldás. A magas költségek miatt sokszor alkalmaznak részleges hálót, ahol az eszközök legalább két másikkal állnak

[6] Forrás: Cisco CCNA Discovery2 – 3.1.2 -es fejezet, Letöltés dátuma: 2018. 11. 23.

kapcsolatban. Az olyan hálózatoknál gyakran alkalmaznak háló topológiát, ahol kiemelten fontos a hibamentes működés (Pl. gerinchálózatok).



5. ábra: Gyűrű, Fa, Csillag és Háló topológia

Kép forrása:
https://www.tankonyvtar.hu/en/tartalom/tamop425/0005_24_szamitogepes_halozatok_scorm_02/2352_hlzati_topolgia_szerinti_csoportosts.html
Letöltés dátuma: 2018. 11. 27.

4 Az OSI modell felépítése

4.1 Hálózati szabványok célja: Mivel maga az Internet globálisan az egész világot felöleli, ahhoz, hogy a hálózati kommunikáció kompatibilitását mindenhol kifogástalanul meg lehessen valósítani, nemzetközileg ki kellett alakítani egy egységes szabályrendszert. „*Nyitott, más hálózatokhoz hozzáférhető rendszerek kialakítása során, gondoskodni kell a kommunikációs feladatok rendszerezéséről, rétegekbe rendezéséről. A több gyártó által elfogadott, alkalmazott technológiákat, illetve szabványügyi szervezetek által kidolgozott ajánlásokat szabványoknak nevezzük.”*[7] A világ egyik legnagyobb szabványügyi hivatala az ISO (International Standards Organization), a Nemzetközi Szabványügyi Szervezet.

4.2 OSI modell: „*A világcégek többsége megalkotta saját hálózati architektúráját, de az eltérések miatt ezeket egységesíteni kellett, amit csak nemzetközi szinten lehetett megoldani. Ezt a feladatot az ISO szakemberei végezték el. A hálózatokra vonatkozó rétegmodell megfogalmazására 1980-ban került sor OSI (Open System Interconnection) néven.”*[8]

A modell a hálózat összetett egységeit külön hierarchia szerint bontja le, amely a hibaelhárítás során is hatalmas segítség a szakembereknek. Az OSI modell hét, hierarchikusan egymásra épülő rétegből épül fel. Az első négy réteget az alsó rétegek csoportjába soroljuk, mivel ezek mind hibamentes adattovábbításért

[7] Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.
[8]Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.

felelősek. A többi a felső rétegekhez tartozik, amelyeknek a kapcsolat logikai összeköttetése a feladatuk. A fizikai, adatkapcsolati, hálózati és szállítási réteg tartozik az alsó rétegekhez, a viszony, megjelenítési és alkalmazási pedig a felső rétegek közé. A továbbiakban nézzük a rétegzett felépítést alulról felfelé, szintről-szintre.

4.2.1 Fizikai: A fizikai réteg feladata az átviteli közeg megvalósítása a fizikai kábelek, vagy a vezeték nélküli technológiák segítségével. Az adó által küldött biteket hibamentesen továbbítania kell a célállomásnak. Hálózati eszközök tekintetében ezen a szinten működik az ismétlő és a hub.

4.2.2 Adatkapcsolati: Az adatkapcsolati réteg célja, hogy az adatfolyamot kisebb keretekből (Ethernet keret) építse fel, és hibamentesen továbbítsa a célállomásnak a fizikai rétegen keresztül. A hálózatoknál ez a réteg az, amely kapcsolatot teremt a helyi hálózaton belüli állomások körében, szabályozza az adatforgalmat, szükség esetén hibajavítást végez. A hálózati kártyák és kapcsolók tartoznak ebbe a rétegbe, amelyek a fizikai MAC-címek segítségével kommunikálnak.

4.2.3 Hálózati: A 3. réteg a forgalomirányítók szintje, ahol már IP címek segítségével történik a kommunikáció. Ebben a zónában a forgalomirányításé az-az a megfelelő útvonalválasztásé a fő szerep. Ez a réteg köti össze magukat a hálózatokat egymással.

4.2.4 Szállítási: Az alsó rétegek legfelsőbb szintje, amely „*feladata a végpontok közötti hibamentes adatátvitel biztosítása. További feladata: összeköttetések felépítése, bontása, csomagok sorrendbe állítása, hibaérzékelés, helyreállítás és az adatáramlás vezérlése.”*[9] Ezt a réteget már jellemzően a protokollok szabályozzák, ide tartozik a TCP és UDP szállítási protokoll.

4.2.5 Viszony: A logikai rétegek első szintje a viszonyréteg. „*Lehetővé teszi, hogy a számítógépek felhasználói kapcsolatot létesítsenek egymással. Jellegzetes feladata a logikai kapcsolat felépítése és bontása, párbeszéd szervezése. Szinkronizációs feladatokat is ellát, ellenőrzési pontok beépítésével.”*[10]

4.2.6 Megjelenítési: „*A fogadó rendszer számára biztosítja az adatok olvashatóságát. A megjelenítési réteg feladatai közé tartozik az adatok titkosítása, és visszafejtése is. A rétegek közül az egyetlen, amely megváltoztathatja az üzenet tartalmát.*”[11]

[9] Forrás: http://www.miau.gau.hu/szgep/szgep3_05.html, Letöltés dátuma: 2018. 11. 25.
[10] Forrás: http://www.miau.gau.hu/szgep/szgep3_05.html, Letöltés dátuma: 2018. 11. 25.
[11]Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos

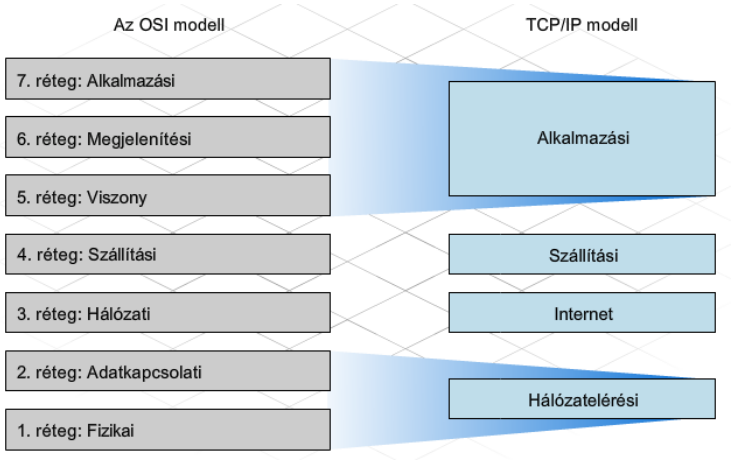
4.2.7 Alkalmazási: *„Az alkalmazások számára biztosít hálózati szolgáltatásokat. Az adó oldalon elfogadja és feldolgozza a felhasználó által továbbítandó adatokat, a vevő oldalon pedig gondoskodik azok felhasználó felé történő továbbításáról. Pl.: fájlok gépek közötti másolása.”*[12]

Csoport	#	A réteg neve	Tipikus protokollok és technológiák	A réteg tipikus hálózati komponensei
Felső rétegek	7	Alkalmazás	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Hálózaton futó alkalmazások, e-mail, web-böngészők és -szerverek, fájl átvitel, névfeloldás
	6	Megjelenítési	SSL, shell-ek és átirányítók, MIME	
	5	Viszony	NetBIOS, alkalmazási program-illesztés (API), távoli eljáráshívások	
Alsó rétegek	4	Szállítási	TCP és UDP	A lejátszással egyidejű videó- és hangletöltési mechanizmusok, tűzfalak szűrőlistái
	3	Hálózati	IPv4, IPv6, IP NAT	IP-címzés, forgalomirányítás
	2	Adatkapcsolati	Ethernet család, WLAN, Wi-Fi, ATM, PPP	Hálózati kártyák és meghajtók, hálózati kapcsolók, WAN kapcsolat
	1	Fizikai	Elektromos jelfeldolgozás, fényhullám minta, rádióhullám minta	Fizikai közeg, (réz csavart érpár, üvegszálas optikai kábel, vezeték nélküli átjátszók), hubok és ismétlők.

6. ábra: Az OSI modell felépítése
Kép forrása: Cisco CCNA Discovery2 – 2.2.1-es fejezet, Letöltés dátuma: 2018. 11. 27.

4.3 TCP/IP modell: „*Habár az OSI modell általánosan elfogadottá vált, az Internet nyílt szabványa történeti és technikai okokból mégis a TCP/IP protokollkészlet lett. A TCP/IP modellt az Amerikai Védelmi Minisztérium definiálta, mert egy olyan hálózatot kívánt létrehozni, amely minden körülmények között (még egy atomháború esetén is) működőképes marad.”*[13] Ez a modell az OSI modell hét rétegét összesen négy rétegben öleli fel.

A TCP/IP rétegeinek jellemzőt lásd a 2 sz. mellékletben!



7. ábra: Az OSI és a TCP/IP modell összehasonlítása
Kép forrása: Cisco CCNA Discovery2 – 7.2.1-es fejezet,
Letöltés dátuma: 2018. 11. 27.

Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.
[12]Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos
Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.
[13] Forrás: https://docplayer.hu/13671448-3-eloadas-a-tcp-ip-modell-jelentosege.html,
Letöltés dátuma: 2018. 11. 25.

5 Ethernet szabvány

5.1 A Protokollokról általánosan: A protokollok elengedhetetlenül fontosak az informatikai hálózat működése érdekében. Vegyük például, amikor egy nemzetközi üzleti találkozón vagyunk éppen, ahol számos, különböző nemzetiségű emberrel találkozunk. Tételezzük fel, hogy jól beszélünk angolul, viszont az ügyfelünk ezt a nyelvet kevésbé ismeri. Hogyan fogunk vele komoly üzletről beszélgetni? Talán sehogyan! Meglehetősen nagy gondjaink lehetnek még a leg apróbb társalgási szinten is. Amennyiben mindenki jól beszéli a közös nyelvet, a kommunikáció megvalósul. Így van ez a számítógépek körében is, amelyek „közös nyelvét" a protokollok szabályozzák. Ha egy hálózatban az eszközök nem ugyanazt a protokollrendszert használják, akkor hasonlóképpen az előbb említett példához, nem lesznek képesek kommunikálni egymással.

Régen, amikor a hálózatépítés még gyerekcipőben járt, a számítógépeket és a többi eszközt minden gyártó a saját módszerével kötötte össze. A probléma ott kezdődött, amikor különböző gyártóktól származó eszközöket kapcsoltak össze, és azok nem tudtak kommunikálni egymással. Ki kellett alakítani egy egységes szabályrendszert, amiket a protokollok definiálnak.

5.1.1 Protokollok fogalma: „*Minden kommunikációt – akár emberi, akár számítógépes – előre lefektetett szabályok, a protokollok irányítják. A protokollokat a forrás, a csatorna és a cél jellemzői határozzák meg. A protokollok definiálják az üzenet formátumára, az üzenet méretére, az időzítésre, a beágyazási módra, a kódolásra és a szabványos üzenetsémára vonatkozó követelményeket."*[14]

Ebben a fejezetben az Ethernet protokollkészletről lesz szó, amely a hálózatok során a legelterjedtebb LAN technológia.

5.2 IEEE szabvány: A Villamos- és Elektronikai Mérnökök Társasága (IEEE - Institute of Electrical and Electronic Engineers) szervezet felelős az Ethernet ill. a vezeték nélküli szabványokért. „*Az IEEE bizottságok a felelősök a kapcsolatokra, az átviteli közegek követelményeire és a kommunikációs protokollokra vonatkozó szabványok jóváhagyásáért és karbantartásáért. Minden technológiai szabvány*

[14] Forrás: Cisco CCNA Discovery1 – 3.2.8-as fejezet, Letöltés dátuma: 2018. 10. 03.

kap egy számot, ami azt a bizottságot jelzi, amelyik felelős az adott szabványért. Az Ethernet szabvány a 802.3-as számú bizottsághoz tartozik.

Az Ethernet 1973-as megszületése óta, a folyamatos fejlődési képessége a fő oka annak, hogy ilyen népszerű lett. Minden Ethernet verzióhoz tartozik egy szabvány. Például a 802.3 100BASE-T a 100 megabites csavart érpárt használó Ethernet szabványt jelöli. A szabvány rövidítése az alábbiakat jelöli: A 100 a sebesség jelölése Mbit/s-ban, a BASE az alapsávi átvitelt, míg a T (csavart érpár) a kábel típusát jelzi."[15]

5.3 Ethernet keret: Amikor Ethernet szabványú hálózatunk van, az információ a forrástól a célállomásig Ethernet keretben jut el. Ez a keret, másik nevén PDU (Protokol Data Unit) egy megadott szerkezetre van bontva (lásd az ábrán) és az egyes mezői különböző feladatot látnak el. Amikor egy állomás kommunikál egy

Előtag	SFD	a cél MAC-címe	a forrás MAC címe	Hossz/típus	Beágyazott adat	Keretellenőrző összeg
7	1	6	6	2	46-től 1500-ig	4

8. ábra: Az Ethernet keret (PDU) mezői (a számok a biteket jelölik)
Kép forrása: Cisco CCNA Discovery1 – 3.3.4-es fejezet, Letöltés dátuma: 2018. 11. 27.

másikkal, akkor az Ethernet keretben beágyazásra kerül a saját ill. a célállomás MAC-címe. Térjünk vissza a konferenciás példához és tegyük fel, hogy az üzleti előadás során valakit a teremben felszólítanak. Mi történik ilyenkor? Miután a címzett a saját (hallott) nevét beazonosította, a neki szánt üzenetre válaszolni fog. A teremben ülő összes többi ügyfél is hallani fogja az üzenetet, de ők nem válaszolnak rá, mivel nem nekik címezték. Párhuzamot vonva ezzel az informatika világában az üzenetküldés is tökéletesen így működik. Az-az állomás amelyik fogad egy üzenetet, dekódolja azt, majd kiolvassa a cél MAC-címet az Ethernet-keretből és amennyiben az megegyezik a sajátjával akkor feldolgozza és válaszol rá. Más esetben csupán figyelmen kívül hagyja azt.

A szabványban meg van határozva az Ethernet keret mérete, amely 64-1528 bájt közötti lehet. Egy Ethernet hálózatban az állomások csak ebbe az intervallumba beleeső üzeneteket dolgozzák fel.

[15] Forrás: Cisco CCNA Discovery1 – 3.3.2-es fejezet, Letöltés dátuma: 2018. 10. 04.

5.3.1 MAC-cím: A MAC cím (Media Access Control), amelyet közeghozzáférés-vezérlési címnek is szoktak hívni és az eszközök fizikai azonosításáért felelnek. A gyártás során minden egyes olyan interfész egyedi címet kap, amellyel az eszköz csatlakozhat a hálózathoz. A 12 számjegyből álló, hexadecimális számsorozat, kettesével van elválasztva egymástól, amely 6 bájt méretű. A MAC-cím első hat számjegyét rendszerint az IEEE szervezet határozza meg, a maradék részét az eszköz saját gyártója adja meg.

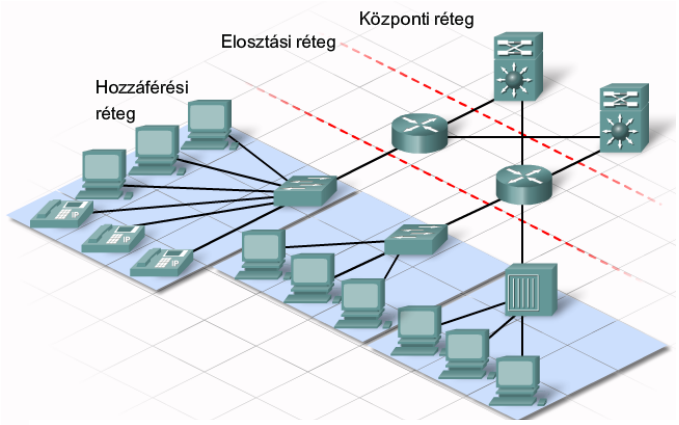
```
Physical Address. . . . . . . . . : 74-86-7A-49-69-65
```

9. ábra: Egy hálózati kártya MAC-címe
Kép forrása: Saját forrás

5.4 Ethernet hálózatok szegmentálása: Egy hálózat kialakításával nem csak az a célunk, hogy a benne lévő munkaállomások kapcsolatot tudjanak teremteni egymással, ezeket össze kell kapcsolnunk a külvilággal, az-az magával az internettel is.

Sajnos a túl sok állomást tartalmazó rendszerek, elsősorban az optimalizálatlanság miatt nem kellőképpen hatékonyak. Az Ethernet egy kézenfekvő megoldást vezetett be, és a bonyolultabb, összetettebb hálózatokat hierarchikusan kisebb részekre osztotta. A rétegzett felépítéssel az egymásra épülő szegmenseket három különálló eszközcsoportra bontotta fel, aminek számos előnye van. *„Ez a kialakítás biztosítja a hatékonyságot és a sebesség növekedését, a funkciók optimalizálását. Lehetővé teszi, hogy a hálózat igény szerint bővíthető legyen, vagyis további helyi hálózatokat adhatunk hozzá anélkül, hogy ez befolyásolná a meglévő teljesítményét.”*[16]

Az Ethernet hozzáférési, elosztási és központi réteget határozott meg:



10. ábra: Az Ethernet hálózat hierarchikus felépítése
Kép forrása: Cisco CCNA Discovery1 – 3.3.5-ös fejezet,
Letöltés dátuma: 2018. 11. 27.

5.4.1 Hozzáférési réteg: A hozzáférési réteg a hálózat belső részét jelenti, ahol jelen vannak a számítógépek és más, a felhasználók által használt eszközök. Ezek rendszerint össze vannak kapcsolva az

[16] Forrás: Cisco CCNA Discovery1 – 3.3.5-ös fejezet, Letöltés dátuma: 2018. 10. 05.

adatforgalmat megvalósító olyan hálózati eszközökkel, amelyek a munkaállomások fizikai címét használják. Ide tartozik a hub, a kapcsoló, valamint a repeater. Az Ethernet 802.3-mas szabványa szerint, a munkaállomások rendszerint kábelen keresztül csatlakoznak a hálózati eszközökhöz. Ahogy növekszik a hálózatunk, javasolt azt több hozzáférés rétegbeli részre osztani, nagyon sok esetben az állomások fizikai elhelyezkedései miatt.

5.4.2 Elosztási réteg: A hozzáférési réteg felett álló szintet hívjuk elosztási rétegnek. Az a feladata, hogy a több, egymástól függetlenül működő hozzáférési rétegbeli hálózatot összekapcsolja egymással, ill. szabályozza a közöttük áramló forgalmat. Ebben a rétegben működnek a forgalomirányítók (Routerek), amelyek információ irányítási szerepet látnak el.

5.4.3 Központi réteg: A központi réteg elsődleges célja, hogy nagy hálózati sávszélességgel kapcsolatot teremtsen a hálózatok között. Gyakorlatilag ez a gerinchálózat, amely sok esetben redundáns, az-az tartalék összeköttetéseket tartalmaz. Ez azért fontos, mert amennyiben hiba történik, akkor az eszközök ezeken az alternatív útvonallakon továbbítják az információt. A gerinchálózatokat általában teljes, vagy részleges háló topológia szerint alakítják ki, ezzel is biztosítva a redundanciát. „*A költségek csökkentése érdekében a saját központi réteg helyett sok üzleti hálózat használja az internetszolgáltató gerinchálózatát.”*[17]

6 Hálózati címzés

Az előző fejezetben beszéltünk az eszközök fizikai címzéseinek szerepéről. A MAC-címzés azonban nem elegendő feltétel az állomások kommunikációjához, minden hálózatba kötött állomásnak rendelkeznie kell logikai címzéssel is. Ezt IP (Internet Protocol) címnek hívjuk. Azért logikai, mert a MAC-címmel ellentétben ez folyamatosan változhat, annak függvényében, hogy milyen módszerrel történik annak hozzárendelése az eszközhöz.

Képzeljük el, hogy egy távoli barátunknak postán levelet szeretnénk küldeni. Nem elég csupán a nevét ismernünk, amiből a világon rengeteg lehet, tudnunk kell a pontos ország, város és utca nevét is. Mint már volt róla szó, egy munkaállomás MAC-címe szolgál

[17] Forrás: Cisco CCNA Discovery3 – 1.1.2-es fejezet, Letöltés dátuma: 2018. 12. 01.

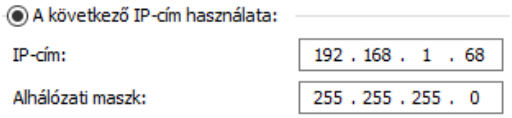
annak azonosítására, – tulajdonképpen a személynévhez is hasonlíthatnánk. Mint ahogy a személynév is csak a tulajdonosát azonosítja, de arról nem ad információt, hogy hol találhatjuk meg a világban. Többek között ez az oka annak, hogy a hálózatba kötött minden állomás rendelkezik egy logikai (IP) címmel is, amely az előbb említett példában hasonló egy személy lakcíméhez.

6.1 IPv4 és IPv6: Biztosra veszem, hogy mindenki látott már IP címet, az otthoni számítógépén, vagy okostelefonján, legalábbis, ha az IPv4-es címről van szó. A világháló exponenciális bővülésével egyre több IP címre van szükség, amely azt a problémát jelentette, hogy 2016-ban gyakorlatilag elfogytak az IP címek. Ennek köszönhetően már évekkel korábban bevezették az IPv6-os verziót, amely a 128 bites, hexadecimális címtartományával szinte kimeríthetetlen kapacitással rendelkezik. A mai számítógépjeink már alapértelmezésként kezelik az új verziót is, de az IPv4 várhatóan nem fog eltűnni, mivel vállalati szinten, belső címzésnél a jóval egyszerűbb felépítése miatt ezt használják. A továbbiakban erről a címzésről fogunk részletesen beszélni.

6.2 IP cím felépítése: Mindösszesen négy darab, ponttal elválasztott számról van szó, viszont, ha részletesen kielemezzük, ez bizony messze nem ilyen egyszerű! (Vegyük példának a 192.168.1.68 -as IP címet.) A négy darab számot úgy kapjuk, hogy a 4 bájtos (32 bit) IP címet felosztjuk négy 8 bites oktettre. A számítógépek mivel kettes (bináris) számrendszerben dolgoznak, ez 1-esek és 0-ák 32-es sorozata. Nekünk embereknek nagyon nehéz lenne ezen a módon konfigurálni őket, ezért a számítógép automatikusan decimális (tízes) számrendszerbeli számként jeleníti ezt meg. A 8 biten történő számábrázolás 0-tól 255-ig lehetséges, és ha belemegyünk egy kis valószínűségszámításba, kiszámolhatjuk, hogy a négy biten összesen 2^{32} féle lehetőség van, ami több mint 4 milliárd különböző címnek felel meg (A világhálón azonban már ez a mennyiség sem elegendő).

Egy IP cím két részből tevődik össze. A cím első része a hálózat azonosítására szolgál, míg a második az állomást jelöli azon a hálózaton. Adódik a kérdés, hogy pontosan meddig tart az első ill. a második rész. Az állomásoknak és a hálózati eszközöknek tudniuk kell, hogy melyik a hálózat és állomás azonosító. Erre szolgálnak az alhálózati maszkok.

6.2.1.1 Alhálózati maszk: Ez a fogalom ismerős lehet abban az esetben, amikor manuálisan beállítjuk az IP címünket. Az IP cím konfigurálás alhálózati maszk nélkül nem lehetséges, hiszen a maszk határozza meg, hogy a cím mely része felel a hálózat ill. az állomás felismeréséért. Az alhálózati maszkot is 4 bájton ábrázoljuk. Működése egyszerű, az 1-esek a hálózatot, a 0-ák az állomásokat azonosítják.



11. ábra: Az IP cím és alhálózati maszk beállítása
Kép forrása: Saját forrás

6.3 IP cím osztályok: Az IP címek kiosztását osztályokba rendezve alakították ki, úgy, hogy az első oktett értéke egy meghatározott intervallumban mozoghat. Öt osztályt határoztak meg, A -tól F -ig terjedő szeparálással.

12. ábra: IP címosztályok
Kép forrása: https://docplayer.hu/17591112-5-halozati-cimzes-ccna-discovery-1-5-fejezet-halozati-cimzes.html
Letöltés dátuma: 2018. 11. 28.

Címosztály	Első oktett tartomány (decimális)	Az első oktett bitek (a zöld bitek nem változnak)	Egy cím hálózati (N) és állomás (H) részei	Alapértelmezett alhálózati maszk (decimális és bináris)	A lehetséges hálózatok és hálózatonkénti állomások száma
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 hálózat (2^7-2) 16777214 állomás hálózatonként (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16382 hálózat (2^14-2) 65534 állomás hálózatonként (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2097150 hálózat (2^21-2) 254 állomás hálózatonként (2^8-2)
D	224 - 239	11100000 - 11101111	Nem használható üzleti célra mint állomás		
E	240 - 255	11110000 - 11111111	Nem használható üzleti célra mint állomás		

6.3.1 A osztály: Az ebbe az osztályba tartozó címek első oktettje 1-127 közé esik. Az ezekhez a címekhez rendelt alhálózati maszk rendszerint 255.0.0.0, tehát az első oktett felel a hálózat azonosításáért. Általában nagyobb szervezeteknek rendelnek A típusú címet, mivel így nagyon sok állomás cím osztható ki.

6.3.2 B osztály: A B osztálynak, amely 128-191 értéket vehet fel, az első 2 oktettje azonosítja a hálózatot, mivel ehhez a 255.255.0.0 -ás maszk tartozik. Közepes vállalkozások gyakran használhatnak ilyen típusú címet.

6.3.3 C osztály: C osztályú címeket (192-223) a kisebb cégek használják, mivel a 255.255.255.0-ás maszk csupán az utolsó oktettet teszi lehetővé a munkaállomások címzésére, amelynek a maximális száma 254 lehet hálózatonként.

6.3.4 D és E osztály: Ezek az osztályok már előre lefoglaltak, mivel a D-t csoportos címzés céljából (multicast) az E-t kísérleti célokra tartanak fent.

6.4 Nyilvános és privát IP címek: Az internetszolgáltatók (ISP) azzal, hogy a felhasználók számára biztosítják a hálózati hozzáférést, mindenkinek egy egyedi, nyilvános IP címet osztanak ki. Ezt nevezzük a külső IP címnek, amellyel maga a hálózat felcsatlakozik az internetre.

Mivel már nem csupán a vállalatoknál, de otthon is számos IP címmel rendelkező eszköz van, a címek gazdaságosabb kiosztása miatt vezettek be a privát, vagy magánhálózati IP címtartományokat. Ez azt jelenti, hogy egy hálózat során nem szükséges minden egyes munkaállomásnak nyilvános IP címmel rendelkeznie, hiszen azok közvetlenül nem csatlakoznak az internethez. Így a privát címeket belső hálózatok során használjuk, az egymástól különböző hálózatok ugyanazt a címzést is használhatják. Három féle címtartományt vezettek be (A, B, C), amelyeket annak tükrében kell jól megválasztani, hogy egy hálózat mennyi állomással rendelkezik, az-az mennyi belső IP címre van szüksége. Az A típusút rendszerint a hatalmas méretű hálózatok használják, ahol 16 milliónál is több címet ki lehet osztani, a 196.168-assal kezdődő C-t (Bizonyára sokaknak ismerős lehet ez a tartomány.) pedig a kisebbek. (Lásd az ábrán)

Címosztály	A lefoglalt hálózatazonosítók száma	Hálózatcímek
A	1	10.0.0.0
B	16	172.16.0.0 - 172.31.0.0
C	256	192.168.0.0 - 192.168.255.0

13. ábra: A privát IP címek három osztálya
Kép forrása: Cisco CCNA Discovery1 – 5.5.2-es fejezet, Letöltés dátuma: 2018. 11. 28.

6.5 Hálózat azonosító és szórásos címek: Amit az IP címekről feltétlenül tudnunk kell, az utolsó oktetten az első ill. az utolsó címet nem oszthatjuk ki az állomások azonosításáért. Alapesetben mindig a 0-val végződő cím azonosítja magát a hálózatot, az utolsó, 255-ös pedig szórásos üzenetküldésre használatos. A 6.2-es pontban említett 192.168.1.68-as cím (ami ugye egy privát címnek felel meg), a 192.168.1.0-ás hálózathoz tartozik. Ennek a szórásos címe pedig a 192.168.1.255.

6.6 IP címek további típusai: Az IP címeket még megkülönböztetjük egymástól, hogy azok milyen funkciót töltenek be. Beszélünk egyedi, szórásos és csoportos címzésről.

6.6.1 Egyedi címkiosztás: Minden olyan esetben, amikor pl. két számítógép kommunikál egymással, vagy bármilyen más eszközzel – egyedi címzés történik. Ezt nevezhetjük egy az egyhez kapcsolatnak is, a kommunikáció kizárólag két fél között valósul meg.

6.6.2 Üzenetszórásos kiosztás: Amikor az előző pontban említett szórásos üzenetek kiosztásra kerülnek, akkor a helyi hálózat összes állomása megkapja az üzenetet. Ebben az esetben beszélünk szórási tartományról. Ez az egy a mindenkihez kapcsolat, amelyet több hálózati protokoll is használ, mint pl. a DHCP is.

6.6.3 Csoportos címkiosztás: Az üzenetküldés ezen típusát akkor használják a hálózati eszközök, ha a belső hálózat csak egy bizonyos csoportjának küldenek üzenetet. Az egy a többhöz kapcsolatot a D típusú IP címtartomány valósítja meg, amely a 224.0.0.0 és 239.255.255.255-ös tartományban mozoghat. Egy online játék tökéletes példa, ahol a szerver csak az ebbe a csoportba tartozó felhasználókkal áll kapcsolatban.

6.7 IP cím kiosztás módjai: Az IP címek statikusan és dinamikusan konfigurálhatóak a munkaállomásokon.

6.7.1 Statikus címkiosztás: Statikus formában minden egyes eszközön külön el kell végezni a beállítást, az-az megadjuk az adott IP cím mellett az alhálózati maszkot és az alapértelmezett átjárót is (Az alapértelmezett átjárót a 8. fejeztben taglaljuk). Ez a megoldás abban az esetben hasznos, ha egy adott eszköznek folyamatosan elérhetőnek kell lennie a felhasználók számára. Ilyenek pl. a szerverek, vagy a megosztott nyomtatók.

6.7.2 Dinamikus címkiosztás: Nemcsak vállalati hálózatok során, de a legtöbb esetben otthon is dinamikus IP cím kiosztást használunk. Mindenki hallott már a DHCP-ről (Dynamic Host Configuration Protocol), ami a rendelkezésre álló logikai címek automatikus kiosztásáért felelős. Nagyobb hálózatokban sok esetben DHCP szervert használnak erre a célra, de szinte az összes forgalomirányító is rendelkezik ezzel a képességgel. Egy otthoni, vezeték nélküli hálózatban pl. a Wi-Fi router osztja ki a címeket, így könnyedén felcsatlakozhatunk a hálózatra anélkül, hogy még a telefonunkon is külön beállítanánk azt. A DHCP minden egyes hálózatba történő felcsatlakozáskor új címet rendel az állomáshoz a maszk és az átjáró mellett.

7 Hozzáférési réteg hálózati eszközei

Az 5. fejezetben az Ethernet hálózatok hierarchikus felépítéséről volt szó. Ebben a részben az Ethernet hozzáférési rétegének hálózati eszközeiről fogunk beszélni.

A számítógépek, amelyek amennyiben felcsatlakoznak a hálózatra, már munkaállomásokként funkcionálnak. A legtöbb végfelhasználói eszköz ilyen jellegű. Az állomások körében nem csak számítógépekről beszélünk, hanem minden olyan eszközről, amelyek a hálózaton keresztül üzenetet küldenek és fogadnak. Ide tartozhat egy okostelefon, egy kiszolgáló (szerver), vagy akár egy megosztott periféria, mint pl. a hálózati nyomtató. Nagyon fontos megjegyeznünk, hogy az állomások nem tartoznak a hálózati eszközök körébe, csak úgy, mint a perifériák. A hálózati eszközök (A hozzáférési rétegben leggyakrabban a hub és kapcsoló) továbbítják és szabályozzák a forgalmat, hogy az információ megfelelően célba érjen.

7.1 Ismétlő (Repeater): Egy nagyon egyszerű hálózati eszközről van szó, *„ami mindössze a jelek ismétlését és erősítését végzi. Semmilyen szűrést, illetve irányítást nem végez, csupán a jeleket erősíti fel.*[18] *Olyankor használjuk, amikor egy hálózati szegmens már elérte a maximális hosszát, és szükséges az analóg, vagy digitális jelek újragenerálása. Mivel a repeater csak a bitek jeleinek erősítésével foglalkozik, kijelenthetjük, hogy ez az eszköz az OSI modell fizikai szintjén működik.”*[19]

14. ábra: Repeater
Kép forrása: https://www.shure.com/americas/products/accessories/discussion-systems/rp-6004-repeater, Letöltés dátuma: 2018. 11. 28.

7.2 Hub: A hubokat az állomások hálózatba történő csatlakoztatására használjuk. Egyszerű hálózati eszközökről van szó, mivel csak adattovábbítási szerepet látnak el. Ennek köszönhetően az OSI modell fizikai rétegéhez tartozik. Az üzeneteket nem képes dekódolni és meghatározni, hogy azt mely állomásnak kell továbbítania. Gyakorlatilag az egyik portján

15. ábra: Egy D-Link-es hub
Kép forrása: http://www.antkh.com/project/Computer%20Science/pages/hub.htmlLetöltés dátuma: 2018. 11. 28.

[18] Forrás: https://www.tferi.hu/kabelek?showall=&start=3, Letöltés dátuma: 2018. 11. 21.
[19]Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.

bejövő üzenetet a többi portján automatikusan továbbküldi. Egy bonyolultabb, nagy méretű hálózatban nem tanácsos hubokat alkalmazni, mivel elég instabillá tehetik a rendszer működését. A legnagyobb hátránya, hogy egyidőben csak egy üzenetet képes küldeni. Amennyiben több állomás egyszerre próbál kommunikálni, úgy ezek az üzenetek ütköznek egymással és megsérülnek. A hub az ilyen üzenet töredékeket is ugyan úgy továbbküldi a hálózatban. Amint az állomások észlelik a sérült fájlt, újraküldik azt. Ebben az esetben beszélünk ütközési tartományról, amely azt a területet jelöli, ahol az üzenetek ütközhetnek. Amint ez a tartomány elég nagy, egyre csak nőhet az ütközések esélye. A sok ütközés következtében sok újraküldés történik, ami torlódást eredményezhet, és nagyban lelassíthatja a hálózati forgalmat.

7.3 Kapcsoló (Switch): A Switchek jóval intelligensebb eszközök, mint a hubok voltak, hiszen dekódolja az üzeneteket. A kapcsoló MAC-cím táblával rendelkezik, amely tartalmazza a vele összeköttetésben lévő állomások fizikai címeit, és az azokhoz vezető utat, az-az a port számait. A beérkező Ethernet keretekből kiolvassa a cél MAC-címet, összehasonlítja a táblájában lévővel, majd az ahhoz rendelt portján továbbküldi a megfelelő célállomásnak. Amennyiben egy olyan keretet kap, aminek a cél MAC-címe nem szerepel a táblájában, abban az esetben a kapcsoló hubként működik. Tehát szórásos eljárásként az összes vele kapcsolatban álló eszköznek elküldi az üzenetet. Ezt elárasztásnak nevezzük. A továbbküldött üzenetet mindegyik állomás dekódolja és csak a megfelelő célcímmel rendelkező host fogja feldolgozni, majd válaszolni rá.

16. ábra: Egy nagy teljesítményű ipari kapcsoló a D-Link-től
Kép forrása: http://eastasiaeg.com/en/d-link-_switch-28-port-des-1210-28pe, Letöltés dátuma: 2018. 11. 28.

Egy kapcsolóval összekötött hálózat bővítésénél nagyon fontos, hogy az eszköz minél hamarabb „megtanulja” az összes állomás MAC-címét és útvonalát. Amikor egy új állomás üzenetet küld, a switch azonnal rögzíti annak a forrás MAC-címét és azt az interfészt, amelyen keresztül az állomás csatlakozik hozzá. Minden ilyen esetben a tábláját automatikusan frissíti. A hubbal ellentétben egyidőben több üzenet továbbítására is alkalmas, így a csak kapcsolóval ellátott hálózatokban nem történik ütközés. Amennyiben a kapcsolók mellett hubok is szerepelnek, az

```
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.c7ad.e316    DYNAMIC     Fa0/24
  10    0002.4ab7.1701    DYNAMIC     Fa0/24
  11    0001.c7ad.e316    DYNAMIC     Fa0/24
  11    0002.4ab7.1701    DYNAMIC     Fa0/24
  12    0001.c7ad.e316    DYNAMIC     Fa0/24
  12    0002.4ab7.1701    DYNAMIC     Fa0/24
  12    000d.bd94.6b58    DYNAMIC     Fa0/1
  12    0060.3e5c.ba1d    DYNAMIC     Fa0/2
  12    00e0.f934.e3c4    DYNAMIC     Fa0/3
  13    0001.c7ad.e316    DYNAMIC     Fa0/24
  13    0002.4ab7.1701    DYNAMIC     Fa0/24
Switch#
```

17. ábra: A kapcsolók által használt MAC-cím tábla
Kép forrása: https://stackoverflow.com/questions/39797288/how-would-you-design-a-mac-address-table-essentially-a-fast-look-up-table, Letöltés dátuma: 2018. 11. 28.

esetleges ütközések által létrejött sérült kereteket a switchek nem továbbítják. Gyakorlatilag a kapcsoló minden egyes portja egymástól elkülönülő, kisebb ütközési tartományokat hoz létre.

7.3.1 Szórásos üzenetek: Számos esetben nagyon fontos, hogy a LAN eszközei egyszere tudjanak kommunikálni egymással. Egy ilyen eset, amikor egy új munkaállomás kerül a hálózatba. Emlékezzünk vissza a konferenciás példánkhoz és tételezzük fel, hogy mindenki számára egy új ügyfél érkezik. Az első dolog, hogy mindenki megismerje, az, ha mindenkinek bemutatkozik. Ez a folyamat zajlik le egy új állomásnál, olyan formában, hogy a hálózat összes tagjának szórásos üzenetet küld. Ebben az üzenetben a cél MAC-cím binárisan csak 1-esekből áll, amelynek a hexadecimális megfelelője az FF-FF-FF-FF-FF-FF. Ezt az üzenetet látva a kapcsoló is automatikusan továbbküldi mindenkinek. A hálózatnak azt a részét, ahol szórásos üzenetek vándorolnak, szórási tartománynak hívjuk. *„Amennyiben túl sok állomás csatlakozik egyazon szórási tartományhoz, a szórásos forgalom mértéke túlságosan is megnövekedhet. Újabb állomások hozzáadásával a hálózat növekszik, ami egyre nagyobb hálózati, és ezzel együtt szórásos forgalmat is jelenthet. A teljesítmény javítása érdekében gyakran szükség van egy helyi hálózatot vagy szórási tartományt több hálózatra bontani.”*[20]

7.3.2 ARP: Az ARP (Address Resolution Protocol) egy címmeghatározó protokoll, amelynek akkor van jelentősége, amikor egy állomás csupán a cél IP címet ismeri, a MAC-címet nem. Mivel a helyi hálózatban az eszközök a fizikai címek alapján tájékozódnak, az IP címek nem adnak iránymutatást. Erre szolgál az ARP protokoll. A folyamat úgy működik, hogy

```
Interface: 192.168.1.6 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.66          54-2a-a2-f2-6a-d4     dynamic
  192.168.1.254         b0-89-00-22-4b-30     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

18. ábra: Egy munkaállomás ARP táblája
Kép forrása: Saját forrás

[20] Forrás: Cisco CCNA Discovery1 – 3.4.4.2-es fejezet, Letöltés dátuma: 2018. 11. 21.

a cél MAC-címet nem ismerő állomás elküld egy ARP kérést, egy speciális, szórásos üzenetet, amely tartalmazza a célállomás IP címét, amelyre a megfelelő állomás válaszolni fog a saját MAC-címével együtt. Minden munkaállomásnak saját ARP táblája van, amiben tárolja ezeket az információkat. (Lásd 18. ábra!)

7.4 Híd (Bridge): „*A hálózati híd különböző hálózati szegmenseket köt össze az OSI-modell második rétegében. Ez az eszköz a MAC-cím alapján irányítja az egyes adatcsomagokat.”*[21] Helyi hálózatok összekapcsolására tökéletesen alkalmas.

19. ábra: Hálózati Híd
Kép forrása: https://www.indiamart.com/aakashindustries-hyderabad/network-device.html, Letöltés dátuma: 2018. 11. 28.

7.5 Vezeték nélküli hozzáférési pont: Az ilyen eszközöket Wi-Fi routereknek is szoktuk nevezni, amelyek mindenki számára ismerősek lehetnek. Szinte már minden háztartásban létezik vezeték nélküli hálózat, amelyet a legkönnyebb ill. a legolcsóbb megvalósítani és az okos eszközöket is maximálisan kiszolgálja. Kizárólag egy hozzáférési pont (AP – Access Point) szükséges hozzá. „*A Wi-Fi routerek sugározzák az SSID (Service Set Identifier, beállított szolgáltatóazonosító) csomagokat, amelyek alapján a kliensek csatlakozni tudnak a hálózathoz. Az AP-k saját antennával rendelkeznek, kapcsolódási lehetőséget pedig meghatározott területen nyújtanak, amit cellának nevezünk. A cella méretét döntően befolyásolja az antenna mérete és teljesítménye. Nagyobb terület lefedéséhez, több AP telepítésére van szükség átfedésekkel.”*[22]

20. ábra: Egy TP-Link-es Wifi router
Kép forrása: https://edigital.hu/dual-band-router/tp-link-archer-c7-ac1750-ketsavos-gigabites-vezetek-nelkuli-router-p263748, Letöltés dátuma: 2018. 11. 28.

8 Forgalomirányítás az elosztási rétegben

A forgalomirányító használata nélkülözhetetlen a hálózati kommunikáció során. Ez a hálózati eszköz nem munkaállomásokat köt össze, mint a switch és a hub, hanem hálózatokat kapcsol össze egymással. A legtöbb háztartásban is már működnek helyi

[21] Forrás: https://www.tferi.hu/kabelek?showall=&start=3, Letöltés dátuma: 2018. 11. 22.
[22]Forrás: Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf, Letöltés dátuma: 2018. 11. 16.

hálózatok, pl. vezeték nélküli Wi-Fi hálózat, amelyet szintét csak a forgalomirányító segítségével tudunk összekötni az Internettel. Nagyobb vállalatok esetén, ahol a sok host miatt több helyi hálózat is előfordulhat, szintén forgalomirányítóra van szükség.

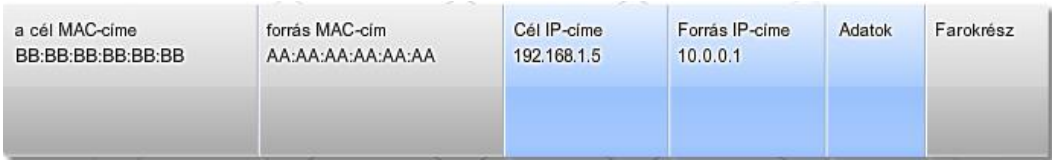
8.1 Forgalomirányító működése: Ez az eszköz, mint ahogy a neve is tartalmazza, forgalomirányítási feladatokat lát el. Működése a kapcsolóhoz hasonló, dekódolja a rajta keresztül haladó üzeneteket. Ezeknél az üzeneteknél már nem keretekről, hanem IP csomagról beszélünk. Amikor a router egy keretet fogad, kicsomagolja belőle az IP csomagot, majd kiolvassa belőle a cél IP címet és annak a hálózati része segítségével tudja megválasztani a megfelelő útvonalat a megfelelő hálózatba való továbbításához. A router irányítótáblával rendelkezik, ami hasonlít a kapcsolók esetében a MAC-cím táblára. Az irányítótábla tartalmazza az összes vele kapcsolatban álló hálózat címeit, a hozzájuk vezető útvonalakkal együtt. Egy üzenet fogadásakor a forgalomirányító automatikusan összehasonlítja a cél IP címet az irányítótáblájában lévő hálózati címekkel, és amennyiben a cél IP cím hálózati része megtalálható benne, beágyazza az IP csomagot a keretbe és továbbítja azt a megfelelő útvonalon. Ezt a folyamatot nevezzük forgalomirányításnak. Az előző fejezetben megbeszéltünk, hogy a kapcsolók esetén szórási tartományok alakulnak ki a hozzáférési rétegben. A routerek megfelelő lezárást biztosítanak a szórásos üzenetekkel szemben, hiszen azokat nem engedik át a másik hálózatba.

21. ábra: Egy Cisco Integrált forgalomirányító
Kép forrása: https://www.senetic.hu/product/ISR4331/K9,
Letöltés dátuma: 2018. 11. 28.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1        10.0.0.75     35
         10.0.0.0    255.255.255.0         On-link         10.0.0.75    291
        10.0.0.75  255.255.255.255         On-link         10.0.0.75    291
       10.0.0.255  255.255.255.255         On-link         10.0.0.75    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link       192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link       192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link       192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link        10.0.0.75     291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
```

22. ábra: Egy router irányítótáblája
Kép forrása: https://www.howtogeek.com/howto/windows/adding-a-tcpip-route-to-the-windows-routing-table/
Letöltés dátuma: 2018. 11. 28.

8.1.1 IP csomag: Az IP csomag, egy olyan logikai, üzenet egység, amely segítségével a forgalomirányítók kommunikálnak. Ez az IP csomag kerül beágyazásra az Ethernet keretbe, amely az adatokon kívül tartalmazza a forrás és cél IP címeket. (Lásd az ábrán!)



23. ábra: Az IP csomag (kéken) az Ethernet keretbe ágyazva
Kép forrása: Cisco CCNA Discovery1 – 3.5.2-es fejezet, Letöltés dátuma: 2018. 11. 28.

8.2 Forgalomirányítási útvonalak:

8.2.1 Alapértelmezett átjáró: Amikor a munkaállomások egy másik hálózatban lévőnek küldenek üzenetet, tudniuk kell, hogy melyik útvonalon tehetik ezt meg. Pontosan ezért a forgalomirányítók minden portján saját IP címe van, amin azonosítható a hostok és a többi eszközök számára. Ez az IP cím a router annak az interfésznek az azonosítására szolgál, amellyel csatlakozik az adott hálózathoz. *„A helyi hálózat minden állomása az alapértelmezett átjáró címét használja ahhoz, hogy üzenetet küldjön a forgalomirányítónak. Amint az állomás megtudja az alapértelmezett átjáró IP címét, használhatja az ARP protokollt a MAC-cím meghatározásához.”*[23]

24. ábra: Az alapértelmezett átjáró beállítása az IP cím és maszk mellett, Kép forrása: Saját forrás

A számítógép hálózati beállításainál nem véletlenül látható az alapértelmezett átjáró, az IP cím és az alhálózati maszk mellett. A forgalomirányítók interfész címzésénél általában az adott címtartomány első vagy az utolsó logikai címét érdemes hozzárendelni. Ennek tükrében egy 192.168.1.0-s hálózatban a router általában a 192.168.1.1, vagy a 192.168.1.254-es címet kapja.

8.2.2 Közvetlen csatlakozású útvonalak: Minden olyan útvonalat, amelyen keresztül a forgalomirányító egy másik eszközhöz csatlakozik, közvetlen útvonalaknak hívjuk. A legtöbb útvonalbejegyzés ilyen típusú, amelyek az irányítótáblában automatikusan frissülnek.

8.2.3 Statikus útvonal: Statikus útvonalakat a rendszergazda manuálisan állíthat be egy forgalomirányító konfigurációjában. Az irányítótáblából ez nem fog törlődni, az eltávolítását szintén a rendszergazda végezheti el.

8.2.4 Alapértelmezett útvonal: A router minden olyan üzenetet figyelmen kívül hagy, amely cél IP címét nem tud párosítani az irányítótáblájában lévőkkel. „*Az alapértelmezett útvonal az az interfész, melyen keresztül a forgalomirányító az ismeretlen cél IP-hálózati címet tartalmazó csomagokat továbbítja.”*[24] Gyakorlatilag ez is statikus útvonal és szintén manuálisan történik a konfigurálása a routeren, hogy az eszköz ne dobja el a csomagot. „*Az alapértelmezett útvonal általában egy másik forgalomirányítóhoz csatlakozik, amely képes a csomagot annak célhálózata felé továbbítani.”*[25]

8.2.5 Dinamikus útvonal: A forgalomirányítási protokollok a felelősek a dinamikus útvonalak létrehozásáért és kezeléséért. „*Az forgalomirányító protokollok irányítási információkat cserélnek egymással a hálózaton.”*[26]

A forgalomirányítási protokollokról az 3 sz. melléklet egy részletes fejezetet tartalmaz!

8.3 Forgalomirányító ARP-táblája: Az előző fejezetben volt szó az ARP funkciójáról. Mivel a routerek a hálózatok között irányítják a forgalmat, az irányítótábla mellett rendelkezik minden egyes hálózathoz ARP táblával is, csak úgy, mint az állomások. Az irányítótábla nem tartalmazza az állomások fizikai címeit, ezeket az ARP táblában listázza, hogy mely fizikai címhez mely IP cím tartozik.

8.4 Hálózati címfordítás (NAT): A forgalomirányítás során egy olyan probléma merül fel, hogy egy belső hálózat állomásai nem tudnak kommunikálni közvetlenül az internettel, mivel azok csak magánhálózati IP címekkel rendelkeznek és mint tudjuk azok nem kompatibilisek a publikus címekkel. Itt jön a NAT (Network Address Translation), aminek a feladata, hogy a sok belső címhez párosítson egy vagy maximum néhány külső, privát címet. Tökéletes példa erre egy szolgáltatást nyújtó cég, pl. az internetszolgáltató ügyfélszolgálata. Amikor egy esetleges hiba során betelefonálunk a megadott telefonszámon, minket a cég a megfelelő, vagy éppen elérhető szakemberhez fog kapcsolni. Minden hibabejelentő ugyanazt a

[24] Forrás: Cisco CCNA Discovery1 – 3.5.4-es fejezet, Letöltés dátuma: 2018. 11. 05.
[25] Forrás: Cisco CCNA Discovery1 – 3.5.4-es fejezet, Letöltés dátuma: 2018. 11. 05.
[26] Forrás: Cisco CCNA Discovery2 – 6.1-es fejezet, Letöltés dátuma: 2018. 11. 05.

telefonszámot használja, mégis sok esetben nem ugyanazzal a munkatárssal fognak beszélni.

Ezt a hálózati címfordítást a forgalomirányító végzi, aminek számos előnye van. Először is biztonságos, mivel elrejti a belső hálózat eszközeit az internet felöli eléréstől, tehát védelmet nyújt egy esetleges külső behatolás ellen. A módszerrel nyilvános IP címek takaríthatók meg, hiszen azok többszörös felhasználásra kerülnek, a sok helyi állomás megosztottan fogja használni őket. A NAT konfigurációja statikusan ill. dinamikusan lehetséges.

(A típusok a 4 sz. mellékletben megtalálhatóak! A NAT egy fejlettebb változatáról a PAT-ról pedig az 5 sz. mellékletben lesz szó!)

8.5 Integrált Forgalomirányítók (ISR): Egy integrált forgalomirányító használata (Integrated Services Router) nagyban megkönnyíti még a kisebb vállalatok hálózati kommunikációját is, hiszen számos funkciót ellát. *„Az ISR egy eszközben kínálja a forgalomirányítási, LAN kapcsolási, biztonsági, hangátviteli és WAN kapcsolódási funkciókat.”*[27] Nem véletlenül nagy népszerűségnek örvend, sok esetben olcsóbb a telepítése, mint másik routerek esetén.

Saját tapasztalatomból is csak ajánlani tudom őket, egy jól bekonfigurált ISR kellő rugalmasságot, gyorsaságot, bővíthetőséget, megbízhatóságot és nem utolsó sorban biztonságot nyújt a belső hálózat számára.

9 Kábelezési eljárások

Egy hálózatban a kommunikáció létrejöttéhez a forrás és cél állomás összeköttetéséhez meg kell teremtenünk a csatornát, az-az az átviteli közeget, amelyen keresztül az információ biztonságosan továbbítva lesz. Gyakorlatilag kétféle típust különböztetünk meg egymástól. Vállalatok esetében meghatározó a fizikai, vagy vezetékes, ill. a háztartásokból jól ismert vezeték nélküli technológia (Pl. WI-FI). Ebben a fejezetben a kommunikáció fizikai megvalósításáról lesz szó.

A fizikai hálózati kábelek három leggyakrabban használt változata a csavart érpár, koaxiális és az optikai kábel.

9.1 Csavart érpár (TP): Gyakorlatilag a legnépszerűbb kábeltípusról van szó, köszönhetően annak, hogy megfelel az Ethernet, a legtöbb hálózat alapvető szabványának. Mint ahogy a nevében is benne van, a kábelekben lévő rézvezetékeket páronként egymással összecsavarják, ez kisebb fokú védelmet nyújt

az adatátvitel mértékének. Amennyiben a cégen belül nincs elektromágneses interferencia (EMI), abszolút ajánlott a használata. A TP-s kábeleknél kb. 100 méter a maximálisan összeköthető távolság. A csavart érpáras kábelek két fő fajtáját különböztetjük meg, az árnyékolt és árnyékolatlan kábeltípust.

9.1.1 Árnyékolatlan csavart érpár (UTP): Az UTP kábel nagy népszerűségnek örvend, talán a legelterjedtebb típusról van szó, mivel ez a legolcsóbb mind közül. E mellett könnyen telepíthető és nagy sávszélességgel rendelkezik. Jellemzően telefonfonalak esetén használatos a Cat 3 UTP kábel, mivel csak hang alapú kommunikációra képes. A Cat 5, ill. Cat 5e jellemzően gyors, eléri az 1 Gbps-os átviteli sebességet. A Cat 6 -os elérheti a 10 Gbps sebességet. Ennél a típusnál az egyes érpárakat szigetelőanyaggal különítik el egymástól.

25. ábra: UTP kábel RJ-45-ös csatlakozóval
Kép forrása: https://kabel-csatlakozo.arukereso.hu/e132-25-cat6-utp-kabel-25m-p411457233/
Letöltés dátuma: 2018. 11. 28.

9.1.2 Árnyékolt csavart érpár (STP): Ennél a kábeltípusnál meg kell jegyezni, hogy a réz vezetékeket egyenként árnyékoló fóliával veszik körbe, majd mind a négy érpárat egy közös szigetelő réteggel vonják be. Jóval nagyobb védelmet nyújt, mint az UTP, de sajnos ennek köszönhetően sokkal drágább is. Ide tartozik jellemzően a Cat 7-es típus, az ScTP.

9.2 Koaxiális kábel: Mindenkinek ismerős lehet ez a típus, hiszen jellemzően az otthoni televíziót szoktuk csatlakoztatni vele a fali aljzathoz. E mellett vállalati szinten célszerű használni nagy sebességű interfészek összeköttetéséhez. A koaxiális kábel is elektromos jelek segítségével működik. A kábel belsejében egy réz mag továbbítja az adatokat, amelyet általában műanyagból készült szigetelő réteggel vonnak be. Ennek köszönhetően valamelyest ellenállóbb az elektromágneses interferencia ellen, mint a csavart érpár. Mivel azonban sokkal drágább a beszerzése, telepítése, ill. a hibaelhárítása is nehezebben történik, nem mondható túl gyakorinak a koax használata.

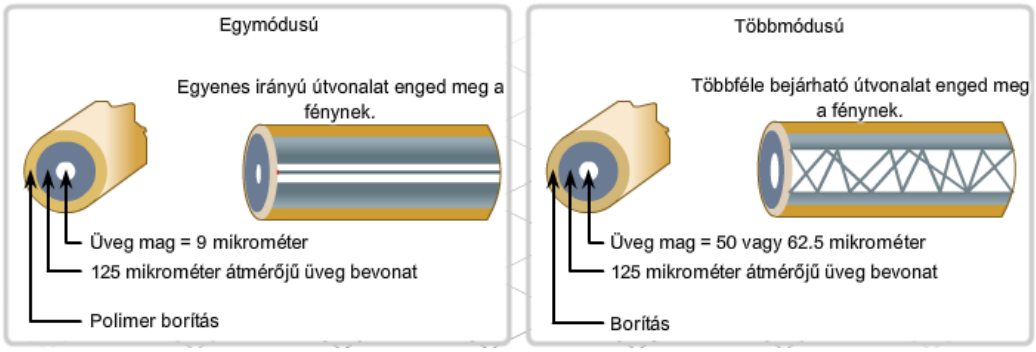
26. ábra: Koaxiális kábel
Kép forrása: https://www.alza.hu/koaxialis-kabel-f-csatlakozo-10-m-d241751.htm
Letöltés dátuma: 2018. 11. 28.

9.3 Optikai kábel: Minden olyan vállalati környezetben, ahol problémát okozhat az elektromágneses interferencia, optikai szálas kábelt kell használni. Ez a kábeltípus

teljesen érzéketlen az EMI-ra, hiszen fényimpulzusok segítségével működik, így nem vezeti az elektromosságot. Különösen nagy átviteli sebességüknek köszönhetően gyakran alkalmazzák gerinchálózatok összeköttetésére. Az optikai kábeleknek két fajtáját különböztetjük meg: az egymódusút és többmódusút.

27. ábra: Optikai szálas kábel
Kép forrása: https://www.infolex.hu/termekek/adatlap/52013/hq-toslink-15m-optikai-kabel-hqss462315,
Letöltés dátuma: 2018. 11. 28.

9.3.1 **Többmódusú:** A többmódusú optikai kábel használata valamelyest szélesebb körben elterjedt, mivel beszerzése olcsóbb. Ennél a típusnál az információ LED technológia alapján továbbítódik. Ahogyan a 28. ábrán is látható, az üveg magon egyszerre több fénysugár halad keresztül, így a távolság növekedésével egyre inkább csökken a jel minősége. 1-2 km távolságig alkalmazható a telepítése.



28. ábra: Az egymódusó és többmódusó optikai kábel összehasonlítása
Kép forrása: Cisco CCNA Discovery1 – 4.4.4-es fejezet, Letöltés dátuma: 2018. 11. 28.

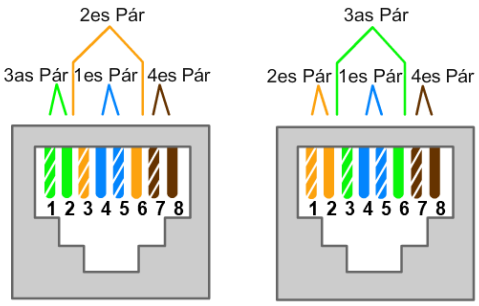
9.3.2 **Egymódusú:** A sokkal költségesebb egymódusú optikai kábel egy fejlettebb technológiát használ. A kisebb magátmérőjű üveg magban lézer fény továbbítja az információt. Az optikai szál egyenes irányú útvonalat biztosít a fénynek, ezért sokkal intenzívebb átvitelre képes, mint a többmódusú. További előnye, hogy nagyon nagy, több kilométeres távolságok összeköttetése is megvalósítható.

9.4 **Kábel végi csatlakozó:** Amikor egy informatikai boltban megfelelő méretű hálózati kábelt vásárolunk, természetesnek vesszük, hogy azzal már semmilyen dolgunk nincs. Egy rendszergazdának azonban tisztában kell lennie a kábelek végződésével, hiszen kisebb vállalatok esetében is bármikor előfordulhat kábelhiba, szakadás. Különösen igaz ez a savart érpárú kábelek esetében, azok telepítése és hibaelhárítása egy informatikus alapvető feladatai közé tartozik.

Valamennyi UTP és STP kábelt RJ-45-ös csatlakozóval látnak el, amely az érpáraknak megfelelően 8 érintkezővel rendelkezik. Kétféle bekötési séma létezik:

a T-568A és T-568B. Tapasztalataim szerint gyakrabban használják a B típusút. Ez esetben az 1-8-ig terjedő érintőknek megfelelően narancs-fehér, narancs, zöld-fehér, kék, kék-fehér, zöld, barna-fehér, barna színkód szerint kell az érpárakat csatlakoztatni. Fontos, hogy az érpárak ütközésig be legyenek toldva a csatlakozó végébe, utána krimpelő fogó segítségével lezárhatjuk azt.

A csavart érpárú vezetékeknél a hálózati működés érdekében kétféle kábeltípus létezik. Egyenes ill. keresztkötésű kábelt az A és B séma megfelelő kombinációjával hozhatunk létre. Ez azért fontos, mert a két összekötött eszköz nem mindig ugyanazokat az érintőket használja adásra és vételre.



29. ábra: A T-568A -és B típusú kábel színkódja
Kép forrása: Cisco CCNA Discovery1 – 4.5.2-es fejezet, Letöltés dátuma: 2018. 11. 28.

9.4.1 Egyeneskötésű kábel (Patch): Egyeneskötésű kábelről beszélünk, amikor az adott UTP vagy STP kábel mindkét végén T-568A-s, vagy T-568B-s sémájú RJ-45-ös csatlakozó van, tehát a kötési sablon megegyezik. Másik nevén patch kábelnek is szoktuk nevezni.

Vegyük példának egy személyi számítógép és egy kapcsoló csatlakoztatását:

„Egy személyi számítógép RJ-45-ös csatlakozóján az 1-2 érintkezők felelnek a küldésért, a 3-as és a 6-os a fogadásért. Egy kapcsoló hálózati csatlakozóján az 1-2-es érintkezők fogadnak, a 3-as és a 6-os érintkezők küldenek. A számítógépnél küldésre használt érintkezők, a kapcsoló esetén fogadásra használtak."[28] Ezáltal egyeneskötésű kábelt kell alkalmaznunk. Egyeneskötésű kábelezést használunk még a PC – Hub és Forgalomirányító – Kapcsoló csatlakoztatásához.

9.4.2 Keresztkötésű kábel (Cross-link): Ezen kábel esetében az egyik vége T-568A, a másik T-568B típusú csatlakozót használ. A közvetlenül kapcsolódó hálózati eszközök esetén a küldés-fogadás ugyanazon az érpárakon keresztül történnek. Ebben az esetben keresztkötésű kábelre, vagy másik nevén cross-link kábelre van szükségünk. Keresztkötésű kábelt kell használni a következő esetekben: Kapcsoló – Kapcsoló; Kapcsoló – Hub; Hub – Hub; Forgalomirányító – Forgalomirányító;

[28] Forrás: Cisco CCNA Discovery1 – 4.5.2-es fejezet, Letöltés dátuma: 2018. 10. 04.

PC – Forgalomirányító; PC – PC. Mindenképpen meg kell jegyeznünk, hogy a technológia fejlődésével, a mai korszerű számítógépek már automatikusan felismerik, amennyiben patch kábellel kötöttük össze őket és ugyanúgy képesek a kommunikációra, mint Cross-link esetén.

9.5 Kábelek telepítése, kábelmenedzsment: Egy hálózat építésénél a kábelezésre mindig is különösen nagy gondot fordítsunk. A tervezésnél jól meg kell gondolnunk, hogy a leg megfelelőbb kábeltípust használjuk, különösen a már említett tényezők miatt (pl. EMI). Tisztában kell lennünk, hogy a céges hálózati eszközök mely kábel szabványokat támogatják. Fontos, hogy azoknak olyan átviteli közeget biztosítsunk, amely során kompatibilisek lesznek egymással és a legjobb működésre lesznek képesek. Figyelnünk kell, hogy a különböző kábeltípusoknál eltérő a maximálisan telepíthető kábelhosszúság.

30. ábra: Rack szekrény hálózati eszközökkel
Kép forrása: http://lvnetwork.hu/index02.html
Letöltés dátuma: 2018. 11. 28.

Több vállalat rendelkezik telekommunikációs helyiséggel, ahol rendszerint kábelszekrények kapnak helyet, patch panelokkal kiegészítve. Nagyobb hálózat működéséhez ez elengedhetetlen, hiszen kapcsolódási pontként összeköti a munkaállomásokat a többi hálózati eszközzel. Mivel nagyszámú kábelekre kell számítanunk, azok csatlakozóba történő illesztéséhez betűznünk kell őket, betűző szerszám (punchdown tool) segítségével. Lényeges, hogy minden hálózati kábel esetén pontosan tudjuk, hogy melyik eszközt csatlakoztattuk vele.

31. ábra: Betűző szerszám
Kép forrása: https://www.infolex.hu/termekek/adatlap/54784/valueline-betuzo-szerszam-vlcp89555l
Letöltés dátuma: 2018. 11. 28.

Ahhoz**,** hogy egy teljesen átlátható hálózatot alakítsunk ki, igyekezzük menedzselni a kábelezést. Ez azt jelenti, amikor egy strukturált rendszert alakítunk ki és a rendezett hálózatban könnyebb lesz diszkriminálni az esetleges kábel problémákat. Minden kábelt a megfelelő működés érdekében még a bekötés előtt érdemes letesztelnünk. (A kábel ellenőrző eszközökről a 17. fejezetben bővebben beszélünk!)

10 Vezeték nélküli technológiák

Az előző fejezetben az adatátvitel fizikai megvalósításáról volt szó, most ennek a vezeték nélküli megvalósításáról fogunk beszélni. Bizonyára mindenki ismeri a Wi-Fi-t, amely a legismertebb és leggyakoribb változata ennek. Mivel az információcsere elektromágneses hullámok segítségével valósul meg, számos előnye van a vezetékes összeköttetésekkel szemben. Ide tartozik, hogy meglehetősen olcsó és könnyen telepíthető. Egyszerű kapcsolódási lehetőséget biztosít az olyan eszközök számára, amelyek nem helyhez kötöttek (Pl. laptop, okostelefon). Ezzel szemben hátrányuk, főleg biztonsági szempontból, hogy a könnyű hozzáférés miatt nem elég védettek. Mivel az elektromágneses hullámok egyes frekvenciás tartományaiban több eszköz is üzemelhet, gyakran interferenciát okozhatnak és zavarhatják egymás jeleit.

A vezeték nélküli hálózatokat kiterjedés szerint három típusba soroljuk:

10.1 WPAN (Wireless Personal Area Network): „*Ez a legkisebb méretű hálózattípus. melyet általában olyan perifériális eszközök számítógéphez való csatlakoztatására használnak, mint például egerek, billentyűzetek és PDA-k. Ezen eszközök mindegyike kizárólag egy állomáshoz csatlakoznak, és általában IR vagy Bluetooth technológiát használnak.”*[29] Ebbe a hálózat típusba soroljuk az infravörös és rádiófrekvenciás eszközöket.

10.1.1 Infravörös technológia (IR): Ez az átviteli típus már viszonylag elavultnak számít, hiszen elég alacsony energiaszintű jelekkel, kis hatótávolsággal rendelkezik, amelyeknek még a falak is nagy akadályt jelentenek. Csak pont-pont típusú és rálátást igénylő átvitelre képes. A régebbi mobiltelefonok rendszerint fel voltak szerelve infravörös porttal, amelyeket az információküldésnél lényegesen közel kellett helyezni egymáshoz. A távirányítók már régóta használják ezt a technológiát. Emlékezhetünk rá, hogy a televíziós csatornaváltásnál a távirányítót sok esetben pontosan a TV-re kell irányítanunk.

10.1.2 Rádiófrekvenciás technológia (RF): Az IR-hez képest mindenképpen egy fejlettebb átviteli módszer, hiszen a jelek nagyobb hatótávval bírnak és áthatolnak a falakon. A Bluetooth rendszerint rádiófrekvenciát használ a kommunikációhoz, amelyet számos eszköz alkalmaz. A számítógépes perifériák, mint pl. a vezeték nélküli egerek, billentyűzetek RF segítségével működnek.

[29] Forrás: Cisco CCNA Discovery1 – 7.1.3-mas fejezet, Letöltés dátuma: 2018. 10. 18.

10.2 WLAN (Wireless Local Area Network): *„Általában a vezetékes helyi hálózatok határainak kiterjesztése érdekében használják. A WLAN RF technológiát használ, és megfelel az IEEE 802.11-es szabványoknak. Számos felhasználó számára teszi lehetővé a vezetékes hálózathoz való csatlakozást egy hozzáférési pontként (Acces Point, AP) ismert eszközön keresztül. A hozzáférési pont kapcsolatot biztosít a vezeték nélküli állomások és az Ethernet kábeles hálózat állomásai között.”*[30]

10.2.1 Wi-Fi (Wireless Fidelity): Manapság a leggyakoribb vezeték nélküli forma. Az 5. fejezetben taglaltuk, hogy az Ethernet a 802.3-mas szabvány szerint működik. Ennek a vezeték nélküli változata a WI-FI, a 802.11-es specifikációra épül, amelyet szintén az IEEE fejlesztett ki.

A 802.11-es szabvány köszönhetően az Apple-nek, az évek során rengeteget fejlődött, életútját generációkra csoportosítjuk. A 90-es évek végén kezdetben a 802.11a és b változat volt a meghatározó, majd jött a jóval gyorsabb 802.11g. A 2009-ben kifejlesztett n-es verzió a mai napig is meghatározó a gyors átviteli sebessége és nagy hatótávolsága miatt. Ezen felül kompatibilis a korábbi változatokat használó eszközökkel. Ennek a változatnak is van már egy továbbfejlesztett változata, mégpedig a 802.11ac. A majdnem 7 Gbps-os átviteli sebességgel jelentős előrelépést mutat. Mivel a legtöbb Wi-Fi router a 802.11n-es szabványt használja, egyelőre nehezen terjed el a piacon. A Wi-Fi legújabb generációja az ax-es szabvány lesz, amelyet várhatóan 2019-re adnak ki.

(A szabványok jellemzőit lásd az ábrán)

	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz

32. ábra: A Wi-Fi szabványok általános jellemzői

Kép forrása: https://theruckusroom.ruckuswireless.com/wired-wireless/technologytrends/the-theory-of-wi-fi-evolution-and-ieee-802-11-selection/, Letöltés dátuma: 2018. 12. 05.

A vállalatok számára manapság teljesen elvárt a Wi-Fi hálózat megléte, hiszen így nemcsak az alkalmazottaknak, de az ügyfelek számára is biztosított az internetelérés.

[30] Forrás: Cisco CCNA Discovery1 – 7.1.3-mas fejezet, Letöltés dátuma: 2018. 10. 18.

10.3 WWAN (Wireless Wide Area Network): „*A WWAN hálózatok óriási méretű területeken biztosítanak lefedettséget. Ilyenek például a mobiltelefonos hálózatok. Olyan technológiákat használnak, mint a kódosztásos többszörös hozzáférés (Code Division Multiple Access, CDMA) vagy a Mobil kommunikáció globális rendszere (Global System for Mobile Communication, GSM), melyek használatát gyakran kormányzati szervek szabályozzák."*[31]

11 Hálózat fejlesztési fázisok

Többféle okból kifolyólag, gyakran szükséges egy meglévő hálózat korszerűsítése, annak fejlesztése, bővítése. Egy informatikai hálózatnak maximálisan ki kell szolgálnia az adott vállalatot, így ha az pl. növekedésnek indul, annak hálózatát is bővíteni kell. Az internet alapú gazdaságban mindegyik cégnek fejlett informatikai eszközökkel kell rendelkeznie, számos esetben szükség van az elavult hálózatot modernizálni. Maga a hálózatfejlesztés egy több összetevőből álló folyamat.

11.1 Helyszín felmérése: A hálózatfejlesztés első lépésben a meglévő hálózat feltérképezése a cél. Dokumentálni kell a hálózati struktúrát, annak jelenlegi állapotát. Az új logikai, és fizikai topológiai térkép elkészítéséhez a telephely alaprajzára feltétlenül szükségünk lesz. A helyszíni felmérés alatt a következőkről kell információt gyűjtenünk:

- *„Felhasználók száma és a berendezések típusa*
- *Tervezett növekedés mértéke*
- *Jelenlegi internet hozzáférés típusa*
- *Alkalmazásokra vonatkozó követelmények*
- *Meglévő hálózati infrastruktúra és fizikai elhelyezkedése*
- *Új szolgáltatásokra vonatkozó követelmények*
- *Biztonsági és titoktartási megfontolások*
- *Megbízhatósági és rendelkezésre állási elvárások*
- *Költségvetési megszorítások"*[32]

11.2 Követelmények dokumentálása: A hálózat meglévő eszközeiről nagyon fontos, hogy információt szerezzünk., azokról elemzési jelentést készíteni.

A következőket érdemes leltárban összefoglalni:

- *„Eszköz neve*
- *Beszerzés időpontja*
- *Jótállási információk*

[31] Forrás: Cisco CCNA Discovery1 – 7.1.3-mas fejezet, Letöltés dátuma: 2018. 10. 19.
[32] Forrás: Cisco CCNA Discovery2 – 3.1.1-es fejezet, Letöltés dátuma: 2018. 11. 04.

- *Hely*
- *Márka és modell megnevezése*
- *Operációs rendszer*
- *Logikai címzési információk*
- *Átjáró*
- *Kapcsolódás típusa*
- *Telepített víruskereső szoftverek*
- *Biztonsági információk"*[33]

11.3 Tervezés: A hálózat korszerűsítés egyik legfontosabb része a tervezés. Miután meghatároztuk a szükségleteket, célszerű egy projekthez hasonlóan megtervezni a munkamenetet. Mivel a leendő, új hálózat kialakítását számos tényező befolyásol, célszerű egy SWOT analízist készíteni. A SWOT nagy segítséget nyújt az erősségek, gyengeségek, lehetőségek és veszélyek kiértékelése terén. Ennek köszönhetően a leg optimálisabban tervezhetjük meg a rendszert. A tervezés során nagyon fontos az ügyféllel való folyamatos kapcsolattartás, elsősorban a költségvetés miatt. Sokszor a legnagyobb korlátot az anyagi megszorítások jelentik. A tervezőnek tisztában kell lennie, hogy az ügyfél mennyi költséget tud rááldozni a projektre. Egy hálózattervezési folyamatban rendkívül előnyös, ha lemodellezzük az új rendszerünket, hiszen így egyből látni fogjuk az esetleges tervezési hiba előfordulásokat. Dokumentálnunk kell az új hálózat fizikai és logikai topológiáját, topológiai térkép segítségével. Meg kell határozni, hogy mely informatikai eszközök hol fognak elhelyezkedni, milyen összeköttetésekkel és azok kapcsolódása az IP címzéssel együtt kerül kialakításra. Fontos a precíz, figyelmes, átlátható munkavégzés, mert így nagy eséllyel elkerülhető a hálózat problémás megvalósítása. A terv végeztével rendszerint be kell mutatni azt az ügyfélnek, aki amennyiben az azzal járó költségvetéssel elfogadja, elindulhat a kivitelezés.

11.4 Kivitelezés: Ez a fázis az elméletben létrehozott rendszer fizikai megvalósítását jelenti. Amennyiben jól végeztük az eddig lépéseket, a kivitelezés nagy eséllyel könnyedén fog menni. Mindig előfordulhatnak váratlan gikszerek, amiket a legjobb szakértelem szerint meg kell oldani. Ahogy a tervezésnél, itt is nagyon fontos a folyamatos kommunikáció az ügyféllel. Az esetleges tervhez képesti változások miatt, az ügyfélnek mindenről tudnia kell!

[33] Forrás: Cisco CCNA Discovery2 – 3.1.3-mas fejezet, Letöltés dátuma: 2018. 11. 04.

11.5 Üzembe helyezés: A kivitelezési fázist követően a rendszer üzembe helyezése következik. Itt történik a hálózat üzemkész állapotba hozása, a hálózati eszközök, kiszolgálók konfigurálásával együtt.

11.6 Értékelés: A hálózat elkészítése után, a projekt utolsó szakaszában meg kell figyelni, hogy az a terveknek megfelelően működik-e. El kell végeznünk a hálózat teljes működésének a dokumentációját, hogy az egy jövőbeli meghibásodás esetén könnyen helyreállítható legyen.

12 Hálózat tervezési megfontolások

Egy hálózat továbbfejlesztésének szakaszairól az előző fejezetben beszéltünk, most a fizikai környezet megfelelő kialakításáról lesz szó. A tervezés folyamán részletesen meg kell vizsgálni, hogy a hálózatot milyen épületben kell létrehozni. Fontos a megfelelő kábelezés, a hálózati eszközök és egyéb informatikai berendezések szakszerű kiválasztása.

12.1 Kábelrendezők:

12.1.1 MDF: Nagyobb helyi hálózatoknál lényeges, hogy kialakítsunk egy olyan helyiséget, ahol a szerverek, hálózati eszközök, kábelszekrények kapnak helyet. Ezt a kommunikációs szobát szoktuk hívni MDF-nek (Main Distribution Facility), amely magyarul központi kábelrendezőt jelent. Ezen a ponton kapcsolódnak össze a hálózati kábelek patch panelon keresztül a hálózati eszközökkel. Nagy, vállalati rendszereknél nélkülözhetetlen az MDF megléte, hiszen minél nagyobb egy hálózat, annál több kábellel és az adatforgalmat megvalósító eszközzel rendelkezik. Egy jól kialakított kommunikációs helyiségben a rendszergazdák számára gyakorlatilag minden egy helyen van, a szerverek, kapcsolók, forgalomirányítók, – a hálózat karbantartását és hibaelhárítását lényegesen megkönnyítve.

12.1.2 IDF: Az MDF mellett a hálózat kiterjedésének függvényében gyakran szükség van további kábelrendezőkre. Ezeket a további, kisebb elosztási központokat nevezzük IDF-nek (Intermediate Distributing Frame). Minden ilyen elosztó központ csatlakoztatva van a vállalat telekommunikációs helyiségéhez. Ez az összeköttetés alkotja a gerinchálózatot, ezért nagyon fontos, hogy minél nagyobb átviteli sebességgel rendelkezzen. „*Egy IDF-ben az MDF-nél alacsonyabb sebességű kapcsolók, hozzáférési pontok és hubok találhatók. Általában*

nagyszámú Fast Ethernet porttal rendelkeznek, hogy biztosítsák a felhasználók számára a hozzáférési rétegben történő csatlakozást."[34]

12.2 Megfelelő kábelezés kiválasztása: A helyszíni szemle során már a tervezés előtt tisztában kell lenni, hogy milyen épülettel van dolgunk. Egy meglévő hálózat korszerűsítésénél előfordulhat, hogy az eredetinél egy teljesen más kábelezési formát kell kialakítanunk. Számos befolyásoló tényező van. Elsősorban meg kell vizsgálnunk, hogy kapcsolódásukat tekintve milyen fajta hostok szerepelnek a vállalaton belül. Az olyan helyiségekben, ahol helyhez kötött számítógépek szerepelnek, vezetékes kapcsolaton gondolkodhatunk. Előfordulhat, hogy Pl. egy konferenciateremben csak vezeték nélküli, Wi-Fi hálózatot lehet létrehozni, ahol okostelefonokkal és laptopokkal fognak a hálózathoz csatlakozni. Miután megtörtént az igények felmérése, az épület elemzését kell elvégeznünk.

Vannak olyan esetek, ahol előfordulnak az elektromágneses, vagy rádiójeles zavarok (Pl. gyárépületekben). Az ilyen esetekben nem alkalmazhatóak a gyakori csavart érpáras kábelek, főleg nem az UTP. Ahol esetleg vastag falakkal van dolgunk, egy vezeték nélküli hálózat kialakítása meglehetősen nehézkesen lenne működőképes. Megtörténhet, hogy egy műemlék épületben kell hálózat létrehozni, és ebben az esetben nem fúrhatunk falakat. Külön kell választanunk a hozzáférési réteg eszközeinek összekötését és a gerinchálózati kapcsolat kialakítását. A hozzáférési réteg vezetékes és vezeték nélküli módon is megvalósítható, de a gerinchálózatokat kizárólag kábelek segítségével valósíthatjuk meg.

12.2.1 Hozzáférési réteg kábelezése: A hozzáférési rétegben nagyon sok esetben alkalmaznak párhuzamosan Wi-Fi-t, a fali aljzatok mellett. Fizikai kábelezésnél, amennyiben nincs elektromágneses, netán rádiófrekvenciás zaj, véleményem szerint az UTP kábelezés a leg kézenfekvőbb megoldás. Az olcsón beszerezhető, ill. könnyű telepíthetősége miatt számtalan helyen használják. Pl. egy számítógépes teremben a sok munkaállomás miatt a vezetékek méretre szabása és azt követően a kábelmenedzsment is jóval egyszerűbb feladat a szakemberek számára, mint pl. a koaxiális kábelek esetében. Arról nem is beszélve, hogy minden számítógép és a hálózati eszközök elsősorban RJ-45-ös hálózati porttal vannak ellátva, amivel a csavart érpár rendszerint kompatibilis.

[34] Forrás: Cisco CCNA Discovery3 – 2.1.3-mas fejezet, Letöltés dátuma: 2018. 12. 01.

12.2.2 Gerinchálózati kábelezés megvalósítása: Gerinchálózatok esetében nem alkalmazhatunk vezeték nélküli technológiát. Ennek oka, a gyors átviteli sebesség, a megfelelő biztonság és megbízhatóság biztosítása, amelyet csak a vezetékes összeköttetés elégít ki. A lehető legnagyobb sebességű főkapcsolatok kialakításánál először szükség van a minimum gigabites interfészeket támogató kapcsolókra, vagy hubokra. Ezt követően gondolkodhatunk a fizikai kábel kiválasztásán. Három befolyásoló tényezőt kell figyelembe vennünk, amelyek a távolság, a zavaró jelek és a redundancia.

A távolság az adott szervezet kiterjedését jelenti. Általában egy épületen belül kell hálózatot létrehozni, de előfordulhat, hogy a vállalkozás több épületből áll. Több épületet átszövő gerinchálózatnál gyakorlatilag kizárhatjuk a csavart érpárak használatát, hiszen több mint valószínű, hogy a két végpont közti távolság meghaladja az ilyen kábeltípus által támogatott, maximális 100 méter kiterjedést. Mivel az épületet között lévő kábeleket nem védik falak a külső veszélyforrásoktól, az elsősorban villámok által keltett többletfeszültség miatt is ajánlatos optikai kábeleket használni. A fényimpulzusokkal működő átviteli csatorna az ilyen veszélyek ellen tökéletesen védve van. A nagyon gyors és nagy távolság lefedésére alkalmas optikai kábel a legjobb megoldás a gerinchálózat kiépítéséhez. Abban az esetben, amennyiben egy kisméretű épületről van szó, a gerinc is kialakítható csavart érpáras, vagy koaxiális kábelezéssel. Ebben az esetben meg kell bizonyosodnunk arról, hogy nincs-e bármilyen zavaró jel.

Összességében a strukturált kábelezés nagyon fontos. A tervezésnél egyértelműen meg kell határozni a fizikai topológiában a megfelelő típusú kábelvezetékek pontos helyét a tervrajz alapján.

(A harmadik fontos tényezőről a redundancia megfelelő alkalmazásáról a következő fejezetben fogunk beszélni.)

12.3 Eszközök kiválasztása: Egy beruházásban a vállalati hálózati eszközök a legköltségesebb összetevők közé tartoznak, ezért a kiválasztásnál jelentős szerepet játszik a költségvetés. Amennyiben támogatott szolgáltatásról van szó, akkor az internetszolgáltató a felelős az eszközök beszerzéséért és karbantartásáét. Minden más esetben az ügyfelet terhelik a ráfordítások. *„Az igények elemzése után a tervező csoport javaslatot tesz az új hálózati összekötés és szolgáltatás biztosítására*

alkalmas hálózati eszközök beszerzésére."[35]

12.3.1 Kapcsolók beszerzése: A 7. fejezetben említettem, hogy amennyiben lehetséges inkább kapcsolókat használjuk a munkaállomások összeköttetése céljából, mint a hubokat. Igaz, hogy jóval drágábbak, de sokkal optimálisabb hálózati működést tesznek lehetővé. Ez lényeges, hiszen sok vállalat megköveteli a gyors sávszélességet, tehát fontos, hogy az átbocsátóképességnek eleget tegyen. Hubokat csak a nagyon kis méretű hálózatokban alkalmazzunk, ahol elenyésző állomás található, így csökkenthető az ütközési tartomány terjedelme. A megfelelő kapcsoló kiválasztásánál figyelembe kell vennünk, hogy hány felhasználó fog hozzá kapcsolódni, tehát mennyi interfészre van szükség. A kapcsoló által támogatott portoknak kompatibilisnek kell lennie a beépített kábelekkel. Amennyiben a jövőben bővítik a hálózatot és új munkaállomások kerülnek telepítésre, előnyös, ha még rendelkezésre állnak tartalék interfészek is erre az esetre. Az eszköz kiválasztásnál fontos szempont, hogy moduláris eszközöket vásároljunk, amennyiben fennáll az esélye az adott hálózat növekedésének. *„A moduláris berendezések bővítőhelyekkel rendelkeznek, így új modulok hozzáadásával rugalmasan lehet követni az igényeket."*[36]

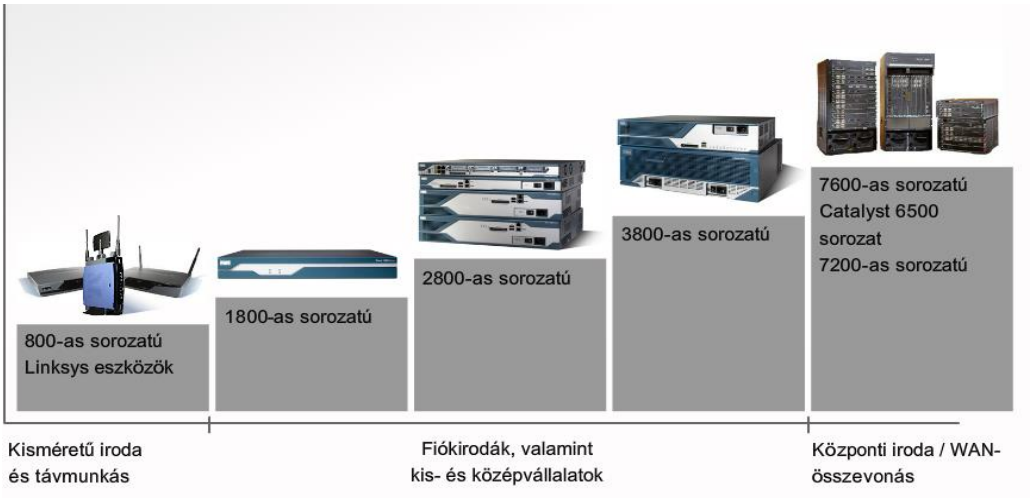
„Egy vállalati MDF kapcsoló gigabites optikai vagy rézkábellel csatlakozik az IDF kapcsolókhoz. Az IDF kapcsolóknak általában mindkét RJ-45-ös Fast Ethernet portra szükségük van, de kell legalább egy gigabites Ethernet port is (réz vagy optikai) az MDF kapcsolóhoz történő felcsatlakozáshoz."[37]

Lényeges, hogy felügyelhető, konfigurálható switcheket alkalmazzunk, hiszen így *„lehetőség van az egyes portok vagy akár az egész kapcsoló forgalmának szabályozására. A szabályozás lehetőségei közé tartozik többek között az eszköz beállításainak megváltoztatása, a port biztonság bevezetése, valamint a teljesítmény felügyelet. Így például egy felügyelhető kapcsoló portjai különállóan be, illetve kikapcsolhatók. Továbbá a rendszergazda azt is megszabhatja, mely számítógépek csatlakozhatnak egy adott porthoz."*[38]

12.3.2 Forgalomirányítók beszerzése: A hálózat kiterjedésétől, annak szolgáltatásaitól, funkcióitól függ, hogy milyen forgalomirányítóra van szükség. A kapcsolókhoz

[35] Forrás: Cisco CCNA Discovery2 – 3.3.2-es fejezet, Letöltés dátuma: 2018. 11. 10.
[36] Forrás: Cisco CCNA Discovery2 – 3.3.3-mas fejezet, Letöltés dátuma: 2018. 11. 10.
[37] Forrás: Cisco CCNA Discovery3 – 2.3.4-es fejezet, Letöltés dátuma: 2018. 12. 02.
[38] Forrás: Cisco CCNA Discovery2 – 3.3.3-mas fejezet, Letöltés dátuma: 2018. 11. 10.

hasonlítva, itt is lényeges szempont, hogy inkább moduláris felépítésű eszközt válasszunk, ill. hogy az a hálózati kábelezéssel azonos típusú interfészekkel rendelkezzen. Egy közepes méretű vállalatnál már ajánlott az integrált forgalomirányító (ISR) használata. Az ilyen készülékek rendszerint rendelkeznek Gigabit Ethernet, soros, és optikai interfészekkel. Az ISR számos hálózatban egy gyakran használt eszköz, mivel számos funkciót ellát: „*biztonság, vezeték nélküli hozzáférési pont, szolgáltatás minősége (QoS), IP-alapú hangátvitel (VoIP), NAT, DHCP, virtuális magánhálózat (VPN)”*[39]



33. ábra: Forgalomirányítók a megkívánt igények kielégítésére
Kép forrása: Cisco CCNA Discovery3 – 2.3.1-es fejezet, letöltés dátuma: 2018. 12. 02.

Tanulmányaim során a gyakorlati órákon rendszerint használtunk integrált forgalomirányítót, a mi esetünkben Cisco fejlesztésűt. Tapasztalatomból állítom, hogy egy rendkívül fejlett eszközről van szó, amely minden értelemben kielégíti a nagyobb vállalatok igényeit. Az egyetlen hátránya, hogy a forgalomirányító megfelelő beprogramozása egy meglehetősen nehéz feladat, a rendszergazdának értenie kell az adott készülék konfigurálásához, amely a különböző gyártótól származó készülékek esetében más és más lehet.

A Cisco forgalomirányítók grafikus és parancssoros kezelőfelülettel is rendelkeznek, amelyek sávon kívüli és belüli felügyelettel konfigurálhatóak. Sávon kívüli vezérlésnél azt értjük, amikor az eszközt közvetlenül, konzolkábel segítségével egy számítógéppel konfiguráljuk. Sávon belüli felügyeletnél a készülékhez távolról fér hozzá a rendszergazda, sok esetben Telnet segítségével.

[39] Forrás: Cisco CCNA Discovery2 – 3.3.4-es fejezet, Letöltés dátuma: 2018. 11. 11.

13 Redundancia alkalmazása

13.1 Hibatűrő rendszerek kialakítása: A hálózat kiépítésének a legfontosabb célja a „*magas szintű megbízhatóság fenntartása, valamint a meghibásodásra érzékeny és kritikus pontok minimalizálása. A hálózat működésképtelensége komoly üzleti károkat, bevétel kiesést és az üzletfelek elégedetlenségét eredményezheti.”*[40] E mellett egy hálózattervezésnél törekedni kell, hogy a rendszer hosszútávú működésre legyen képes, a felhasználók számára a folyamatos rendelkezésre állás és megbízhatóság mellett. Ez azt jelenti, hogy tartalék útvonalakat és kapcsolódási pontokat hozunk létre. A megbízhatóság így rohamosan megnő, egy esetleges meghibásodás esetén az alternatív útvonalak biztosítják az információ továbbítást.

„Természetesen adódhatnak olyan helyzetek, amikor az összes összeköttetés és eszköz megduplázása nagyon költséges lenne. A hálózati mérnököknek általában mérlegelniük kell és egyensúlyt kell találni a redundanciával járó költségek és a hálózat rendelkezésre állási követelménye között.”[41]

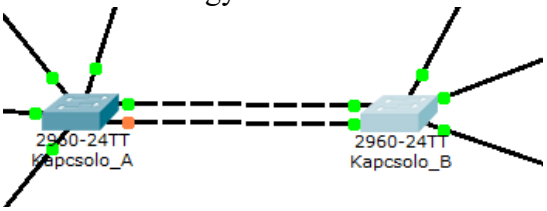
A redundancia biztosításához tartoznak még a szünetmentes tápegységek, illesztőkártyák, bővítőkártyák, és a bárminemű olyan alkatrész, amely menet közben cserélhető.

13.1.1 Szünetmentes tápegység jelentősége (UPS): A hálózat olyan eszközeinél, mint pl. a szerverek, amelyek működését napi 24 órában kell biztosítani. Az ilyen eszközöket UPS-sel (Uninterruptible Power Supply) kell ellátni. Bármikor jöhet egy váratlan áramszünet, és az adatvesztés elkerülése végett a szünetmentes tápellátás biztosítása nélkülözhetetlen. Az USP-k akkumulátorokkal rendelkeznek, amik a hálózati áram megszűnése esetén biztosítják a hozzájuk csatlakoztatott eszközök számára az áramot és a feszültségingadozástól is védik őket (Pl. villámcsapások esetén). Az USP-k költsége igen eltérő annak függvényében, hogy mekkora kapacitással bírnak és mennyi csatlakozóval rendelkeznek. Ezeknek a feltételeknek kell kellően megválasztani őket.

13.2 Gerinchálózati redundancia: Több szó is esett már róla, hogy a nagyméretű hálózatok esetében a gerinchálózati összeköttetés kiemelten fontos jelentőséggel bír, amelyeknek tökéletesen megbízhatónak kell lenniük. Ahogyan gerincsérülés

[40] Forrás: Cisco CCNA Discovery3 – 3.2.1-es fejezet, Letöltés dátuma: 2018. 12. 02.
[41] Forrás: Cisco CCNA Discovery3 – 3.2.1-es fejezet, Letöltés dátuma: 2018. 12. 02.

esetében egy ember is lebénulhat, úgy egy létfontosságú hálózati eszköz meghibásodása, vagy főkapcsolati kábelhiba is súlyos következményeket jelenthet. Különösen a nagy szervezeteknél létfontosságú jelentőségű, hogy a hálózat kritikus pontjaiból legyen tartalék. A működő forgalomirányítók és kapcsolók mellett előfordul, hogy tartanak tartalék eszközöket is egy esetleges vészhelyzet esetére. Amennyiben a büdzsé megengedi, ajánlatos betartani ezt a tanácsot. Sok esetben dupla gerinchálózatot alakítanak ki a kábelek megkettőzésével.



34. ábra: Gerinchálózati redundancia szemléltetése
Kép forrása: Saját forrás (Cisco Packet Tracer használatával)

13.3 Kábelezési redundancia hátránya: A kábelezés tartalék képzésénél azonban óvatosan kell bánni, hiszen *„a kapcsolók között létrehozott összekötések problémák forrásai is lehetnek. Az Ethernet forgalom szórásos jellege miatt például kapcsolási hurkok jöhetnek létre. A szórásos keretek körbe-körbe járnak minden irányban, szórási viharokat eredményezve. A szórási viharok az elérhető sávszélességet lefoglalják, így előfordulhat, hogy újabb hálózati kapcsolatok létrejöttét akadályozzák meg, valamint régiek megszakítását eredményezik."*[42]

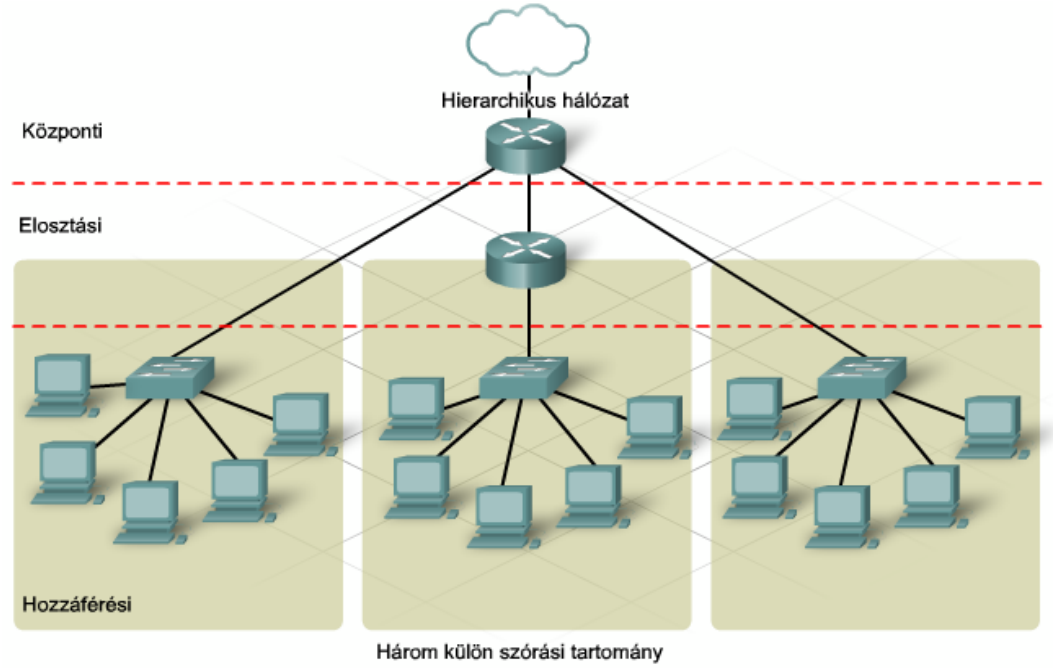
Amikor két kapcsolót több út is összeköt egymással még az egyedi Ethernet keretek is kellemetlenséget okozhatnak. A kapcsoló működésénél megbeszéltük, hogy amikor az eszköz egy olyan keretet kap, amelynek a cél MAC-címét nem ismeri, elárasztással kiküldi azt minden portján. A több útvonal következtében könnyen előfordulhat, hogy a kiküldött üzenetek visszatérnek a kezdeményező switchez. *„A folyamat így újra meg újra megismétlődik, a keret többszörös példányát létrehozva a hálózaton. Esetenként a célállomás több másolatot is kap az eredeti keretből. Ez három problémát is okozhat: sávszélesség felesleges lefoglalása, CPU időveszteség, valamint az adatforgalom esetleges duplázása. Redundáns hálózatokban előfordulhat, hogy a kapcsoló egy állomás elhelyezkedéséről rossz információt tanul meg. Ha létezik hurok, akkor a kapcsoló egy állomás MAC-címét akár két külön porttal is összefüggésbe hozhatja. Ez nem egyértelmű helyzetet és az optimálistól elmaradó kerettovábbítást okozhat. „*[43]

[42] Forrás: Cisco CCNA Discovery3 – 3.2.1-es fejezet, Letöltés dátuma: 2018. 12. 02.
[43] Forrás: Cisco CCNA Discovery3 – 3.2.1-es fejezet, Letöltés dátuma: 2018. 12. 02.

13.3.1 Feszítőfa protokoll (STP): Az előző pontban említett problémák megoldására szolgál a kapcsolóknál használt feszítőfa protokoll (Spanning Tree Protocol). Ez a megoldás gyakorlatilag megszűnteti a redundáns hálózatokban létrejövő hurkokat azzal, hogy a készülék tartalék útvonalakhoz kapcsolódó interfészeit letiltja. A protokoll folyamatosan figyeli a hálózati topológiát és amikor hurkot észlel, az érintett pontokat letiltja.

14 Hierarchikus hálózatkialakítás alhálózatokkal

Már többször beszéltünk a hierarchikusan kialakított hálózatok jelentőségéről. Csak a kisebb vállalatok engedhetik meg maguknak az egyszintű rendszert, ahol az állomások mind ugyanabba a hálózatba tartoznak és mindegyikük részese a szórási tartománynak. Ahogy növekszik a hálózat, az elosztási réteget javasolt több,



35. és 36. ábra: Az egyszintű és az Ethernet által kialakított hierarchikus hálózati modell összehasonlítása
Képek forrása: Cisco CCNA Discovery3 – 4.1.1-es fejezet, Letöltés dátuma: 2018. 12. 04.

logikailag különálló részre osztani. A legegyszerűbb módszer, ha alhálózatokat – az-az virtuális LAN-okat hozunk létre. Az ilyen részekre bontást nevezzük VLAN-nak (Virtual Local Area Network). A hálózat átviteli sebessége, annak konvergenciája sokban javulhat a megfelelően részekre bontott alhálózatokkal, hiszen a hálózat forgalmi terhelése csökken. A létrehozott alhálózatok a teljes rendszer független szegmensei lesznek.

14.1 VLAN-ok kialakításának legfőbb okai:

- *„Fizikai elhelyezkedés*
- *Logikai csoportosítás*
- *Biztonság*
- *Alkalmazási követelmények*
- *Szórások hatókörének korlátozása*
- *Hierarchikus tervezés”*[44]

14.2 VLAN-ok létrehozása: Virtuális helyi hálózatok kialakításához az IP címzés megfelelő ismerete szükséges. A hálózati címzésnél a 6. fejezetben megvitattuk, hogy az alhálózati maszk határozza meg az IP cím hálózat és állomás azonosító részét. Megfelelő alhálózati maszk használatával lehetőség van alhálózatokra bontásra. VLAN-ok létrehozásánál az alhálózati maszkot lehetőségünk van a kívánt belső állomások számának függvényében módosítani, úgy hogy az állomásokhoz tartozó címrészből viszünk át biteket a hálózat azonosításáért felelős címrészbe.

14.3 Alhálózat példa megoldása: Vegyünk egy példát a szemléltetés miatt. Egy C osztályú hálózatban (192.168.1.0) négy, egyforma méretű alhálózatot szeretnénk kialakítani, mivel 55, 50, 59, 47 munkaállomásunk van. Ez a cím alapesetben 254 állomást tud kiszolgálni, 192.168.1.1 – 192.168.1.254 [mivel az utolsó cím (255) mindig szórási cím]. Az IP címhez alapesetben a 255.255.255.0 maszk tartozik, és amennyiben 2 bitet átviszünk a hálózat címrészébe, akkor a maszk a 255.255.255.192-re módosul, amely négy alhálózatot hoz létre.

A hálózat alapértelmezett maszkja tehát:	255. 255. 255. 0
amely bináris formában így írható fel:	11111111.11111111.11111111.00000000
A módosított maszk a következő:	255. 255. 255. 192
binárisan:	11111111.11111111.11111111.11000000

[44] Forrás: Cisco CCNA Discovera3 – 4.1.3-mas fejezet, letöltés dátuma 2018. 12. 04.

A négy alhálózat a következőképpen fog kinézni:

192.168.1.0-ás hálózat:	192.168.1.1 – 192.168.1.62
192.168.1.64-es hálózat:	192.168.1.65 – 192.168.1.126
192.168.1.128-as hálózat:	192.168.1.129 – 192.168.1.190
192.168.1.192-es hálózat:	192.168.1.193 – 192.168.1.254

Látható, hogy a négy alhálózat létrehozása csak akkor lehetséges, amennyiben alhálózatonként nincs 62 állomásnál több bennük, hiszen ennél nem lehet több címet kiosztani. A szórásos üzenetek kiosztásáért mindig az alhálózatok utolsó címei lesznek a felelősek. Ebben az esetben az 1.0-ás hálózatnál a 192.168.1.63-mas IP cím, az 1.64-es hálózatnál a 127-es, majd a 191 és 255.

A példában négy VLAN-t hoztunk létre. – abban az esetben, ha csak 1 bitet viszünk át, (255.255.255.128 maszk) csupán két alhálózat létrehozása lehetséges, de kétszer annyi (126) állomással. Ha 3 bitet, (255.255.255.224) akkor 8 alhálózatunk van, egyenként maximum 30 állomással. A bontás így folytatódik tovább, a kettő hatványaira alapozva. Minél több alhálózatunk van, annál kevesebb állomásnak van hely benne.

A módszer segítségével számos olyan vállalat informatikai rendszere optimalizálható, amelyek sok felhasználóval rendelkeznek. Az egyetlen hátrány, hogy csupán azonos méretű helyi LAN-okra bontható és eltérő számú állomások esetén nagyon sok IP cím veszhet kárba. A probléma megoldására kifejlesztettek egy speciális változatot. A VLSM és a CIDR segítségével egy hálózat a kívánt méretnek megfelelő, eltérő nagyságú alhálózatra bontható. „*Ennek köszönhetően az IP-címek ezrei lesznek megmenthetők, amelyek a hagyományos osztályalapú alhálózatokra bontással elvesznének.”*[45]

15 Hálózati veszélyforrások

Egy hálózat megbízgató működésének alappillére, hogy az megfelelően védve legyen a veszélyektől. A komplex internet világában számos külső veszéllyel kell számolnunk, egy jogosulatlan személy hálózatba történő behatolása nagymértékű károkat okozhat. A hekkerek a hálózat gyenge, sebezhető pontjait használják ki, legtöbbször információlopás céljából. Ebben a fejezetben a behatolási veszélyekről fogunk beszélni.

[45] Forrás: Cisco CCNA Discovery2 – 4.1.4-es fejezet, Letöltés dátuma: 2018. 10. 16.

15.1 Behatolási források: A hálózatba történő behatolások terén vállalaton belüli ill. vállalaton kívüli veszélyekről beszélhetünk. Amikor a behatolásokról beszélünk, mindenkinek általában a hekkeres támadás jut az eszébe. Az igazat megvallva a biztonsági kockázatok legnagyobb része a hálózat belső részéhez tartozik. Itt a legnagyobb sebezhetőségi tényezők a felhasználók, akik hozzáférési joggal rendelkeznek. Akaratlanul is bármelyik alkalmazott vírust hozhat be egy külső hálózatból, amelyek komoly veszélyt jelentenek a rendszernek. Nagy kockázatot jelent egy belső támadó, aki az adott cég munkatársa. Az ilyen emberek azért nagyon veszélyesek, mert tisztában vannak a vállalat informatikai rendszerének működésével és nagyon könnyen hozzá tudnak férni az értékes információkhoz. „*A külső veszélyek a szervezeten kívül dolgozó személyekkel kapcsolatban merülnek fel. A külső támadók a hálózatba való bejutásukat főleg az Interneten, vezeték nélküli kapcsolatokon vagy a szerverekhez történő behívásos hozzáférésen keresztül hajtják végre.”*[46]

15.1.1 Megtévesztési technika: „*Egy behatoló számára a hozzáféréshez jutás egyik legegyszerűbb módja akár belülről akár kívülről, az emberi hiszékenység kihasználása.”*[47] Megtévesztési technikának (Social Engineering) nevezzük azt az esetet, amikor valamilyen ürüggyel ráveszik a belső felhasználókat arra, hogy azok titkos információkat, azonosítókat (Pl. jelszavak) juttassanak el a támadók számára.

15.1.2 Hamis ürügy (Pretexting): „*A hamis ürügy a megtévesztési technika egyik olyan formája, ahol egy előre megtervezett esetet használnak fel az áldozat megtévesztésére azért, hogy információkat adjon vagy végrehajtson egy tevékenységet.”*[48]

15.1.3 Adathalászat (Phishing): „*Az adathalászat során az adathalászok úgy tesznek mintha egy a szervezeten kívüli hivatalt képviselnének. Tipikusan elektronikus levélen keresztül személyesen lépnek kapcsolatba a célszeméllyel. Az adathalász olyan hitelesítési információkat kérhet, mint a jelszó vagy a felhasználói név azért, hogy valami szörnyű következmények bekövetkezésétől óvjon meg.”*[49]

[46] Forrás: Cisco CCNA Discovery1 – 8.1.2-es fejezet, Letöltés dátuma: 2018. 11. 15.
[47] Forrás: Cisco CCNA Discovery1 – 8.1.3-mas fejezet, Letöltés dátuma: 2018. 11. 15.
[48] Forrás: Cisco CCNA Discovery1 – 8.1.3-mas fejezet, Letöltés dátuma: 2018. 11. 15.
[49] Forrás: Cisco CCNA Discovery1 – 8.1.3-mas fejezet, Letöltés dátuma: 2018. 11. 15.

Személyes tapasztalatomból is állíthatom, hogy ez egy nagyon veszélyes támadási mód, főleg az idősebb, felkészületlenebb korosztály számára. Hadd említsek meg egy példát, ami velem történt: „Egyik nap kaptam egy e-mailt, miszerint kisorsolták a közösségi oldalam profilját. Egy megadott e-mail címre kellett válaszolnom ezzel kapcsolatban, de már gyanús volt, hogy nem kis nyereményről volt szó! (Jó, eddig még ez nem veszélyes, amíg levelezünk. ☺) Nem sokkal később jött is a válaszlevél, amelyben magyarnak éppen nem nevezhető nyelvhasználaton arra kértek, hogy adjam meg adataimat, majd azután iránymutatást fognak adni a nyereménnyel kapcsolatban. (Ez már több, mint gyanús! ☹) Szerencsére ebben az internetes világban bárminek utána lehet nézni, és konkrétan hamar ki is derült, hogy itt bizony nagy átverésről van szó. Azért válaszoltam egy szép hangvételű levéllel az illetőnek, amire a mai napig nem érkezett válasz. Nyilván, amennyiben valóban nyereményről lenne szó, megerősítenék a bizonyosságát!”

15.2 Rosszindulatú szoftverek: Ez a fajta támadás típus szerintem mindenki számára ismerős lehet, hiszen rengetegszer törnek borsot az orrunk alá. Rengeteg féle problémát okozhatnak a kisebb számítógépes gikszerektől egészen az operációs rendszer újratelepítéséig. Rendszerint sohasem könnyítik meg az életünket. Az ilyen fajta szoftverek mindegyike egy támadási forma, amelyek a számítógépek sebezhető pontjait használják ki. Alapvetően három fajtájukat különböztetjük meg egymástól: vírusok, férgek, trójai falovak.

Az ártalmas szoftverek fajtáit az 6. sz. melléklet tartalmazza!

15.3 Szolgáltatás-megtagadás (DoS - Denial of Service): Előfordulnak olyan esetek, amikor a támadó nem információt akar szerezni, hanem egyszerűen csak kárt okozni egy hálózati rendszerben, megakadályozni annak megfelelő működését. Az ilyen típusú támadást DoS támadásnak hívjuk. Legtöbbször a hálózati kiszolgálókat támadják meg, hogy a felhasználók ne tudják az azok által nyújtott szolgáltatásokat igénybe venni.

15.3.1 SYN elárasztás: A szolgáltatás-megtagadás egy gyakori fajtája, amikor a támadó folyamatos forgalommal leterheli az erőforrást (Pl. a szervert), amíg az túlterheltté nem válik. „*A SYN elárasztás lényege, hogy a támadó rengeteg hamis SYN csomagot küld el egy állomásnak, tehát a csomagok látszólag egy olyan gépről*

érkeznek, amely nem érhető el."[50] A hamis csomagok érvénytelen forrás IP címmel rendelkeznek. Ennek következtében a kiszolgáló nem lesz képes megfelelően ellátni a feladatát és a hálózat megbénul.

15.3.2 Halálos ping (Ping mindhalálig): A halálos pingnek az a lényege, hogy a támadó nagyon nagy, 64-nél nagyobb kilobájt méretű csomagot küld a célállomásnak. Mivel egy IP csomag mérete nem lehet ennél nagyobb, így a fogadó állomás ezt nem tudja értelmezni és lefagyhat.

15.4 Elosztott szolgáltatás-megtagadás: (DDoS – Distributed Denial of Service): A DoS támadás egy továbbfejlesztett változatáról van szó, amely sokkal nagyobb kárt tehet a rendszerben. A folyamat úgy zajlik, hogy a támadó az Interneten keresztül megfertőzi a hálózat belső munkaállomásait egy biz. DDoS kóddal. Amikor a DDoS kódok aktiválódnak az állomásokon, azok a tudtuk nélkül árasztják el nagymértékű forgalommal a hálózatot (sokszor a kiszolgálókat), amelyek a túlterhelés következtében megbénulnak. A támadás következtében gyakorlatilag a hálózat folyamatosan saját magát fertőzi.

16 Hálózati biztonság

Egy szervezet hálózatának a legfontosabb jellemzője, hogy az biztonságos legyen, az-az védve legyen az előző fejezetben is megemlített veszélyforrásoktól. Az adatvédelem az egyre fejlettebb technológiáknak köszönhetően egyre nehezebbé vált, ezért a biztonsági intézkedéseknek is haladni kell a korral, – az informatikai rendszerek kritikus pontjainak védelme alapvető feladat. Minél összetettebb egy szervezet informatikai rendszere, annál nagyobb energiát kell fordítani annak biztonságára.

16.1 Jogosultságkezelés: Napjainkban már alapkövetelmény, hogy a cégeknél dolgozó, számítógépeket használó összes dolgozó saját felhasználói névvel és jelszóval férjen hozzá a vállalati számítógépekhez és magához a hálózathoz. Ezt hitelesítésnek nevezzük, amikor egy személy azonosítása történik. A biztonság növelésének érdekében sok esetben korlátozzák a felhasználók hozzáférését a rendszerhez, különböző jogosultságkezelő szoftverekkel. *„Legjobb megoldásként a felhasználóknak csak azt a hozzáférési szintet szabad engedélyezni, amely a*

[50] Forrás: https://ikomm.webgobe.com/5ttipus.html, Letöltés dátuma: 2018. 11. 16.

mindennapi munkájukhoz elengedhetetlen."[51] Egy nagyon ismert jogosultság, adatbázis és erőforrás kezelő program az Active Directory (AD), amelyet címtárszolgáltatásnak is szoktak hívni. A Microsoft fejlesztette ki, világszerte széles körben elterjedt a használata.

Sok felhasználó esetén érdemes naplózást is alkalmazni, amellyel nyomonkövethetők a felhasználók tevékenységei – tehát, hogy milyen alkalmazásokat hol, mikor, mennyi ideig használtak.

16.2 Adattitkosítás: Mivel az adatok folyamatos áramlásban vannak, azoknak a biztonságos átvitelét biztosítani kell. A különböző átviteli protokollok mellett sokszor szükség van segéd protokollokra a megfelelő titkosítás biztosításához. Amikor böngészünk az interneten, a weboldalak URL címének első része többnyire HTTP vagy HTTPS. Hiperszöveg átviteli protokollokról van szó, de csak a HTTPS nyújt kellő biztonságot. A levelezőrendszerek a POP3, IMAP4, vagy SMTP protokollok segítségével működnek, de az SSL (Secure Socket Layer) teszi őket kellően biztonságossá. Amikor a Cisco forgalomirányító Telnet-tel történő hozzáféréséről beszéltem (12. fejezet), az magában szintén nem biztonságos kapcsolatot eredményez. „*SSH (Secure Shell) protokoll használatával a hitelesítés és a munka biztonságos módon történik."*[52] Szintén az SSH a felelős egy FTP kapcsolat biztonságossá tételéhez. A biztonságos protokollok közé tartozik még az IPSec (Internet Protocol Security), „*amely egy hálózati rétegbeli protokoll, és segítségével bármely alkalmazás rétegbeli protokoll használata biztonságos kommunikációt eredményez."*[53]

16.3 Hálózati eszközökön alkalmazott védelem: Az előző fejezetben volt szó a DoS ill. DDoS támadásokról, amelyekkel szemben a titkosítás sem nyújt megfelelő védelmet. A fejlett hálózati kapcsolók és ISR-ek rendelkeznek olyan biztonsági funkciókkal, amelyekkel az ilyen támadások kivédhetők.

16.3.1 Portbiztonság: Portbiztonságot, vagy portszűrést kapcsolók esetében alkalmazhatunk, segítségével megakadályozhatók az illetéktelen behatolások. Az eljárás úgy történik, hogy a kapcsoló a vele összeköttetésben álló állomások MAC-címét egy külön adatbázisban tárolja. Amennyiben egy nyilvántartásban

[51] Cisco CCNA Discovery2 – 8.1.1-es fejezet, Letöltés dátuma 2018. 12. 05.
[52] Cisco CCNA Discovery2 – 8.1.3-mas fejezet, Letöltés dátuma 2018. 12. 05.
[53] Cisco CCNA Discovery2 – 8.1.3-mas fejezet, Letöltés dátuma 2018. 12. 05.

nem szereplő fizikai című host próbál kommunikálni a hálózattal, a switch letiltja az adott interfészt és jelzi azt a rendszergazdának.

16.3.2 Forgalomszűrés (ACL): Forgalomszűrés a forgalomirányítókon alkalmazott biztonsági megoldás. Ezt ACL (Access Control List – Hozzáférési, vezérlési lista) segítségével valósíthatjuk meg. Az ACL-lel konfigurált routerek az IP címek, protokollok, szolgáltatások alapján, folyamatosan figyelik a be – és kimenő adatforgalmat.

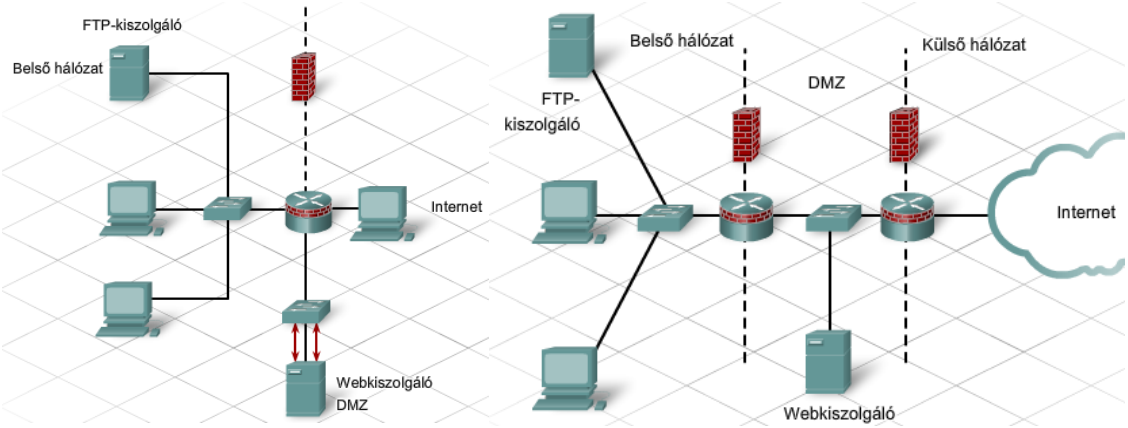
16.4 Tűzfal: A tűzfalak a hálózatok alapvető követelményei, mivel a leghatékonyabb biztonsági eszközök a veszélyek ellen. Kisebb hálózatok esetén elégségesek a szoftver alapú tűzfalak, de a nagy adatforgalom védelméhez gyakran szükség van hardveres eszközre. Ezek a nagy teljesítményű eszköz alapú tűzfalak nagyon hatékony és gyors működésűek, de a méretük (interfészek száma) függvényében nagyon költséges lehet a beszerzésük. A tűzfalak gyakorlatilag hozzáférési listák segítségével működnek. Funkciójukat tekintve megkülönböztetünk csomagszűrő, alkalmazás – vagy webhelyszűrő, ill. állapot alapú tűzfalakat. Sok forgalomirányító, – az ISR-ek általában rendelkeznek saját tűzfalas védelmi rendszerrel, de egy otthoni Wi-Fi router is tartalmazhat tűzfalat, legalábbis alap funkciókkal.

37. ábra: Egy hardveres tűzfal
Kép forrása: https://shop.secpoint.com/shop/protector-p8-10-390p.html, Letöltés dátuma: 2018. 12. 05.

16.4.1 Demilitarizált zóna (DMZ): Tűzfalas védelemnél a hálózat rendelkezik egy olyan területtel, amely az Internet és belső felhasználók felől is egyaránt hozzáférhető. Ezt nevezzük demilitarizált zónának. Sok esetben itt helyezkednek el az olyan szerverek (Pl. webkiszolgálók), amelyeknek az Internet számára is elérhetőnek kell lenniük, de a DMZ biztosítja a megfelelő védelmet a belső hálózat számára.

16.4.2 Egy – és két tűzfalas rendszerek: Egytűzfalas védelmi rendszert jellemzően a kisebb hálózatok engedhetnek meg maguknak, amelyek kisebb adatforgalmat generálnak. A kéttűzfalas konfigurációval jóval védettebb lesz a hálózat, a DMZ a belső és külső tűzfal között helyezkedik el. *„A külső tűzfal kevésbé korlátozó és megengedi, hogy az Internet felhasználók hozzáférjenek a DMZ-ben levő*

szolgáltatásokhoz, valamint megengedi, hogy bármely belső felhasználó által kért forgalom áthaladjon rajta. A belső tűzfal jóval korlátozóbb és védi a belső hálózatot a jogosulatlan hozzáféréstől."[54] (A kétfajta védelmi rendszert lásd az ábrán!)



38. és 39. ábra: Az egy és két tűzfalas hálózat összehasonlítása
Képek forrása: Cisco CCNA Discovery1 – 8.4.2-es fejezet, Letöltés dátuma: 2018. 12. 06.

16.5 Vírusírtó szoftverek: Vírusírtó programokkal magukat a számítógépeket védjük a vírusoktól, férgektől, trójai kártevőktől. Minden hálózatra kapcsolódó állomásnak rendelkeznie kell saját vírusírtó programmal. Számos ilyen szoftver ingyenesen is letölthető az Internetről, vagy csak próbaverzió, ill. demó változatban (Pl. Avast, Panda, Nod 32). Vállalati környezetben nagyon fontos, hogy teljes funkciókörű szoftverrel rendelkezzünk, ezeket külön meg kell vásárolni.

16.6 Vezeték nélküli hálózati biztonság: Mivel a vezeték nélküli hálózatokhoz könnyű a hozzáférés, így azok jóval védtelenebbek a vezetékes összeköttetésekkel szemben. Amikor egy új wireless routert üzembe helyezünk, először meg kell változtatnunk az alapértelmezett beállításait, mint pl. az SSID-t (hálózati név), és a csatlakozási jelszót. Már az egy jó biztonsági megoldás, ha kikapcsoljuk az SSID szórását. Ez azt eredményezi, hogy az idegen eszközök számára rejtve lesz a hálózat, így azok még csak tudomást sem vesznek róla. Sok esetben azonban láthatóvá kell tenni a hálózatot a felhasználók számára.

Három hitelesítési forma létezik:

16.6.1.1 Nyílt hitelesítés: Nyílt hitelesítés folyamán bárki kaphat hálózati hozzáférést, bármilyen jelszó nélkül. Nyilvános helyekre, mint pl. benzinkutakra, vasút – és buszállomásokra gyakran jellemző.

[54] Forrás: Cisco CCNA Discovery1 – 8.4.2-es fejezet, letöltés dátuma: 2018. 12. 06.

16.6.1.2 Előre megosztott kulcs (PSK): A leggyakoribb hitelesítési forma, amikor csak a forgalomirányítón beállított jelszót ismerő felhasználó tud csatlakozni.

16.6.1.3 Kiterjeszthető hitelesítő protokoll (EAP): A hitelesítési folyamatban a forgalomirányító egy hitelesítő szerver segítségével ad a felhasználónak hozzáférést.

16.6.2 Vezeték nélküli titkosítás: Vezeték nélküli kommunikáció során is elengedhetetlen a megfelelő titkosítási eljárás.

Kétféle titkosítási formát használunk:

***16.6.2.1* WEP (Wired Equivalent Privacy):** A titkosítás egy régebbi változata, amely a vezetékessel egyenértékű titkosítást jelent. „*Vezetéknélküli csomópontok között küldött adatok titkosítására szolgál. 64, 128, vagy 256 bites, előre kiosztott kulcsokat alkalmaz. Legnagyobb hibája a kulcsok állandóságából adódik, az-az minden eszköznél ugyanazt a kulcsot használja az adatok titkosítására.”*[55]

16.6.2.2 WPA/WPA2 (Wi-Fi Protected Access): Manapság már szinte minden vezeték nélküli hálózat WPA-t, az-az Wi-Fi védett hozzáférést használ. Annyiban különbözik a WEP-től, hogy minden egyes kapcsolatnál új, egyedi kulcsot hoz létre a felhasználók számára, egy titkosítási szabvány által. A régebbi WPA-nál ez a TKIP volt, az újabb változatában, a WPA2-nél az AES protokoll.

16.6.3 MAC-cím szűrés: Az olyan Wi-Fi hálózatoknál, ahol szigorúan meg kell határozni, hogy mely felhasználók kapcsolódhatnak hozzá, a leg kézenfekvőbb megoldás a MAC-cím szűrés használata. Ebben az esetben a forgalomirányítón egyesével konfigurálni kell az engedélyezhető állomások fizikai címeit. Ezt követően az eszköz csak nekik fogja engedélyezni a hálózati hozzáférést.

16.7 Archiválás: Amellett, hogy számos módszer létezik az informatikai rendszerek biztonságossá tételéhez, a vállalat kulcsfontosságú adatait rendszeresen archiválni kell. Hiába egy korszerű, rendszeresen karban tartott hálózat, meghibásodás bármikor történhet. Észben kell tartanunk Murphy törvényét: „Ami elromolhat, az el is romlik”! Amennyiben gyakran készítünk másolatot a fontos adatokról, egy bármikor bekövetkező, bármilyen katasztrófa után, adatvesztés nélkül helyreállítható a rendszer az eredeti változatába.

16.8 Archiválási tárolók

[55] Forrás: Cisco CCNA Discovery2 – 8.2.4-es fejezet, Letöltés dátuma: 2018. 12. 06.

16.8.1 Optikai lemezek: A kisebb mennyiségű adatmentésre még mindig kiválók a CD-k, DVD-k, Blue-Ray lemezek. Tárolásoknál figyeljünk, hogy megfelelően védett helyen tartsuk őket, nehogy megsérüljenek.

16.8.2 Flash tárolók: A memória alapú tárolók, mint pl. a közkedvelt pendrive-ok szintén megfelelnek a célnak. Nagy előnyei, hogy kapacitásuk már meghaladta az optikai lemezekét, könnyen használhatók és kis helyen is elférnek

16.8.3 Merevlemezek: A mágneses alapú háttértárolók rendelkeznek a legnagyobb tárhellyel. Kapacitásuk a 12 TB-ot is elérheti, ezért nagymennyiségű adatmentésre a legalkalmasabb kellékek.

17 Hálózati hibaelhárítás

A hibaelhárítás a rendszergazdák legfontosabb kompetenciái közé tartozik, mivel a fennálló problémát a leggyorsabban és leghatékonyabban meg kell oldania. A hibaelhárítási folyamat nem egy egyszerű feladat, különösen, amikor fogalmunk sincs, hogy hol is kezdjük. Gondoljunk vissza az (4. fejezet) OSI modell rétegzett felépítésére, hiszen egy kézenfekvő mankó lehet, ha pontosan tudjuk, mely probléma melyik szinthez köthető és könnyebb azt behatárolni. Fontos megjegyezni, hogy „*dokumentáljuk a kezdeti tüneteket és minden előfordulást a probléma okának megtalálása és annak kijavítása érdekében! Ez a dokumentáció értékes eszközként szolgálhat egy ilyen vagy ehhez hasonló probléma bekövetkezése esetén.”*[56] Amikor nem tudjuk meghatározni a probléma forrását, a próbálgatást, vagy helyettesítést alkalmazhatjuk feltéve, ha már kellően rutinosak vagyunk ezen a téren. Sok esetben működhet az ilyen problémamegoldó módszer, de előfordulhat olyan eset, amikor olyan, mintha tűt keresnénk a szénakazalban. Az ilyen esetekben javasolt inkább egy meghatározott algoritmus alapján megközelíteni a problémát. Az ajánlott módszerek az OSI modell rétegeire épülnek és itt lépegetünk szintről-szintre. Ezek lehetnek a következők:

17.1.1 Fentről lefelé: Ez a módszer az OSI tetejéről indulva az alkalmazásitól halad lefelé.

17.1.2 Alulról lefelé: A módszer megfordítva, a fizikai rétegtől indulunk felfelé.

17.1.3 Oszd meg és uralkodj: Az OSI modell valamelyik középső rétegénél kezdődik a folyamat, majd lefelé vagy felfelé halad. A tapasztalt szakemberek sokszor ezt a módszert alkalmazzák.

[56] Forrás: Cisco CCNA Discovery3 – 9.1.4-es fejezet, Letöltés dátuma: 2018. 12. 06.

„A hibaelhárítás során felbecsülhetetlen értéket képviselnek a pontos fizikai és logikai topológiarajzok.”[57] Emlékezhetünk rá, hogy a topológia térképeket a hálózattervezésnél használtuk, de a probléma megoldásnál is szükség van rá, hiszen több, pontosabb információt szolgáltat a hálózat működéséről, mint amivel feltehetően a rendszergazda rendelkezik.

A következőkben nézzük a hibaelhárítást az alulról-felfelé módszert követve.

17.2 Fizikai szintű hibák: Az OSI modell fizikai rétegében többnyire kábelezési vagy vezeték nélküli átviteli hibákkal találkozhatunk, esetleg az ezen a szinten működő hub, vagy repeater problémájával. Előny, ha rendelkezünk hibaelhárító eszközökkel, mint kábel teszterrel, multiméterrel. A kábel teszter jelzi, ha a vezetékkel bármilyen gond van, a multiméter pedig áramerősség, feszültség mérésére alkalmas. Vannak hálózatanalizátor készülékek, amelyekkel az egész hálózati forgalom leellenőrizhető. Segítségével a külső támadások, mint pl. egy DoS támadás is kiszűrhető. „*Az 1. és a 2. rétegben előforduló hibák zöméért hardveres vagy kompatibilitási problémák okolhatók.”*[58] Amikor egy host nem képes csatlakozni a hálózathoz, vizsgáljuk meg, hogy a kapcsoló kapcsolatjelző LED-je világít-e. Amennyiben nem, elsősorban vizsgáljuk meg, hogy az adott port az eszközön nincs-e tiltott állapotban. Amennyiben aktív a port, valószínűleg 1. rétegbeli hiba van. Tipikus fizikai szintű hibák: eszközök tápellátása, kábel sérülés, rossz kábelbekötés, érintkezési problémák, csavart érpárú kábel felcserélt érpárai, sérült interfészcsatlakozó, rövidzár ill. az eszközök, vagy azok panel meghibásodása. Vezeték nélküli hálózatok esetén általában a rossz Wi-Fi router konfiguráció jelentkezik.

40. és 41. ábra: Kábel teszter és multiméter
Képek forrása: https://www.emag.hu/sprotek-kabel-teszter-stm850/pd/DTPP4MBBM/ és https://www.emag.hu/digitalis-multimeter-00081617-sma-64/pd/DHDC67BBM/
Letöltés dátuma: 2018. 12. 06.

17.3 2. rétegbeli hibák: Az adatkapcsolati rétegben gyakran a hálózati csatoló és a kapcsoló hibás működése okozhatja a problémát. Amennyiben valószínűsíthető, hogy a hálózati kártya a probléma forrása, cseréljük ki egy másikkal. Egy rosszul működő switch az elosztási réteg végpontjainak a kommunikációját megbéníthatja.

[57] Forrás: Cisco CCNA Discovery2 – 9.1.3-mas fejezet, Letöltés dátuma: 2018. 12. 06.
[58] Forrás: Cisco CCNA Discovery3 – 9.1.1-es fejezet, Letöltés dátuma: 2018. 12. 06.

Vizsgáljuk meg a kapcsolót, és ha a kapcsolatjelző LED világít, de még sincs kapcsolat, valószínűleg konfigurációs probléma merülhet fel. Nézzük meg az eszköz beállításait! Mivel a kapcsolók a MAC-cím táblában nyilvántartást vezetnek a csatlakoztatott állomásokról, könnyen leellenőrizhető, hogy az eszköz az adott állomás címét tartalmazza-e. Ezt követően, ellenőrizzük az eszköz biztonsági beállításait, (Pl. portbiztonság). Ne feledjük, hogy portszűrés során minden újonnan csatlakoztatott végfelhasználói eszköz fizikai címét konfigurálni kell a kapcsolón.

További problémák lehetnek az adatkapcsolati rétegben a kapcsolási hurkok, amelyek a redundancia alkalmazása során léphetnek fel. Ráutaló jelei a hálózat lassú konvergálása, lassuló adatforgalom, túlterhelt processzorok. (A 13. fejezetben megbeszéltük, hogy a helyes megoldás a feszítőfa protokoll alkalmazása erre az esetre.)

17.4 Hálózati szintű hibák: Ahogy haladunk a felsőbb rétegek felé, egyre több típusú problémával találkozhatunk és a hibaelhárítási folyamat egyre nehezebbé válik. A 3. rétegbeli problémák nagy százaléka az IP címzéssel és a forgalomirányítással kapcsolatos. *„A kapcsolónál a forgalomirányítónak nagyobb befolyása van a hálózat működésére nézve, ezért nagyobb hibatartománnyal bír.”*[59] Az IP címzésnél bizonyosodjunk meg róla, hogy helyesek a beállítások (címzés, alhálózati maszk, alapértelmezett átjáró). Megfelelően működik-e a DHCP és DNS szolgáltatás.

Minden forgalomirányítóval kapcsolatos probléma erre a szintre tartozik. Minél összetettebb hálózatról van szó, annál komplikáltabb lehet a probléma megoldás. hiszen a forgalomirányítás rengeteg összetevőből áll. Sok probléma forrása a helytelenül beállított router, vagy egy hálózati bővítés során elmulasztott routerkonfiguráció miatt lehetséges. Ezek közül a legjellemzőbb hibaforrások: Rosszul konfigurált VLAN-ok, hibás hozzáférési port, trönkport és WAN interfész, rossz WAN kapcsolati beállítások, hibás forgalomirányító protokollok, rosszul működő biztonsági szolgáltatások (Pl. ACL), DHCP, DNS, NAT, PAT problémák.

A parancssoros felület nagy segítségünkre lehet ezen a szinten, amit bárki meg tud nyitni a saját számítógépén a ’cmd’ paranccsal. Nézzünk néhányat:

17.4.1 Ipconfig: Ez a parancs az ’ipconfig /all’ beírásával megjeleníti az adott állomás IP és MAC-cím beállításait. Amennyiben nem megfelelő az IP címzés egy DHCP-

[59] Forrás: Cisco CCNA Discovery3 – 9.1.3-mas fejezet, letöltés dátuma: 2018. 12. 06.

s hálózatban, kísérletet tehetünk az ’ipconfig /release’, majd ’ipconfig /renew’ alkalmazásával a konfiguráció törlésére és újbóli lekérésére.

17.4.2 Ping: A ping parancs segítségével csomagokat küldünk a célállomásnak, amelyik ha megkapja, válaszol rá. Nagyon hatékonyan leellenőrizhető, hogy az adott végpont elérhető-e egy másikról.

```
C:\Users\Bence>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=3ms TTL=64
Reply from 192.168.1.254: bytes=32 time=2ms TTL=64
Reply from 192.168.1.254: bytes=32 time=5ms TTL=64
Reply from 192.168.1.254: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

42. ábra: A ping parancs, Kép forrása: Saját forrás

17.4.3 Tracert: A tracert parancs segítségével nyomon tudjuk követni a kiküldött csomag útvonalát a célig. A képen is látható, a tracert számozza, hogy a csomag mennyit ugrik, az-az hány forgalomirányítón halad keresztül, amíg megérkezik a célhoz. A jobb oldalon látható címek az átjárók, majd a cél végpont IP címei. Amennyiben címzésbeli probléma van, könnyen kideríthető, hogy a csomag hol akad el a hálózaton. „*A tracert főként nagy hálózatok esetében hasznos, ahol egy adott ponthoz több útvonal vezet, illetve amelyben sok köztes összetevő (útválasztó és híd) található. „*[60]

```
C:\>tracert 11.1.0.1
The output from the command:

  Tracing route to 11.1.0.1 over a maximum of 30 hops
  ------------------------------------------------------
  1      2 ms       3 ms       2 ms       157.54.48.1
  2     75 ms      83 ms      88 ms       11.1.0.67
  3     73 ms      79 ms      93 ms       11.1.0.1

  Trace complete.
```

43. ábra: Tracert parancs használata
Kép forrása: https://www.pcwdld.com/what-is-traceroute, Letöltés dátuma: 2018. 12. 07.

17.5 Szállítási rétegbeli hibák: Amikor egy hálózat probléma során elvégeztük az első 3 szint ellenőrzését, a szállítási réteget kell megvizsgálnunk. Ebben a rétegben működnek a biztonságért felelős rendszerek, mint pl. a tűzfalak. Tipikus probléma lehet erre a rétegre, amikor pl. a felhasználónak nem működik egy hálózati szolgáltatás, vagy nem ér el egy alkalmazást, esetleg nem tud megnyitni biz. internetes weboldalakat. Nagy eséllyel tűzfalas problémák vannak, nézzük meg annak a beállításait! Meg kell vizsgálni, hogy a szállítási protokollok (TCP, UDP) megfelelően engedélyezve vannak e a portszámokkal. „*Egyes alkalmazások kizárólag az egyiket használják, mások mindkettőt. Éppen ezért a portszámokon alapuló forgalomszűrésnél meg kell határozni a protokollt is. Előfordulhat, hogy a tűzfal olyan forgalmat szűr ki, amelynek kiszűrése nem volt cél. Ha egy*

[60] Forrás: https://support.microsoft.com/hu-hu/help/314868/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows, Letöltés dátuma: 2018. 12. 07.

engedélyezett forgalomtípus nem szerepel a tűzfal utasításai között, vagy egy új alkalmazás jelenik meg a hálózaton anélkül, hogy a megfelelő engedélyek bekerülnének a tűzfal konfigurációjába, forgalomszűrési problémák keletkezhetnek."[61]

17.6 Felső rétegbeli problémák: Az alulról felfelé történő hibaelhárítás során nem feltétlenül kell különválasztani az OSI modell felső három rétegét, hiszen a TCP/IP alapértelmezésben is egyesíti őket. Mivel ezekben a rétegekben számos protokoll működik, így egy felső rétegbeli hiba szinte kivétel nélkül azok valamelyikéhez kapcsolódik. A hibák többnyire a weboldalas szolgáltatások elérhetetlenségével nyilvánulnak meg, de gyakran csupán egy, vagy néhányat érintenek.

Tipikus probléma, a levelezőkiszolgálók helytelen működése, amelyekért a levelezőprotokollok, mint pl. a POP3, IMAP4, SMTP a felelősek. Sokszor hallottam olyan esetről, amikor az ügyfél nem kapta meg a leveleit az e-mail fiókjában.

A DNS kiszolgáló is a felsőbb rétegekbe tartozik, amelynek a feladata, hogy az IP címeket átalakítsa URL címekké, ill. fordítva. Számos esetben velem is előfordult, hogy az otthoni hálózaton valamiért nem működött megfelelően a DNS. Ilyen esetben egyes weboldalakat rendszerint nem lehetett megnyitni. Egy nagyon jó Windows-os szoftver az nslookup, amellyel leellenőrizhető a DNS kiszolgáló működése. (A beírt weboldal névhez azonnal lekéri az IP címet.) Sok esetben a DHCP osztja ki a DNS címeket, a probléma megoldásáért a DHCP kiszolgáló vagy a forgalomirányító beállításait kell megvizsgálni, esetleg újraindítani az eszközt.

```
Non-authoritative answer:
Name:    www.index.hu
Address:  217.20.130.99
```

44. ábra: Nslookup
Kép forrása: Saját forrás

A netstat szintén egy kíváló parancssori segítség, ha kíváncsiak vagyunk, milyen protokollokat használ az adott állomás. A parancs kilistázza a szállítási protokollokkal együtt az állomás által használt protokollokat ill. azok állapotát.

„A böngészők különböző beépülő moduljai, mint például az Adobe Reader, gyakran felsőbb rétegbeli hálózati funkciókat is megvalósítanak. A weboldalak

Proto	Local Address	Foreign Address	State
TCP	192.168.1.6:55663	204.79.197.222:https	FIN_WAIT_1
TCP	192.168.1.6:55681	40.67.248.104:https	ESTABLISHED
TCP	192.168.1.6:55687	a23-7-207-201:https	ESTABLISHED
TCP	192.168.1.6:55690	a23-7-207-159:https	ESTABLISHED
TCP	192.168.1.6:55693	152.199.19.161:https	TIME_WAIT
TCP	192.168.1.6:55696	152.199.19.161:https	TIME_WAIT
TCP	192.168.1.6:55698	104.46.14.236:https	TIME_WAIT

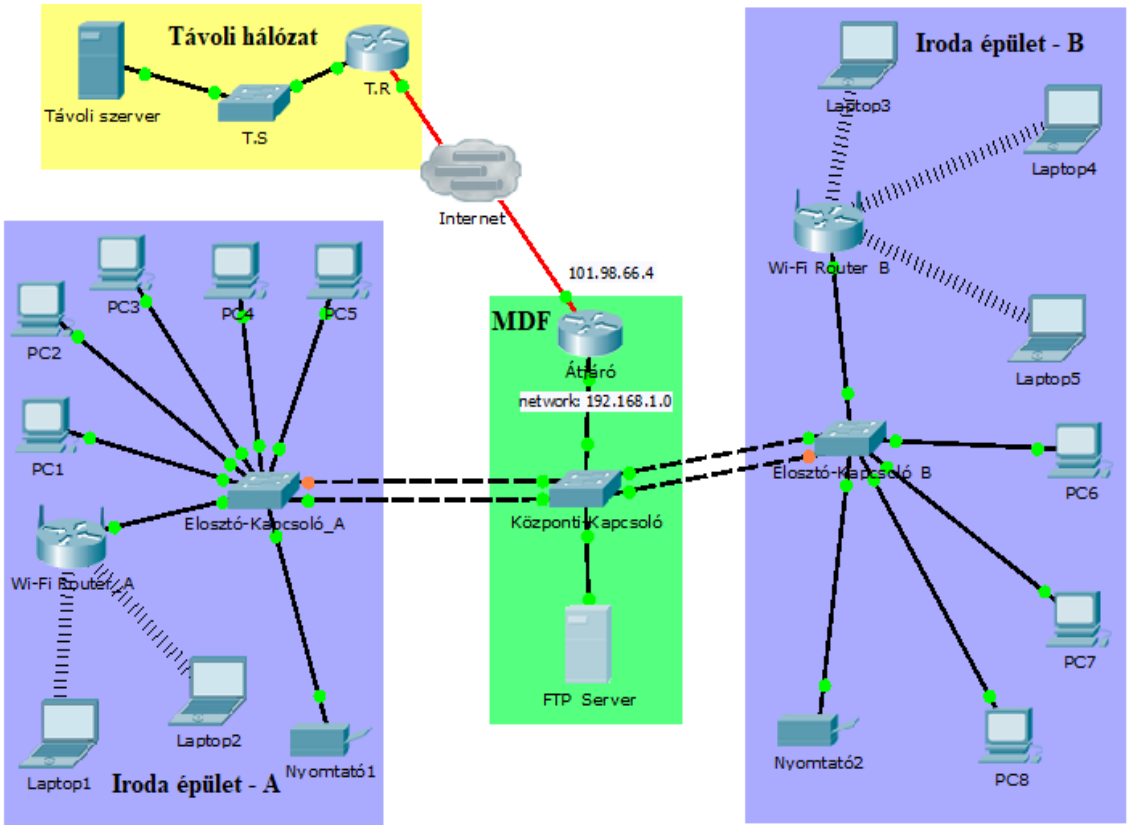
45. ábra: Részlet a netstat listájából,
Kép forrása: Saját forrás

[61] Forrás: Cisco CCNA Discovery2 – 9.5.1.4-es fejezet, Letöltés dátuma: 2018. 12. 10.

helyes megjelenítése érdekében ezeket a modulokat rendszeresen frissíteni kell."[62]

A fejezetben említett problémákon kívül természetesen még millió féle előfordul. Nyilván valóan a hibaelhárításról egy külön könyvet lehetne írni, de itt csupán a probléma megoldó módszer bemutatása volt a cél. Egy hálózati szakember az évek során nagyon sok problémával találkozik, a kellő rutin és tapasztalatszerzés idővel a hibaelhárítás gyorsaságát és hatékonyságát is növeli.

18 Hálózati modell



46. ábra: Egy irodaház hálózata, Kép forrása: Saját forrás (Cisco Packet Tracer használatával)

A dolgozat zárásaként a Cisco Packet Tracer segítségével kialakítottam egy virtuális hálózati modellt az eddigiek alkalmazásával. A fent látható ábrán egy kisebb irodaház topológiája látható, amit az egyszerűség és a könnyebb szemléltetés miatt választottam.

18.1 Hálózati elemzés: Az informatikai rendszer két épület részből áll (A, B – kék háttéren), közöttük a központi kábelrendező, (zöld háttéren) az MDF látható. Ebben a helyiségben helyezkedik el a forgalomirányító (Átjáró), a központi kapcsoló, és a

[62] Forrás: Cisco CCNA Discovery2 – 9.5.2-es fejezet, Letöltés dátuma: 2018. 12. 10.

hálózati szerver is. A megbízható és gyors működés érdekében 1841-es Cisco ISR-t és 2960-as Cisco kapcsolókat választottam. Mivel egy épületen belüli rendszerről van szó és tételezzük fel, nincs az átvitelt befolyásoló zavaró jel, – UTP kábelezést használtam mindenhol az elosztási rétegben. Az MDF-ben lévő központi switch köti össze a másik két elosztó kapcsolót, megalkotva a gerinchálózatot. Ebben az esetben alkalmaztam a redundanciát, a kapcsoló eszközök dupla keresztkötésű csavart érpárral vannak egymással összekötve. A hálózatban elérhetők Wi-Fi hozzáférési pontok is.

18.2 Konfiguráció: Mivel egy kisebb hálózatról van szó, a kevesebb munkaállomás miatt nem tartottam szükségesnek az alhálózatra bontást, így minden végfelhasználói eszköz a 192.168.1.0-ás hálózathoz tartozik. Statikus IP címekkel a hálózati eszközök, a tűzfal és az FTP szerver rendelkezik csak, a többi címet DHCP szolgáltatás adja, ami az integrált forgalomirányítón (Átjáró) van konfigurálva. Mivel vannak statikus, és Wi-Fi-s címmel rendelkező eszközök, a címütközés elkerülése végett a routeren kizártam az 1-10 és 100-254 közötti kiosztást. A Wireless router csak a 100 utáni címeket osztja ki. A ISR a felelős a DNS szolgáltatásért is. Mint látható a VLAN csatlakozik az interneten keresztül egy távoli kiszolgálóhoz (sárga háttéren), ezért hogy a többi eszköz elérje azt, konfigurálva van alapértelmezett útvonal is az átjárón, amely a 101.98.66.4-es külső címmel rendelkezik. A PAT alkalmazása pedig lehetővé teszi, hogy az állomások elérjék az internetet.

A gerinchálózat két végén lévő elosztó kapcsoló köti össze a számítógépeket és a hálózati nyomtatókat, FastEthenet portokon keresztül. A gerinchálózati kapcsolat keresztkötésű kábelen, gigabites Etherneten keresztül fut. A redundancia miatt a központi kapcsolón konfiguráltam STP-t, így a tartalék útvonalakat letiltotta. A kapcsolók azon portjain, ahol közvetlenül kapcsolódnak a többi kapcsolóhoz, az interfészek trönk üzemmódba vannak konfigurálva.

18.3 Biztonsági intézkedések: A megfelelő biztonság érdekében a hálózati eszközök kétszintű jelaszavas védelemmel rendelkeznek. Az elosztó switcheken sticky portbiztonságot állítottam be, amely tárolja a hozzá kapcsolódó eszközök fizikai címeit és idegen eszközökhöz nem enged hozzáférést. A Wi-Fi routerek WPA2-es titkosítást használnak, jelszavas hitelesítéssel. A forgalomirányító ACL segítségével szűri az adatforgalmat.

19 Összefoglalás

A téma zárásaként bízom bene, hogy a dolgozat figyelemfelkeltő és hasznos volt mindazok számára, akik érdeklődnek az informatika ezen területe iránt. Az informatika elképesztő mértékű fejlődése miatt azonban nem garantálható, hogy a dolgozatban elhangzott és a napjainkban még korszerűnek mondható technológiák és eszközök néhány év múlva is azok lesznek. Számos ilyen példát említhetünk, – gondoljunk csak bele, hogy tíz évvel ezelőtt a legmodernebb számítógépek manapság már milyen elavultnak számítanak. Egészen biztos, hogy nem felelnek meg a mai felhasználói igényeknek. Biztosra veszem, hogy tíz év múlva ugyan ez lesz a helyzet és a mai technológiát fogjuk kőkorszakinak nevezni. Sajnos az informatika nem matematika, olyan értelemben, hogy a matematika legtöbb ismerete sohasem fog elavulni és mindig használni fogjuk. Visszatérve, éppen ezért nagyon fontosnak tartom, hogy a szakemberek készek legyenek folyamatosan tanulni és fejlődni, követve az technikai változásokat, amely évről-évre változhat.

Az elhangzottak miatt számomra a dolgozat megírása rendkívül időigényes volt, amely alapos kutatómunkát igényelt. Mivel már évekkel ezelőtt tanultam ezt a szakterületet, nem hagyatkozhattam csupán az akkori ismereteimre, jegyzetemre, mindennek újból, alaposan utána kellett néznem. Mint a többszöri hivatkozásaimból kiderül, a Cisco oktatási képzés, a Cisco Hálózati Akadémia nagyon nagy segítségemre volt a témafeldolgozás során. Tanulmányaim alatt, az éveken át tartó Cisco képzésre alapozva szereztünk informatikai szakképesítést, amely három moduljából külön OKJ-s záróvizsgát tettünk. Ez egy nemzetközi, elektronikus tananyag, és szerte a világon teljesen ugyanazt az ismeretet oktatják a megfelelő nyelveken. *„(Ma már 165 ország tízezernél is több akadémiáján 1.000.000-nál is több hallgató tanulja a különböző tananyagokat.)”*[63] Csak is ajánlani tudom mindenkinek, az ezzel kapcsolatos weboldalakat ide mellékeltem:

https://www.netacad.hu/

https://www.cisco.com/c/hu_hu/index.html

Logo forrása: https://www.netacad.hu/hu/ciscohalozatiakademia

[63] Forrás: https://www.netacad.hu/hu/ciscohalozatiakademia, Letöltés dátuma: 2018. 12. 16.

A Cisco a képzésben résztvevő oktatási intézményeknek kedvező feltételeket teremtett a leghatékonyabb tanulás elősegítésére. Az ilyen intézmények, az amúgy nagyon költséges hálózati eszközöket a piaci ár töredékéért vásárolhatják meg, biztosítva az elméletre épülő tananyag gyakorlati alkalmazását. Szerencsére a mi képzésünk során sem volt ez másként. Az órák keretében kiváló színvonalon tanultuk legfőképpen az integrált forgalomirányító és hálózati kapcsoló programozását parancssoros felületen. A dolgozatban elhangzott, különböző konfigurációs módszereket mind megvalósítottuk gyakorlati szinten is. Rengeteg alkalommal használtuk a Cisco szoftverét, a Packet Tracert a hálózatok virtuális kialakítására és működésének szimulálására. A gyakorlati dolgok elsajátításában rendkívül sokat segített, amely számos funkciója szinte tökéletesen megegyezik a valódi eszközök alkalmazásával. Véleményem szerint létfontosságú, hogy egy vállalati rendszergazdának pontos ismeretei legyenek a hálózati eszközök konfigurációja terén, hiszen ez a rendszer folyamatos karbantartása miatt elengedhetetlen. A hibaelhárítás során bebizonyosodott, hogy a hálózati problémák nagy százaléka összefüggésbe hozható az eszközök megfelelő beállításaival. A hibaelhárítási módszerek ismerete nyilvánvalóan csak a kellő szakmai tudás mellett lehet elégséges. Az eltöltött évek során ehhez társul a tapasztalatszerzés, és ezek együttesen teszik teljesen komplex tudásúvá a szakembert.

A dolgozatban a hálózati eszközök programozása konkrétan nem szerepelt, hiszen az maga egy külön tanfolyamot igényelne és feltételezem, hogy a különböző gyártóktól származó informatikai készülékek eltérő módszerrel konfigurálhatók. Igyekeztem bemutatni az általam gyakorlatban is használt legfontosabbnak vélt módszereket, amelyeket a Cisco képzés keretében elsajátítottunk. Ezen kívül bízom benne, hogy sok hasznos dologgal tudtam segíteni egy informatikai hálózat optimális kialakítását. Törekedtem az egész témát egy jól kezelhető keretbe foglalni és hierarchikusan felépíteni a legfontosabb gondolatokkal.

Szójegyzék

Kifejezés	Leírás	Old. sz.
ACL	Hozzáférési-vezérlési lista	53
AD	Adminisztratív távolság	73
AD	Active Directory (címtárszolgáltatás)	52
Adware	Reklámprogram	75
AES	Fejlett titkosítási szabvány	55
Alhálózati maszk	IP cím hálózat és állomás azonosítására szolgáló cím	20
AP	Hozzáférési pont	26
ARP	Címmeghatározó protokoll	25
ARPANET	Világon az első számítógépes hálózat	6
Bridge	Hálózati híd (Hálózati eszköz)	26
CIDR	Osztályok nélküli tartományközi forgalomirányítás	48
Cross-link kábel	Keresztkötésű kábel	33
DDoS	Elosztott szolgáltatás-megtagadás	51
DHCP	Dinamikus állomáskonfiguráló protokoll	22
DMZ	Demilitarizált zóna	53
DNS	Tartománynév rendszer	60
DoS támadás	Szolgáltatás-megtagadás	50
EAP	Kiterjeszthető hitelesítő protokoll	55
EIGRP	Távolságvektor alapú forgalomirányítási protokoll	72
EMI	Elektromágneses interferencia	31
Extranet	Külső kapcsolódással ellátott védett privát hálózat	70
GAN	Globális kiterjedésű hálózat	9
Halálos ping	Szolgáltatás-megtagadás egy típusa	51
HTTP	Hiperszöveg átviteli protokoll	52
HTTPS	Biztonságos hiperszöveg átviteli protokoll	52
Hub	(Hálózati eszköz)	23
IDF	Közbenső kábelrendező	39
IEEE	Villamos- és Elektronikai Mérnökök Társasága	15
IMAP4	Internetes üzenet-hozzáférési protokoll	52
Intranet	Védett privát hálózat	70
IP	Internet Protokoll	18
IP cím	Logikai cím	19
Ipconfig	Állomás IP konfigurációját megjelenítő parancs	58
IPSec	Internet protokoll biztonság	52

Kifejezés	Leírás	Old. sz.
IR	Infravörös technológia	35
ISO	Nemzetközi Szabványügyi Szervezet	12
ISP	Internetszolgáltató	21
ISR	Integrált forgalomirányító	30
LAN	Helyi hálózat	9
LSA	Kapcsolatállapot-jelzés	72
MAC-cím	Fizikai cím	17
MAN	Városi hálózat	9
MDF	Központi kábelrendező (Telekommunikációs helyiség)	39
NAT	Hálózati címfordítás	29
Netstat	Hálózati kapcsolatok, protokollok megjelenítésére szolgáló parancs	60
NIC	Hálózati kártya	7
Nslookup	Tartománynév és IP cím keresésére szolgáló parancs	60
OSI modell	Hétszintű hálózai rétegmodell	12
OSPF	Kapcsolatállapot alapú forgalomirányítási protokoll	73
PAN	Személyi hálózat	8
PAT	Hálózati portcímfordíttás	74
Patch kábel	Egyeneskötésű kábel	33
PDU	Ethernet keret	16
Peer-to-peer hálózat	Egyenrangó hálózat	9
Phishing	Adathalászat	49
Ping	Kapcsolatellenőrző parancs	59
POP3	Postafiók protokoll	52
Pretexting	Hamis ürügy	49
PSK	Előre megosztott kulcs	55
Punchdown tool	Betűző szerszám	34
Repeater	Ismétlő (Hálózati eszköz)	23
RF	Rádiófrekvencia	35
RIP	Távolságvektor alapú forgalomirányítási protokoll	72
RJ-45	Kábel végi csatlakozó típus	32
Router	Forgalomirányító (Hálózati eszköz)	27
SMTP	Egyszeű levéltovábbító protokoll	52
Social Engineering	Megtévesztési technika	49
Spam	Levélszemét	76
SPF	"Legrövidebb út először" protokoll	73
Spyware	Kémprogram	75
SSH	Biztonságos Parancshéj	52

Kifejezés	Leírás	Old. sz.
SSID	Szolgáltatáskészlet azonosító	26
SSL	Biztonságos átviteli réteg	52
STP	Árnyékolt csavart érpáras kábel	31
STP	Feszítőfa protokoll	46
Switch	Kapcsoló (Hálózati eszköz)	23
SYN elárasztás	Szolgáltatás-megtagadás egy típusa	50
T-568A	Kábel végi bekötési séma	33
T-568B	Kábel végi bekötési séma	33
TCP	Nyugtázó szállítási protokoll	13
TCP/IP	Négyszintű hálózati rétegmodell	14
TKIP	Átmeneti kulcsintegritásos protokoll	55
TP	Csavart érpáras kábel	30
Tracert	Csomag nyomonkövetésére szolgáló parancs	59
Tracking cookie	Nyomonkövető süti	75
UDP	Nyugta nélküli szállítási protokoll	13
UPS	Szünetmentes tápegység	44
UTP	Árnyékolatlan csavart érpáras kábel	31
VLAN	Virtuális helyi hálózat	47
VLSM	Változtatható hosszúságú alhálózatra bontás	48
WAN	Nagy kiterjedésű hálózat	9
WEP	Vezetékessel egyenértékű titkosítás	55
Wi-Fi	Vezeték nélküli helyi hálózati szabvány	36
WLAN	Vezeték nélküli helyi hálózat	36
WPA	Wi-Fi védett hozzáférést	55
WPAN	Vezeték nélküli személyi hálózat	35
WWAN	Vezeték nélküli nagy kiterjedésű hálózat	37

Irodalomjegyzék

- Cisco CCNA Discovery1
- Cisco CCNA Discovery2
- Cisco CCNA Discovery3
- http://info.berzsenyi.hu/halozatok
- http://www.agr.unideb.hu/ebook/szamitogephasznalat/az_internet_fogalma_kialakulsa.html
- http://www.viszki.sulinet.hu/tananyagtar/informatika/Kapin/9_evfolyam/internet.htm
- https://informatika.gtportal.eu/index.php?f0=halozatok
- http://www.kiborgbt.hu/halozat-kiepitese.html
- http://soft-tech.eu/networks.php
- http://www.zipernowsky.hu/~naszlaci/alapok+hardver/halo_FE.pdf
- http://erettsegi.com/tetelek/informatika/a-szamitogepes-halozat-fogalma-fajtai-lehetosegei/
- http://ptibor.netbuild.hu/tananyag/halozat/network_1.pdf
- http://www.inf.u-szeged.hu/~borde/res/szamhalo/szghalo_n06.pdf
- http://hasznaltcikk-letavertes.hu/cikkek6.html
- http://www.macmag.hu/ieee80211/
- https://www.magyar-elektronika.hu/10005-tartalom/2068-gyorsabb-kommunikacio-a-wlan-802-11ax-szabvannyal-tobbfelhasznalos-kornyezetben
- https://computerworld.hu/tech/a-wifi-uj-hullama-217488.html
- http://www.e-times.hu/01jun/inftech.html
- https://www.szabilinux.hu/trendek/trendek5312.html
- https://ikomm.webgobe.com/5ttipus.html
- http://centroszet.hu/tananyag/szoftver/a_a_hlzatok_mret_szerinti_felosztsa.html
- http://derko.hu/tananyag/informatika/7osztaly/topolgik.html
- https://www.tankonyvtar.hu/hu/tartalom/tamop425/0005_24_szamitogepes_halozatok_scorm_02/2352_hlzati_topolgia_szerinti_csoportosts.html
- https://www.tferi.hu/kabelek?showall=&start=3
- http://www.miau.gau.hu/szgep/szgep3_05.html
- https://docplayer.hu/13671448-3-eloadas-a-tcp-ip-modell-jelentosege.html
- https://www.agendaage.hu/szekrenyek/rack-szekrenyek/rack-szekrenyek-kabelezese
- https://support.microsoft.com/hu-hu/help/314868/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows
- http://www.stud.u-szeged.hu/Deak.Kristof/gyakorlat/05gyakorlat_deak_kristof.pdf
- Szabó Bálint, Márföldi Endre: Számítógépes hálózatok (2011), Felelős kiadó: dr. Kis-Tóth Lajos Pdf file neve: 0005_24_szamitogepes_halozatok_pdf
  Letöltés URL címe:
  https://www.tankonyvtar.hu/hu/tartalom/tamop425/0005_24_szamitogepes_halozatok_pdf/24_szamitogepes_halozatok.pdf

Mellékletek listája

1. sz. melléklet: **Hálózatok kiterjedés szerinti további csoportosítása**
2. sz. melléklet: **TCP/IP modell rétegeinek jellemzői**
3. sz. melléklet: **Forgalomirányítási protokollok**
4. sz. melléklet: **NAT fajtái**
5. sz. melléklet: **PAT (Portcímfordítás)**
6. sz. melléklet: **Ártalmas programok típusai**
7. sz. melléklet: **Főbb hálózati protokollok és portszámai**

Mellékletek

1 sz. melléklet: Hálózatok kiterjedés szerinti további csoportosítása

1.1 **Internet:** Az Internet a hálózatok hálózata, amely az összes nyilvánosan elérhető helyi, városi és globális hálózatot magába foglalja.

1.2 **Intranet:** Intranet esetén olyan helyi (LAN) hálózatról beszélünk, amely az Internet felé oly módon zárt, hogy általában egy tűzfalon keresztül kapcsolódik hozzá. Gyakorlatilag egy védett belső hálózatról van szó. Tökéletes példa egy vállalat hálózata, amelyet csak az arra jogosult személyek használhatnak. „*Mivel az ilyen rendszerek bizalmas információkat tartalmaznak, kizárólag a vállalat alkalmazottai számára vannak kialakítva.”*[64]

1.3 **Extranet:** „*Extranetnek hívjuk az olyan intranetet, ami külső kapcsolódást biztosít a vállalat beszállítói és más szerződéses partnerei számára. Az extranet tehát egy olyan privát hálózat (intranet), amely szervezeten kívüli egyének és társaságok számára biztosít ellenőrzött hozzáférést.”*[65]

2 sz melléklet: TCP/IP modell rétegeinek jellemzői

2.1 **Hálózatelérési:** A TCP/IP legalsó szintje, amely az OSI modell fizikai és adatkapcsolati rétegének felel meg és az adatátvitel biztosítása a feladata.

2.2 **Internet:** Az Internet réteg és annak a feladata az OSI hálózati rétegével egyezik meg.

2.3 **Szállítási:** A szállítási réteg elnevezésben és feladatkörben is megegyezik az OSI modellével. „*A szolgáltatás minőségi kérdéseivel foglalkozik, vagyis a megbízhatósággal, az adatfolyam-vezérléssel és a hibajavítással.”*[66]

2.4 **Alkalmazási:** Ez a réteg az OSI mindhárom felső rétegét magába foglalja. „*A protokollok feladatait tartalmazza, a megjelenítést, kódolást és párbeszéd-szabályozást. A TCP/IP minden alkalmazás szintű feladatot ebbe a rétegbe foglalja bele.”*[67]

---

[64] Cisco CCNA Discovery3 – 1.1.4 -es fejezet, Letöltés dátuma: 2018. 11. 22.
[65] Cisco CCNA Discovery3 – 1.1.4 -es fejezet, Letöltés dátuma: 2018. 11. 22.
[66] Forrás: https://docplayer.hu/13671448-3-eloadas-a-tcp-ip-modell-jelentosege.html, Letöltés dátuma: 2018. 11. 25.

3 sz. melléklet: Forgalomirányítási protokollok

Mivel napjainkban az internet kiterjedése is egyre nagyobb léptékben fejlődik, sokszor több hálózat integrálódik egymásba. Az ezeket összekötő forgalomirányítóknak nincs könnyű dolguk az ilyen többszörösen összetett hálózatokkal. Mivel az útvonalak bármikor módosulhatnak, mindig meg kell találni a leg optimálisabb utat a gyors kommunikációhoz. Elsősorban az ilyen problémák megszűntetése céljából van szükség irányító protokollokra, amelyek segítségével a forgalomirányítók kezelni tudják a többi routertől megkapott információt és így a hálózatban történő változásokra azonnal reagálni tudnak. A forgalomirányítási algoritmusnak két típusa létezik, a távolságvektor és a kapcsolatállapot alapú protokollok. Fontos megjegyeznünk, hogy a forgalomirányítók csak abban esetben tudják egymást informálni, ha ugyanazt a protokollrendszert alkalmazzák.

3.1 Távolságvektor alapú protokollok: Az ilyen típusú protokollrendszert alkalmazó forgalomirányító két fő szempont alapján választja meg a megfelelő útvonalat. A nevében is szerepel – távolság ill. vektor alapján. *„A távolságvektorok olyanok, mint a kereszteződésekben lévő jelzőtáblák. A tábla a cél irányába mutat, és jelzi a célhoz vezető út hosszát. Az út mentén további táblák mutatnak a cél felé, de a hátralévő távolság már egyre kevesebb. Amíg a távolság csökken, addig a forgalom a legjobb útvonalon halad.”*[68] A folyamat úgy történik az egymással összekapcsolt routerek esetében, hogy minden eszköz elküldi a szomszédjának a saját irányítótáblájában szereplő információkat, amely szintén küldi azt tovább az ő szomszédjának. A szomszédos routerek között ez a folyamat játszódik le, amíg miden egyes forgalomirányító rendelkezik a többiek irányítótábláival. A folyamatban a forgalomirányítók a kapott információk alapján nyilvántartják az útvonalak költségét, amit ugrásszámnak hívunk. Az ugrásszám megmutatja, hogy pontosan hány forgalomirányítón halad keresztül az üzenet, amíg az megérkezik a célállomáshoz. Amikor egy forgalomirányító változást észlel az irányítótáblájában, azonnal küldi az útvonalfrissítéseket (Nevezzük eseményvezérelt frissítéseknek is) és a hálózatfelderítési folyamat ismételten megtörténik.

[67] Forrás: https://docplayer.hu/13671448-3-eloadas-a-tcp-ip-modell-jelentosege.html, Letöltés dátuma: 2018. 11. 25.
[68] Forrás: Cisco CCNA Discovery2 – 6.1.2-es fejezet, Letöltés dátuma: 2018. 11. 08.

3.1.1 RIP: A RIP (Routing Information Protocol) a leggyakrabban használt forgalomirányítási protokoll szerte a világon. Elsősorban a kisebb hálózatok esettében javasolt a használata. Nagyon sok router által támogatott, könnyen konfigurálható protokollról van szó. Működése során az ugrásszám segítségével határozza meg a leg optimálisabb útvonalat, viszont maximálisan csak 15 ugrást tud értelmezni. Ennek értelmében olyan hálózatoknál alkalmazható, amelyek legfeljebb 15 forgalomirányítót tartalmaznak.

Nagy előnye, hogy nagyon konvergálttá teszi a rendszert, hiszen a routerek 30 másodpercenként elküldik egymásnak a saját irányítótáblájuk információit. Nagyobb hálózatok esetén ez a protokoll hátránya is egyben, hiszen a rendszeres frissítések miatt, a generált forgalommal lassíthatja a rendszert. A RIP-nek két verziója létezik, a RIPv1 és RIPv2. Rendszerint a második változatát használják mert jóval fejlettebb az elődjénél.

3.1.2 EIGRP: A távolságvektor alapú protokollok másik ismert változata az EIGRP (Enhanced Interior Gateway Routing Protocol), amelyet a Cisco fejlesztett ki. A Cisco a RIP gyengeségeit igyekezett kiküszöbölni, és egy összetettebb, DUAL (Diffused Update Algorithm) algoritmus segítségével választja meg az utat. Az EIGRP jóval nagyobb hálózatok kezelésére alkalmas, mint a RIP, hiszen 224 ugrás költségig is használható. A tökéletesebb útvonalválasztása abban rejlik, hogy az irányítótáblán kívül szomszédtáblát és topológiatáblát is tartalmaz a protokoll. „*A szomszédtáblában találhatók a közvetlenül csatlakozó helyi hálózatokon lévő forgalomirányítók adatai, (pl. interfész IP-címe, típusa, sávszélessége). A topológiatábla a szomszédos forgalomirányítók hirdetményei alapján épül fel, és tartalmaz minden szomszéd által hirdetett útvonalat.”*[69]

3.2 Kapcsolatállapot alapú protokollok: A távolságvektoros forgalomirányítási protokollok többnyire nem alkalmasak a nagyon távoli hálózatok összeköttetésére, hiszen a forgalomirányító a távolban lévő hálózatokról rendszerint kevés információval rendelkezik, és elég megbízhatatlan lenne a működése. Erre szolgálnak a kapcsolatállapot alapú protokollok, amelyek kisméretű csomagok (LSA – Link-state advertisement) segítségével egy teljes adatbázist vezetnek minden forgalomirányítóról. Az ilyen hirdetményekből építi fel a router a topológiai adatbázist. A meglévő információk alapján egy hálózati térképet készít

[69] Forrás: Cisco CCNA Discovery2 – 6.1.3.3-mas fejezet, Letöltés dátuma: 2018. 11. 05.

és egy biz. SPF (Shortest Path First) algoritmus segítségével meghatározza a legjobb útvonalat. Minden egyes LSA hirdetmény beérkezésekor elvégezi a számítási műveleteket.

3.2.1 OSPF: Az ilyen forgalomirányítási protokollok legismertebb fajtája az OSPF (Open Shortest Path First), vagy legrövidebb út protokoll. Előnye, hogy gyors konvergenciát biztosít a hálózatok számára. A frissítéseit (LSA) csak a hálózatban történő változások esetén továbbítja, ezzel meggátolva a rendszer túlterhelését.

3.3 Adminisztratív távolság (AD): A forgalomirányítás során előfordulhat az-az eset, amikor egy router egyszerre több forgalomirányító protokollt is használ. Ilyenkor több előnyben részesített útvonal jöhet létre, attól függően, hogy melyik protokoll milyen útvonalat preferál. A forgalomirányítónak döntenie kell, ezt pedig az adminisztratív távolság (Advertised Distance) segítségével teszi meg. Ez egy olyan érték, amely az útvonal megbízhatóságát jelöli. 0 és 255 között határozták meg az értékét. Minél kisebb egy útvonal adminisztratív távolsága, annál megbízhatóbbnak van titulálva, tehát a router mindig a legkisebb AD szerint fog dönteni. Ennek értelmében a közvetlenül elérhető eszközök útvonala a legmegbízhatóbbak, amelyek AD értéke mindig 0. A manuálisan konfigurált útvonalak, mint a statikus útvonalak 1 adminisztratív távolsággal rendelkeznek. Az OSPF 110, a RIP 120 AD-vel van meghatározva.

Az útvonal forrása	Adminisztratív távolság
Közvetlenül csatlakozó	0
Statikus	1
EIGRP összevont-útvonal	5
Külső BGP	20
Belső EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Külső EIGRP	170
Belső BGP	200

47. ábra: Irányítóprotokollok a meghatározott adminisztratív távolságokkal
Kép forrása: Cisco CCNA Discovery3 – 5.3.2-es fejezet, Letöltés dátuma: 2018. 12. 06.

4 sz. melléklet: NAT fajtái

4.1 Dinamikus NAT: A dinamikus NAT során a forgalomirányító a belső hálózat számára a regisztrált globális címeket párosítja, lehetővé téve az internet elérést.

4.2 Statikus NAT: Abban az esetben, amikor egy belső hálózatban lévő eszköznek az internet felől is elérhetőnek kell lennie, statikus NAT-ot használunk. Ez azért fontos, mert ezen a módon az „*adott eszköz privát IP-címe mindig ugyanarra a*

regisztrált globális IP-címre lesz lefordítva. Ezt a regisztrált címet más állomás garantáltan nem használja."[70]

5 sz. melléklet: PAT (Portcímfordítás)

A PAT-ot (Port Address Translation) szokták túlterheléses NAT-nak is nevezni, amely használata abban az esetben hasznos, amikor viszonylag kevés külső IP cím áll rendelkezésre. Amennyiben nagyon sok munkaállomásra egyetlen külső cím jut, a NAT a portcímfordítás segítségével továbbra is képes azokat összekapcsolni az internettel. Ez az IP cím és a portszám kombinálásával jön létre. Vegyük példának, hogy csak egy, a 101.10.5.5-ös külső IP címünk van, amelyet 40 állomás használ. A PAT minden fordításánál hozzárendel ehhez a címhez egy 1024-nél nagyobb portszámot. A válasz ugyanarra az IP cím és port szám kombinációra érkezik, majd a forgalomirányító visszafordítja azt az eredeti belső címre és továbbítja. A 101.10.5.5:8302 egy teljesen különböző cím, mint a 101.10.5.5:6778. „*A fordítás csak a kapcsolat idejéig áll fenn, így egy adott felhasználó nem tartja meg magának ugyanazt a globális IP-cím és portszám kombinációt a kapcsolat befejezése után. Ennek köszönhetően egy külső felhasználó nem tud megbízhatóan kapcsolatot létesíteni egy olyan állomással a hálózaton, amelyik PAT-ot használ."*[71]

6 sz. melléklet: Ártalmas programok típusai:

6.1 Vírusok: „*A vírus egy program, mely lefut és más programok vagy fájlok módosításával terjed. A vírus önmagát nem tudja futtatni, szüksége van arra, hogy aktiváljak. Ha egyszer aktiválva lett, a vírus nem képes mást tenni, mint sokszorosítja magát és továbbterjed. Egyszerűsége ellenére ez a fajta vírus veszélyes, mivel gyorsan felemészti az összes rendelkezésre álló memóriát és a rendszer leállását idézheti elő. A még veszélyesebb vírust úgy is programozhatják, hogy meghatározott állományokat töröljön vagy megfertőzzön, mielőtt továbbterjed".*[72]

[70] Forrás: Cisco CCNA Discovery2 – 4.2.3.2-es fejezet, Letöltés dátuma: 2018. 11. 05.
[71] Forrás: Cisco CCNA Discovery2 – 4.2.5-ös fejezet, Letöltés dátuma: 2018. 11. 05.
[72] Forrás: Cisco CCNA Discovery1 – 8.2.1-es fejezet, Letöltés dátuma: 2018. 11. 16.

6.2 Férgek: „*A féreg hasonló a vírushoz, de a vírustól eltérően nincs szüksége arra, hogy egy programhoz kapcsolódjon. A féreg a hálózatot használja arra, hogy elküldje saját másolatát bármelyik kapcsolódó állomásra. A férgek önállóan tudnak futni és gyorsan terjednek."*[73]

6.3 Trójai falovak: „*A trójai faló úgy készült, hogy hivatalos programként jelenjen meg, miközben valójában egy támadási eszköz. Hivatalos megjelenésére alapozva veszi rá az áldozatot arra, hogy indítsa el a programot. Viszonylag ártalmatlan lehet, de olyan kódot is tartalmazhat, mely károsíthatja a számítógép merevlemezének tartalmát. Ezenkívül a trójai vírusok egy hátsó kaput (back door) is létesíthetnek a rendszeren, mely a hekkerek hozzáféréshez jutását teszi lehetővé."*[74]

6.4 Egyéb ártalmas veszélyforrások: A számítógépes hálózatok számára rengeteg fenyegetés rejtőzik a falakon túlról. Ezek leggyakrabban előforduló és legsúlyosabb típusait az előző pontokban összegyűjtöttük. Ezeken kívül vannak olyan ártalmasságok, amelyek szerencsére nem okoznak kifejezetten nagy káoszt, de a felhasználó munkáját kellőképpen megzavarhatják. Ezekkel nap mint nap, otthon is találkozunk.

6.4.1 Kémprogramok: A kémprogramok (spyware), miután települtek a felhasználók tudta nélkül gyűjtenek információt az adott számítógépről, számtalanszor rosszindulatú célból. Jelentősen lassíthatják a számítógép működését, és sebezhetőbbé tehetik azt. A nyomkövető sütiket (tracking cookie) is ide lehet sorolni, de ez nem rosszindulatú kémprogram. Weboldalaknál használják, amelyek információt gyűjtenek az adott lapot látogatókról. A reklámprogram (adware) is a kémprogram egy fajtája, amely egy nagyon bosszantó szoftver. Miután kinyomozta, hogy a felhasználó milyen webhelyeket látogat, beépül a böngészőkbe és célzott hirdetéseket jelenít meg a felületén. Elképesztően kellemetlen tud lenni és nagyon nehéz eltávolítani. Sok esetben az adott böngésző újratelepítése sem hoz eredményt, amennyiben a reklámprogram egy különálló szoftverként fut. A reklámprogramok egy kellemesebb típusa az előugró (pop-up) és mögényíló (pop-under) ablakok. Weboldalak látogatásakor jelenhetnek meg egy új ablak keretében és legtöbbször hirdetéseket tartalmaznak.

[73] Forrás: Cisco CCNA Discovery1 – 8.2.1-es fejezet, Letöltés dátuma: 2018. 11. 16.
[74] Forrás: Cisco CCNA Discovery1 – 8.2.1-es fejezet, Letöltés dátuma: 2018. 11. 16.

6.4.2 Levélszemét (spam): A levélszemét az elektronikus kommunikáció használatánál lehet ismert. Nemkívánatos elektronikus levelekről van szó, amelyek ártalmasak lehetnek a felhasználók számára, hiszen nagyon sokszor vírusokat tartalmazhatnak. E mellett plusz hálózati forgalmat generálnak, és túlterhelhetik a levelezőkiszolgálókat. Nem véletlenül, a legtöbb levelezőrendszer már fel van szerelve spamszűrővel.

7 Főbb hálózati protokollok és portszámai:

Célport száma	Rövidítés	Meghatározás
20	FTP Adat	Fájlátviteli protokoll (File Transfer Protocol) (adatátvitelhez)
21	FTP Vezérlés	Fájlátviteli protokoll (File Transfer Protocol) (kapcsolat felépítéshez)
23	TELNET	Távgépíró hálózat (TELetype NETwork)
25	SMTP	Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol)
53	DNS	Tartománynév szolgáltatás (Domain Name Service)
67	DHCP v4 ügyfél	Dinamikus állomáskonfiguráló protokoll (ügyfél)
68	DHCP v4 kiszolgáló	Dinamikus állomáskonfiguráló protokoll (kiszolgáló)
69	TFTP	Triviális fájlátviteli protokoll (Trivial File Transfer Protocol)
80	HTTP	Hipertext átviteli protokoll (Hypertext Transfer Protocol)
110	POP3	Postahivatal protokoll (Post Office Protocol) (3-as verzió)
137	NBNS	Microsoft NetBIOS névszolgáltatás (NetBios Name Service)
143	IMAP4	Internetes levél hozzáférési protokoll (Internet Message Access Protocol) (4-es verzió)
161	SNMP	Egyszerű hálózatfelügyeleti protokoll (Simple Network Management Protocol)
443	HTTPS	Hipertext átviteli biztonsági protokoll (Hypertext Transfer Protocol Secure)

48. ábra

Kép forrása: Cisco CCNA Discovery2, – 9.5.1.4-es fejezet, Letöltés dátuma: 2018. 12. 06.

BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI NYILATKOZAT

Alulírott, Cseh Bence büntetőjogi felelősségem tudatában nyilatkozom, hogy a szakdolgozatomban foglalt tények és adatok a valóságnak megfelelnek, és az abban leírtak a saját, önálló munkám eredményei.
A szakdolgozatban felhasznált adatokat a szerzői jogvédelem figyelembevételével alkalmaztam.
Ezen szakdolgozat semmilyen része nem került felhasználásra korábban oktatási intézmény más képzésén diplomaszerzés során.

Zalaegerszeg, 2019. 01. 02.

Cseh Bence
hallgató aláírása

BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

BGE GAZDÁLKODÁSI KAR ZALAEGERSZEG

ÖSSZEFOGLALÁS

(benyújtandó két példányban)

Informatika hálózati rendszerek fejlesztése vállalati szinten
szakdolgozat címe

Cseh Bence, Nappali tagozat / Gazdaságinformatika szak / Logisztika szakirány
Hallgató neve
tagozat/csoport/szak/szakirány

Szakdolgozatom témája az informatikai hálózatok és azok vállalati környezetben való korszerűsítésére irányul. Mivel egy nagyon összetett témáról van szó, törekedtem azt egy jól kezelhető keretbe foglalni és hierarchikusan felépíteni a legfontosabb gondolatokkal.

A dolgozatot alapjául véve két részre bontható: Az első fejezetek a téma megalapozása miatt elmélet orientáltak, ahol a informatikai hálózatok felépítésén, összetevőin van a hangsúly. Ezt követően fokozatosan a hálózatok optimális megvalósítására kerül a szerep. Egészében a témakör sok fogalmat és szakkifejezést tartalmaz, ezért a dolgozat végén ezek külön szójegyzékben is megtalálhatóak.

A tartalmi rész összefoglalása:

A bevezetést követően a hálózatok fogalmi meghatározásáról és azok kialakulásukról, annak okairól beszéltem. A következő fejezetben a különböző csoportosítási szempontok alapján volt szó azok kiterjedéséről, hálózati modellekről és topológiákról. A nagyon fontos hálózati hierarchiamodell, az OSI modell a 4. fejezetben volt elemezve a TCP/IP-vel együtt. Mivel a helyi hálózatok többsége az Ethernet protokoll segítségével működik, ezért ezt a szabványt és tulajdonságait az 5. fejezet tartalmazza. Az IP cím ismerete elengedhetetlenül fontos, ezért a következő pont minden fontos tudnivalót ismertet a címzéssel

kapcsolatban. A következő két részben a hálózati eszközök és azok feladatainak bemutatása történik. Részletesen elemezve van a forgalomirányítás menete. A 9. pontban a hálózatokban használatos fizikai kábelek, a 10-ben a vezeték nélküli átvitel biztosításáért felelős technológiák bemutatása történt. A 11. fejezet már konkrétan a hálózattervezéssel foglalkozik, itt egy új rendszer kiépítésének a fejlesztési szakaszai találhatóak. A következő részben, hosszabb terjedelemben javaslatok vannak az optimális hálózatkialakítással kapcsolatban. Konkrétan tartalmazza a kábelezés és hálózati eszközök megfelelő kiválasztását az adott helyszín figyelembevételével. Ez után a redundancia alkalmazásáról volt szó, valamint annak helytelen működésének kiaknázásáról. A 14. pontban az IP címzés segítségével bemutattam az egyforma méretű alhálózatok kialakítását, amiket nagyméretű hálózatokban előnyös elvégezni. A dolgozat vége felé közeledve a hálózati veszélyforrásokról volt szó, majd az ezektől való védelem biztosításáról. Mivel problémák mindig vannak, a hibaelhárítás menetét az OSI modell segítségével a 17. fejezetben ismertettem. Zárásként a Cisco Packet Tracer alkalmazásával egy saját kisméretű, virtuális hálózatot alakítottam ki, amelyben szemléltettem a dolgozatban elhangzott és alkalmazható technológiákat.